COMPUTACIÓN FORENSE

Descubriendo los RASTROS INFORMÁTICOS

Jeimy J. Cano M.
Ph.D. CFE

Alfaomega

SYNAPS PREMIUM

Datos catalográficos

Cano, Jeimy J.

Computación forense. Descubriendo los rastros informáticos

Primera Edición

Alfaomega Grupo Editor, S.A. de C.V., México

ISBN: 978-958-682-767-6

Formato: 17 x 23 cm Páginas: 344

Computación forense. Descubriendo los rastros informáticos
Jeimy J. Cano Martínez

Primera edición: Alfaomega Grupo Editor, México, julio 2009

Pitágoras 1139, Col. Del Valle, 03100, México D.F.

Miembro de la Cámara Nacional de la Industria Editorial Mexicana
Registro No. 2317

Pág. Web: **http://www.alfaomega.com.mx**
E-mail: **atencionalcliente@alfaomega.com.mx**

ISBN: 978-958-682-767-6

Empresas del grupo:

México: Alfaomega Grupo Editor, S.A. de C.V. – Pitágoras 1139, Col. Del Valle, México, D.F. – C.P. 03100.
Tel.: (52-55) 5089-7740 – Fax: (52-55) 5575-2420 / 2490. Sin costo: 01-800-020-4396
E-mail: atencionalcliente@alfaomega.com.mx

Colombia: Alfaomega Colombiana S.A. – Carrera 15 No. 64 A 29 – PBX (57-1) 2100122, Bogotá, Colombia,
Fax: (57-1) 6068648 – E-mail: scliente@alfaomega.com.co

Chile: Alfaomega Grupo Editor, S.A. – General del Canto 370-Providencia, Santiago, Chile
Tel.: (56-2) 235-4248 – Fax: (56-2) 235-5786 – E-mail: agechile@alfaomega.cl

Argentina: Alfaomega Grupo Editor Argentino, S.A. – Paraguay 1307 P.B. "11", Buenos Aires, Argentina,
C.P. 1057 – Tel.: (54-11) 4811-7183 / 8352, E-mail: ventas@alfaomegaeditor.com.ar

Agradecimientos

Los momentos y las experiencias que se viven en el arte de darle vida a una publicación son muchos. Hay momentos de oscuridad, momentos de inspiración, momentos de verdad. En este sentido, la construcción de esta obra que usted tiene en sus manos ha sido el esfuerzo continuado de muchas personas que han creído que es posible avanzar donde otros no lo hacen, ver lo que otros no ven y creer lo que otros no viven.

Hablar de informática forense, en el contexto latinoamericano, es un reto que no hubiese sido posible gracias a la oportunidad que inicialmente me ofreció el Departamento de Sistemas y Computación de la Universidad de Los Andes, en Colombia, entre 1999 y 2005. Dicho camino actualmente continúa en la Pontificia Universidad Javeriana, con el espacio de investigación y cursos que se tiene dentro del desarrollo curricular de la carrera de Ingeniería de Sistemas, así como en el programa de especialización en seguridad informática que se ofrece en la Universidad Pontificia Bolivariana, Sede Bucaramanga.

Mis agradecimientos a todos mis estudiantes que me han aportado con sus reflexiones y propuestas, a lo largo de mis más de 10 años de ejercicio docente, en temas de seguridad de la información y computación forense, y quienes a diario me recuerdan el valor infinito de aprender como una forma de vivir la pasión misma de enseñar. Gracias a ellos, quienes actualmente son destacados profesionales, se armonizan los capítulos de este libro con sus investigaciones: por la Pontificia Universidad Javeriana: Guillermo Fonseca, María Camila González y Bernardo Andrés Neira, y por la Universidad de Los Andes: Jonathan Córdoba, Ricardo Laverde, Diego Ortiz, Diana Puentes, Daniel Castro, Camilo Cuesta, Leonardo Rodríguez y Sonia Vivas.

Un reconocimiento especial al doctor Roberto Gómez, profesor-investigador en el Departamento de Tecnologías de Información y Computación de la Escuela de Ingeniería y Computación, del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Estado de México, quien se sumó a este esfuerzo académico con un artículo, donde se muestran con claridad las tendencias en visualización de bitácoras de auditoría, como una forma de apoyar las labores de la computación forense.

No hay duda de que hay un terreno importante para avanzar en estos temas. Y el doctor Gómez y sus estudiantes estarán allí para continuar con este esfuerzo.

Si bien hay muchas personas que han contribuido para materializar este proyecto, y corriendo el riesgo de que muchas de ellas se queden fuera de la enumeración, quiero resaltar la confianza y el apoyo de Luz Stella Vaca, ex funcionaria de la Biblioteca Luis Ángel Arango (BLAA), Jefe de Adquisiciones y Desarrollo de Colecciones hasta el 2007, quien me animó en muchas ocasiones para que esta iniciativa se hiciera realidad. Así mismo, el entusiasmo de Rosa Francisca López, Jefe de Catalogación, y de María Helena Escorcia, Jefe de Desarrollo de Colecciones, ambas destacadas funcionarias de la BLAA.

Mi gratitud y mi aprecio a todos mis amigos y profesionales, que constantemente con su ejemplo me ayudan a creer que es posible "hacer realidad nuestros sueños": el Grupo de Estudios de Comercio Electrónico, Telecomunicaciones e Informática (GECTI), de la Universidad de Los Andes, Ángela Carrillo, Alexandra Méndez, Gabriela Saucedo Meza, Andrés Almanza, Beatriz Caicedo, Angélica Flórez Abril, Amparo Camacho, Adalgisa Abdala, María Lucía Ferro, Jorge Alberto Gil, Julio Álvarez, Luz Myriam Leguizamón, Ciro Alfonso Barajas, María Clemencia Martínez, Martha Pasiminio, Jorge Ramio, Pino Caballero, Amparo Fúster, Arturo Ribagorda, Benjamín Ramos, Manuel Mora Tavares, Erick Iriarte, Mariliana Rico, Elia Fernández, Ana Virginia Escalante de Vargas, Tatiana Sancho, Vilma Córdova, Niurka Hernández, Fredy Bautista, Marco Gelvez, y a cada uno de ustedes que bien saben lo importante y valioso que es su presencia en mi vida.

No quiero concluir este breve espacio de agradecimientos, sin dedicar un momento para mi familia, para mis amigos espirituales y para la Editorial Alfaomega, particularmente para mi editor, Luis Javier Buitrago, quien, con su especial dirección y acierto, ha hecho realidad este proyecto editorial.

El agradecimiento es un acto de grandeza y madurez, un momento de vida y verdad que reconoce en el otro su virtud y saber. Gracias a todos ustedes, quienes tienen este libro en sus manos, por permitirme acompañarlos en su camino de aprendizaje y conocimiento.

Jeimy J. Cano, Ph.D., CFE.

Nota del editor

Los conocimientos son esenciales en el desempeño profesional. Sin ellos es imposible lograr las habilidades para competir laboralmente. La universidad o las instituciones de formación para el trabajo ofrecen la oportunidad de adquirir conocimientos que serán aprovechados más adelante en beneficio propio y de la sociedad. El avance de la ciencia y de la técnica hace necesario actualizar continuamente esos conocimientos. Cuando se toma la decisión de embarcarse en una vida profesional, se adquiere un compromiso de por vida: mantenerse al día en los conocimientos del área u oficio que se ha decidido desempeñar.

Alfaomega tiene por misión ofrecerles a estudiantes y profesionales conocimientos actualizados dentro de lineamientos pedagógicos que faciliten su utilización y permitan desarrollar las competencias requeridas por una profesión determinada. Alfaomega espera ser su compañera profesional en este viaje de por vida por el mundo del conocimiento.

Alfaomega hace uso de los medios impresos tradicionales en combinación con las tecnologías de la información y las comunicaciones (IT) para facilitar el aprendizaje. Libros como éste tienen su complemento en una página Web, en donde el alumno y su profesor encontrarán materiales adicionales, información actualizada, pruebas (test) de autoevaluación, diapositivas y vínculos con otros sitios Web relacionados.

Esta obra contiene numerosos gráficos, cuadros y otros recursos para despertar el interés del estudiante, y facilitarle la comprensión y apropiación del conocimiento.

Cada capítulo se desarrolla con argumentos presentados en forma sencilla y estructurada claramente hacia los objetivos y metas propuestas. Cada capítulo concluye con diversas actividades pedagógicas para asegurar la asimilación del conocimiento y su extensión y actualización futuras.

Los libros de Alfaomega están diseñados para ser utilizados dentro de los procesos de enseñanza-aprendizaje, y pueden ser usados como textos guía en diversos cursos o como apoyo para reforzar el desarrollo profesional.

Alfaomega espera contribuir así a la formación y el desarrollo de profesionales exitosos para beneficio de la sociedad.

Sobre el autor

El doctor Jeimy J. Cano es miembro fundador e investigador del Grupo de Estudios de Comercio Electrónico, Telecomunicaciones e Informática (GECTI), de la Facultad de Derecho de la Universidad de Los Andes, en Colombia, Miembro investigador de la Red Iberoamericana de Criptología y Seguridad de la Información (CriptoRED), en España, y Miembro de la Red Latinoamérica de Especialistas en Derecho Informático (Alfa-Redi). Es Ingeniero de Sistemas y Computación y Magíster en Ingeniería de Sistemas y Computación de esta misma universidad. Tiene un Ph.D. en Business Administration conferido por la Newport University, CA., EE.UU.

Así mismo, es Profesional certificado en Computer Forensic Analysis (CFA), del World Institute for Security Enhacement, EE.UU.; Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Antiterrorist Specialist (CAS), con especialidad en Cyber terrorism. Es egresado del programa de Formación ejecutiva "Leading Change in Complex Organization", ofrecido por la Escuela de Administración de Negocios del Instituto Tecnológico de Massachusetts (MIT), Boston, en EE.UU.

Ha participado como conferencista en diferentes eventos nacionales e internacionales, como son ISACA LatinCACS, ISACA Information Security Conference, High Technology Crime Investigation Association (HTCIA) Conference, Cybercrime Security Summit, Congreso Iberoamericano de Seguridad Informática, Jornadas Nacionales de Seguridad Informática, organizadas por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), entre otros. Es miembro del comité editorial de revistas, como *Sistemas de ACIS, IEEE Transactions Latinamerica, Journal of Information Systems Security, Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, de la Facultad de Derecho de la Universidad de Los Andes, entre otras.

Ha hecho más de 70 publicaciones internacionales en revistas y conferencias académicas, como *Sistemas, ISACA Information System Control Journal, Conferencia Latinoamericana de Informática-CLEI, Revista Electrónica de Derecho Informático*, entre otras. Es miembro activo de asociaciones como Association for Information Systems –AIS, ACM, IEEE y HTCIA.

Contacto con el autor: jjcano@yahoo.com

Prólogo

Dentro de la seguridad de la información, una de las especializaciones con mayor futuro es aquella que tiene que ver con el uso de técnicas forenses en la informática. Precisamente, esta obra, Rastros informáticos, investigación a través de la computación forense, trata sobre estas técnicas.

La seguridad de la información es muy reciente. Sus implicaciones van desde el análisis forense de un incidente común de pérdida o de ocultamiento de información en un computador personal, hasta aspectos de defensa nacional. La acción de malware puede afectarnos en cualquier momento. Cuando nos adentramos en el ciberterrorismo y en la guerra en el ciberespacio, pasando por aquellos escenarios más característicos de un crimen, en este caso, con el uso de la informática, o por medio de esta misma, esta obra se convierte en un material y en una información de valioso interés, cuya lectura se torna emocionante.

Cuando mi colega y buen amigo, el Dr. Jeimy J. Cano, me propuso que le escribiera este Prólogo, por cierto un verdadero placer y honor para mí, servidor suyo, no dudé en agradecerle ese gesto y aceptar gustosamente ese reto. Y efectivamente lo es, porque si bien he estudiado algunos conceptos de la informática forense en estos más de 15 años en los que me he dedicado a la seguridad informática, mi especialidad ha estado centrada en la criptografía aplicada y en la gestión de la seguridad.

Antes de comentar esta obra del Dr. Cano, debo reconocer que su lectura me ha resultado muy amena y, en muchos apartados de los capítulos, simplemente apasionante. Es como si el lector estuviese presente en la misma escena del crimen. Y que alguien, en este caso un experto, le fuese susurrando al oído paso a paso cómo debe hacer un análisis riguroso y sistemático del incidente, para poder llegar a las conclusiones que le permitan esclarecer lo ocurrido. Todo ello contando además con la experiencia literaria del autor, lo cual, de por sí, es ya una garantía.

El texto está compuesto de seis capítulos. Tras una introducción al tema y a las técnicas forenses, vistas desde la perspectiva de los tres roles descritos (intruso, administrador e investigador), el autor nos lleva a

profundizar en el intruso informático y en sus técnicas. Luego nos conduce a la visión, a las tareas y las responsabilidades que debe asumir el administrador de infraestructuras. Sigue con la criminalística digital, vista bajo la lente del investigador. Y termina con los nuevos retos a los que se enfrentará la computación forense, teniendo en cuenta los riesgos y las amenazas que se ciernen sobre las redes, los sistemas y los ciudadanos. Para aquellos lectores que cuenten con una mayor formación en informática y redes, los anexos en donde se presentan temas relacionados bajo un enfoque más técnico les serán de gran ayuda.

Desde el panorama de docente, cabe destacar los objetivos planteados al comienzo de cada capítulo, y muy especialmente un cuidado resumen al final del mismo, así como una selección de preguntas y ejercicios que invitan al lector a la reflexión y a profundizar en estos contenidos.

La lectura de este libro ayudará a despejar una batería de preguntas y dudas: ¿Cómo podemos y debemos enfrentarnos a un problema de intrusión? ¿Con qué herramientas contamos? ¿Qué conjunto de buenas prácticas debe considerar el administrador del sistema para mitigar las amenazas de seguridad de forma proactiva? ¿Qué hacer cuando se produce un incidente de seguridad? ¿Cómo se hace un informe pericial? ¿Qué formación se necesita para trabajar en seguridad forense, y dónde puedo encontrarla? ¿A qué nuevos retos deberá enfrentarse la investigación forense en seguridad? Y muchas otras más preguntas que con seguridad le surgirán al lector y sobre las que esta obra le irá entregando luz.

Para finalizar, no puedo dejar escapar esta excelente oportunidad para reconocer en el amigo Jeimy al verdadero evangelizador de la causa de la seguridad de la información, en un buen número de países, desde su Colombia natal, lo cual se une a una capacidad de trabajo francamente encomiable, y cuyo resultado palpable es la alta productividad de material y documentación de referencia en este importante sector de las nuevas tecnologías de la información y las comunicaciones.

Dr. Jorge Ramió Aguirre
Profesor Universidad Politécnica de Madrid
Coordinador de la Red Temática Criptored

Contenido

INTRODUCCIÓN
LA INFORMÁTICA FORENSE, UNA DISCIPLINA TÉCNICO-LEGAL **1**

CAPÍTULO 1
LA COMPUTACIÓN FORENSE, UNA PERSPECTIVA DE TRES ROLES **13**
Introducción 13
1.1 Las evidencias tradicionales 14
1.2 El informático forense 14
1.3 La faceta del intruso 15
1.3.1 Los roles del intruso 16
1.4 El investigador 17

CAPÍTULO 2
EL INTRUSO Y SUS TÉCNICAS **19**
Introducción 19
2.1 Breve historia de los hackers 20
2.2 La mente de los intrusos 26
2.2.1 Técnicas básicas de hacking 35
2.2.2 Técnicas avanzadas de hacking 43
2.3 Identificación de rastros de los ataques 49

PARA PROFUNDIZAR
PRÁCTICA DE ASALTO A UNA SESIÓN TCP **59**
1. Conceptos básicos 59
2 Estructura de un asalto a una sesión TCP 62
3 Herramientas para asaltar una sesión TCP 64
4. Herramienta Hunt 65
5. Práctica del asalto de una sesión TCP 66
6. Rastros del asalto a la sesión TCP 69
7. Corrección del asalto 70

CAPÍTULO 3
EL ADMINISTRADOR Y LA INFRAESTRUCTURA DE LA SEGURIDAD INFORMÁTICA **75**
Introducción 75
3.1 Roles y responsabilidades del administrador de sistemas 76
3.2 Consideraciones de diseño de infraestructuras de seguridad 82
3.2.1 Inseguridad centralizada 83
3.2.2 Inseguridad decentralizada 84
3.2.3 Inseguridad en el Web 89
3.2.4 Inseguridad orientada a los servicios 92
3.2.5 Evolución de la inseguridad informática 94
3.3 Técnicas básicas para el diseño y la generación del rastro 96
3.4 Auditabilidad y trazabilidad 100

3.4.1 Auditabilidad 100
3.4.2 Trazabilidad 104
3.5 Consideraciones jurídicas y aspectos de los rastros en las plataformas tecnológicas 107
3.5.1. Autenticidad 108
3.5.2 Confiabilidad 110
3.5.3 Suficiencia 111
3.5.4 Conformidad con las leyes y las regulaciones de la administración de la justicia 112

PARA PROFUNDIZAR
LOS IDS Y LOS IPS: UNA COMPARACIÓN PRÁCTICA 117
1. IDS: Sistemas de detección de intrusos 117
1.1 Clasificación por la metodología empleada 120
1.2 Clasificación por características intrínsecas del sistema 121
2. IPS: Sistemas de prevención de intrusos (Intrusion Prevention Systems) 123
2.1 Los IPS inline 125
2.2 Switches de nivel de aplicación 126
2.3 Firewalls de aplicación / IDS 127
2.4 Switches híbridos 128
2.5 Aplicaciones engañosas (deceptive) 129
2.6 Una comparación práctica entre un IDS y un IPS 129
2.6.1 Detección del ataque con el IDS 132
2.6.2 Detección del ataque con el IPS 135

CAPÍTULO 4
EL INVESTIGADOR Y LA CRIMINALISTICA DIGITAL 141
Introducción 141
4.1 Introducción a la criminalística digital 143
4.2 Roles y responsabilidades del investigador forense en informática 148
4.3 Modelos y procedimientos para adelantar investigaciones forenses en informática 153
4.3.1 Algunos modelos de investigaciones forenses en informática 154
4.4 Credenciales para los investigadores forenses en informática 159
4.4.1 Iacis 161
4.4.2 HTCN 161
4.4.3 Iisfa 163
4.4.4 Isfce 163
4.4.5 SANS Institute 164
4.5 Informes de investigación y presentación de pruebas informáticas 169
4.5.1 Teoría básica de la preparación de informes 169
4.5.2 Consideraciones básicas sobre los informes periciales 172
4.5.3 Estructura base de un informe pericial 173
4.5.4 Estructura general 173

PARA PROFUNDIZAR
ANÁLISIS DE DATOS: UNA PROPUESTA METODOLÓGICA Y SU APLICACIÓN EN THE SLEUTH Y ENCASE 179
1. Metodología de examen y análisis de datos 180
2. Introducción a Encase 185
3. Introduccióna a Sleuth Kit y Autopsy 191
4. Caso de prueba 197

CAPÍTULO 5
RETOS Y RIESGOS EMERGENTES PARA LA COMPUTACIÓN FORENSE 217
5.1 La formación de especialistas en informática forense 217
5.2 Confiabilidad de las herramientas forenses en informática 222
5.3 Técnicas antiforenses y sus implicaciones para las investigaciones actuales y futuras 225
5.3.1 Destrucción de la evidencia 229
5.4 Cibercrimen y ciberterrorismo: amenazas estratégicas y tácticas de las organizaciones modernas 231
5.4.1 Ciberterrorismo 231
5.4.2 Cibercrimen: viejos hábitos del mundo *offline*, nuevas armas en el mundo *online* 234
5.4.3 Retos tecnológicos para los investigadores forenses en informática 236
5.4.4 Archivos cifrados 236
5.4.5 Esteganografía en video 237
5.4.6 Rastros en ambientes virtuales 238
5.4.7 Información almacenada electrónicamente en memoria volátil 239
5.4.8 Análisis de sistemas en vivo 240

PARA PROFUNDIZAR
RECUPERACIÓN DE INFORMACIÓN: NTFS *VS.* FAT 245
1. Sistemas de archivos 246
1.1 NTFS 248
1.1.1 Estructura de NTFS 249
1.1.2 Sector de arranque 251
1.1.3 Tabla Maestra y Metadata 255
1.1.4 Atributos de archivos 257
2. Borrado 264
2.1 Borrar *vs.* Eliminar 264
2.2 Metodologías para eliminar 264
3. Recuperación de información en FAT 265
3.1 Borrado en FAT 265
3.2 Eliminar en FAT 266
3.3 Evidencias de borrado para recuperación 268
3.4 Recuperar borrado en FAT 268
4. Recuperación de información en NTFS 269
4.1 Recuperación automática de NTFS 269
4.2 Borrado en NTFS 270
4.3 Eliminar en NTFS 270
4.4 Evidencias de borrado para recuperación 270
4.5 Recuperar borrado en NTFS 270
4.6 Recuperar el sector de arranque 271
5. Demostración 272

CAPÍTULO 6
ANEXOS COMPLEMENTARIOS 289
Introducción 289
A6.1 Buenas prácticas en la administración de evidencia digital 292
A6.2 Fuentes potenciales de evidencia digital 300
A6.3 Evidencia digital en la práctica 303
A6.4 Características para seleccionar un informático forense 304
A6.5 Consejos y sugerencias para los abogados litigantes frente a las pruebas informáticas 307
A6.6 Consejos prácticos para sustentar un reporte técnico en una audiencia 310

PARA PROFUNDIZAR
CORRELACIÓN Y VISUALIZACIÓN DE BITÁCORAS PARA EL ANÁLISIS FORENSE 313
1. Bitácoras y cómputo forense 315
2. Correlación de bitácoras 316
2.1 Basados en probabilidades 317
2.2 Basados en escenarios de ataques predefinidos 317
2.2.1 Sec 317
2.3 Basados en prerrequisitos y consecuencias 318
2.4 Basados en múltiples fuentes de información 320
3. Visualización de eventos 321
3.1 Herramientas de visualización 322
3.1.1 RazorBack 323
3.1.2 SnortSnarf y ACID 323
3.1.3 SnortView 324
3.1.4 Spinning cube of potential doom 325
3.1.5 Starmine 325
3.1.6 Visual 325

INTRODUCCIÓN:
La informática forense, una disciplina técnico-legal

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas, bien sea humanas, procedimentales o tecnológicas, sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos (Kshetri 2006, Sundt 2006). Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos especiales de investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

A pesar del escenario anterior, la criminalística nos ofrece un espacio de análisis y estudio que nos permite procurar una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones que permitan descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio.

Así es como la informática forense hace su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, lo mismo que como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

En consecuencia, este documento busca ofrecer un panorama general de esta especialidad técnico-legal, para ilustrar a los lectores sobre los fundamentos generales y las bases de actuación de aquellos que se han dedicado a procurar el esclarecimiento de los hechos en medios informáticos, unos nuevos científicos que, mediante la formalidad de los procesos y la precisión de la técnica, buscan decirles a los intrusos informáticos que están preparados para confrontarlos y procesarlos.

Definiciones

A la fecha, existen múltiples definiciones sobre el tema forense en informática (McKemmish 1999). Una primera revisión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, *digital forensics* (forensia digital), *network forensics* (forensia en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos.

Conviene anotar que, al ser esta especialidad técnica un recurso importante para las ciencias forenses modernas, asume dentro de sus procedimientos las tareas propias asociadas con la evidencia en la escena del crimen, como son: identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección.

Iniciemos con *computer forensics*, cuya traducción por lo general se hace como computación forense. Esta expresión podría interpretarse de dos maneras: (1) disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o (2) como la disciplina científica y especializada que, entendiendo los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente en dichos equipos.

Estas dos definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses, y la otra en la especialidad técnica, pero en últimas ambas procuran el esclarecimiento y la interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática.

Cuando se habla de *network forensics* (forensia en redes), estamos en un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, las configuraciones y las infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que, entendiendo las operaciones de las redes de computadores, siguiendo los protocolos y la formación criminalística, es capaz de establecer los rastros, movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, poco frecuentes en equipos particulares.

Finalmente, *digital forensics* (forensia digital) trata de conjugar de manera amplia la nueva especialidad. Podríamos hacer semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes, o como una disciplina especializada que procura el esclarecimiento de los hechos de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada, o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Como hemos revisado, las definiciones abordan aspectos generales y específicos que en todos los casos convergen hacia la identificación, la preservación, la extracción, el análisis, la interpretación, la documentación y la presentación de evidencia digital, para detallar, validar y sustentar las hipótesis que sobre un evento se hayan formulado. No obstante lo anterior, es pertinente tener en cuenta que aquellos dedicados a esta disciplina emergente, como la informática forense, deben ser profesionales no con altos niveles de ética y respeto por las instituciones, sino con los más altos niveles, pues en ellos está el soporte de las decisiones que sobre los hechos analizados se tomen.

Evidencia digital

De acuerdo con el *HB:171 2003 Guidelines for the Management of IT Evidence*, la evidencia digital es: "cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". En este sentido, la evidencia digital es un

término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".

En este sentido, el documento mencionado establece que la evidencia digital puede ser dividida en tres categorías, a saber:

1. Registros almacenados en el equipo de tecnología informática (p. e., correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.).
2. Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno. La evidencia digital, para aquellos que la identifican y analizan en la búsqueda de la verdad, posee, entre otros elementos que la hacen un constante desafío, las características siguientes:

1. Es volátil
2. Es anónima
3. Es duplicable
4. Es alterable y modificable
5. Es eliminable

Estas características nos advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Por tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y los procesos que permitan mantener la confiabilidad de

los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

Procedimientos

Considerando la fragilidad del insumo con el cual trabajan los especialistas en informática forense, es preciso extremar las medidas de seguridad y control que éstos deben tener a la hora de adelantar sus labores, pues cualquier imprecisión en las mismas puede llevar a comprometer el proceso bien sea legal u organizacional (Wilson 2003, Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E. y Liederbach, J. 2006).

En este sentido, detallamos de manera básica algunos elementos que deben ser considerados para mantener la idoneidad del procedimiento forense adelantado:

1. *Esterilidad de los medios de informáticos de trabajo.* Los medios informáticos utilizados por los profesionales en esta área deben estar certificados, de tal manera, que éstos no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares, so pena de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues, al igual que en la medicina forense, un instrumental contaminado puede ser causa de una interpretación o un análisis erróneo de las causas de la muerte del paciente.
2. *Verificación de las copias en medios informáticos.* Las copias efectuadas en los medios previamente esterilizados deben ser idénticas al original del cual fueron tomadas. La verificación de éstas debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia. Adicionalmente, es preciso que el *software* o la aplicación soporte de esta operación haya sido previamente probado y analizado por la comunidad científica, para que, conociendo su tasa de efectividad, sea validado en un procedimiento ante una diligencia legal.

3. *Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados*. El investigador debe ser el custodio de su propio proceso; por tanto, cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera que cualquier persona externa pueda validar y revisarlos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos le ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

4. *Mantenimiento de la cadena de custodia de las evidencias digitales*. Este punto es complemento del anterior. La custodia de todos los elementos allegados al caso, y en poder del investigador, debe responder a una diligencia y una formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

5. *Informe y presentación de resultados de los análisis de los medios informáticos*. Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones.

6. *Administración del caso realizado*. Los investigadores forenses en informática deben prepararse para declarar ante un jurado o juicio; por tanto, es probable que en el curso de la investigación o del caso, los puedan llamar a declarar en ese instante o mucho tiempo después. Por consiguiente, el mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control, es labor necesaria y suficiente para

salvaguardar los resultados de las investigaciones y el debido cuidado, la diligencia y la previsibilidad del profesional que ha participado en el caso.

7. *Auditoría de los procedimientos realizados en la investigación*. Finalmente, y no menos importante, es recomendable que el profesional investigador mantenga un ejercicio de autoevaluación de sus procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad: PHVA –Planear, Hacer, Verificar y Actuar– sea una constante que permita incrementar la actual confiabilidad de sus procedimientos y cuestionar sus prácticas y técnicas actuales para el mejoramiento de su ejercicio profesional y la práctica de la disciplina.

Herramientas

Hablar de informática forense, sin revisar algunas ideas sobre herramientas, es hablar en un contexto teórico de procedimientos y formalidades legales. Las herramientas informáticas son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y el conocimiento del investigador que las utiliza. Estos dos elementos hacen del uso de las herramientas una constante reflexión y un cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática, detallamos algunas para conocimiento general de los lectores, las cuales son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática (*cuadro 1.1*):

	Licencia	Imagen	Control de integridad	Análisis	Administración del caso
Encase	SÍ	SÍ	SÍ	SÍ	SÍ
Forensic Toolkit	SÍ	SÍ	SÍ	SÍ	SÍ
Winhex	SÍ	SÍ	SÍ	SÍ	SÍ
Sleuth Kit	NO	SÍ	SÍ	SÍ	SÍ

Cuadro 1.1

Herramientas utilizadas en procedimientos forenses en informática

Encase –http://www.encase.com/products/ef_index.asp
Forensic Toolkit –http://www.accessdata.com/products/utk/
Winhex –http://www.x-ways.net/forensics/index-m.html
Sleuth Kit –http://www.sleuthkit.org

Si bien las herramientas detalladas anteriormente son licenciadas y sus precios oscilan entre los 600 y los 5.000 dólares americanos, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, las cuales generalmente son aplicaciones en software de código abierto. Estas últimas, a pesar de que son utilizadas con frecuencia como estrategia de validación en el uso de otras herramientas, vienen haciendo una importante carrera en la práctica de la informática forense, con lo cual no se descarta que en un futuro próximo éstas estén compitiendo mano a mano con las licenciadas mencionadas anteriormente. Para mayor información de otras herramientas forenses en informática, se sugiere revisar el enlace: http://www.e-evidence.info/vendors.html.

Retos

La informática forense es un desafío interdisciplinario que requiere un estudio detallado de la tecnología, los procesos y los individuos que permitan la conformación de un cuerpo de conocimiento formal, científico y legal para el ejercicio de una disciplina que apoye directamente la administración de la justicia y el esclarecimiento de los hechos alrededor de los incidentes o los fraudes en las organizaciones. En este sentido, se tienen agendas de investigación a corto y mediano plazos, para que se avance en temas de especial interés en la conformación y el fortalecimiento de las ciencias forenses aplicadas a los medios informáticos. Dentro de los temas seleccionados, están:

1. *El reconocimiento de la evidencia digital como evidencia formal y válida*. En muchas partes del mundo la evidencia digital en la administración de justicia continúa siendo una situación problemática por resolver (Brungs, A. y Jamieson, R. 2003). Dadas las características mencionadas previamente, se hace un elemento que requiere un tratamiento especial, más allá de las características legales requeridas, pues éstas deben estar articuladas con los esfuerzos de seguridad de la información vigentes en las organizaciones.

2. *Los mecanismos y estrategias de validación y confiabilidad de las herramientas forenses en informática*. Las herramientas utilizadas actualmente en investigaciones forenses en informática están cumpliendo una función importante para esclarecer los hechos ante incidentes informáticos. Sin embargo, la fragilidad inherente del software, la vulnerabilidad presente en las mismas y las limitaciones propias de los lenguajes y prácticas de programación hacen que la comunidad académica y científica redoble sus esfuerzos para hacer, de estos programas, herramientas más confiables y predecibles para los cuerpos de investigaciones judiciales y organizacionales.

3. *La formación de especialistas en informática forense, que apoyen labores de peritaje informático tanto en la administración de justicia como en investigaciones organizacionales internas*. Al ser la informática forense una ciencia aplicada naciente, es necesario iniciar las reflexiones sobre la formación de un especialista en informática forense (White, D., Rea, A., McKenzie, B. y Glorfled, L. 2004, Cano 2006). Esta formación necesariamente deberá ser interdisciplinaria, y para ello se requiere el concurso de los profesionales del derecho, la criminalística, las tecnologías de información y la seguridad de la información, como mínimo, sin perjuicio de que otras disciplinas académicas puedan estar presentes en la estrategia de profesionalización de estos nuevos profesionales.

A lo largo de este documento hemos querido mostrar, de manera básica y concreta, una aproximación a la informática forense, no con el ánimo de sugerir un curso de acción sobre el tema, sino de ilustrar los diferentes escenarios y elementos que componen esta naciente disciplina auxiliar de la criminalística. Es preciso aclarar que los conceptos expresados en este libro responden a una revisión de la práctica internacional sobre el tema.

La informática forense es la manifestación natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas (en medios informáticos y a través de medios informáticos), con el fin de enviar un mensaje claro a los intrusos: estamos preparados para responder a sus acciones, y continuamos aprendiendo para dar con la verdad de sus acciones.

Conclusiones

La presentación efectuada anteriormente es un resumen base de lo que implica la identificación, la administración, el análisis, la presentación y el reporte de las evidencias en medios electrónicos e informáticos, así como los retos exigentes que deben afrontar todos aquellos que se dedican a combatir la criminalidad informática en el contexto de un escenario global.

En razón de lo anterior y con el fin de profundizar en cada uno de estos aspectos, se presenta esta obra que busca ser un recurso literario práctico y básico para todos aquellos que quieran aproximarse a conocer las herramientas, la formación y los procedimientos de los nuevos criminalistas del siglo XXI, así como ilustrar algunos elementos tecnológicos necesarios para adelantar investigaciones que demanden un análisis exhaustivo de recursos informáticos.

La informática forense es una disciplina técnico-científica que cree más en las posibilidades que en las probabilidades, que busca filtrar los datos y la información irrelevante, y condensar los datos y la información relevante. Es una disciplina que busca el entendimiento de lo que ocurre o ha ocurrido, en las respuestas a las preguntas que empiezan con un "por qué", un cuerpo de conocimiento que constantemente se renueva y se adapta; una adaptación que, según Ackoff (Ackoff 1999, p. 167), no es otra cosa que un aprendizaje constante en condiciones cambiantes.

Bibliografía

Ackoff, R. (1999). Recreación de las corporaciones. Un diseño organizacional para el siglo XXI. Oxford Press.

Association of Certified Fraud Examiners. (s.f.). Proceedings of 14th Annual Fraud Conference. Chicago, IL. August.

Brungs, A. y Jamieson, R. (2003). Legal issues for computer forensics. Proceedings for 14th Australasian Conference on Information Systems. Perth, Western Australia. November.

Cano, J. (2006). Estado del arte del peritaje informático en Latinoamérica. Alfa-Redi.

Digital crime and digital terrorism. Pearson Prentice Hall. Caps. 11 y 12. Disponible en: http://www.alfa-redi.org/ar-dnt-documento.shtml?x=728

Kshetri, N. (2006). The simple economics of cybercrime. IEEE Security & Privacy. January/ February.

McKemmish, R. (1999). What is forensic computing? Australian Institute of Criminology. Issues and Trends in crime and criminal justice. No. 118.

Sundt, C. (2006). Information security and the law. Information Security Technical Report. Vol. 2, No. 9.

Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E y Liederbach, J. (2006) *Digital Crime and digital terrorism*. Pearson Prentice Hall.

White, D., Rea, A., Mckenzie, B. y Glorfled, L. (2004). A model and guide for an introductory computer security forensic course. Proceedings of the Tenth Americas Conference on Information Systems, Nueva York, August.

Wilson, A. (2003). Investigation by computer. Digital evidence –data in the box!

1 La computación forense. Una perspectiva de tres roles: El intruso, el administrador y el investigador

Objetivos

- ✓ Precisar qué es la computación forense.
- ✓ Resumir los roles del informático forense en los análisis de la información guardada en dsipositivos tecnológicos.
- ✓ Plantear la pedagogía para entender los análisis de la evidencia digital.
- ✓ Esbozar las características básicas de los intrusos informaticos.

INTRODUCCIÓN

La computación forense es una disciplina naciente que desde sus inicios ha establecido un reto tanto para los profesionales de ciencias de la computación y tecnología de información, como para los criminalistas tradicionales y la administración de justicia en general. La necesidad de contar con un profesional que reconozca y actúe conforme a los requisitos de ley y siga los procedimientos básicos en criminalística, ahora en fenómenos o casos donde la informática y la tecnología se hacen presentes, es una ventana para repensar la práctica de las ciencias forenses en un entorno digital.

1.1 LAS EVIDENCIAS TRADICIONALES

La computación forense establece un reto para los profesionales de ciencias de la computación y tecnología de información.

Éstas son recabadas en las escenas del crimen como "el arma ensangrentada", "las huellas digitales del vaso", "el lápiz labial de la colilla del cigarrillo", "las manchas de fluidos corporales", entre otras, hoy están acompañadas de discos duros, CD Roms, dispositivos USB de almacenamiento, Ipods, access points inalámbricos, direcciones IP, teléfonos celulares, entre otros elementos. En este nuevo orden de rastros, la combinación de la escena física con los análisis de los objetos tecnológicos establecen una nueva forma de pericia que extiende las habilidades de los criminalistas, no solamente para conocer lo que ocurrió en el sitio, sino la información y los detalles de los eventos con la información residente en las tecnologías de información presentes en el sitio.

1.2 EL INFORMÁTICO FORENSE

La combinación de la escena física con los análisis de los objetos tecnológicos establecen una nueva forma de pericia...

Este nuevo profesional, que de manera general denominamos Informático Forense (IF), será quien nos permita avanzar en la búsqueda de la verdad, en el análisis de la información residente en los dispositivos tecnológicos, en la construcción del caso con las evidencias digitales requeridas para esclarecer los móviles de los hechos, que se han podido presentar, bien sea en medios informáticos o electrónicos, o en combinación de hechos físicos y tecnológicos.

El IF permite avanzar tras la verdad, en el análisis de la información residente en los dispositivos tecnológicos.

Para ello, en este libro desarrollamos un enfoque particular para conocer las habilidades del IF, planteando un discurso pedagógico de tres roles y competencias requeridas para comprender y profundizar en los análisis de casos donde la evidencia

digital es parte inherente de la solución del caso. Los roles que debe conocer, afianzar y desarrollar el informático forense son tres: el del intruso, el del administrador y el del investigador.

1.3 LA FACETA DEL INTRUSO

Ésta es una forma de aproximarse a ver cómo éstos piensan, actúan y operan, para desarrollar el olfato y la pericia para predecir y analizar los posibles rastros y acciones que se desarrollen en medios tecnológicos. Conocer la mente y actuar de los atacantes le ofrece al IF una ventaja estratégica y conceptual sobre el caso que revise, pues se pondrá en el lugar del infractor y tratará de ver cómo actuaría en un caso semejante. Adicionalmente, el estudio detallado de otros ataques y fallas utilizadas en otros casos le dará mayores elementos de juicio para reconocer o para establecer patrones de análisis que ayuden a detallar lo que ha ocurrido, y así apoyar las investigaciones relacionadas con el caso (*cuadro 1.1*).

Conocer la mente y actuar de los atacantes le ofrece al IF una ventaja estratégica.

Características	Intruso interno	Intruso externo
Psicológicas	• Generalmente motivado por situación personal o laboral • Inestabilidad emocional • Socialmente hábil para recabar información y conocer a sus víctimas	• Generalmente motivado por reto tecnológico y compensación económica • Sensación de control y poder sobre un tercero • Relaciones basadas en conocimiento y logros
Técnicas	• Conocimiento detallado de fallas en procedimientos y regulaciones internas • Conocedor y estudioso de la operación de la organización y su modelo de procesos y controles • Conocedor de los mecanismos de seguridad y control	• Conocedor y estudioso de las fallas tecnológicas de los sistemas objetivo • Conocedor y usuario de técnicas de evasión de investigaciones • Cuenta con un laboratorio de pruebas para verificar previamente sus acciones

Cuadro 1.1

Características básicas de los intrusos informáticos

1.3.1 Los roles del intruso

Si bien el rol del intruso es interesante y atractivo, no es posible conocer los detalles de los rastros, si no nos adentramos en la mente del administrador, el profesional de tecnologías de información a cargo de la administración y control de las máquinas que posiblemente están involucradas. En este rol, el IF debe comprender los conceptos de protección y control de tecnologías de información, no sólo para detallar las medidas tecnológicas de seguridad y control configuradas, sino para identificar y analizar las diferentes formas de alerta, detección, registro y monitoreo que la infraestructura tiene definidas para prevenir algún tipo de incursión no autorizada. En este papel el IF se enfrentará al reto de la inseguridad informática y sus diferentes fuerzas, reconocerá las relaciones entre las tecnologías de protección y las fallas de seguridad informática, para afianzar su visión de intruso presentada previamente (*gráfico 1.1*).

Gráfico 1.1

Características del administrador de sistema

El IF debe enfrentarse a la inseguridad de la información, y así reconocer la visión del intruso.

El intruso y el administrador son dos roles complementarios y requeridos dentro de la gestión de la inseguridad de la información, pero se requiere un rol adicional que, con mirada emergente y superior, descubra las relaciones y los móviles de lo ocurrido; siga los procedimientos exigidos y

establezca las evidencias requeridas para reconstruir la escena de lo anormal identificado. El investigador, ese rol natural de mirada aguda y persistente, es el elemento complementario que el IF debe conocer y desarrollar en sus acciones (*gráfico 1.2*).

Gráfico 1.2
El perfil del investigador

1.4 EL INVESTIGADOR

Éste es escéptico de lo obvio, observador, detallista y riguroso. Es un profesional científico, formal en los procedimientos y el uso de las herramientas disponibles, que no busca otra cosa que las relaciones y causales que pudieron llevar a materializar el caso. Por lo general, este perfil se forma en la carrera de criminalística, que actualmente en los países latinoamericanos está confinada a profesionales y personas adscritas a instituciones militares, de policía o de administración de justicia.

El investigador es el elemento complementario que el IF debe conocer y desarrollar.

Como podemos ver, analizar al informático forense y sus acciones en estos tres roles nos permite recorrer los diferentes escenarios de la posible acción punible en medios tecnológicos, avanzando hacia una renovación y una extensión de la criminalística tradicional, una que podría llamarse criminalística digital.

Resumen

El desarrollo de este libro estará articulado en cinco capítulos, tres de ellos donde se explora en detalle cada uno de los roles presentados, como una excusa académica para comprender las acciones, los procedimientos y conceptos de la computación forense aplicados a situaciones reales e hipotéticas, que ayudarán a los lectores, profesionales de la seguridad informática, analistas forenses, directores de tecnología y niveles gerenciales a percibir cómo esta nueva disciplina se hace parte inherente de la atención de incidentes de las organización, así como del soporte legal y administrativo de las acciones que se deriven de las investigaciones que se adelanten en el interior o el exterior de la misma.

La computación forense con sus componentes tecnológicos, formación especializada, detalles profundos de las tecnologías y sus implementaciones, ésta nos abre la puerta a un mundo lleno de retos intelectuales, criminológicos y criminalísticos que introducen a todos sus conocedores en una actualización permanente en temas jurídicos, tecnológicos, humanos y organizacionales que no permiten que entren en una zona de confort, pues, de hacerlo, saben que la lucha contra el crimen organizado estará cediendo terreno valioso que posiblemente no podrá recuperar.

Estamos en un mundo interconectado y global; por tanto, la delincuencia sabrá aprovechar estas dos características para proponer escenarios de ataque y falla donde confronten las mejores prácticas de las organizaciones. En este sentido, es necesario que la función de tecnología no sólo piense en las posibilidades y oportunidades de negocio con tecnología, sino que, de manera integrada, la gestión de la inseguridad de la información sea la constante ante la inevitabilidad de la falla humana, tecnológica o procedimental.

2 El intruso y sus técnicas

Objetivos

- ✓ Revisar y analizar la historia de los hackers.
- ✓ Detallar y profundizar en la mente de los intrusos, como una forma de avanzar en el análisis de incidentes y situaciones de falla.
- ✓ Describir y estudiar algunas técnicas básicas de ataques, para conocer ciertos elementos técnicos de las fallas generalmente utilizadas por los intrusos.
- ✓ Profundizar en algunas técnicas avanzadas de ataque y sus impactos en las organizaciones.
- ✓ Identificar los lugares en donde posiblemente puedan quedar los rastros de la materialización de los ataques de los intrusos.

INTRODUCCIÓN

La inseguridad es y continuará siendo la constante en un mundo interconectado. En este sentido, la mente de los atacantes y apasionados por la inseguridad informática continuará produciéndose y avanzando, pues cada vez más habrá retos y desafíos que sortear con la tecnología actual y futura. En consecuencia, estudiar la mente de los atacantes, el estilo de los hackers, sus técnicas, es una manera de aprender de las vulnerabilidades, y cómo la materialización de éstas puede utilizarse para establecer los rastros requeridos para seguir a los atacantes.

> La inseguridad informática continuará produciéndose y avanzando, pues cada vez más habrá retos y desafíos que sortear con la tecnología actual y futura.

Si lo anterior es correcto, los informáticos forenses deben profundizar en este rol para comprender la mente de los intrusos, detallar sus estrategias y avanzar en el reconocimiento de rastros informáticos de manera ordenada, profunda y consistente. Los informáticos forenses deben aprender la lección de que esta mente no descansa, busca siempre al margen del camino y explora las posibilidades que se presentan al "eliminar" las autorrestricciones (Ackoff, R. 2002), que imponen los diseños de las soluciones de informática.

2.1 BREVE HISTORIA DE LOS HACKERS

> Los hackers son los constructores del manual de lo "no documentado", de la realidad inmersa en las soluciones de informática que aún no se descubren.

Hablar de hackers, término derivado de Hacking, es contar la historia actual de aquellos inconformes con lo establecido, con los que "ven" más allá de lo que establece el manual; esos que constantemente exploran posibilidades en las entrañas de los códigos ejecutables, o procesos de la máquina, para ver comportamientos que los documentos técnicos no tienen documentados. Se podría decir que los hackers son los constructores del manual de lo "no documentado", de la realidad que está inmersa en las soluciones de informática que aún no se descubre, o se escribe para que otros la observen.

> El movimiento hacking es y será una fuerza motriz del desarrollo de mejoras en software, pero una motivación de los profesionales que quieren dejar su huella en el mundo...

Repetir la historia de los hackers sería contar una historia vigente de personajes reales y creativos, que solamente buscan la profundidad de las fallas, aquellos momentos inesperados que sorprenden a los ingenieros de software, pero que alegran a otros. El movimiento *hacking* es y será una fuerza motriz del desarrollo de mejoras en el mundo del software, pero igualmente una motivación permanente de los profesionales que quieren dejar su huella en el mundo, porque la filosofía del mundo hacker es trabajo continuado, persistencia y mucha imaginación para cambiar lo establecido y desafiar el statu quo.

Podríamos decir que el *hacking* nace en el Instituto Tecnológico de Massachusetts, conocido como MIT por sus siglas en inglés, según varias revisiones documentales, como fruto de una motivación por conocer, descubrir y entender cómo funcionaba la máquina de comunicaciones TX-0 (computador con transistores). Esa máquina era el "juguete" tecnológico más sofisticado para la época cuando un grupo afortunado de estudiantes de ese instituto decidieron experimentar, para conocer su funcionamiento y detalles de implementación. Era 1960 y ese grupo de estudiantes que se hizo cargo de esta pieza de tecnología estaba dispuesto a sumergirse en jornadas de 36 horas de programación y conocimientos, porque la máquina no tenía software o aplicaciones disponibles, lo cual obligaba a las mentes inquietas a crear las herramientas y estrategias requeridas para sacarle el mayor provecho a esta novedad tecnológica.

El hacking nació en el MIT como fruto de una motivación por conocer, descubrir y entender cómo funcionaba la máquina de comunicaciones TX-0.

Con el avance tecnológico hace su aparición el PDP-1, otra máquina computacional con mayores posibilidades que el Tixo (como cariñosamente llamaban al TX-0). El *Programmed Data Processor-1* fue el primer computador en serie PDP de la Digital Equipment, producido por primera vez en 1960, y a la vez el hardware original en donde se jugó el primer videojuego computarizado de la historia, el Spacewar de Steve Russell. Con este nuevo dispositivo tecnológico el desarrollo de programas y capacidades de las máquinas estuvo a cargo de los llamados hackers, esos individuos que hacían cosas o tenían logros que otras personas no tenían. Ellos fueron los responsables de que cada vez se les exigiera a los proveedores de los equipos PDP (Digital Equipment Corporation, DEC)

El Programmed Data Processor-1 fue el primer computador en serie PDP de la Digital Equipment, producido en 1960, y el hardware con el cual se jugó el primer videojuego computarizado..., el Spacewar de Steve Russell.

para contar con máquinas más fuertes y avanzadas. Con el paso del tiempo, la DEC desarrolló toda una generación de PDP (el PDP-2 nunca fue producido y el PDP-3 se creó para un cliente específico, y la serie siguiente desde el PDP-4 al PDP-10).[1]

Con el PDP-11, el más exitoso de toda la serie, se abre la puerta a la computación integrada, como la conocemos hoy. Esta computadora fue la primera en interconectar todos los elementos del sistema (procesador, memoria y periférico), a un único bus de comunicación, bidireccional, asíncrono. Este dispositivo, llamado Unibus, permitía a los dispositivos enviar, recibir o intercambiar datos sin necesidad de dar un paso intermedio por la memoria. Ésta fue una de las primeras computadoras en las que corrió el sistema UNIX, desarrollado en los Laboratorios Bell.

Por aquella época, desde finales de los años 60 hasta principios de los años 70, la guerra hace que las naciones desarrollen nuevas posiciones estratégicas en temas de comunicaciones, para defenderse y comunicarse en caso de un ataque nuclear. Los científicos de los Laboratorios Bell, que habían creado un sistema operacional de multiusuario, multiproceso, altamente avanzado para la época, participan en la convocatoria que hace el gobierno americano para desarrollar un nuevo concepto de redes y computación, ante la amenaza de Cuba con los misiles de que la antigua Unión Soviética (URSS) le había provisto al gobierno de la isla.

Desde los años 60 hasta los 70, la guerra hizo que las naciones desarrollaran nuevas posiciones estratégicas en temas de comunicaciones, para defenderse de un ataque nuclear.

De nuevo, las mentes más brillantes de las universidades, de las industrias y del gobierno se unen para dar un nuevo salto en el desarrollo tecnológico, debido a la guerra y a la defensa ante una amenaza nuclear. Todos los participantes en esta iniciativa de defensa, coordinada por la ARPA (Advanced Research Project Agency) eran los hackers más destacados del momento. Entre otros nombres, Dennis Ritchie, Brian Kernighan, Ken Thompson, Vinton Cerf, Leonard

[1] Adaptado y traducido de: http://www.pdpplanet.org

Kleinrock (autor conceptual de la teoría de redes de paquetes) fueron los responsables (bajo la coordinación de Paul Baran, de la Rand Corporation, contratista del gobierno americano para el proyecto de la red de comunicaciones) de la creación de la red militar de ARPA (Arpanet), que luego se transformaría en lo que conocemos como Internet.

Con el desarrollo tecnológico que se da entre 1970 y 1980, se crean muchas industrias y muchos hackers aprovechan para crear nuevas y novedosas distinciones que cambiaron la manera como la computación afectaba la vida del mundo. Así, surgen desarrollos como nuevos procesadores (Motorota 68000, Z-80, la Serie x86, entre otros), nuevas aplicaciones y servicios (correo electrónico, sistemas de noticias, accesos telefónicos, entre otros). Este momento de la evolución de la tecnología se podría llamar la etapa de los hackers empresarios, los cuales estaban en universidades (UCLA, MIT, Stanford), laboratorios avanzados (Bell Labs, Xerox, Stanford Research Institute) o empresas (IBM, Wang, luego más tarde Burroughs), desarrollando las bases de productos y aplicaciones que darían a las empresas una forma más eficiente de hacer las cosas: bases de datos relacionales, sistemas de procesamiento compartido, sistemas operacionales, estrategias de seguridad de la información, entre otros. De esta etapa se podría concluir que personas, como C.J Date (Padre de las Bases de datos), Edsger Wybe Dijkstra (científico eminente de algoritmos de programación), Niklaus Wirth (diseñador de lenguajes de programación y estructuras de datos), fueron hackers de alto desempeño que lograron desafiar lo conocido para el momento, y abrir la puerta a todo un nuevo mundo de programación y computación avanzada.

Entre 1970 y 1980, se crean muchas industrias y los hackers aprovechan para crear nuevas y novedosas distinciones que cambiaron la manera como la computación afectaba la vida.

Con el inicio de los años 80 las redes son parte natural de las interconexiones de las universidades, gracias a los logros de dos importantes investigadores que diseñaron y pusieron en operación el conjunto de protocolos TCP/IP. Vinton Cerf y Robert Kahn, investigadores residentes tanto de la Universidad de California como de Stanford. Estos hackers son los responsables de que tengamos hoy por hoy una red mundial de computadores interconectada. Durante 1982, Cerf diseñó el primer servicio de correo electrónico comercial para MCI, empresa de comunicaciones norteamericana.

Durante la década de los años 80 la presencia de las redes en las universidades, la disponibilidad del sistema operacional UNIX, el flujo importante de recursos para adelantar investigaciones (generalmente en el ámbito militar), y el desarrollo de los lenguajes de programación, se tiene un caldo de cultivo ideal para que una nueva generación de hackers haga su aparición. Esta nueva generación, cautivada por la máquina y por las posibilidades de los sistemas operacionales, abre la posibilidad para explorar fallas inherentes a los programas que para ese entonces se presentaban en los programas. Muchas herramientas, como los depuradores y los compiladores, fueron las preferidas para sumergirse en los posibles efectos de borde de los programas disponibles a la fecha.

El término virus informático se adoptó en 1984, pero esta amenaza ya se había materializado en los sistemas IBM 360, en 1972, al presentrse el programa Creeper (enredadera).

Si bien el término virus informático, no se adopta hasta 1984, esta amenaza ya previamente se había materializado en los sistemas IBM 360 en 1972, cuando se presentó un programa denominado Creeper (enredadera), que aparecía en las pantallas del mencionado equipo de manera aleatoria. Esta nueva especie de programas, que hacían operaciones catalogadas como "anormales", daban cuenta de que existía un espacio para mentes creativas dentro de los códigos vigentes en los programas.

Con el avance de los 80, ya hacia finales de esa misma época, se presentan los primeros enfrentamientos de grupos de hackers por tener el control de empresas de telefonía y el primer gusano masivo en la red extendida de ARPA, Arpanet, ahora denominada Internet. La lucha de territorios informáticos y electrónicos de grupos de mentes

creativas, para demostrar que las máquinas tenían posibilidades aún inexploradas, hace que pierdan la visión inicial planteada por los pioneros de MIT, llegando a ser detenidos y procesados por entes como el FBI. Desde ese momento, el término hacker pasó de un título que se ganaba por sus méritos y logros diferenciadores, a uno que se asociaba con "vándalo o intruso informático".

La cultura que con muchas horas de trabajo un grupo de mentes pensantes desarrolló, con logros científicos y una ética basada en el avance de la ciencia, se transformó en una cultura oscura, llena de historias de asaltos, pérdidas económicas e inframundos que terminaron confinando la esencia del mundo hacker.

La cultura que las mentes pensantes desarrollaron se transformó en una cultura oscura, de historias de asaltos, pérdidas económicas e inframundos que terminaron confinando la esencia del mundo hacker.

La historia reciente del mundo hacker, ahora con la connotación y la carga emocional de ilegalidad y maldad, se traduce en asaltos y cambios no autorizados de páginas Web (por cierto creado en 1989, por otro hacker, en su concepción original, Tim-Berneers Lee), manipulación de contraseñas, alteración de configuraciones, acceso no autorizados, entre otras acciones que muestran que existe una alta probabilidad de que aquello que se conoce como seguridad pronto será vulnerado y deberá ser reparado, cambiado o repensado a la luz de las nuevas noticias que nos proveen los hackers.

Varios nombres, como Kevin Mitnick, Legion of Doom, Master of Deception, Mafia Boy, entre otros, se convierten en iconos de una nueva imagen de personajes, que se siguen denominando hackers, por su manto de misterio, por sus logros (aplaudidos por unos y repudiados por otros), y sobremanera por su especial modo de cautivar la atención de las organizaciones, la fallas de seguridad de los sistemas. Esta nueva etapa de vulnerabilidades fortalece y hace avanzar la industria de seguridad de la información, cuyos inicios se remontan a 1975 con los desarrollos internos del Departamento de Defensa Norteamericano y la propuesta de IBM.

Ya para el año 2000, los temas de *hacking* son naturales e inherentes a las discusiones de las personas y las organizaciones. El término se utiliza aún en su aspecto negativo y eso lo hace llamativo y misterioso.

Los avances tecnológicos se hacen cada vez con más rapidez, y las aplicaciones más intuitivas y versátiles para los usuarios finales. Ahora en este contexto, con mayores recursos disponibles, mayor información diseminada vía Internet y acceso desde el hogar, los hackers tienen un reto importante que asumir: dejar que el lado oscuro de la fuerza los cautive, o continuar con el descubrimiento de nuevas posibilidades que les lleven a retos mayores. Si se dejan cautivar por el lado oscuro, la transformación hacia la delincuencia será contagiosa y destruirá la esencia del motor de su vida, el reto, para cambiarlo por bienes materiales y beneficios personales. Ya no serán más hackers, sino delincuentes que serán perseguidos por sus acciones, que no tienen ya la connotación de avances valiosos, sino de acciones punibles que vulneran derechos y libertades de ciudadanos.

En este punto recordar el *Manifiesto Hacker*, emitido por Mentor en sus inicios, permite concluir que el hacking y otras manifestaciones que se han gestado a la luz de las acciones de los chicos del *Tech Model Railroad Club* (TMRC) del MIT, en 1960, abren la posibilidad de crecer y mirar la futuro con la confianza de que las guerras que se librarán serán las de los retos inteligentes, las confrontaciones serán por alcanzar nuevos horizonte científicos y que las treguas que se firmen sean para descansar, depurar y repensar lo existente. De esta manera, ser hacker será nuevamente el título que se alcanza por nuevos retos superados y distinciones alcanzadas.

Ser hacker será el título logrado por nuevos retos superados y distinciones alcanzadas.

2.2 LA MENTE DE LOS INTRUSOS

Hablar de la mente de los intrusos es referirse a las motivaciones, esos disparadores de acción y su manera de actuar para avanzar donde otros no lo hacen. Revisar la mente de los atacantes es avanzar en un terreno donde la imaginación es más importante que el conocimiento. No podemos comparar un intruso, cuya motivación está más allá del reto y el reconocimiento por sus capacidades, con un hacker que busca una manera de mostrarnos que el manual no está completo y requiere completarlo con cada nueva experiencia y comportamiento inesperado del sistema.

Teniendo claras las consideraciones anteriores, trataremos de adentrarnos en la mente de aquellos cuyas acciones atentan contra los derechos y libertades del otro, muchas veces llevados por motivadores egoístas y ególatras que deben ser señalados y perseguidos por la sociedad.

Según Furnell (2002, p. 55), existen diferentes consideraciones para concebir o para clasificar a los atacantes, así como las motivaciones que los mueven a actuar en una situación particular. (*cuadro 2.1*).

Motivaciones	Ciberterroristas	Phreakers	Script kiddies	Crackers	Desarrollo de virus	Atacante interno
Reto		X			X	X
Ego		X	X		X	
Espionaje				X	X	X
Ideología	X					
Dinero		X		X	X	X
Venganza	X		X		X	X

Cuadro 2.1

Algunos tipos de atacantes y sus motivaciones. Adaptado de: Furnell, S. 2002, p. 55

Furnell habla de atacantes con perfil de, entre otros términos, *ciberterrorista, phreakers, script kiddies, crackers,* desarrollador de virus. Cada uno de ellos se mueve por motivos diferentes que llevan una carga emocional que es importante analizar y no solamente, las consideraciones técnicas de sus acciones, que dicen del nivel de conocimiento del individuo. Además de los perfiles establecidos por Furnell, se agrega uno que muchas veces pasa inadvertido, como son los empleados insatisfechos o atacantes internos. Esos funcionarios o colaboradores que no encuentran en su trabajo una motivación real para seguir creciendo, o que se llenan de resentimientos o sentimientos encontrados hacia personas específicas o hacia la organización y sus directivas. Este perfil es un elemento fundamental para estudiar los intrusos, pues con él se hace evidente que éstos pueden ser tanto externos como internos, resultando estos últimos los de mayor nivel de riesgo, dadas las características que revisten dentro de la organización.

A continuación revisaremos cada uno de los tipos de atacantes propuestos, detallando sus motivaciones y acciones para visualizar con mayor detalle los alcances de cada uno de ellos.

Iniciemos con el *ciberterrorista*; es la etiqueta más reciente y actual que se puede evidenciar para un atacante. Cuando se habla de terrorismo pensamos en personas radicales con ideales y motivaciones religiosas que nos llevan a pensar en ataques de grandes proporciones y acciones de alcance global. En el contexto de un mundo interconectado y global, el terrorismo cambia sus estrategias de acción y utiliza los medios electrónicos para recabar información, efectuar inteligencia estratégica e interconectar a todos sus simpatizantes alrededor de una red de comunicación eficiente, práctica y efectiva. El terrorista sabe que su causa merece y vale toda la coordinación para no fallar a la causa, y la red se vuelve su aliado, pues es un espacio virtual y omnipresente que le permite estar en todas partes al mismo tiempo y en ninguna a la vez.

> Las redes de comunicación le ofrecen al terrorista un escenario de anonimato, imperceptibilidad y mimetismo que canaliza en comunicaciones y actividades que aparentemente son normales para los navegantes de Internet, pero que llevan mensajes que sólo pueden ser identificados y analizados por sus compañeros ideológicos. Las técnicas de *information operations, information wafare y psychology operations* (Hutchinson, B. y Warren, M. 2001) son las constantes para mantener el control y el monitoreo de sus planes, sin despertar sospechas de sus acciones. Cuando reconocen que la red no sólo es una manera de apoyo logístico y coordinación de sus acciones y cuentan entre sus filas, personajes que saben que todo se articula con tecnologías de información diseñan nuevas estrategias, ya no para intimidar y penetrar sistemas, sino para infundir terror.

Las redes de comunicación le ofrecen al terrorista un escenario de anonimato, imperceptibilidad y mimetismo.

El ciberterrorista, enterado de las interconexiones de los sistemas, genera inestabilidad en los sistemas, incertidumbre sobre la

operación y fallas de las comunicaciones, creando un ambiente propicio para iniciar una guerra de desinformación y actuar para generar y potenciar la sensación de "pérdida de control" que llevará a las autoridades, sin un adecuado manejo de crisis, a una experiencia semejante al terror y vulnerabilidad que se experimenta con un carro bomba o explosiones masivas en territorio civil.

Pareciera que el ciberterrorista fuese un perfil extraído de los mejores relatos de Hollywood, pero no es así. Estamos en una nueva era de conocimiento y comunicaciones donde todo está a un click de distancia y, por tanto, el crimen organizado sabe que existe un nuevo espacio para actuar y desatar la confusión requerida para actuar sin mayores bajas, y con el menor número de rastros identificables o reconstruibles. Este perfil se está difundiendo en las más importantes organizaciones delincuenciales, y no debemos esperar a que situaciones que pueden ser prevenidas y contenidas se materialicen por falta de preparación y acciones que mitiguen este riesgo. Esto es lo que podríamos llamar una "sorpresa predecible". [2]

Los *phreakers* o los amantes de los teléfonos, a pesar de que no fueron mencionados en la historia de los hackers, se detallan en este punto como esa fuerza básica que reconoció en las líneas telefónicas un mundo nuevo para descubrir y conquistar, más allá del control de las autoridades o especialistas de tecnología. Un *phreaker* es un individuo que ha sido iluminado por la frecuencia de los tonos que emiten los dispositivos de comunicaciones, de las ondas hertzianas y los espacios electromagnéticos para distinguir los códigos que ellas llevan, que se traducen en números, indicaciones o llamadas que se hacen de un lugar a otro.

Los *phreakers* o los amantes de los teléfonos no se mencionaron en la historia de los hackers, pero son esa fuerza básica que reconoció en las líneas telefónicas un mundo nuevo.

El *phreaker* cree en la telefonía sin costo, en un mundo abierto para construir y crear lazos de conexión más allá del mundo real. Sabe que los dispositivos de comunicaciones codifican y decodifican señales

[2] Para mayor información sobre las "Sorpresas predecibles", revisar el libro de Bazerman, M. y Watkins, M. (2004). *Predictable Suprises. The disasters you should have seen coming and how to prevent them.* Harvard Business School Press.

El phreaker cree en la telefonía sin costo, para construir y crear lazos de conexión más allá de la realidad.

para sincronizarse y lograr la transmisión de la información, pero igualmente saben que hay dispositivos que rarifican y controlan el uso del canal de comunicación. El reto que impone el mundo de las telecomunicaciones es lograr expandir y evadir el cerco de los controles establecidos, bien sea por convicción propia o por alguna recompensa no necesariamente personal sino económica. Las comunicaciones son un negocio que mueve millones de dólares al año, y cualquier atentado contra alguna de sus infraestructuras puede implicar pérdidas para los operadores y accionistas de esas empresas.

En algunos momentos el *phreaker* se siente como el reivindicador de los derechos de los usuarios, al decirles a los operadores que sus tarifas no compensan el servicio que prestan, dado que la autopista de la información fue creada para compartir y crear un mundo interconectado, y no monopolios de accionistas que alquilan una autopista para transitar en algo que por definición es para servicio de la sociedad. Suena como a discurso izquierdista, pero es parte de la ideología de estos personajes, que aún se encuentran en la maraña de la red y continúan expectantes por los nuevos desarrollos en Internet, pues saben que todo se inicia en los tonos de las comunicaciones y allí terminan indefectiblemente. Ahora con la nueva propuesta del iPhone se plantean nuevos retos donde la consigna será eliminar o restringir las restricciones.

Se ha llamado *script kiddies* a todos aquellos que mirando los logros de los hackers, phreakers o similares, utilizan las herramientas y técnicas utilizadas por éstos, para lograr penetrar sistemas o inutilizar sistemas de comunicaciones o tecnologías de información. Los script kiddies, motivados por su curiosidad para experimentar y ver qué tan reales son los efectos de las armas de los hackers o phreakers, establecen un perfil de posibles atacantes intencionales o no, que pueden generar cierta conmoción en las organizaciones.

En una comunidad es relativamente fácil de identificar un perfil de *script kiddies*. Son personas que constantemente experimentan con sus máquinas, son amantes de las fallas de las mismas y con frecuencia

quieren demostrar sus conocimientos frente a otros, a quienes impresionan con sus aparentes logros. Son de cuidado en la medida en que pueden perder el control de sus actos y generar fallas o incidentes de magnitud importante, sin que ellos lo puedan notar o percibir. Estos "utilizadores de herramientas" son una *ola fashion,* modas que se pueden desarrollar por las noticias o anuncios de sitios vulnerados donde las autoridades generalmente no logran dar con el paradero de los atacantes, generando la sensación de emoción y logro a ser imitada.

El perfil de *script kiddies* corresponde a personas que experimentan con sus máquinas, aman las fallas de estas mismas y quieren demostrar sus conocimientos a otros.

Los *script kiddies* siempre serán una amenaza latente, las herramientas diseñadas por hackers o curiosos informáticos estarán disponibles en la red, esperando que algún curioso experimente qué puede hacer con ellas, exponiendo a las organizaciones a situaciones inesperadas, que deben ser parte de los ejercicios de preparación ante eventos informáticos que están fuera de los reportes normales de operación

Los *script kiddies* son una amenaza latente; las herramientas diseñadas por hackers estarán disponibles en la red, para que algún curioso experimente qué puede hacer con ellas, exponiendo a las organizaciones a situaciones inesperadas...

Hablar de *crackers* es hacer referencia al lado oscuro de la fuerza. El quebrar, destruir y desestabilizar son palabras que se materializan con las acciones de un intruso con esta mentalidad. El cracker tiene como objetivo vulnerar un sistema con una motivación de venganza o económica; es un individuo cuyo resentimiento lo ciega y lleva a utilizar sus conocimientos para traspasar la línea de lo permitido y lo legal. El *cracker* es catalogado en la literatura como un mercenario que vende sus conocimientos al mejor postor, para tener una ventaja competitiva en un mundo dominado por la tecnología.

El *cracker* se propone vulnerar un sistema con una motivación de venganza o económica... Es como un mercenario que vende sus conocimientos al mejor postor.

Este mercenario tecnológico sabe que las tecnología siempre tendrá fallas y, por tanto, las estudia y analiza para concebir nuevas formas de vender sus servicios, no para proteger a las organizaciones sobre nuevas amenazas, sino para crearlas y esperar el tiempo requerido para lucrarse ante la sensación de vulnerabilidad evidente. Se podría decir que los crackers son los criminales online que han repensado su actuar en el mundo físico, ahora en los medios informáticos; esos cuya mentalidad temeraria, evasiva y asociativa se hace presente a través de mensajes irrastreables e intimidaciones electrónicas, que hace que las autoridades establezcan nuevos controles y estrategias para limitar las acciones de esta amenaza delictiva.

Los crackers son los criminales online que han repensado su actuar en el mundo físico, usando mensajes irrastreables e intimidaciones electrónicas.

A un *cracker* no lo mueve necesariamente el ego, o el reto, ni busca un reconocimiento positivo; es una mente que engaña, se aprovecha y genera ventaja para su propio beneficio o el de su clan. Es una industria de engaños y desestabilización que solamente requiere una víctima para hacer crecer su negocio de extorsión y amenaza. Los *crackers* pueden tener las habilidades de los hackers (en el buen sentido de la palabra), pero no sus motivaciones. Por tanto, combinar la habilidad y la capacidad de innovación de los hackers, con motivaciones diferentes, es crear un perfil oscuro que tendrá las herramientas para atacar pero también para evadir cualquier intento de seguimiento. Casi podríamos decir que el *cracker* es un hacker en desgracia ética y personal.

Los *desarrolladores de virus* o programas de código malicioso *(malware)* son otra especie de especial interés que puede ser *catalogada* como atacante. El creador de virus o gusanos (tan de moda en Internet por estos días) es un personaje que resulta bastante enigmático para los investigadores forenses en informática. Lo mueven el reto, su ego, el dinero, la necesidad de revancha, los sentimientos encontrados que se traducen en frustraciones personales o laborales, que terminan en un nuevo estilo de vida que conjuga lo mejor de una carrera técnica y sus detalles de implementación, con una vida profesional y personal que se debate entre el reconocimiento y la insatisfacción.

El *creador de virus* no es un insatisfecho, pero tampoco es una persona realizada. Está atrapado por su potencial y su talento técnico en un mundo que para él aún no es el ideal y, por tanto, quiere demostrar que existen nuevas formas de pensar y concebir lo que se ve en la realidad. La necesidad de ir más allá de lo que se muestra en la realidad, lo lleva a generar estrategias de espionaje silencioso y estratégico, que le permiten recabar información necesaria para mantener una posición de ventaja sobre cualquier otra persona u organización. Los gusanos recientes en Internet recaban información, revisan y actualizan software en las máquinas que atacan, verifican que otras personas no tengan control sobre ellas, entre otras acciones, como un signo distintivo del creador sobre el escenario que ha creado para demostrar su superioridad.

El creador de virus no es un insatisfecho, ni una persona realizada. Es alguien atrapado por su potencial y su talento técnico en un mundo que aún no es el ideal para él.

El *desarrollador de virus* es un hacker desfigurado; es la construcción de un ser no inspirado por la tecnologías y sus desafíos, sino controlado por ella y sus posibilidades. Es una persona o grupo de personas que han desviado el camino de la luz, por un atajo oscuro que sólo los conduce a una realidad de la que quieren escapar, pero que tarde o temprano los alcanza: su propia identidad.

El desarrollador de virus es una persona o grupo de personas que han desviado el camino de la luz, por un atajo oscuro que sólo los conduce a una realidad de la que quieren escapar pero que los alcanza: su propia identidad.

Finalmente y no menos importante, tenemos los empleados o personas insatisfechas o aquellas que han terminado en malos términos con la organización. Esta amenaza interna es una realidad en todas las empresas en el mundo. Los empleados son seres humanos que buscan en su lugar de trabajo un escenario para potenciar sus capacidades y avanzar en su desarrollo personal y profesional. Muchas pueden ser las razones por las cuales una persona se siente insatisfecha con la organización y, por tanto, muchos pueden ser los escenarios para abordar el análisis de esta posible amenaza.

El *atacante interno* puede ser cualquier persona, sólo se requiere un disparador o detonante para que se transforme en un potencial delincuente que encuentre en la organización y su infraestructura la manera para demostrar que existe y que requiere atención a su situación. Situaciones de carácter personal, familiar, laboral o de celos profesionales pueden ser ocasión para que se desvíen las actividades de una persona hacia acciones que puedan impactar la infraestructura de comunicaciones, o computación de una empresa.

El atacante interno puede ser cualquier persona; basta un disparador o detonante para transformarse en un potencial delincuente que en la organización encuentre cómo demostrar que existe y requiere atención a su situación.

Si adicionalmente esta persona insatisfecha posee la curiosidad técnica de un script kiddie y la perseverancia de un hacker, estamos en una ruta para gestar un incidente de seguridad informática de proporciones importantes, donde las acciones que se adelantarán se planearán de manera cuidadosa, hábilmente mimetizadas y ejecutadas detalladamente, pues conocen los procedimientos internos y los alcances de los mismos cuando un evento anormal se presenta. Por lo general, se dice que el atacante se vincula a la investigación como parte de estrategia para no ser descubierto o implicado.

El atacante interno, ese empleado insatisfecho, no debe estigmatizar a los demás empleados que están a gusto con su trabajo y encuentran en él su forma de potenciar sus capacidades y profesionalismo. Por tanto, las organizaciones deben desarrollar estrategias y mecanismos para avanzar en el desarrollo de índices de amenaza informática interna que permitan identificar, con el área de talento humano y tecnología de información, los referentes básicos para proponer acciones preventivas que disminuyan esa amenaza y fortalecer las medidas de seguridad y control de acuerdo con la situación evidenciada. Ese índice debe ir más allá de las consideraciones técnicas que identifiquen el área de tecnología,

El atacante interno no debe estigmatizar a los demás empleados que están a gusto con su trabajo.

y combinarse con las apreciaciones que el talento humano considere necesarias para su concepto.

Como se puede evidenciar, la mente de los intrusos es compleja y sus motivaciones variantes. Se preguntarán si es posible tener un perfil que combine lo mejor de cada uno de los anteriormente detallados, para tener un atacante perfecto, imperceptible, que engañe los diferentes controles y estrategias de seguridad. La respuesta podría ser sí y no. Sí en la medida en que este atacante sea lo suficientemente cuidadoso para mantener su mundo de engaño y control, bajo las reglas que el escenario considera normales. Y no, pues el ser humano no puede mentir todo el tiempo sin quedar expuesto a la verdad. En el fondo, el atacante sabe que será identificado, pero lo que él no sabe ni nosotros es cuándo será ese día. Por consiguiente, hay que perseverar en el estudio de la mente de los intrusos como un referente académico y científico que siempre es causal de nuevas propuestas, y objetivo de muchas investigaciones.

2.2.1 Técnicas básicas de *hacking*

Luego de revisar con algunos detalles la mente del intruso, retomamos los caminos del hacking, como una excusa académica y conceptual para penetrar los secretos de los amigos de la incertidumbre y de aquellos que experimentan las emociones y los resultados de haber eliminado sus propias autorrestricciones

Podemos visualizar dos modelos de técnicas para ser llamado hacker. Uno conceptual y otro operacional. Los dos son mutuamente complementarios y no excluyentes. En el conceptual detallamos qué se busca alcanzar, y en el operacional el cómo se desarrolla. Estas dos visiones les darán a los analistas más elementos de actuación y revisión, antes de profundizar en los detalles técnicos de los ataques realizados.

"Las técnicas de hacking son la materialización de una mente que va más allá del manual".

El modelo conceptual presenta tres etapas o fases claramente identificadas: reconocimiento, vulneración u ataque y eliminación y salto (Horton, M. y Mugge, C. 2003). Cada una de ellas es parte del sello de la investigación y perseverancia del hacker para lograr su cometido: una nueva distinción para la seguridad de la información (*gráfico 2.1*).

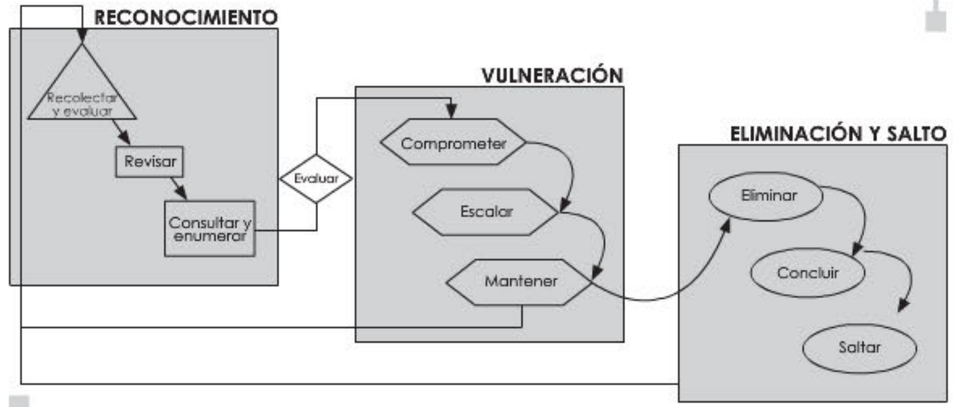


Gráfico 2.1

Modelo conceptual de Hacking. Adaptación de: Horton, M. y Mugge, C. 2003, p. 39.

En la fase de reconocimiento, se ofrece un escenario de análisis que implica recolectar y evaluar información.

En la fase 1, *reconocimiento*, como en el ámbito militar, es un escenario de análisis que implica recolectar y evaluar información, revisar los alcances de la misma y su importancia, para luego consultar y enumerar las posibilidades que se pueden llevar a cabo. Ésta es una primera etapa en la cual el hacker abre las puertas a un mundo de información, por lo general inconsistente y contradictoria, que poco a poco decantará para mirar opciones que hasta el momento no se hubiesen considerado.

Parte del secreto de esta etapa de reconocimiento es la evaluación consciente y detallada de los posibles sucesos que se pueden dar o generar con la información recolectada, con los datos extraídos y con las conclusiones parciales que ha generado. Ubicando estas actividades en contexto, el atacante hace un escenario de riesgos actuales y emergentes a los que está expuesto el objetivo, para, sobre este plano de incertidumbre identificado, poder avanzar en situaciones que desestabilicen el orden de las operaciones y actividades del objetivo.

Es importante tener en cuenta que el reconocimiento efectuado por el posible atacante puede ser activo o pasivo. Pasivo utilizando

información pública o de acceso relativamente fácil que se puede adquirir en la red, o mediante ingeniería social (engaño, manipulación y habilidad conversacional) sobre terceras personas cercanas al objetivo. Esto podría asemejarse a los perfiles de espionaje, pero concebidos como armas tácticas para generar u obtener información particular de la organización objetivo. El activo hace referencia a una incursión discreta sobre el objetivo, como acceso a la información de sus instalaciones, monitoreo de llamadas telefónicas o canales de información y datos, que permitan contar con los antecedentes requeridos para modelar sus escenarios de ataques y vulnerabilidades con mayor precisión.

El reconocimiento puede ser pasivo (mediante información pública o de acceso fácil adquirido en la red, usando ingeniería social: engaño, manipulación y habilidad conversacional); o activo, incursionando sobre el objetivo (acceso a la información, monitoreo de llamadas telefónicas o canales de información y datos).

Los detalles sobre la configuración de la infraestructura de comunicaciones y cómputo, marcas de equipos y sistemas operacionales, sistemas de monitoreo y control, horarios del personal de mantenimiento o soporte, claves de acceso y fallas reportadas para esos equipos o posibles ataques no conocidos son parte de los datos que se analizan, detallan y evalúan antes de producir un plan de ataque a la infraestructura del objetivo.

La fase dos (2) del modelo conceptual es la vulneración o el ataque que implica comprometer el sistema, escalar y avanzar hasta el nivel más alto de privilegios permitido, y mantener el control de sistema atacado, o sencillamente inutilizar y generar pérdida de disponibilidad del sistema bajo hostigamiento. El ataque no se efectúa sin la debida preparación y análisis; es una estrategia planeada que si bien no cobija todas las variables requeridas, sí expone el objetivo a situaciones anormales (o incluso parecer como normales) que pueden pasar inadvertidas por los encargados de la protección del sistema objetivo.

La vulneración o el ataque implica comprometer el sistema, escalar y avanzar hasta el nivel más alto de privilegios permitido, y mantener el control de sistema atacado.

La vulneración o la pérdida de disponibilidad debe ser lo más silenciosa posible, y tener la ventaja de que su identificación y control se puedan dilatar en el tiempo. Es claro que el atacante debe tener sus estrategias de evasión y eliminación de rastros que limiten las investigaciones posteriores.

El ataque es parte del objetivo de la técnica; es el logro evidente y comprobable, pero su objetivo no ha concluido, menos sus intenciones previstas. El ataque materializa el escenario de riesgos diseñado en la etapa de reconocimiento y, al igual que en el contexto militar, el ataque es exitoso en la medida en que podemos mantener el control del sitio atacado; sin esa condición toda la preparación desarrollada no ha cumplido su cometido. El atacante sabe que debe actuar rápidamente para posicionarse en el terreno atacado y así evitar ser descubierto y mimetizarse en medio del campo comprometido.

El ataque materializa el escenario de riesgos diseñado en la etapa de reconocimiento, y es exitoso si se mantiene el control del sitio atacado.

El ataque, como efecto neto sobre el objetivo seleccionado, no debe convertirse en el trofeo del intruso, porque, de ser así, éste será el error que lo llevará a ser identificado y rastreado de manera inmediata. La vanidad del atacante por su logro es muchas veces la forma como es rastreado y evidenciado en las diferentes manifestaciones de opiniones que hay en la red: listas de discusión, blogs, chats, mensajes instantáneos, entre otros. Es importante anotar que mientras más técnico sea el ataque más silencioso será y menos oportunidades para rastrear habrá.

Ya en la fase tres (3), eliminación y salto, el atacante se ha posicionado en el terreno, ha sometido a las fuerzas disidentes (mecanismos de monitoreo y control) y ha implantado las condiciones de su presencia, como situación normal y operacionalmente válida. Por tanto, es tiempo de alterar, mimetizar o desaparecer toda evidencia de una posible intrusión en el sistema, de tal manera que si existiese una investigación posterior, lo que se recabe solamente generará indicios de posibles fallas, pero no evidencia concluyente

En la fase de eliminación y salto, el atacante está posicionado en el terreno, y ha sometido a las fuerzas disidentes (mecanismos de monitoreo y control).

de ataque o de pérdida de control en la máquina. Del cuidado con que se adelante esta fase, dependerá la permanencia invisible del intruso en el sistema.

El atacante sabe que luego de tener la situación controlada a su favor, es hora de mirar qué otros dominios puede alcanzar desde su posición. Ahora en esta condición privilegiada del atacante, es posible conocer detalles de otros objetivos (máquinas, aplicaciones o servicios) que pueden convertirse en nuevos escenarios de ataque, para lo cual retomará lo adelantado en la fase de reconocimiento, pero ya en este momento con mayor información de la infraestructura, de la cual ahora hace parte.

Podríamos comentar que este modelo de hacking desarrolla la mente de un analista de riesgos y vulnerabilidades que se concentra en las posibilidades y actúan conforme a ellas, alejándose del perfil tradicional del analista de riesgos que se concentra en la protección de los activos y los controles requeridos. El primero piensa en la inseguridad de la información como oportunidad para avanzar y conocer, mientras el tradicional reconoce a la inseguridad como el riesgo que se debe evaluar, controlar, mitigar o transferir.

En el modelo operacional de hacking se complementa lo expuesto en la propuesta conceptual previamente revisada. Operacionalmente, para lograr sus propósitos, el hacker adelanta los siguientes pasos (Cole, E. 2002, p. 23):

1. Reconocimiento pasivo
2. Reconocimiento activo –scanning
3. Explotación o vulneración del sistema
    a. Intrusión
        i. Ganar acceso a través de:
            1. Ataques al sistema operacional
            2. Ataque a las aplicaciones
            3. Scripts o programas que materializan ataques
            4. Ataques por fallas en la configuración
        ii. Elevación de privilegios
        iii. Carga o instalación de programas maliciosos
        iv. Descarga de datos
    b. Inutilización del sistema
        v. Negación del servicio

4. Mantener el control o acceso del sistema a través de:
    a. Puertas traseras
    b. Caballos de Troya
    c. Rootkits
5. Eliminación de rastros
    a. Eliminación segura de
        i. Registro o pistas de auditoría

El reconocimiento pasivo está asociado con todas las formas de recabar información del objetivo: visitas a las instalaciones, indagar en los desechos de la organización, charlas con las personas, observación de sus hábitos y comportamientos, acceso a redes sociales, información en motores de búsqueda, entre otros. Mediante este reconocimiento pasivo, el atacante sabe que no tendrá acceso, pero que puede tener múltiples opciones para hacerlo con la información recolectada.

El reconocimiento activo es una fase avanzada de la información recolectada.

El reconocimiento activo es una fase avanzada de la información previamente recolectada. Se trata de probar que la información identificada es útil y se puede utilizar para evidenciar las posibles "puertas de acceso" que pueden ser vulneradas. Técnicamente (Cole, E. 2002, p. 26) estamos hablando de cosas, como:

- ¿Qué máquinas son accesibles?
- Localización de enrutadores y cortafuegos (firewall)
- Tipo de sistema operacional que se ejecuta en computadores clave (Fingerprinting)
- Puertos o servicios abiertos (BannerGrabbing)
- Servicios que se ejecutan (BannerGrabbing)
- Versiones de los servicios de bases de datos o servidores de aplicaciones (BannerGrabbing)
- Configuraciones de máquinas y servicios[3]

Ya la explotación o la vulneración del sistema es la fase crítica para el atacante, y la complicación para el analista o el profesional de seguridad de la información. El acceso, generalmente no autorizado, se materializa utilizando los datos de "puertas de acceso" previamente enumerados. Este acceso se puede dar de manera general por una falla en la configuración del sistema operacional, por un defecto

[3] Elemento adicional sugerido por el autor.

de programación de una aplicación que, al generarse una condición de error, deja las puertas abiertas para el acceso, o por programas (llamados en la literatura como *exploits*) conocidos o desconocidos que realizan la vulneración del sistema objetivo, bien sea por las aplicaciones base (sistema operacional), configuración o problema de implementación que impacta el comportamiento de las aplicaciones (*gráfico 2.2*).

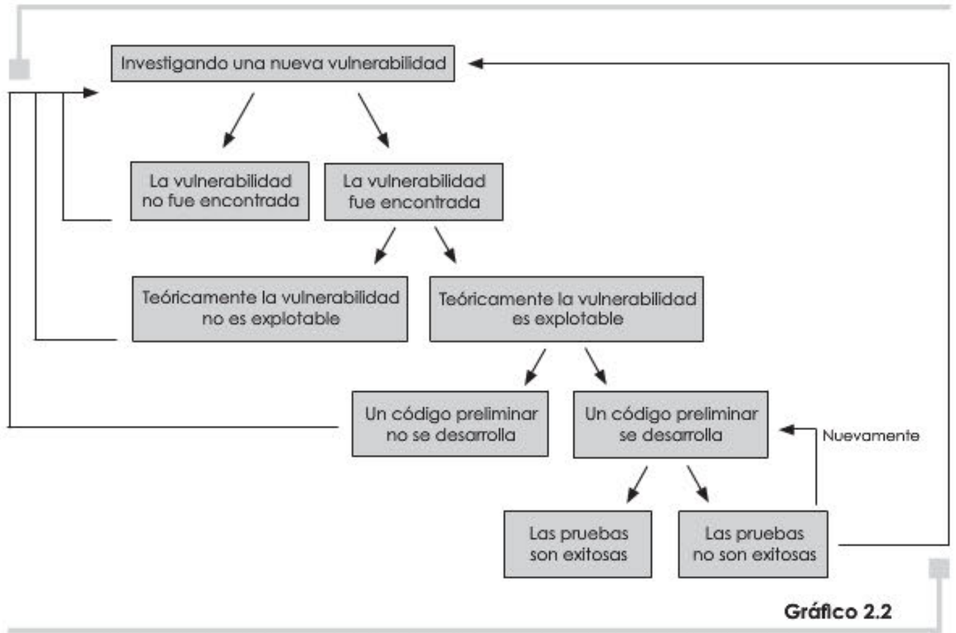


Gráfico 2.2

Encontrando vulnerabilidades. (Adaptado de: Honeynet Project 2004, p. 534).

El objeto de la vulneración en sí misma no es ocasionar la falla; es continuar con lo establecido en el modelo operacional para este aparte: elevar privilegios. Al atacante de nada le sirve generar la falla, si no puede elevar sus privilegios en el sistema, o crear cuentas o cargas de acceso manipulables u ocultables que le permitan estar en el sistema sin ser detectado y, claro está, con los más altos permisos.

Al atacante de nada le sirve generar la falla si no puede elevar sus privilegios en el sistema, o crear cuentas o cargas de acceso manipulables u ocultables.

La negación del servicio es una posibilidad presente para el atacante. Puede ser una alternativa para evitar ser identificado o la forma de participarle al objetivo que él es capaz de eso y mucho más.

La negación del servicio, por sí misma, puede ser la intencionalidad del atacante, pero lograr penetrar el sistema y esconderse sin ser detectado es un logro mayor y, por tanto, la negación del servicio puede ser un preámbulo de cosas con mayor alcance.

La carga de programa malicioso es parte del conjunto de herramientas de sometimiento del sistema atacado.

La carga de programa malicioso es parte del conjunto de herramientas de sometimiento del sistema bajo ataque. Es la instalación de programas que inhiban la generación de rastros, controlen o entreguen información manipulada a los sistemas de monitoreo y mantengan los aspectos de normalidad del sistema. Tanto la carga de programas de esta clase como la descarga de datos son fases operacionales importantes para el atacante, pues son actividades que aseguran la permanencia dentro del sistema y mejorar el conocimiento del mismo.

La descarga de información se debe hacer con cuidados especiales, de tal manera que los puertos que se utilicen no generen mayores alarmas, y se confundan con la información que generalmente se transfiere con las labores administrativas u operacionales del sistema.

Si se han seguido las acciones revisadas anteriormente, contamos con la información y el cuidado necesario para ahora mantener el control de sistema con programas diseñados para tener acceso privilegiado, en sitios o puertos en uso por aplicaciones u operaciones conocidas, que se utilizan por lo general en horarios conocidos o actividades normales, nuevamente para no despertar sospechas. Los caballos de Troya, las puertas traseras, y los rootkits en la actualidad hacen referencia a programas altamente sofisticados que de manera imperceptible (haciéndose parte del núcleo del sistema operacional o de módulos cargables en los mismos) logran altos niveles de invisibilidad y resistencia a sistemas de detección de código malicioso.

Finalmente y consistente con lo planteado en el modelo conceptual, se requiere evadir posibles investigaciones o acciones para identificar, y evidenciar el posible ataque o intrusión. Lograr este

cometido está directamente relacionado con el nivel de experiencia y conocimiento técnico del atacante. Es decir, mientras más especializado sea el atacante en el sistema operacional, aplicación o dispositivo de hardware, menos espacio para rastros habrá para el investigador forense, pues éste sabrá adelantar las acciones requeridas para que lo que se encuentre sea inconsistente, no coincida con lo que ha pasado, o se confunda con una falla normal del sistema objetivo.

Esto último pasó con el tiempo: los atacantes se han volcado a estudiar las maneras de identificar y manipular sus rastros, para hacerse menos susceptibles de investigaciones y seguimientos.

Los atacantes estudian cómo identificar y manipular sus rastros, para hacerse menos susceptibles de investigaciones.

Las técnicas y estrategias utilizadas por los hackers, bien sea de manera conceptual u operacional, nos ilustran que se hace necesario estudiar el escenario del ataque y sus posibles implicaciones para identificar los cómos y los caminos utilizados, para comprender el alcance de los incidentes y, de paso, caracterizar al posible atacante y sus motivaciones, pues si la investigación es lo suficientemente formal, se puede identificar el sello de intruso en la evidencia recabada, así sea inconsistente.

2.2.2 Técnicas avanzadas de hacking

Hablar de técnicas avanzadas de *hacking* es explorar publicaciones como *Phrack* (http://www.phrack.org), insecurity magazine (http://www.insecuremag.com) y los sitios proyecto metasploit (http://www.metasploit.com), CGI Security (http://www.cgisecurity.com), entre otros, como una muestra básica de tantos esfuerzos internacionales por ir en profundidad del conocimiento de la inseguridad, más allá de lo que el manual puede sugerir.

En la revista *Phrack* encontramos artículos relacionados con ataques al kernel de los sistemas operacionales, manipulación de memoria, técnicas antiforenses, ingeniería inversa, sobrepaso de mecanismos de seguridad, generación de código Shell, entre otras tendencias, que con el paso de tiempo se han acumulado y documentado para que todos aquellos curiosos de la inseguridad revisen las propuestas y las implementaciones propuestas en estos documentos.

En la revista *Insecure Magazine* se balancean los artículos técnicos con comentarios y entrevistas. Dentro de los temas analizados en sus ediciones hasta este momento tenemos ataques a PDA's, análisis estructurado de tráfico de red, PHP y SQL Security, administración de logs, administración de derechos digitales, entre otros. A diferencia de *Phrack*, esta revista está orientada a un público menos técnico.

El CGI Security es uno de los sitios más importantes sobre la seguridad en las aplicaciones Web.

El *CGI Security* es uno de los sitios más importantes sobre la seguridad en las aplicaciones Web. Desde el año 2000, cuando inició operaciones (a la luz del proyecto OWASP –*Open Web Application Security Project*), se hace evidente la necesidad de avanzar en el análisis, el descubrimiento y el control de las vulnerabilidades de los desarrollos orientados al Web. Si bien el servicio World Wide Web nace a finales de los años 80, este sitio es de los primeros en ofrecer buenas prácticas para generar aplicaciones más confiables o menos inseguras. Los temas que trata versan sobre Cross-Site Scripting, Browser Security, Phishing, Web Services, Sql Injection, Java Security, Database Security, entre otros.

El proyecto Metasploit es un referente internacional de avances en técnicas antiforenses y de manipulación de memoria y aplicaciones, que ha creado un marco operacional y práctico de códigos.

En este punto sólo comentaremos que el proyecto Metasploit se ha convertido en un referente internacional de avances en técnicas antiforenses y de manipulación de memoria y aplicaciones, que a la fecha ha creado todo un marco operacional y práctico de códigos Shell que otras personas pueden utilizar para crear nuevos productos o propuestas que repiensen la seguridad y el manejo de la memoria. Sobre este sitio, hablamos posteriormente en este libro (*gráfico 2.3*).

Actualmente las técnicas que atacan y manipulan la memoria de las aplicaciones y servicios son el reto y el desafío tanto para los especialistas en seguridad como para los informáticos forenses. Sin embargo, desde 1996, la revista *Phrack* ya registraba adelantos

importantes en esta área. El artículo publicado en el volumen 7, número 49 del 11 de agosto de 1996, artículo 14° de 16 registrados, denominado *Smashing the Stack for Fun and Profit*, detalla con claridad los procesos en memoria y sus estructuras, y cómo a través de ellas se pueden ocasionar desbordamientos de pila. Este artículo es el precursor de los códigos Shell que se implementarían posteriormente.

Para los especialistas en seguridad y los informáticos forenses, las técnicas que atacan y manipulan la memoria de las aplicaciones y servicios son su reto y su desafío.

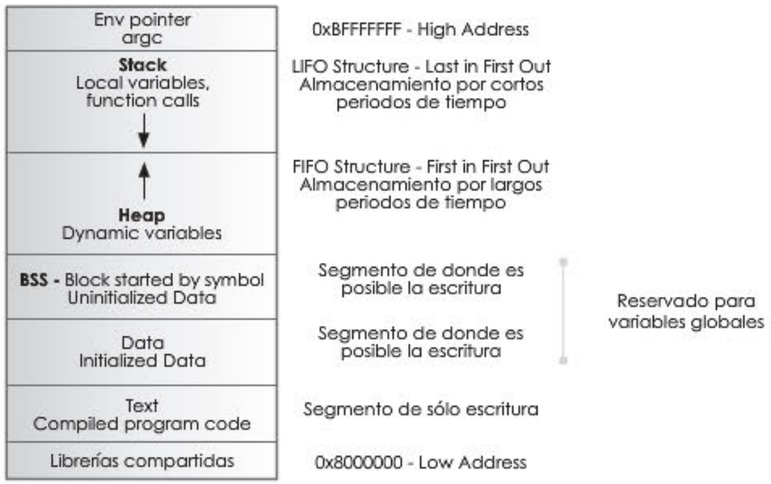


Gráfico 2.3

Estructura de la memoria. Adaptado de: Koziol, J., Aitel, D., Litchfield, D., Anley, C., Eren, S., Mehta, N. y Hassell, R. 2004, p. 6.

Es interesante ver que la técnica que se utilizó para coordinar los ataques del 11 de septiembre de 2001, se haya presentado y analizado en la revista *Phrack*, volumen 8, número 52 de enero 26 de 1998, artículo número 08 de 20 registrados bajo el nombre de *Steganography Thumbprinting*. En este documento se presenta el análisis de algunas herramientas más populares hasta ese momento en Internet, para materializar la esteganografía (S-tools y steganos), así como sus posibles estrategias de detección. Se destacan los elementos técnicos sugeridos sobre imágenes BMP y GIF, para esconder la información en ellos.

Otro de los artículos que se ha seleccionado de la revista *Phrack* es el documento original de Fyodor, creador del NMAP, publicado en el volumen 8, número 54 de diciembre 25 de 1998, artículo 09 de 12 registrados, denominado *Remote OS detection via TCP/IP Stack FingerPrinting*. En este documento se detalla una técnica de hacking que busca el reconocimiento y la enumeración de las máquinas que son susceptibles de atacar. En este manuscrito, el autor expone un discurso metodológico de huellas de las máquinas basado en el comportamiento de protocolos, como TCP, ICMP, entre otros, que permite establecer qué tipo de sistema operacional se ejecuta en la máquina objetivo. A la fecha, el NMAP es una de las herramientas básicas dentro de cualquier *toolkit* de un curioso de Internet.

Las técnicas antiforenses, o todos aquellos esfuerzos para desviar la atención de una investigación, se hacen presentes en las estrategias de los atacantes. La revista *Phrack* es una de las publicaciones que presenta los primeros avances en estas técnicas. En el artículo publicado en el volumen 11, número 59 de julio 28 de 2002, artículo 06 de 12 registrados, denominado *Defeating Forensic Analysis on Unix*, el investigador presenta las limitaciones de las herramientas forenses hasta el momento más difundidas, y cómo se puede evitar el rastreo de las acciones de los intrusos en el sistema. En este sentido, presenta dos herramientas (NecroFile y KlismaFile), las cuales materializan las propuestas del autor en el documento.

Las técnicas antiforenses, o todos aquellos esfuerzos para desviar la atención de una investigación, se presentan en las estrategias de los atacantes. La revista *Phrack* refiere los primeros avances en estas técnicas.

En su último número, la revista *Phrack* establece un nuevo movimiento y una tendencia en técnicas de hacking avanzadas. En el artículo publicado en el volumen 12, número 64 de mayo de 2007, artículo 12 de 17 registrados, denominado *Hacking Deeper in the System*, el autor presenta ideas y desarrollos conceptuales sobre lo que llama *hacking hardware*. El documento presenta detalles del acceso directo a memoria, los procesos de entrada/salida, ubicación del BIOS, microcódigo que se ejecuta en la Unidad Central de Proceso (cuyas siglas en inglés son CPU), los cuales utiliza para indicar posibilidades de acceso que hasta el momento no han sido intentados. El autor sugiere

bien que el documento plantea las ideas, y sugiere algunos programas que materializan sus hipótesis pero no implementan completamente el hacking del hardware.

De otra parte, como otro elemento, no menos interesante e importante que los anteriores, tenemos los *rootkits*, como aquellos conjuntos de programas que alteran y modifican otros existentes dentro del sistema operacional donde se instalan. Estos programas violan la integridad y la confiabilidad del sistema, insertando puertas traseras o cargando módulos ejecutables en memoria, que generan brechas de seguridad en el mismo. En el artículo publicado en el volumen 9, número 55 de septiembre de 1999, artículo 5 de 19 registrados, denominado *A *REAL* NT Rootkit, Patching the NT Kernel,* el autor detalla esa técnica para los sistemas Windows, mostrando con claridad la forma como puede ser comprometido ese sistema.

Los rootkits violan la integridad y la confiabilidad del sistema, insertando puertas traseras o cargando módulos ejecutables en memoria.

Revisando uno de los artículos registrados en el sitio CGI Security, nos encontramos con uno titulado *Anatomy of the Web Application Worm*, lo que podría traducirse como "La anatomía de una aplicación Web tipo gusano". Este artículo, publicado por primera vez en el año 2002, establece un referente de los posteriores gusanos que surgieron en el Web y que a la fecha continúan evolucionando ahora en reciente plataforma de desarrollo, como AJAX (*Asynchronous JavaScript and XML –JavaScript Asincrónico y XML*). Básicamente, una aplicación Web que se comporte como gusano debe, de acuerdo con el autor del artículo, tener las funcionalidades básicas siguientes (http://www.cgisecurity.com/articles/worms.shtml):

- Identificar servidores Web en las IP objetivo. Se debe verificar que el puerto 80 está activo.
- Identificar y escudriñar las diferentes formas y variables disponibles en el sitio Web, buscando aplicaciones y programas que se encuentren activos.

- Ejecutar una lista de ataques (entre los cuales se cuentan *Sql Injection,* problemas de manejo de cadenas, desbordamiento de *buffer*) contra cada una de las aplicaciones y variables identificadas.
- Se tiene éxito al regresar nuevamente a uno (1).

Los atacantes saben que trabajando en conjunto y de manera coordinada pueden generar mayores impactos.

En la actualidad los atacantes saben que trabajando en conjunto y de manera coordinada pueden generar mayores impactos en las infraestructuras. Esto, combinado con la falta de conciencia de seguridad informática de los usuarios finales, genera un caldo de cultivo lo suficientemente atractivo para proponer una nueva forma de ataques que involucre a más gente y haga menos visible al atacante. Esta técnica, denominada *Botnets*, la cual consiste en redes subordinadas y controladas por terceros para someter computadores remotos de usuarios caseros, con el fin de generar spam, ataques de denegación de servicio, lanzamiento de virus, entre otras amenazas, es la nueva tendencia de riesgos a los cuales está expuesto el usuario común de Internet.

Sin saberlo, por una falta de cuidado mínimo en sus controles de seguridad en su hogar, puede ser cómplice de un ataque masivo donde su máquina esté involucrada. Si bien no será un cómplice directo, pues no sabe de la existencia de un posible programa que se encuentre infiltrado en su máquina, sí es parte del conjunto de personas investigadas y deberá responder por su falta de previsibilidad y debido cuidado con su máquina.

En Internet los archivos ya no se descargan con el protocolo FTP, sino con software para crear redes P2P –Peer to Peer– que hacen menos perceptibles los intercambios de información y las posibles infecciones de las máquinas.

Cada vez más en Internet las personas comparten archivos de todo tipo de extensiones, los cuales ya no se descargan utilizando el bien conocido protocolo FTP –*File Transfer Protocol*, sino utilizando software para crear redes P2P –*Peer to Peer*–, las cuales vienen creciendo y masificándose, lo que hace menos perceptible los intercambios de información y las posibles infecciones de las máquinas.

El avance de las técnicas de hacking es directamente proporcional a la imaginación de los curiosos de Internet, e inversamente proporcional a la atención que los analistas de seguridad hacen de éstas, y a la concienciación de sus usuarios finales. En este sentido, no es raro que nuevas técnicas avanzadas de *hacking* basadas en combinaciones de estrategias conocidas se materialicen pronto. Por ejemplo, cruzar dos especies como los *keylogger* y los *spyware* para darle vida a una nueva generación de amenazas que denominaríamos *Spylogger*, una raza que viaje a través de Internet como Javascript o Applet de Java, que se descarga a través del navegador y se instala en la máquina, teniendo la capacidad de monitorear todas las conexiones entrantes o salientes, así como el acceso al disco del usuario objetivo.

Como hemos podido ver en este aparte, las técnicas avanzadas de hacking exigen del hacker un conocimiento más técnico y mayor capacidad de evasión de rastros, con el fin de que su ataque sea efectivo: acceso concedido y mínima cantidad de evidencia de este acceso. Por tanto, en la sección siguiente se presentan algunos elementos básicos de identificación de rastros ante posibles riesgos de seguridad, materializados en las máquinas.

Las técnicas de hacking le exigen al hacker tener un conocimiento más técnico, y mayor capacidad de evasión de rastros.

2.3 IDENTIFICACIÓN DE RASTROS DE LOS ATAQUES

Si la inseguridad informática es la constante en un mundo interconectado, la atención de incidentes debería ser la norma. En este sentido, no solamente es necesario estar preparados para aquellos eventos inesperados que se presenten en una infraestructura de cómputo o comunicaciones, sino comprender en profundidad el alcance de los ataques que se presenten.

En este contexto, se requiere desarrollar estrategias para contar con las evidencias de que algo ocurrió, el rastro del posible ataque que permita entender el comportamiento del intruso y sus movimientos dentro del sistema. En este orden de ideas, no insistiremos en las técnicas naturales de auditoría que se han generalizado en muchos sistemas de información, sino en el desarrollo de estrategias que busquen la trazabilidad de las acciones de los usuarios en el sistema y la autoprotección del sistema de registros de eventos del sistema mismo.

Para rastrear, reconstruir o establecer relaciones entre los objetos monitoreados de un sistema se requieren sincronización, control, integridad de archivos y confiabilidad en la generación de los registros de eventos.

La sincronización, el control, la integridad de archivos y la confiabilidad en la generación de los registros de eventos son elementos requeridos para darle vida a la trazabilidad o a la capacidad para rastrear, reconstruir o establecer relaciones entre los objetos monitoreados de un sistema. En la trazabilidad se hace referencia a un concepto sistémico, asociado con la necesidad de establecer relaciones y observar el todo del sistema atacado, y a uno sistemático, en la manera como se alcanza y se materializa el concepto en las aplicaciones corporativas, mediante el análisis de registros y trazas dejadas por el intruso (*gráfico 2.4*).

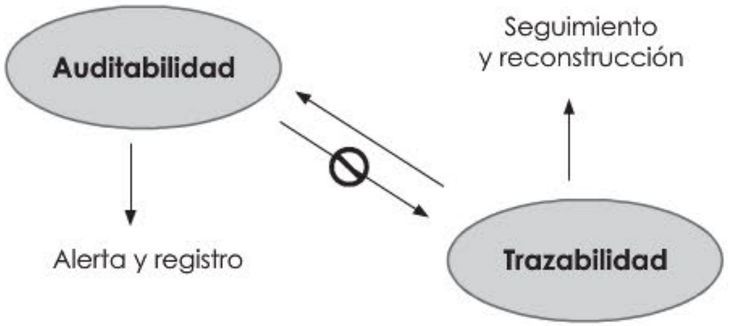


Gráfico 2.4
Auditabilidad versus trazabilidad

Para adelantar el análisis de rastros, conscientes de que lo que queremos es alcanzar la trazabilidad de las acciones del intruso, es necesario tener prevista una serie de elementos de registro que van desde el sistema operacional hasta las políticas de seguridad, pasando por el sistema de archivos, los servicios de bases de datos, el tráfico de red, las aplicaciones y la memoria volátil.

En cada uno de ellos se pueden encontrar rastros de los eventos, dado que cualquier evento que se presente en una aplicación tendrá

efectos sobre la memoria, las bases de datos o los sistemas de archivos donde ubica, lee o elimina información para su ejecución. Es claro que puede haber aplicaciones que ante fallas en su ejecución dejan abierta la posibilidad de acceso con control total, por una inadecuada configuración de su ejecución, pero precisamente esta falla debe afectar las relaciones que tenga con los componentes de bases de datos –BD–, sockets de conexión y disponibilidad del servicio que serán alertas, que estarán a la vista de los administradores y usuarios de la mencionada aplicación (*gráfico 2.5*).

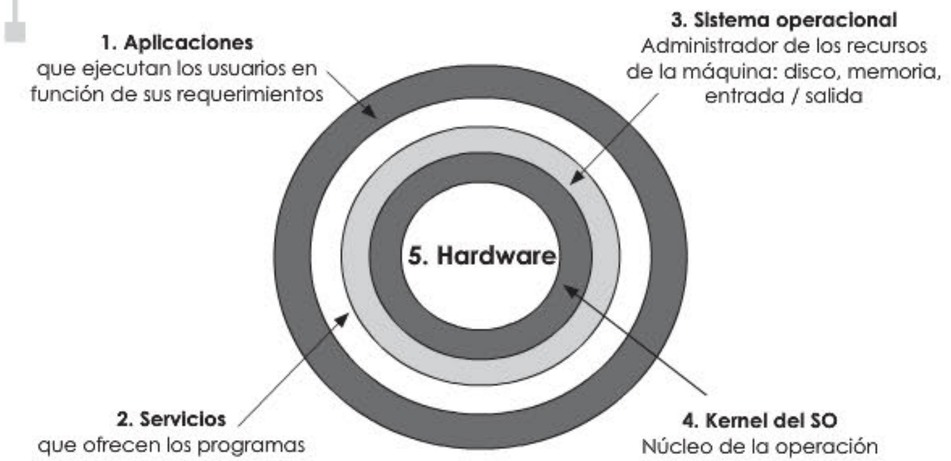


Gráfico 2.5

Análisis concéntrico de rastros

Al configurar el sistema operacional, es decir el software base con el cual funcionará la máquina, se requiere evidenciar y confirmar qué tipo de aseguramiento o de afinamiento es necesario para establecer un ambiente confiable de ejecución, que implica un monitoreo y un registro de acciones básicas que permitan observar el correcto funcionamiento de la máquinas y las aplicaciones allí residentes. Nada ganamos con tener aplicaciones fuertes y exigentes en validaciones de control, si el sistema operacional que las contiene no

Al configurar el software base, se requiere evidenciar y confirmar qué aseguramiento o afinamiento es necesario para establecer un ambiente confiable de ejecución.

cuenta con las características requeridas para una operación confiable. ¿Qué es un sistema operacional confiable? es la pregunta que surge. La respuesta a este interrogante está asociada con las necesidades y configuraciones base establecidas por la organización, para sus sistemas de misión crítica.

Es cierto que en Internet existe un sinnúmero de guías de aseguramiento de sistemas operaciones que exigen controles y medidas, que podrían limitar la materialización de ataques conocidos, pero también podrían impedir que las aplicaciones corporativas se ejecuten correctamente. En este sentido, la respuesta a la pregunta anterior cobra más sentido, pues se hace necesario establecer un balance entre la operación y la seguridad de la misma. La inseguridad de la información es el resultado de una decisión que sabe a qué se expone, cuando decide sobre la configuración de una característica de un componente del sistema.

Ahora bien, el sistema operacional y el sistema de archivos, esta última una estructura lógica que ordena y detalla los archivos, se encuentran residentes en la máquina. El sistema de archivos es manejado por funciones internas del sistema operacional, las cuales interactúan todo el tiempo con los procesos y memoria de la máquina para establecer la mejor forma de tener acceso a ellos y salvaguardarlos ante situaciones de falla de potencia eléctrica, o inconsistencias en manejo de los mismos por parte de aplicaciones. El sistema de archivos es un componente sensible, que al ser lógico y articulado por el kernel del sistema operacional, es susceptible a fallas y a ataques especializados por parte de los atacantes.

Los rastros de ataques directos al corazón del sistema operacional, y a sus estructuras, son imperceptibles o no visibles.

Los ataques directos al corazón del sistema operacional y a sus estructuras lógicas asociadas, como el sistema de archivos y controladores de componentes de hardware, son ataques cuyos rastros no son visibles o mejor aún imperceptibles, porque generalmente se encuentran en memoria o en archivos temporales que son volátiles. En este sentido, consecuente con lo planteado en las técnicas avanzadas de *hacking*, mientras más se acerquen los intrusos a las funciones internas del sistema operacional, mayores

problemas de rastreo tendremos para conocer y detallar sus acciones (*gráfico 2.6*).

Gráfico 2.6

¿Dónde ubicar los rastros?

Las aplicaciones y sus rastros dependen del diseño de las mismas. Generalmente las consideraciones sobre permisos de acceso a objetos y las medidas de seguridad en el desarrollo no son consideradas, lo cual aumenta la posibilidad de un ataque fundado en una inadecuada asignación de permisos para la aplicación que puede comprometer los datos de la compañía. Las aplicaciones deben responder a un modelo de seguridad y programación que defina y formalice las relaciones entre sus componentes, y así evidenciar los cambios y las acciones que se hacen del llamado de una función a un elemento del sistema. Esto exige disciplina de programación y validación de interfaces entre programas, antes de permitir la comunicación entre ellos.

En las bases de datos los rastros están asociados con los diseños previos que se hayan efectuado en el sistema manejador de bases de datos. Es decir, se debe haber configurado un sistema de alertas sobre los objetos críticos que afecten su funcionamiento y el de las aplicaciones que hacen uso de ella. Generalmente esta estrategia está fundada en disparadores cuando se alteran datos u objetos sensibles de la aplicación: tabla de usuarios, tabla de salarios, paquetes de programa, archivos de log, entre otros.

En las bases de datos los rastros se asocian con la configuración de un sistema de alertas sobre sus objetivos críticos.

Sin embargo, es frecuente encontrar que en las bases de datos no se cuente con mecanismos de monitoreo para los usuarios privilegiados de las mismas, como son los Database Administrators –Administradores de Bases de Datos. Estos profesionales, cuya responsabilidad es mantener la continuidad y la seguridad de los datos de la organización, generalmente no son monitoreados, lo que puede generar un escenario de falla, donde se utilice la carga de estos profesionales y materializar un evento, cuyas consecuencias pueden ser desafortunadas.

Por lo general, los sistemas manejadores de bases de datos cuentan con una estructura interna de monitoreo y control que vigila y registra todas las acciones del sistema sobre sus objetos, la cual es fuente de información tanto para los desarrolladores como para el proveedor del producto. Esta estructura es generalmente un tabla interna de acceso por parte de la cuenta superusuario de la base de datos, que no puede ser eliminada o alterada, pues de hacerse estaría comprometiendo la integridad del sistema. De igual forma, sus sistemas de bitácoras, que a pesar de no estar protegidos los archivos que se generan en el sistema operacional, se mantiene un mínimo de control de integridad que se valida antes de usarse para una recuperación de datos.

Hasta este momento hemos validado que existen elementos que se pueden revisar, para identificar rastros ante ataques en una máquina. Es importante anotar que estos elementos, previamente presentados, se deben extrapolar a un escenario de red, donde la variable comunicaciones establece un reto más a los análisis desarrollados. El tráfico de red es volátil y cambiante; a menos de que exista un monitoreo del mismo, es poco factible identificar y recoger las comunicaciones que estén o haya tenido una máquina en su entorno de red.

Un nivel más de análisis podríamos evidenciarlo en las políticas de seguridad y la administración de seguridad de la organización. Este componente, más de corte administrativo, se deja de lado cuando de recoger rastros se trata. En este componente se evidencian realmente las prácticas de la corporación en los temas de seguridad, y éstas funcionan adecuadamente, debe haber actividades y acciones que se materialicen en la infraestructura. Sin una exigente administración de la inseguridad de la información, es decir una constante valoración de la exposición de los riesgos en los sistemas de misión crítica, no podrá

haber una posición vigilante de los incidentes que sobre ella ocurra. La posición será reactiva y no proactiva.

La administración de la seguridad de la información, utilizando las buenas prácticas conocidas, no asegura la no ocurrencia de eventos inesperados o adversos, solamente nos indica las cosas mínimas que debemos hacer y, por lo tanto, son deberes que debemos comprender y repensar para tratar de estar pensando en las posibles fallas y las acciones que se deben tomar para minimizar los impactos. Por tanto, el diseño de registros de eventos y evaluaciones en los diferentes componentes revisados: sistema operacional, sistema de archivos, sistemas manejadores de bases de datos, aplicaciones y sistema de gestión de seguridad, son parte inherente del debido cuidado que hay que tener para enfrentar situaciones no previstas.

La administración de la seguridad de la información no asegura que ocurran eventos inesperados o adversos.

Condensando lo revisado en este aparte, detallamos un cuadro resumen de rastros en los diferentes componentes analizados, resaltando algunos tipos de rastros y registros que pueden ser útiles para revisar cuando se está ante un incidente de seguridad del sistema (*cuadro 2.2*).

	Administración de la seguridad informática	Aplicaciones corporativas	Bases de datos	Sistema operacional
Tecnologías	• Software de monitoreo, control y correlación de logs	• Pruebas de intrusión específicas	• Software de monitoreo y control de acceso	• Software de monitoreo y control de acceso Análisis de vulnerabilidades
Procedimientos	• Informes de auditoría internos y externo	• Aseguramiento de la calidad del software: inspección de código fuente	• Configuración de registros de auditoría y control de acceso	• Aseguramiento del software base, según buenas prácticas de seguridad y control
Personas	• Sesiones de entrenamiento y capacitación	• Aseguramiento de la calidad del software: buenas prácticas de programación	• Definición de permisos, privilegios y perfiles	• Definición de usuarios y permisos

Cuadro 2.2

Resumen general de rastros en sistemas informáticos

Resumen

Hablar del intruso en seguridad informática es hablar de aquellas personas que luchan contra sus habilidades y creaciones. Hablar de los intrusos es reconocer que estamos ante una dualidad de pensamiento que nos invita a "abrir nuestra mente" para ver más allá de lo que nos dice el manual. El intruso, si bien es una persona o grupo que puede ser encuadrado en algún tipo de clasificación, como la sugerida en este capítulo, es un referente de estudio de los analistas de seguridad de la información para repensar sus estrategias de lucha contra la inseguridad.

En este sentido, revisar las técnicas y habilidades de los intrusos es mirar hacia nuestra infraestructura de cómputo y comunicaciones para revisar si hemos visto lo que "ellos" han visto, o mejor, si tenemos la disciplina de cuestionar lo que dice el proveedor para ver el "efecto de borde" que es posible, modificando el contexto de ejecución de la aplicación, el servicio o el protocolo. Las técnicas de los atacantes son el resultado de un estudio dedicado y paciente de las especificaciones (algunas documentadas y otras no) de las funciones del hardware de la máquina, de los sistemas operacionales, de las bases de datos, de las aplicaciones. Así mismo, de la falta de concienciación de los usuarios y los directivos de la organización, entendiendo por esto no mantener un ciclo conformado por las fases de informar, capacitar, entrenar y formar en temas de seguridad de la información. Es decir, entender el "qué" de la seguridad de la información (informar), el "cómo" materializo esos qués (entrenamiento requerido), y finalmente la formación del individuo y sus competencias para un correcto ejercicio de la aplicación de los conceptos de seguridad de la información.

Los ataques o los incidentes de seguridad no se pueden eliminar; hacerlo supondría acabar con la imaginación de los atacantes y la de los analistas de seguridad informática para contenerlos. Por lo tanto, cada persona o cada organización deberá mantener las medidas de seguridad mínimas y acordes con su negocio u operación, para proteger sus activos y estar preparada para enfrentar y seguir a los intrusos en sus sistemas. Esto supone que sabemos dónde están los rastros, que conocemos la integridad de los mismos y la manera de reconstruir sus acciones. Si no es posible saber dónde ubicar los rastros, la ventaja estará en el "lado oscuro" y las probabilidades de verificar la identidad o el modus operandi serán limitadas.

Pensar y analizar la mente del intruso es una forma de ver cómo correr la línea de las posibilidades de ataques, de observar las limitaciones (aún no descubiertas, como las vulnerabilidades de "día cero") de las aplicaciones, de ver al usuario como el eslabón más débil de la cadena, de desafiar a los investigadores forenses para que ubiquen sus rastros; en pocas palabras, de sumergirse en una nueva librería de opciones que espera ser descubierta para hacer avanzar las estrategias y técnicas de seguridad informática, o para advertirles a las organizaciones que todavía es necesario seguir aprendiendo a "desaprender".

Preguntas y ejercicios

Esta sección busca reforzar los elementos conceptuales presentados en este capítulo. Para esto le sugerimos al lector revisar sus reflexiones y anotaciones, para plantear respuestas a los interrogantes propuestos en esta sección.

1. ¿Una persona con una mente de intruso o atacante es un peligro potencial para una organización? En su reflexión, considere las ventajas y limitaciones de la misma.
2. ¿Un hacker y un ciberterrorista qué podrían tener en común? No olvide revisar las motivaciones de ambos personajes.
3. ¿Un atacante interno genera más riesgo que un atacante externo? Haga un cuadro comparativo de motivaciones.
4. ¿Un atacante o intruso se podría comparar con un especialista de combate militar? Para su respuesta, revise las técnicas básicas de hacking.
5. ¿Mientras más técnicas y sofisticadas son los métodos de ataque, menor la capacidad de rastreo que tienen los investigadores forenses? Explique su respuesta.
6. Si fuese a rastrear un incidente de seguridad informática relacionado con botnets, ¿dónde ubicaría la evidencia del mismo?
7. ¿Existe alguna diferencia entre auditabilidad y trazabilidad?
8. ¿Es posible que usted pueda pensar como un intruso para su organización? Piense en cómo podría afectar un proceso, procedimiento, o elemento de soporte tecnológico; escriba los resultados y valide la información?

Apéndice

Para profundizar

Práctica de asalto a una sesión TCP

Fonseca, Guillermo. Gonzales, María Camila y Neira, Bernardo Andrés

En este documento se presenta un caso práctico de asalto a una sesión TCP.

Para entender la estructura de un asalto a una sesión TCP, se deben tener presentes algunos conceptos básicos que se explican en la sección 1. Luego se encuentra la descripción del ataque paso a paso para dar introducción a la práctica realizada con la herramienta Hunt. Más adelante, en la sección 7, se muestran los rastros que deja el ataque, ya que la investigación forense es importante en reconocer las huellas que dejan los atacantes tras cada intrusión. Para finalizar se explica una manera de corregir el ataque y se presentan las conclusiones de la práctica realizada.

1. CONCEPTOS BÁSICOS

A. Sesión TCP

El objetivo de una sesión TCP es coordinar múltiples conexiones TCP concurrentes entre un par de hosts. Una aplicación típica de una sesión TCP es la coordinación entre conexiones TCP concurrentes entre un servidor Web y un cliente, en donde las conexiones corresponden a componentes de una página Web (Padmanabhan, Venkata N. s.f.).

Una sesión TCP se identifica por una tupla con los datos importantes del cliente y del servidor (Stevens, W Richard; KLM s.f.):

Tupla: {Ip-Cliente, Ip-Servidor, Puerto-Cliente, Puerto-Servidor}

La finalidad de este documento es mostrar un ataque a una sesión como la previamente descrita.

Es necesario primero analizar el paquete TCP (*ver gráfico A2.1*).

El paquete contiene el puerto origen y el puerto destino. También contiene un número de secuencia de 32 bits que identifica el flujo de cada octeto de datos. Este número va de 0 a 232 – 1. Cuando se establece una sesión entre dos hosts, éstos intercambian números de secuencia. Para efectos del asalto de una sesión TCP, se explica la importancia de estos números de secuencia y la selección del número de secuencia inicial.

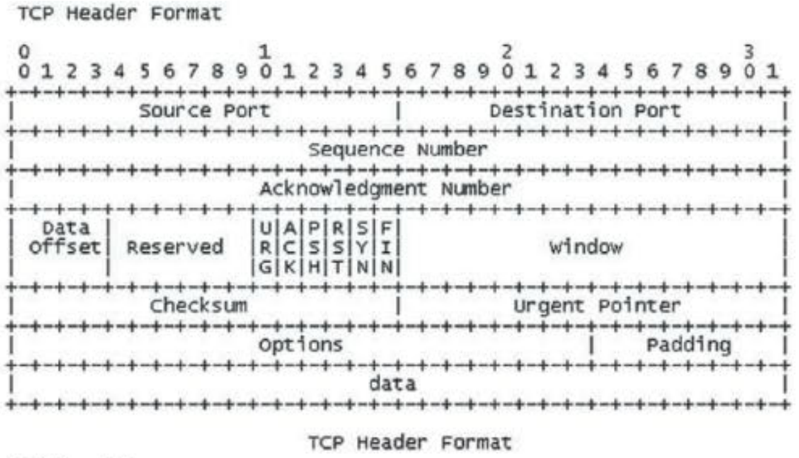


Gráfico A2.1

Paquete TCP

Sobre los demás campos del paquete cabe resaltar las banderas que son 6 bits de control que se utilizan de izquierda a derecha para indicar: URG (el paquete es urgente), ACK (confirmación de recibido el anterior paquete), PSH (el paquete contiene datos), RST (para resetear una la conexión), SYN (para sincronizar números de secuencia) y FIN (no vienen más datos del emisor) (3 RFC 793).

Una sesión TCP empieza por una sincronización entre el cliente y el servidor. Esta sincronización se conoce como el *three way handshake* que se hace para que las dos máquinas, entre las que se va a hacer la conexión, sepan la especificación de la otra y su configuración para manejar sesiones TCP. Suponiendo que se establece una conexión TCP entre la máquina A y la máquina B, la sincronización se muestra a continuación (3 RFC 793):

1. A→B SYN mi número de secuencia es X
   A←B ACK su número de secuencia es X
2. A←B SYN mi número de secuencia es Y
3. A→B ACK su número de secuencia es Y

B. IP Spoofing

El IP Spoofing consiste en suplantar la dirección IP o identidad de una máquina; esto con el fin de beneficiarse de la "confianza" que un host le tenga a otro. Para llevar a cabo este ataque es suficiente con modificar, en el paquete TCP, el campo con la dirección IP origen de la máquina suplantada. Existen dos modalidades de spoofing. La primera se conoce como Non-Blind Spoofing en la cual el atacante se encuentra en la misma subred de la víctima, por lo

que puede tener visibilidad del tráfico de la misma. La segunda modalidad se conoce como Blind Spoofing, la cual ocurre desde afuera de la subred en donde los números de secuencia y de confirmación están fuera del alcance del atacante (Tanase, Mathew; KLM).

Con la utilización de esta técnica se puede asegurar que los paquetes enviados por el atacante no serán rechazados por la máquina destino.

C. SYN Flood

Como se explicó en el numeral A2.1 de esta sección, el protocolo TCP se inicia con una conexión en tres tiempos, si el paso final no se completa, la sesión iniciada queda en un estado incompleto y puede llevar a una denegación de servicio llamada SYN flood. Un cliente que no conteste al segundo ACK del *three way handshake*, logra mantener al servidor (otro lado de la comunicación) en estado de escucha por un tiempo determinado; por esta razón, si se hace una inundación de estas conexiones a "medio terminar", es posible lograr la interrupción del servicio brindado por el servidor o al menos volverlo más lento para responder a otras peticiones (Inundación paquetes SYN). Este ataque, el SYN flood, es utilizado para suspender un servicio en una máquina, para consumir los recursos de un servidor, o para abrir paso a un nuevo ataque, usualmente el bombardeo de SYN se hace conjunto con el IP Spoofing de la máquina atacante para evitar rastreos posteriores.

D. Escaneo de puertos

El escaneo de puertos es una de las técnicas de reconocimiento más populares usadas para encontrar servicios activados que pueden traducirse como huecos de vulnerabilidad existentes (Port Scanning). Básicamente, un escaneo de puertos consiste en el envío de una trama o de un mensaje a la vez, a cada uno de los puertos de una máquina, es el tipo de respuesta a cada uno de estos mensajes lo que da una idea al atacante del estado del puerto; por ejemplo, si una máquina a la que se le ha hecho un escaneo de puertos devuelve un SYN/ACK significa que tanto la máquina como el puerto del servicio están arriba; si devuelve un RST/ACK, la máquina está arriba pero el servicio se encuentra o no disponible o inexistente; si el retorno es un mensaje ICMP de Host unreachable significa que la máquina está abajo, y si este mismo mensaje va acompañado de un admin. Prohibited filter, significa que la máquina está detrás de un firewall con lista de accesos.

E. Envenenamiento de ARP

El protocolo ARP (Address Resolution Protocol) se encarga de asociar las direcciones IP de las máquinas con sus respectivas direcciones físicas (MAC) en una tabla dinámica. El proceso de asociación se realiza de la siguiente manera: Cuando un paquete es enviado a alguna máquina, el módulo ARP busca en su tabla dinámica si la dirección IP de la máquina destino existe. Si

la encuentra registrada ubica la correspondiente MAC y sigue el proceso de envío del paquete. Si no la encuentra en su tabla ARP envía un paquete ARP Request que es un paquete broadcast, preguntando quién tiene la MAC de la dirección IP que está buscando. Luego se recibe un paquete ARP Reply, el cual es unicast, confirmando la MAC de la dirección IP solicitada. Una vez recibido el mensaje de respuesta, se almacena en la tabla ARP la nueva información.

El ataque de envenenamiento de ARP se basa en la debilidad de algunos sistemas operativos, como Linux y Windows, que no manejan estados en el protocolo ARP por lo cual aceptan mensajes ARP Reply, sin importar si han enviado antes un mensaje ARP Request. Un atacante aprovecha esta debilidad para modificar a su gusto la tabla ARP de su víctima.

F. Sniffer

Un sniffer es un programa que es utilizado para monitorear y analizar el tráfico en una red, dando la posibilidad de observar los paquetes que fluyen de un lado a otro. En un segmento de red sin un switch o enrutador de paquetes, todo el tráfico destinado a una máquina es enviado a todos los integrantes del segmento, pero puesto que las direcciones IP no coinciden con las del paquete transmitido, éstas simplemente los rechazan.

El sniffer coloca la tarjeta de red del computador en modo promiscuo, esto es aceptando absolutamente todos los paquetes que transitan por el segmento de red para poder observarlos (e incluso seguir toda una trama) (ethereal) y utilizar la información en ellos. Un atacante usa esta herramienta para observar el tráfico en la red que desea atacar, recopilando la información necesaria para cumplir sus objetivos, como dirección de la IP de la víctima, números de secuencia de los paquetes y protocolos utilizados (Telnet, FTP, entre otros).

2. ESTRUCTURA DE UN ASALTO A UNA SESIÓN TCP

El asalto de una sesión TCP es tomar control de una sesión existente y enviar los paquetes propios en una trama, de tal forma que los comandos y órdenes transmitidos sean procesados como si se fuera el auténtico usuario de la sesión.

Como cualquier ataque realizado por un hacker, el asalto a una sesión TCP inicia por la búsqueda de una víctima. Independientemente de la motivación, al elegir la víctima se averigua su IP y, en el caso del asalto a una sesión, también se conocen la IP del servidor y el puerto por el que se establece la conexión con éste. Conociendo tres de los cuatro datos que identifican una sesión, la tupla {IP-cliente, IP-servidor, Puerto-cliente, Puerto-Servidor} mencionada antes, se procede a averiguar el puerto del cliente.

De la misma forma como se menciona en la sección II, la sesión TCP entre dos hosts consta de la tupla que la identifica y de los números de

secuencia que certifican la identidad de cada una de las máquinas. Posterior al establecimiento de la conexión, no se comprueba la identidad de un host, por lo cual se puede llevar a cabo el ataque. Para esta clase de ataques hay dos tipos de mecanismos. El primero, si el atacante no se encuentra en el mismo segmento de red del cliente, debe hacer un escaneo de puertos, y de esa forma averiguar el puerto abierto por el cual recibe los paquetes del servidor.

Luego es necesario investigar el número de secuencia del servidor. Para esto se puede enviar un paquete SYN al servidor y anotar el número de secuencia que se recibe en el paquete de respuesta al establecimiento de la conexión (SYN, ACK). Al hacer lo anterior, varias veces se puede analizar el número de secuencia que sigue. Cabe aclarar que es necesario hacerlo por medio de software porque debe ser un proceso rápido, ya que el servidor puede recibir otros paquetes SYN. Para evitar un SYN flood es necesario finalizar la conexión, enviando un paquete RST al servidor luego de tener el número de secuencia.

En el momento de realizar el asalto a la sesión, se debe asegurar que el cliente y el servidor no estén comunicados. Para esto se pueden enviar varios paquetes SYN al cliente, ocasionando un SYN flood y dejándolo temporalmente fuera de servicio. Con esta técnica se procede a enviar un paquete de sincronización (SYN) modificado con IP Spoofing con la dirección IP del cliente como la dirección origen. Si el atacante se encuentra fuera del segmento de red del cliente, no podrá ver el paquete de respuesta SYN/ACK, pero ya se aseguró de que el cliente no va a responder, y además ya sabe el número de secuencia con el que debe responder el último ACK, y con eso ya se ha suplantado al cliente (Whitaker, A. y Newman, D.; Stevens, W Richard). En el segundo, la utilización de un sniffer, en caso de que el atacante se encuentre en el mismo segmento de red que las máquinas a las que se planea hacer el asalto de sesión.

Para lograr asaltar una sesión TCP se deben conocer:

- ❒ IP del cliente
- ❒ IP del servidor
- ❒ Puerto del cliente
- ❒ Puerto del servidor
- ❒ Números de secuencia del cliente y del servidor

Una vez se tiene toda la información anterior, el atacante se prepara para ejecutar el asalto de sesión, de la siguiente manera:

Primero se espera hasta que se establezca una conexión TCP; para nuestro caso de estudio se utilizará una sesión Telnet, luego el atacante cambia su dirección IP, realizando un IP Spoofing con la dirección IP de la víctima (máquina que será suplantada); una vez se tiene el cambio, comienza a enviar paquetes ARP al servidor con el fin de forzarlo a actualizar su tabla ARP y, por ende, el reenvío de paquetes a la máquina del atacante. Cuando

se logra la conexión con el servidor, solamente resta realizar las acciones que el atacante se proponía en un principio (ejecutar código, obtener archivos, etc.), y finalmente intentar volver a restablecer la conexión entre la víctima y el servidor. Esta última parte no es trivial dado, pero engañando a la víctima se puede restaurar la conexión. En la sección F sobre Hunt se explica la manera como esa herramienta recupera el control (*gráfico A2.2*).

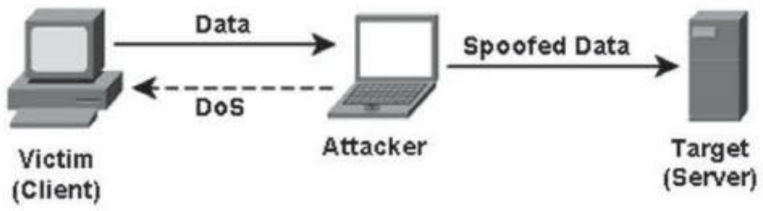


Gráfico A2.2

Recuperación del contol

3. HERRAMIENTAS PARA ASALTAR UNA SESIÓN TCP

Existe un amplio número de herramientas que permiten la realización de un asalto de sesión TCP; la mayoría son gratuitas y pueden conseguirse en Internet; como dato curioso la gran mayoría únicamente funciona en sistemas operativos Unix.

A. Juggernaut

Al igual que la gran mayoría de herramientas Juggernaut, está basada en Linux y fue desarrollada por un hacker conocido como route; apareció por primera vez publicada en la revista *Phrack Magazine* y, aunque fue creada hace bastante tiempo, aún sigue siendo una de las más predilectas, debido a algunas de sus características únicas. Uno de sus principales atributos es la capacidad de rastrear sesiones TCP, usando un criterio de búsqueda (p. e., la palabra Password), al actuar como sniffer, Juggernaut permite ver todo el tráfico de red y le da al atacante la oportunidad de escoger cualquiera de las sesiones activas. Otra característica que hace de Juggernaut una herramienta muy apetecida es la posibilidad de ensamblar paquetes desde cero; esto incluye activar las banderas del encabezado como se desee para pasar inadvertido ante algunos IDS. Sin embargo, una de las desventajas de Juggernaut es que no permite el envío de contraseñas desde el servidor (host) atacado a la máquina del atacante; para realizar esto se necesita usar otras herramientas. Esta herramienta se encuentra disponible en (Whitaker, A. y Newman, D.) http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=Juggernaut&type=archives

B. TTY-Watcher

TTY-Watcher es una herramienta que, a diferencia de Juggernaut, Hunt y otras aplicaciones para el asalto de sesiones, solamente puede ser usada en un tipo de sistema, las máquinas Solaris de SUN. Cuando un usuario está conectado a un sistema Solaris, todos los datos tecleados en la Terminal son automáticamente enviados a la Terminal TTY del atacante, permitiéndole ver todos los comandos ejecutados por la víctima. TTY-Watcher también permite al atacante enviar mensajes a su víctima, los cuales serán mostrados en la Terminal de este último; esta función puede utilizarse para robar todo tipo de contraseñas o para obligar a la víctima a escalar carpetas (Whitaker, A. y Newman, D.). Esta herramienta no es gratuita y está disponible en http://www.engarde.com/software/.

C. DsSniff

Es un conjunto de herramientas para la auditoría de redes y pruebas de penetración; las principales características de este paquete son: monitoreo pasivo de redes, intercepción de paquetes normalmente no disponibles para computadoras sin sniffers y permite implementar ataques de man-in-the-middle contra sesiones SSH y Https. Aunque no es una herramienta tan conocida ni de fácil manejo (necesita la instalación previa de otras aplicaciones), se consigue en Internet y es para la plataforma Unix. El set de herramientas se encuentra en http://www.monkey.org/~dugsong/dsniff/

D. T-Sight

Es una herramienta comercial producida por Engarde y se usa solamente en plataformas Windows. Aunque en sus inicios T-Sight fue diseñada como una herramienta de monitoreo para detectar tráfico sospechoso, actualmente se utiliza para captar todas las comunicaciones de un segmento de red en tiempo real y para realizar asaltos de sesión; por esto la empresa fabricadora Engarde solamente permite utilizar la herramienta con algunas direcciones IP. T-Sight es una herramienta de uso mucho más forense que intrusito; además cuenta con ciertas características, como detección de intrusiones, conjunto de reportes y gráficas para el análisis post mortem (http://www.runsecure.com/ids/id4of5.html).

4. HERRAMIENTA HUNT

Para ejcutar el asalto de sesión TCP, objeto de estudio de este paper, se escogió Hunt, que es una herramienta creada por Pavel Krauz y posee muchas similitudes con Juggernaut; también sirve en los sistemas operativos Unix, permite observar todo el tráfico TCP y brinda la opción de hacer un asalto de sesión simple (inserción de una sola línea de comando durante una sesión Telnet). Una de las principales ventajas de Hunt es su capacidad de restablecer conexiones una vez se ha alcanzado el propósito del ataque.

El control de una sesión puede ser devuelto al cliente original y, si se hace de una manera lo suficientemente rápida, aun así pasa inadvertido tanto para el servidor como para el cliente. Juggernaut, al contrario, requiere hacer un ataque de denegación de servicio; este tipo de asalto no solamente cierra la conexión con el cliente, sino que también imposibilita la comunicación de esa máquina con otro computador en esa subred, levantando sospechas y activando alarmas de un posible ataque. Hunt evita este problema, haciendo parecer la pérdida temporal de conexión un pequeño error de transmisión en red o un error del lado del servidor. Hunt no solamente permite el ataque en una misma subred; también provee formas de realizar el asalto a una sesión TCP en un ambiente switchado o incluso por Internet. Hunt se encuentra disponible en la siguiente dirección http://packetstorm.linuxsecurity.com/sniffers/hunt/.

5. PRÁCTICA DEL ASALTO DE UNA SESIÓN TCP

El caso de estudio de este paper fue realizado con la herramienta Hunt (sección 4). A continuación se explican paso a paso las acciones realizadas durante el asalto de sesión TCP:

1. Se utilizaron cuatro computadores conectados a un hub para la práctica del asalto; en uno se tenía un servidor FTP/Telnet con ambos servicios arriba; la IP de esta máquina era la 192.168.1.1 y el sistema operativo era Windows, el cliente (víctima en este caso) poseía una cuenta en el servidor mencionado antes y estaba comenzando una sesión Telnet. Su dirección IP era la 192.168.1.2 y su sistema operativo también era Windows. El tercer computador que era la máquina del atacante corría la herramienta Hunt y el sistema operativo era Unix, edición Ubuntu. Por último, el cuarto computador solamente estaba corriendo ethereal y su propósito era capturar el tráfico durante el establecimiento, y posteriormente el asalto de la sesión.
2. El computador cliente accede normalmente al servicio Telnet desde su consola, para lograr la conexión remota con el servidor (*gráfico A2.3*).

Gráfico A2.3

La consola de Telnet aparece en la pantalla del cliente y la sesión es establecida (*gráfico A2.4*).

Gráfico A2.4

3. Al mismo tiempo el atacante que ha ejecutado la herramienta Hunt, comienza a hacer un escaneo en el segmento de red al que pertenecen los 4 equipos involucrados, para buscar sesiones Telnet activas.
4. Una vez la sesión aparece en la consola del atacante, se realiza el ataque con una inundación de paquetes ARP hacia el cliente, para que este último actualice su tabla ARP y piense que el servidor se encuentra en una MAC diferente (*cuadro A2.1*).

CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01
CompalEl_fc:a8:4a	DellComp_a7:07:54	ARP	192.168.1.1 is at ea:1a:de:ad:be:01

Cuadro A2.1

Durante el envío de ARP, Hunt cambia la dirección MAC real del atacante por la del servidor que ofrece Telnet; de esta forma el cliente no se da cuenta de la modificación y sigue la sesión normalmente.

5. Una vez la "falsificación" se ha logrado del lado del cliente, es hora de engañar al servidor; esto se logra cambiando la cabecera de los paquetes enviados por el atacante usando los datos reales de la víctima (*cuadro A2.2*).

192.168.1.2	192.168.1.1	TELNET	Telnet Data ...
192.168.1.1	192.168.1.2	TCP	telnet > 1067 [ACK] Seq=0 Ack=4
192.168.1.2	192.168.1.1	TELNET	Telnet Data ...
192.168.1.1	192.168.1.2	TCP	telnet > 1067 [ACK] Seq=0 Ack=5
192.168.1.2	192.168.1.1	TELNET	Telnet Data ...
192.168.1.1	192.168.1.2	TCP	telnet > 1067 [ACK] Seq=0 Ack=6

Cuadro A2.2

6. Así es como se consuma el asalto de sesión; en este momento es cuando el atacante puede utilizar los permisos de la víctima para escalar privilegios, crear nuevos usuarios o incluso dejar backdoors o puertas traseras para futuras penetraciones. Aunque el cambio de paquetes que hace Hunt evita la detección del asalto, en algunas ocasiones se presenta un fenómeno que es la inundación de ACK o ACK Storm.
7. Cuando la víctima intenta seguir utilizando su sesión y envía los paquetes al verdadero servidor, su número de secuencia para la sincronización ya no funciona (*cuadro A2.3*).

192.168.1.1	192.168.1.2	TCP	[TCP Dup ACK 65#1] telnet > 1071 [ACK]
192.168.1.2	192.168.1.1	TCP	1071 > telnet [ACK] Seq=29 Ack=540 Win=
192.168.1.1	192.168.1.2	TCP	[TCP Dup ACK 65#2] telnet > 1071 [ACK]
192.168.1.2	192.168.1.1	TCP	1071 > telnet [ACK] Seq=29 Ack=540 Win=
192.168.1.1	192.168.1.2	TCP	[TCP Dup ACK 65#3] telnet > 1071 [ACK]
192.168.1.2	192.168.1.1	TCP	1071 > telnet [ACK] Seq=29 Ack=540 Win=
192.168.1.1	192.168.1.2	TCP	[TCP Dup ACK 65#4] telnet > 1071 [ACK]
192.168.1.2	192.168.1.1	TCP	1071 > telnet [ACK] Seq=29 Ack=540 Win=
192.168.1.1	192.168.1.2	TCP	[TCP Dup ACK 65#5] telnet > 1071 [ACK]
192.168.1.2	192.168.1.1	TCP	1071 > telnet [ACK] Seq=29 Ack=540 Win=
192.168.1.1	192.168.1.2	TCP	[TCP Dup ACK 65#6] telnet > 1071 [ACK]

Cuadro A2.3

Entonces es cuando se presenta un ACK Storm, como puede verse en la imagen; el cliente envía paquetes ACK con un número de secuencia no válido para esa sesión y, por su lado, el servidor intenta sincronizarlo nuevamente enviándole el nuevo número de secuencia; este proceso puede ocurrir muchas veces (pues es un ciclo), haciendo que Hunt cancele el asalto de la sesión, y es una de las formas más comunes de detectar un asalto de sesión.

Una característica única de Hunt es la posibilidad de restablecer la sesión TCP asaltada; para lograrlo, se envía un mensaje al cliente, el cual indica que el servidor se ha caído y, por lo tanto, se necesita una resincronización (*gráfico A2.5*).


```
#) The server has suffered a power failure, please write 22 characters in order
to re-synchronize the session_
```

Gráfico A2.5

De esta forma, los números de secuencia son nuevamente sincronizados y la sesión puede seguir siendo utilizada.

8. Finalmente, es importante anotar que el asalto de una sesión TCP debe hacerse de la forma más rápida posible, evitando así levantar alarmas (p. e., de IDS) y dejar la menor cantidad de rastros posible.

6. RASTROS DEL ASALTO A LA SESIÓN TCP

Aunque en la mayoría de los casos el asalto a una sesión TCP es difícil de detectar (solamente si hay grandes daños causados al sistema o el ataque fue realizado de manera descuidada), se puede detectar una sobrecarga en la red debido al envenenamiento de ARP. Sin embargo, ciertos indicios pueden aparecen durante la ejecución del ataque. Algunos de estos síntomas de que algo no anda bien en la sesión TCP son:

- La aplicación del cliente (p. e., Telnet) comienza a responder de forma lenta o incluso trabada (frozen screen).
- Alta actividad en la red por un corto período de tiempo, haciendo más lento el computador.
- Tiempos de respuesta lentos por parte del servidor (esto ocurre debido a que se está "compitiendo" con el atacante para los servicios que brinda el servidor).

Cuando se utiliza un sniffer de paquetes es necesario enfocarse en 3 factores para intentar detectar el asalto de una sesión TCP: Actualización repetida de la tabla ARP (*cuadro A2.4*).

192.168.200.100	TCP	32772 > telnet [ACK] Seq=150 Ack=544 W
192.168.200.100	ARP	192.168.200.21 is at ea:1a:de:ad:be:ef
192.168.200.100	ARP	192.168.200.21 is at ea:1a:de:ad:be:ef
192.168.200.100	ARP	192.168.200.21 is at ea:1a:de:ad:be:ef
192.168.200.100	TELNET	Telnet Data ...

Cuadro A2.4

Paquetes enviados entre un Cliente y un Servidor con diferentes direcciones MAC, y finalmente tormentas de paquetes ACK repentinas (*cuadro A2.5*).

```
192.168.200.100    TELNET  [TCP Out-Of-Order] Telnet D
192.168.200.21     TCP     [TCP Dup ACK 605#2] telnet
192.168.200.100    TELNET  [TCP Out-Of-Order] Telnet D
192.168.200.21     TCP     [TCP Dup ACK 605#3] telnet
```

Cuadro A2.5

Sin embargo, este último factor es tenido en cuenta por algunas herramientas de asalto de sesión, como Hunt, la cual intercambia direcciones MAC en la tabla ARP, haciendo difícil de ubicar las verdaderas direcciones tanto de la víctima como del servidor (Whitaker, A. y Newman, D. s.f.).

7. CORRECCIÓN DEL ASALTO

Debido a la forma como el protocolo TCP está implementado y la facilidad para cambiar paquetes, una vez se ha establecido una conexión, el asalto de las sesiones TCP es un problema con soluciones restringidas. Sin embargo, una solución que ha probado ser exitosa es la de implementar sesiones con un nivel de seguridad más alto; por ejemplo, encriptación de datos.

El *cuadro A2.6* muestra un paralelo entre métodos de comunicación que permitían un asalto de sesión, sin dificultades y sus nuevas versiones o nuevos mecanismos de seguridad.

Sesiones con problemas	Soluciones actuales
Telnet	SSH (Secure Shell)
FTP	sFTP (Secure FTP)
http	SSL (Secure Socket Layer)
IP	IP sec
Conexiones remotas	VPN (Virtual Private Network)
Redes con HUB	Redes con Switch

Cuadro A2.6

Incluso implementando las soluciones dadas en el cuadro anterior, la mejor práctica para evitar el asalto de sesiones es limitar el número de accesos remotos y el número de conexiones a ciertos servicios. Básicamente, si se tiene un firewall protegiendo un sistema (que es lo más recomendable), se debe dar permiso de entrada y salida solamente a lo que es estrictamente necesario y únicamente con hosts confiables.

Conclusiones

Actualmente existen muchas herramientas para ejecutar un asalto de sesión TCP; hay algunas gratuitas y otras con precio comercial, aunque la gran mayoría solamente funcionan para plataformas Unix; T-Sight es una aplicación que funciona para Windows y ha demostrado ser bastante eficiente tanto para rastreo como para ataque.

Aunque el asalto de sesión es un ataque con muchos años de antigüedad, todavía se usa para atacar máquinas con las debilidades expuestas en Para profundizar; por lo tanto, si no se tienen en cuenta las recomendaciones y no se apagan servicios como Telnet o FTP, o se cambian por las versiones con seguridad (SSH y sFTP), se pueden estar corriendo los mismos riesgos de hace una década o incluso menos.

Una buena forma de evitar un ataque de asalto de sesión es tratar de limitar el número de conexiones remotas permitidas a una máquina, y además utilizar los nuevos protocolos de transmisión que son más seguros en cuanto a comunicación entre 2 máquinas.

✓ ***Resumen:*** En este documento se explica la estructura de un asalto a una sesión TCP, se presenta un ejemplo práctico utilizando la herramienta Hunt y se evidencian los rastros que se dejan tras el ataque.

✓ **Términos clave:** Sesión TCP, Cliente, Servidor, Paquete IP, Telnet, Hunt, IP Spoofing, ARP poisoning.

Enlaces en el Web

Base de datos de conocimiento/Seguridad informática –Asociación Colombiana de Ingenieros de Sistemas –ACIS– http://www.acis.org.co/index.php?id=228

CGI Security – http://www.cgisecurity.com

CriptoRED –Artículos de seguridad informática en castellano – http://www.criptored.upm.es –Sección Docencic

El Hacker.net – http://www.elhacker.net

Insecurity magazine – http://www.insecuremag.com

Proyecto Metasploit – http://www.metasploit.com

Revista Phrack – http://www.phrack.org

SANS –Reading Room– Artículos de seguridad informática en inglés – http://www.sans.org/reading_room/

Securityfocus –Artículos de seguridad informática en Inglés – http://www.securityfocus.com/infocus

Virusprot –Artículos de seguridad informática en caswtellano – http://www.virusprot.com/Articulo.html

Referencias*

Alvisi, Lorenzo. Bressoud Thomas, C. ElK-Khashab, Ayman. Marzullo, Keith. Zagorodnov, Dmitrii. (s.f.). *Wrapping Server-Side TCP to Mask Connection Failures*. Disponible http://citeseer.ist.psu.edu/cache/papers/cs/22156/http:zSzzSzwww.ieee-infocom.orgzSz2001zSzpaperzSz764.pdf/alvisi00wrapping. pdf

Dittrich, Dave. (s.f.). *Anatomy of a Hijack*. University of Washington. Disponible en http://staff.washington.edu/dittrich/talks/qsm-sec/script.htm

Inundación paquetes SYN. (s.f.). disponible en http://www.putoamo.host.sk/hack/textos/syn%20flood.htm

KLM. (s.f.). Remote Blind TCP/IP spoofing, *Phrack Magazine*, issue 64. Disponible en http://www.phrack.org/issues.html?issue=64&id=15#article

Padmanabhan, Venkata N. (s.f.). Coordinating Congestion Management and Bandwidth Sharing for Heterogeneous Data Streams http://citeseer.ist.psu.edu/cache/papers/cs/10117/http:zSzzSzwww.research.microsoft.comzSz~padmanabzSzpaperszSznossdav99-expn.pdf/coordinating-congestion-management-and.pdf

Port Scanning. (s.f.). Disponible en http://www.auditmypc.com/freescan/readingroom/port_scanning.asp

RFC 793. (s.f.). Protocolo TCP, Data Internet Program. Disponible en http://www.rfc-es.org/rfc/rfc0793-es.txt

Stevens, W. Richard. (s.f.). *TCP/IP Illustrated*, Volume 1: The Protocols.

Tanase, Mathew. (s.f.). *IP Spoofing: Aan Introduction*, disponible en http://www.securityfocus.com/infocus/1674

Telnet, guía de Microsoft para usuarios de Windows. (s.f.).

Whitaker, A. y Newman, D. (s.f.). *Penetration Testing and Network Defense, Cisco Press.*

* Referencias de la sección Para profundizar. (N. del E.).

Bibliografía

Ackoff, R. (2002). *El paradigma de Ackoff. Una administración sistémica*. Limusa Wiley.

Adamski, A. (1999). Crimes related to the computer network. Threats and opportunities: A criminological perspective. http://www.infowar.com/

Alberts, C. y Dorofee, A. (2002). *Managing Information Security Risks: The Octave Approach*. Addison Wesley.

Apgar, D. (2006). *Risk Intelligence. Learning to manage what we don't know*. Harvard Business School Press.

Bazerman, M. y Watkins, M. (2004). *Predictable Suprises. The disasters you should have seen coming and how to prevent them*. Harvard Business School Press.

Cano J. (Marzo 1-5 de 2004). Inseguridad informática. Un concepto dual en Seguridad informática. ComputerWorld Colombia. (Disponible en: http://www.virusprot.com/art47.htm).

Casey, E. (2000). *Digital Evidence and Computer Crime*. Academic Press.

Casey, E. (2004). *Digital Evidence and Computer Crime*. Second edition. Elsevier Science. Academic Press.

Cole, E. (2002). *Hackers beware. Defending your network from Wiley Hacker*. News Riders.

Day, K. (2003). *Inside the security mind. Making the tough decisions*. Prentice Hall.

Fontalvo, J. (2002). *Criminología. Un enfoque humanístico*. Tercera edición. Edtorial Temis.

Furnell, S. (2002). *Cybercrime. Vandalizing the information society*. Addison Wesley.

Honeynet Project (2004). *Know your enemy. Learning about security threats*. Addison Wesley.

Horton, M. y Mugge, C. (2003). *Hack Notes. Network Security*. Portable Reference. McGraw-Hill.

Hutchinson, B. y Warren, M. (2001). *Information warfare. Corporate attack and defence in digital world*. Butterworth Heinemann.

Information System Audit and Control Association. (2005). *Cybercrime. Incident Response and Digital Forensics.*

Koziol, J., Aitel, D., Litchfield, D., Anley, C., Eren, S., Mehta, N. y Hassell, R. (2004). *The shellcoder's handbook: Discovering and exploiting security holes*. Wiley Publishing, Inc.

Littlejohn, D. (2002). *Scene of Cybercrime. Computer Forensic Handbook*. Syngress Publishing Inc.

Mandia, K., Prosise, C. y Pepe, M. (2003). *Incident Response & Computer Forensics*. Second Edition. McGraw-Hill.

Marcella, A. y Greenfield, R. (2002). *Cyber forensics*. Auerbach Publications.

Martins, A. (2003). Information security culture. Master Thesis. Unpublished Thesis. Disponible en: http://etd.rau.ac.za/theses/available/etd-04292004-110222/

Osterburg, J. y Ward, R. (2000). *Criminal Investigation*. Third Edition. Anderson Publishing Co.

Parker, D. (1998). *Fighting computer crime. A new framework for protecting information*. John Wiley & Son.

Peikari, C. y Chuvakin, A. (2004). *Security warrior*. O'really.

Power, R. (2000). *Tangled Web. Tales of digital crime from the shadows of cyberspace*. QUE Corporation.
Reyes Echandía, A. (2003). *Criminología*. Cuarta reimpresión de la octava edición. Editorial Temis.
Rogers, M. (1999). *A new hacker taxonomy*. Department of Psychology. University of Manitoba. *Research Paper*.
Rogers, M. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. Doctoral Thesis. Department of Psychology. University of Manitoba. Winnipeg, Manitoba. Canadá.
Schneier, B. (2003). *Beyond Fear*. Copernicus Books.
Shiffman, M. (2003). *Hacker Challenge. Test your incident respond skills using 20 scenarios*. McGraw-Hill.
Stephenson, P. (1999). *Investigation Computer Related Crime*. CRC Press.

3 EL ADMINISTRADOR Y LA INFRAESTRUCTURA DE LA SEGURIDAD INFORMÁTICA

Objetivos

- ✓ Revisar y analizar el papel y las responsabilidades del administrador de sistemas
- ✓ Describir algunas consideraciones de diseño de infraestructuras de seguridad
- ✓ Estudiar algunas técnicas básicas para el diseño y la generación de rastros
- ✓ Presentar los conceptos básicos de auditabilidad y trazabilidad
- ✓ Estudiar y analizar algunas consideraciones jurídicas y aspectos de los rastros en las plataformas tecnológicas

INTRODUCCIÓN

Mucha de la responsabilidad de la configuración de las infraestructuras informáticas recae sobre los llamados administradores del sistema. En el contexto de este libro por administrador del sistema entenderemos aquel profesional especializado en la configuración y el afinamiento de los diferentes elementos de la infraestructura informática, para lo cual debe contar con buenas prácticas de aseguramiento tecnológico, competencia y habilidad técnica, y con un alto sentido de la confidencialidad, integridad y disponibilidad de los activos que tiene a cargo.

El administrador del sistema está especializado en la configuración y el afinamiento de los diferentes elementos de la infraestructura informática.

Estos profesionales se enfrentan al reto de mantener operacional una infraestructura, y a ser los primeros en contacto con la materialización de la inseguridad de la información, bien sea por una falla propia del equipo o de los equipos que se administran, por una acción deliberada desarrollada, efectuada por un intruso o por una falla operacional del mismo administrador. Ante una falla de seguridad de la información los administradores son los primeros que deben reaccionar y aportar su visión integral del entendimiento de la infraestructura, con el fin de orientar y avanzar en la detección y el análisis del incidente de seguridad. Este apoyo se convierte en insumo fundamental de la investigación que se adelante, pues de esta manera se puede avanzar en la identificación del ataque y los atacantes, y así evitar que el probable infractor se mimetice dentro de las evidencias que se puedan recabar.

En las secciones siguientes profundizaremos en aspectos críticos de este profesional informático, para comprender ese segundo papel de los investigadores forenses, ahora en la formalidad de la operación de la infraestructura de computación y las características de seguridad informática, requeridas para detectar e identificar las posibles intrusiones informáticas.

3.1 ROLES Y RESPONSABILIDADES DEL ADMINISTRADOR DE SISTEMAS

El administrador del sistema está a cargo del sistema (hardware, software, procedimientos).

En la actualidad existen muchos profesionales de tecnologías de información, cuyo cargo se denomina "administrador del sistema", esa persona que está a cargo del sistema (hardware, software, procedimientos), a quien se acude cuando existe algún tipo de inconformidad con algún elemento del mismo. En organizaciones pequeñas (menos de 500 empleados) generalmente este cargo es desempeñado por una persona que asume la responsabilidad por mantener la operación, la continuidad, la seguridad y la disponibilidad de la infraestructura informática de la organización.

En organizaciones medianas (más de 500 y menos de 1.000 empleados) este mismo cargo se especializa más, y se entiende cómo el de aquellos profesionales encargados de la configuración y el afinamiento de los componentes de computación y comunicaciones que permiten una adecuada operación y el funcionamiento de los mismos. Ya los temas de seguridad y continuidad se entregan a otras áreas especializadas (que pueden o no estar dentro del área de tecnología) que interactúan de manera coordinada con los administradores, para concretar las estrategias de disponibilidad y protección de la información de sus áreas de responsabilidad.

En organizaciones grandes (más de 1.000 empleados), el administrador del sistema es aquella persona que se denomina un especialista de plataforma, personal especializado en sistemas operacionales, bases de datos, respaldos, afinamientos y ajustes de parámetros de servidores, que mantienen la operación día a día de las organizaciones. En este escenario, la función de seguridad de la información y la de continuidad están fuera del área de tecnología.

Indistintamente sea el tipo de organización el que se analice, el cargo y la función de administración del sistema tiene un componente operacional propio de su papel y de seguridad y control que debe ser parte de las actividades previstas para esa administración. Sin embargo, muchos administradores se encuentran con el dilema de dar prioridad a la funcionalidad que a la seguridad, pues los cambios que se sugieren desde esta perspectiva pueden ocasionar el inadecuado funcionamiento de una aplicación.

La función de administración del sistema tiene un componente operacional propio de su papel y de seguridad y control

Esta disyuntiva lleva a un enfrentamiento de los profesionales de la seguridad de la información y los administradores, donde conciliar una posición al respecto es una labor compleja en la cual intervienen muchas variables; con el agravante de que posiblemente la posición del área de seguridad de la información sea tan válida como la del área de tecnología.

Para tratar de establecer algunos elementos conceptuales básicos que permitan observar con mayor claridad este entorno,

desarrollaremos algunas descripciones de las labores de los administradores del sistema y de los profesionales de seguridad de la información, para detallar sus puntos de coincidencia y coordinación, así como las áreas especializadas de cada cargo.

El cargo de administrador del sistema, o el *system administrator*, nace con la operación de los primeros mainframes.

El cargo de administrador del sistema, o *system administrator*, nace con la puesta en operación de los primeros *mainframes*, donde el trabajo era tan especializado que se tenía el concepto de operador, administrador y programador del sistema. Estos tres cargos, sugeridos por los primeros proveedores de sistemas computacionales, describían con claridad los límites de cada cargo.

Para el operador, su función principal era ejecutar comandos en el sistema (detallados y registrados en una bitácora de actividades), los cuales eran ordenados por el administrador del sistema, así como monitorear el buen funcionamiento de los procesos o los trabajos que se ejecutaban en el *mainframe*.

El administrador se encarga de la historia de cambios, actualizaciones y ajuste de las máquinas y el software.

El administrador del sistema era la persona especializada tanto en el software base de las máquinas, como en la configuración del sistema, el dueño de los parámetros básicos del hardware y del software, siguiendo las recomendaciones del proveedor. El administrador tiene a su cargo la historia de cambios, actualizaciones y ajuste de las máquinas y el software en el transcurso del tiempo. Este cargo no opera el sistema, tiene permisos restringidos y monitoreo de sus acciones sobre los parámetros del hardware y software.

El programador del sistema, a diferencia del administrador, era aquella persona que utilizando la configuración base del sistema ofrecida, implementada por el administrador, desarrollaba y programaba trabajos especializados en la máquina que permiten la funcionalidad de las aplicaciones que allí se ejecutan. Es el cargo que habla con las áreas de negocio para establecer los requerimientos de las operaciones requeridas, para cumplir con las necesidades de

la empresa. Si bien, aún en esta época, el lenguaje del programador del sistema es altamente técnico, las áreas de negocio debían hacer un esfuerzo importante para que ese profesional entendiera sus solicitudes.

El programador del sistema desarrolla y programa trabajos especializados en la máquina que permiten la funcionalidad de las aplicaciones que allí se ejecutan

Como podemos ver, son tres cargos en que cada uno desarrollaba un espectro de actividades que, adecuadamente coordinadas, funcionaban y daban cumplimiento a lo que se especificaba en la organización. Con el paso del tiempo, las organizaciones se hicieron más complejas, con mayores exigencias y requisitos, pues el entorno de negocios y las tecnologías de información cambiaron: de una realidad estática y estructurada, a una dinámica y no estructurada.

En este contexto, concebir los cargos presentados previamente exige un entendimiento de la realidad dinámica de las redes, la movilidad de los individuos y la flexibilidad de los procesos de negocio, los cuales evolucionan con la fuerzas del mercado. Para lograr la reformulación de la seguridad y el control en un entorno como éste, se requiere pensar la seguridad en múltiples variables y especialidades que conjugadas establezcan un cuerpo conceptual semejante a lo que existía en el pasado, no para restringir y especializar, sino para posibilitar y diversificar el concepto de seguridad.

La seguridad y el control no deben estar fundados en la capacidad de restricción, sino en la posibilidad de orientar el sistema hacia lo más conveniente.

El concepto de seguridad y control no debe estar fundado en la capacidad de restricción, sino en la posibilidad de orientar el sistema hacia lo más conveniente, basado en principios propios del negocio y de la protección de la información, como activo fundamental de la organización. Es decir, un elemento que busca conciliar la funcionalidad de los servicios con las regulaciones propias de las operaciones. En este sentido, se establece una promesa compartida entre los dueños del negocio, los profesionales de tecnologías de información y los de seguridad informática: que los clientes puedan utilizar la potencialidad

de las tecnologías, con la confiabilidad requerida y las medidas de protección establecidas de manera natural y efectiva.

Esta promesa exige de los administradores del sistema entender tanto las expectativas de los dueños del negocio, como las del área de seguridad. Poner en una balanza ambas necesidades exige del nuevo administrador del sistema una mente integradora y no especializada, entendiendo esto último como un llamado a estos profesionales para comprender y analizar no solamente las máquinas y sus variables, sino el negocio y sus posibilidades. Es lo que podríamos llamar un arquitecto de seguridad de información, que con pensamiento sistémico comprende la dinámica de los negocios, y allí descubre la inseguridad reinante en cada una de las relaciones que advierte en la infraestructura, y toma las decisiones del caso para comprenderla y enfrentarla.

Con este análisis presente, definir el cargo de administrador del sistema actualmente requiere una reflexión de mínimo cuatro dimensiones: tecnológica, procedimental, humana y de negocio que permitan establecer las responsabilidades y los alcances de esta figura organizacional, ahora en un ambiente cambiante y lleno de actualizaciones y creativas propuestas de negocios, generalmente basadas en interacciones remotas y con servicios sobre las redes.

La dimensión procedimental se conserva como en el pasado, sólo que ahora debe considerar elementos de seguridad y control.

La dimensión tecnológica del administrador es la misma que viene heredada del pasado, su especialidad técnica es la base de su formación y su experiencia lo convierte en un factor clave de éxito para la operación y la funcionalidad de la infraestructura informática de la empresa. La dimensión procedimental, atada al manejo de cambios y actualizaciones tanto de hardware y software, se conserva como en el pasado, sólo que ahora debe considerar elementos de seguridad y control sugeridos tanto por los proveedores como por los especialistas de seguridad. Es decir, se incorpora un nuevo criterio para la administración: no sólo que funcione y opere bien, sino de manera confiable (*gráfico 3.1*).

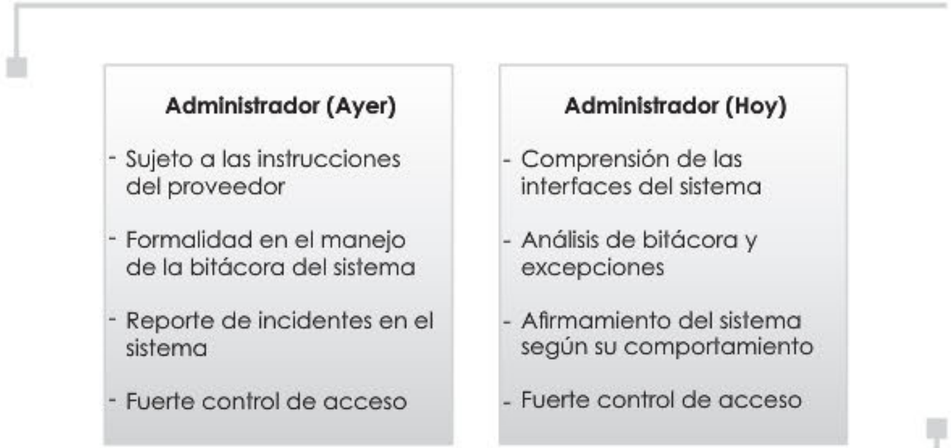


Gráfico 3.1

El administrador de ayer y hoy

Lo relacionado con la parte humana es congruente con su disposición de servicio y hacer las cosas más fáciles para sus clientes. Si bien, su preparación técnica es clave para su trabajo, debe contar con la capacidad de presentar sus propuestas de manera clara y sencilla, evitando la jerga propia de los técnicos. Este profesional debe contar con altos niveles de ética, pues en sus manos están las variables más críticas para la funcionalidad de la organización, su sentido de pertenencia y compromiso debe ser altamente estimado y valorado.

Finalmente y no menos importante es la variable de negocio, la cual busca que este profesional entienda cómo sus acciones encajan en las propuestas de negocio y cómo su labor perfecciona la misma en la operación formal de la empresa. Esto permite una visión más integradora del proceso de administración del sistema, más allá de los ajustes tecnológicos, para convertirla en una administración de tecnologías de información integrada con los dueños del negocio. Es importante aclarar que ésta es una reflexión que debe hacerse en doble vía, es decir, los dueños de los procesos de negocio deben interiorizar y comprender también los esfuerzos que los administradores del sistema hacen en su dominio de responsabilidad.

En este contexto, podríamos decir que el administrador del sistema, transformado en un arquitecto de tecnología, debe establecer los niveles tolerables y medibles de la inseguridad propia de los sistemas que administra y su impacto en el negocio, basado en una

administración de riesgos propia de su cargo, no para alertar sobre las posibles fallas identificadas, sino para aprender de ellas y ajustar la infraestructura para hacerla más resistente a ataques más elaborados.

Un investigador forense debe comprender las responsabilidades de un administrador y sus razonamientos para obtener información.

Para un investigador forense, el comprender las responsabilidades de un administrador y sus razonamientos le permite obtener información valiosa desde el punto de vista técnico, procedimental y de negocio que busque analizar la dinámica de los hechos de los eventos investigados, no sólo como hechos aislados y tecnológicos, sino con el sentido de los procesos y la mente tanto del atacante como de los dueños del negocio.

Encontrar la verdad en el escenario de los administradores del sistema va más allá de un cargo y un perfil dentro de un sistema, pues la herencia tecnológica del administrador del sistema muchas veces nos impide revisar otras relaciones emergentes, que muestran más de este cargo, y nos posibilitan proponer hipótesis más elaboradas y consistentes.

3.2 CONSIDERACIONES DE DISEÑO DE INFRAESTRUCTURAS DE SEGURIDAD

Para detallar algunas consideraciones de diseño de infraestructuras de seguridad, trataremos de ver un poco la evolución de la computación y, con ella, la transformación de la seguridad de la información. En este contexto, detallaremos las características requeridas de la seguridad en cada momento, sus motivaciones y las necesidades propias para las organizaciones.

Con la evolución tecnológica, la seguridad requiere ser repensada y adaptarla a cada una de las realidades de la tecnología actual.

Con la evolución tecnológica, la seguridad ha requerido repensarse y adaptarse a cada una de las realidades de la tecnología del momento. En esta sección trataremos de revisar cada uno de esos momentos tecnológicos pasados y los futuros, mostrando las implicaciones y estrategias de seguridad que se desarrollaron para luchar contra la inseguridad propia de la tecnología y de la arquitectura formulada para ese entonces.

3.2.1 Inseguridad centralizada

Durante los años 60 y 70 la computación centralizada era la realidad evidente en los centros de procesamiento de datos. Los grandes computadores centrales o mainframes eran los que estaban en el primer nivel del uso informático de las organizaciones. Este tipo de computación era la norma que apoyaba los diferentes procesos de la organización, los cuales eran operados por personal especializado para esas labores. Es importante anotar que no todo el mundo tenía acceso a estas máquinas. En este sentido, la seguridad informática alrededor de este escenario, más que concentrarse en el descubrimiento de la inseguridad de los programas, estaba orientada a la seguridad física de los equipos y el buen procesamiento de la información. Una falla en el programa de control de la información, o en la integridad de la misma, generaba una alta desconfianza en los informes y sus cifras.

La computación centralizada, basada en un gran *mainframe*, estaba dominada por las recomendaciones de los proveedores.

La computación centralizada y basada en un gran mainframe estaba dominada por las recomendaciones de los proveedores y no seguirlas era ir en contra del buen funcionamiento de las máquinas. En este mismo sentido, la seguridad de la información se concentraba en el acceso y el control de las máquinas, en el ingreso al sitio donde se encuentran éstas, y en la habilidad y el entrenamiento de las personas encargadas de operarlas. En este contexto, los proveedores de estas máquinas hacían énfasis especial en el uso y la configuración de sistemas elaborados de acceso para velar por el adecuado seguimiento de las acciones en el sistema (*gráfico 3.2*).

En cuanto a la seguridad y el control, los años 60 y 70 se caracterizaron por un énfasis marcado en el control de acceso, la segregación de funciones y el debido registro de las operaciones y transacciones. Los mecanismos de seguridad propios de la época eran los registros de auditoría que, si bien existían y eran frecuentemente consultados, no tenían mayores protecciones, dado que el personal que tenía acceso a ellos eran profesionales con alto nivel de confianza y

Gráfico 3.2
Inseguridad centralizada

con perfiles especiales, claramente registrados e identificados. Ésta es la época de aplicación de modelos de seguridad, como Bell-Lapadula y Biba Model, modelos que hacían hincapié en la confidencialidad y el acceso a la información.

3.2.2 Inseguridad descentralizada

Durante los años 80 se abre la puerta al concepto de las infraestructuras cliente/servidor –c/s.

Durante los años 80 se pasaba de una realidad centralizada y cerrada, a una descentralizada y abierta. Se concluye la época de los mainframes y se abre la puerta al concepto de las infraestructuras cliente/servidor –c/s. En este modelo de interacción existen máquinas que solicitan servicios y otras que los ofrecen. El énfasis se concentra en el tráfico de información a través de la red, y en el uso de puertos de conexión, los cuales están asociados con los servicios que se prestan.

Este cambio abre la puerta a un nuevo tipo de inseguridad, a unas nuevas relaciones que van más allá del servidor centralizado y, por tanto, requiere repensar nuevamente la gestión de la seguridad de la información. Con la llegada de una computación más abierta y con más oportunidades, se inicia la carrera para desarrollar mecanismos de seguridad de la información, particularmente orientadas a las redes: firewalls, sistemas de detección de intrusos, criptografía asimétrica,

SSL (*secure socket layer*), proxies, entre otros, los cuales establecen una nueva responsabilidad para el área de tecnologías de información.

Los nuevos mecanismos de seguridad que se presentan recogen las prácticas de los años 70 y desarrollan nuevas funcionalidades para disminuir los impactos de la inseguridad propia de los protocolos asociados con TCP/IP. A continuación, se hace una breve descripción de los principales mecanismos de seguridad en los ambientes cliente c/s.

Firewall (fw) o cortafuegos, una tecnología de los años 80 que busca desarrollar un control de acceso en el tráfico de red, con el fin de identificar qué paquetes pueden o no ingresar o salir del perímetro de la red de una organización. Para ellos, se plantea un esquema de construcción de reglas, ya previamente vigente en los sistemas de enrutamiento para controlar los recorridos que seguían los paquetes en una red, con el propósito de hacer más granular el control tanto como la organización quisiera. Este portal de control de acceso del tráfico se convierte en la fortaleza de la organización para evitar que personas no autorizadas trataran de invadir desde el exterior la red interna. Luego, con el tiempo, se hace evidente que no solamente el control desde el exterior era necesario, pues en el interior se podían presentar empleados desmotivados que podrían atentar contra la organización misma (*gráfico 3.3*).

Firewall (fw) o cortafuegos busca desarrollar un control de acceso en el tráfico de red.

Los sistemas de detección de intrusos (en inglés IDS, Intrusion Detection System) son otro de los adelantos tecnológicos de seguridad propios del mundo c/s, pues actúan como un monitor del tráfico de red, descubriendo y analizando ahora el contenido de los paquetes que ingresan a la organización. Si bien el fw hace parte del trabajo de control de acceso, no tiene capacidad para observar "la intencionalidad del mensaje" que lleva el

Los sistemas de detección de intrusos (IDS, Intrusion Detection System) son otro de los adelantos tecnológicos de seguridad os del mundo c/s.

paquete. Los sistemas de detección de intruso se asemejan a las alarmas que se instalan en casas, carros y oficinas a fin de advertir la presencia de una persona no deseada. En la primera parte de la evolución de estos sistemas su función era exclusivamente reactiva de la presencia de un posible ataque al sistema protegido, pero su grado de confiabilidad dependía del afinamiento de las reglas propias de detección y el tráfico de red frente a la dinámica de la organización (*ver gráfico 3.3*).

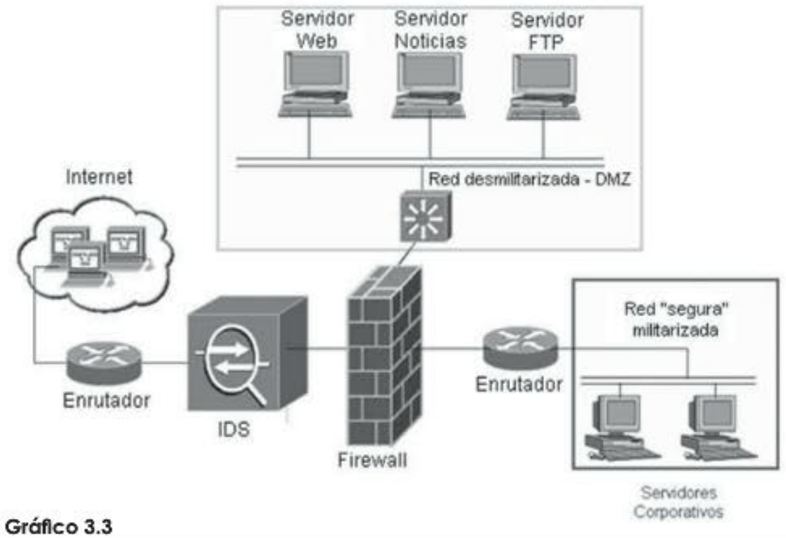


Gráfico 3.3

Configuración de un firewall

Los sistemas de detección de intrusos continuaron su desarrollo, haciéndose cada vez más versátiles en la detección y luego en la reacción contra posibles escenarios de ataques, siempre con el margen de error asociado con los falsos-positivos; es decir, aquellos eventos o paquetes de tráfico de red que, sin ser una amenaza real, fueron reportados como tales. Con el paso del tiempo, en las infraestructuras de seguridad fue necesario combinar la presencia de un firewall y luego un ids, con el fin de aumentar la capacidad de detección y de alerta de los intrusos en una infraestructura de red. Se hicieron parte fundamental de una estrategia de seguridad en el perímetro de las organizaciones y una herramienta clave para monitorear a los usuarios internos.

Por otra parte, tenemos *los proxies*, o estrategias de reducción o ampliación de acceso a conexiones desde o hacia una red, la cual

puede ser normal o inversa. Un proxy es un intermediario que recibe, registra, valida y autoriza la salida o la entrada de un tráfico de red. Está asociado con permitir el acceso de muchas personas a recursos en Internet, donde únicamente se publica una dirección en Internet, protegiendola de cada uno de los usuarios internos de la red. La otra modalidad es que un usuario del exterior envíe una petición a un recurso que se encuentre detrás del proxy y éste remita el paquete, luego de su verificación, al servidor correspondiente. Mientras el primer funcionamiento es el normal de esta estrategia, el segundo se denomina proxy reverso (*gráfico 3.4*).

Un proxy es un intermediario que recibe, registra, valida y autoriza la salida o la entrada de un tráfico de red.

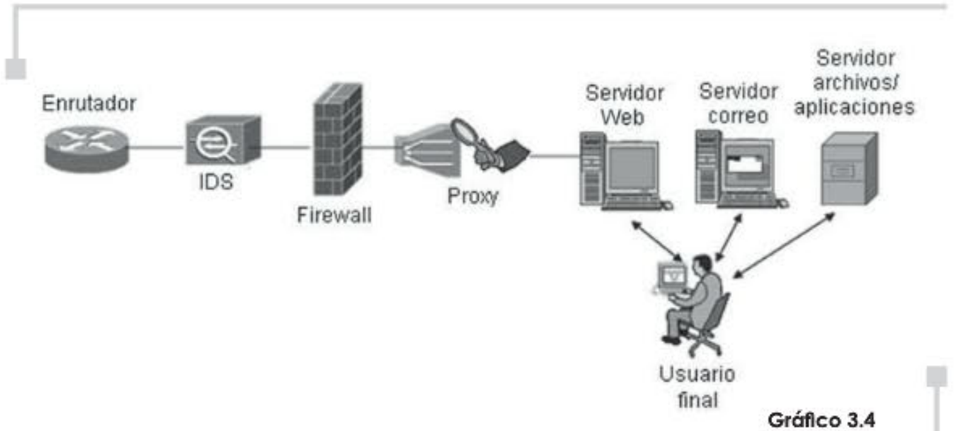


Gráfico 3.4

Inseguridad descentralizada

Basado en el modelo OSI de ISO, promulgado en la década de los 70 y de uso diario en nuestros días, se establece una manera de pensar en las protección de las redes; es decir, recorriendo cada uno de los niveles conocidos (físico, enlace, red, transporte, sesión, presentación y aplicación) se pueden establecer los mecanismos de seguridad requeridos para disminuir el nivel de inseguridad propio de las aplicaciones c/s, y así dimensionar la inversión que habría que hacer para aumentar la confianza de la organización en el uso de las redes, y el transporte confiable de la información (*ver cuadro 3.1*).

	NIVELES OSI						
	1	2	3	4	5	6	7
Autenticación de origen			✓	✓			✓
Autenticación origen de los datos			✓	✓			✓
Servicio de control de acceso			✓	✓			✓
Confidencialidad de la conexión			✓				✓
Confidencialidad del flujo de información	✓		✓	✓			✓
Confidencialidad de campos selectivos						✓	✓
Integridad de la conexión con recuperación				✓			✓
No repudiación de origen							✓
No repudiación de destino							✓
Control de acceso al servicio y aplicaciones					✓		✓

Cuadro 3.1

Algunos servicios de seguridad en el OSI/ISO

Ahora, en el mundo c/s, el director de tecnología no solamente es responsable porque la infraestructura funcione de acuerdo con lo requerido, sino que debe hacerlo con mayor confiabilidad, disponibilidad, trazabilidad e integridad. Este requerimiento se hace en medio de una nueva tendencia de ataques y de incidentes que llevan a las organizaciones a fallas importantes de los sistemas y a pérdidas de continuidad, ya no ocasionadas por una caída del servidor central, sino por acceso no autorizado, una negación de servicio, una suplantación de dirección IP, envenenamiento de caché del DNS (Domain Name Services), monitoreo no autorizado de conexiones, suplantación de direcciones MAC, asalto de sesiones TCP, entre otros.

En el mundo c/s, el director de tecnología es responsable de que la infraestructura funcione según se requiera y debe hacerlo con mayor confiabilidad, disponibilidad, trazabilidad e integridad.

Esta nueva realidad desarrolla y propulsa una dinámica de la seguridad de la información, no solamente motivada por los ataques, sino por las posibilidades que se abren al explorar los protocolos que soporta la suite de protocolos TCP/IP. Las aplicaciones cliente/servidor ofrecen toda una gama de

Las aplicaciones cliente/servidor ofrecen una gama de nuevas posibilidades para utilizar la capacidad de cómputo.

nuevas posibilidades para utilizar la capacidad de cómputo de las máquinas, y abrir la interacción de las mismas a los usuarios de toda la organización.

3.2.3 Inseguridad en el Web

Con el avance de los servicios, gracias a la masificación del uso y la configuración de TCP/IP, se profundiza el cambio que la arquitectura c/s proponía. La interacción a través del Web, por la vía del protocolo http, ofrece nuevas potencialidades para generar aplicaciones y programas que pudiesen ejecutarse en cualquier parte, a cualquier hora y en cualquier momento, sin necesidad de instalar software adicional en el cliente, como ocurría en el modelo c/s. Estas posibilidades de movilidad y versatilidad, acompañadas con una interfaz amigable y conocida por el usuario, establecen un nuevo cambio paradigmático en la tecnología y en la seguridad.

Ahora las tecnologías asociadas con el Web (creadas en los años 90) son las que ofrecen interactividad y transparencia mayores para el usuario, en el uso de los recursos computacionales. En este contexto, la seguridad, previamente basada en redes, tráfico de red y puertos, se orienta hoy hacia el estudio del protocolo http, los servidores de aplicaciones (application servers), los CGI –Common Gateway Interface–, los applets de Java, lenguajes como PHP, Python, Perl, entre otros aspectos, que ofrecen toda una nueva gama de posibilidades y oportunidades para las empresas y los usuarios.

La seguridad, basada en redes, tráfico de red y puertos, se orienta hoy hacia el estudio del protocolo http.

En este mundo posibilitado por el Web, se desarrollan aplicaciones que viajan e interactúan por la vía del protocolo http, cuya especificación se encuentra detallada en el RFC 2616 (http://www.faqs.org/rfcs/rfc2616.html). En este nuevo escenario la seguridad no puede estar basada exclusivamente en los temas de redes, sino ahora en los temas de seguridad en aplicaciones. Este contexto nos exige repensar hoy la seguridad en términos

En el Web la inseguridad de la información es una variable crítica en el desarrollo de las aplicaciones actuales.

de la inseguridad de Java, de PHP, de los servidores de aplicaciones como Tomcat, de la configuración e interacción de los servidores Web (Apache, IIS), pero en particular de las prácticas de programación de los desarrolladores de las aplicaciones. En el mundo Web la inseguridad es una variable que no se percibe directamente en la interacción, sino que se observa en una revisión de las relaciones de los diferentes componentes de la arquitectura de las aplicaciones (*ver gráfico 3.5*).

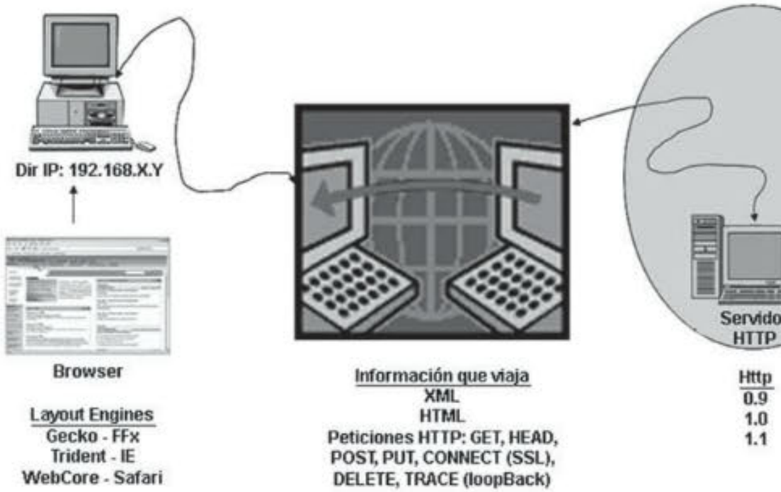


Gráfico 3.5

Funcionamiento del Web

La inseguridad en una aplicación Web es una propiedad emergente, resultado de la relación entre el programador y el administrador, la configuración del sitio Web y las herramientas utilizadas. Una combinación que se hace más explosiva con la impericia y la falta de cuidado de los usuarios finales que la utilizan. Con este último punto se quiere mostrar que, en el proceso de aseguramiento de las aplicaciones, el usuario hace parte fundamental de este proceso, pues en última instancia él es quien va a percibir el valor agregado de la confianza (fruto de una administración de la inseguridad) para el uso de las aplicaciones.

Ya en los años 90, con la explosión del uso del Web, los mecanismos de seguridad heredados de los años 80 no son tan efectivos como antes, porque ahora la interacción y el tráfico de datos

se hacen a través del protocolo http, o lo que es equivalente a decir por el puerto 80, que es un servicio que no es susceptible del filtrado natural de un fw, dado que es la manera como la organización navega y tiene acceso a los recursos de Internet. Esta realidad lleva a reconsiderar la aplicación de los proxies ahora como estrategias de acceso y protección de los servidores Web, que hoy llegan al primer plano de análisis.

La interacción y el tráfico de datos se hacen a través del protocolo http, o sea por el puerto 80.

Los *proxies* reversos, esos que son los intermediarios entre el agente externo y los recursos internos, se convierten en los guardianes de los servidores Web con las aplicaciones de las organizaciones. Estos servidores, configurados de esta forma, reciben la petición externa, validan su procedencia y reenvían el llamado http al servidor interno correspondiente, para que una vez procesada la respuesta por este último, sea retornada al proxy reverso y, de allí, al agente externo. Esta estrategia busca dejar menos expuestos los servidores con las aplicaciones Web disponibles, así como ofrecer una barrera adicional al intruso que intenta obtener acceso a los recursos privados de la organización.

Las palabras, entre otras, como cross-site scripting, Web spoofing, SQL Injection, Token analysis, session attacks, character encoding y generic input validation (mayor información en: http://www.webappsec.org/projects/threat/), se vuelven los referentes más nombrados para hablar de la inseguridad en el Web. Todas ellas requieren un análisis de las conexiones y relaciones que generan las aplicaciones, cuando materializan una petición de un usuario a través de una aplicación orientada al Web. En este sentido, las estrategias de seguridad y control se orientan hacia el servidor Web, la programación de las aplicaciones y las interacciones con las bases de datos, que ahora se vuelven más vulnerables, dadas las características de las limitaciones del protocolo http y la versatilidad requerida en las aplicaciones.

Si bien esta época de transformación y explotación del Web, a través del modelo de múltiples capas (interfaz del usuario, lógica del negocio o middleware y registro en bases de datos –backend) está llena de grandes logros y experiencias positivas, como el surgimiento y desarrollo de la banca en línea, también ha recibido

muchas advertencias sobre su futuro y desarrollo. Por un lado, esta desaforada carrera por llevar todo al Web, como estrategia para vincular a los usuarios al mundo de servicios digitales, ha hecho que los atacantes aprendan cada vez más y perciban mejor las interacciones de los usuarios y los riesgos de estas tecnologías, explotándolas en su favor y minando la confianza en estos servicios.

Se puede observar que si bien esta evolución de la seguridad especializa la detección y el análisis de la inseguridad, se involucran más variables de análisis, las cuales se hacen menos perceptibles, dadas las interacciones definidas entre los componentes de las aplicaciones, que muchas veces obedecen a rutinas propias de los lenguajes o de los programas residentes en los servidores Web. Pese a que esta tecnología nos abre la puerta a importantes avances, nos establece limitaciones que nuevamente son aprovechadas para proponer una nueva forma de comprender las interacciones en el Web y la conectividad de las aplicaciones.

Si bien la evolución de la seguridad especializa la detección y el análisis de la inseguridad, se involucran más variables de análisis.

3.2.4 Inseguridad orientada a los servicios

En la actualidad este cambio exige hablar de un concepto más abstracto, más portable y más modular. Este concepto basado en métodos, invocaciones y códigos encapsulados disponibles en servidores Web, denominado Web Services, abre la posibilidad de un nuevo momento de la seguridad. En este escenario la seguridad que se tenía en el modelo c/s no es funcional, pues los Web Services viajan exclusivamente por la vía del puerto 80 y el puerto 443, que por lo general no son filtrados por los firewalls. Hoy en día la inseguridad propia de este entorno, que es la extrapolación de las estrategias generales de amenazas como son la enumeración, la suplantación, la manipulación de código, el acceso y el monitoreo no autorizados, entre otras, se materializa en un ambiente de llamados a servicios, invocaciones y registros de servicios y acceso a los mismos, a través de protocolos como SOAP –Simple Object Access Protocol–, UDDI –Universal Discovery Description and Integration– y WSDL –Web Service Description Language (*gráfico 3.6*).

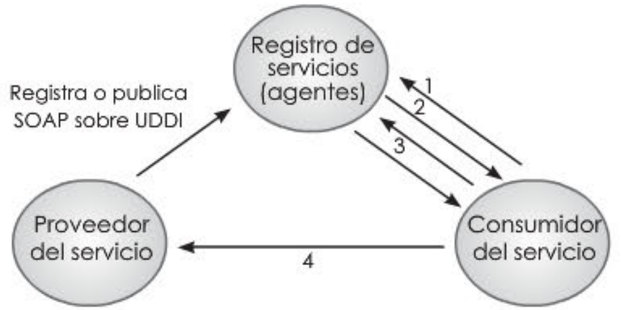


Gráfico 3.6

Interacción de un ambiente orientado a servicios

Estos protocolos usan en sus comunicaciones mensajes XML (Extensible MarkUp Language –mayor información en http://www.w3.org/TR/REC-xml/), los cuales a diferencia de los HTML –Hypertext MarkUp Language (propio del servicio Web) que buscan presentar la información al usuario, modelan los datos. Estos mensajes ahora se convierten en el nuevo "tráfico de red" que debemos entender, manejar y asegurar, para luchar contra la inseguridad en esta nueva evolución tecnológica. Los Web services son un importante paso para el desarrollo de una arquitectura donde se cuente con un bus de servicios, donde no sea necesario conocer el detalle de los mismos, solamente dónde se ubican y cómo se usan. De igual forma, estas nuevas ventajas serán aprovechadas por los intrusos, para poner a prueba las implementaciones y los desarrollos que sobre esta tecnología se definan.

Los Web services son un importante paso para desarrollar una arquitectura donde se cuente con un bus de servicios.

En este punto la pregunta es: ¿Y cuál es ahora la estrategia para luchar contra la inseguridad? Bien. Es necesario introducir dos nuevos

conceptos base para hablar de seguridad en un entorno de Web services: Web Application Firewall-WAF y XML-Content based –XML-C. Los WAF son la nueva cara de los firewalls nacidos en el modelo c/s, ahora orientados al análisis de vulnerabilidades y tráfico http de las aplicaciones, con el fin de limitar los accesos no autorizados a las aplicaciones y sus interacciones con los usuarios, otros programas y las bases de datos. Para aquellos interesados en revisar algunos criterios de evaluación de este nuevo tipo de cortafuegos para aplicaciones, se puede consultar el Web Application Firewall Evaluation Criteria (http://www.webappsec.org/projects/wafec/v1/wasc-wafec-v1.0.html), que ofrece un conjunto base de fundamentos sobre este concepto.

Es necesario desarrollar un módulo de análisis personalizado de las peticiones de los usuarios a los servicios y validar estos mismos.

De otra parte, el XML-C es el complemento del WAF. Mientras el WAF es una estrategia de evaluación de vulnerabilidades propias de las aplicaciones Web, el XML-C es el guardián del tráfico de mensajes entre las diferentes máquinas y servidores Web donde se encuentran los servicios, un vigilante que debe estar hecho a la medida de cada uno de los servicios y objetos registrados en el bus de servicios de la organización. Es decir, es necesario desarrollar un módulo de análisis personalizado de las peticiones de los usuarios a los servicios y validar estos mismos, más allá de las características de seguridad que se ofrecen vía WS-Security.

3.2.5 Evolución de la inseguridad informática

La ventana de exposición siempre estará abierta a nuevas posibilidades y mutaciones de las vulnerabilidades informáticas.

En este momento cuando nos movemos hacia la utilización masiva de Web Services, cabe preguntar: ¿Qué vendrá luego? La respuesta es: Con toda seguridad, algo mejor y de mayor versatilidad; algo que nos permitirá ver mayores integraciones entre lo expuesto en la red, con los sistemas inalámbricos y las estrategias corporativas. La convergencia tecnológica nos llevará a un escenario de tecnologías híbridas de uso cotidiano, donde mayores relaciones y productos estarán en

juego y el usuario será el mayor beneficiado. Sin embargo, siempre estará la ventana de exposición abierta a nuevas posibilidades y mutaciones de las vulnerabilidades informáticas, la generación de plagas electrónicas más adaptables y polimórficas, un escenario en donde la inseguridad sabrá mostrar por qué ella es parte inherente del desarrollo tecnológico, de las organizaciones y de las naciones (*gráfico 3.7*).

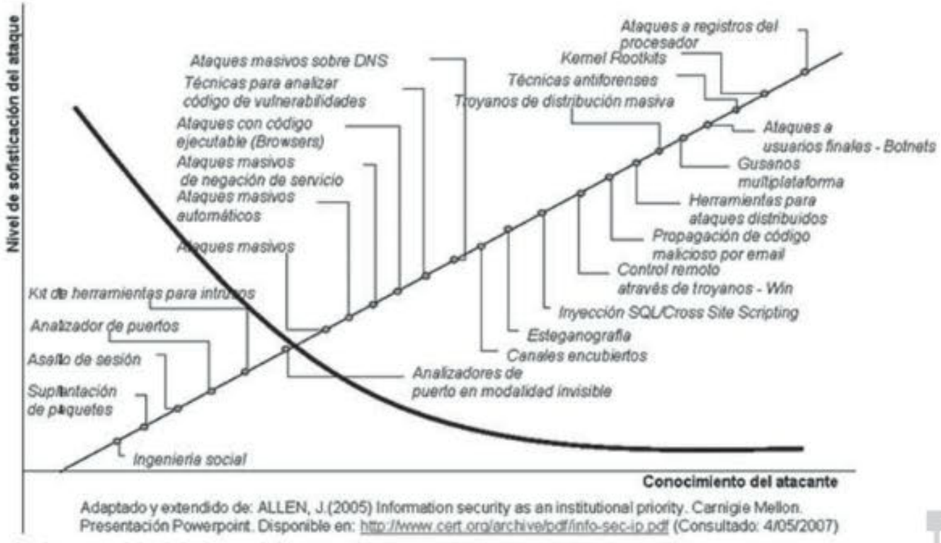


Gráfico 3.7

Evolución de la inseguridad informática

Considerando las diferentes evoluciones tecnológicas revisadas, así como la transformación de la seguridad de la información en cada entorno, es preciso que los investigadores forenses en informática profundicen cada vez más en las posibilidades que ofrece la tecnología y sus efectos de borde, así como las formas como los intrusos pueden aprovecharse de estas posibilidades, bien sea para evadir una investigación o para desviarla. De conformidad con la computación forense, la convergencia tecnológica es un riesgo que se advierte, pues en los puntos de contacto entre tecnologías frecuentemente existen pocos puntos de rastro vinculantes (para realizar la reconstrucción de los hechos), lo cual limita el accionar de los investigadores en este sentido. Si bien, la idea no es aumentar los niveles de registro y de control en un escenario de convergencia, sí lo es constituir alrededor

de las tecnologías de información los conceptos y procedimientos requeridos para lograr el gobierno, la administración de riesgos y el cumplimiento en este tema con un alcance corporativo.

3.3 TÉCNICAS BÁSICAS PARA EL DISEÑO Y LA GENERACIÓN DEL RASTRO

Como se presentó en la sección anterior, los registros de auditoría eran propios de los años 70, como una manera de reconocer qué actividades se habían desarrollado en el sistema. Durante esta época, los auditores de sistemas informáticos encontraban en esos registros la forma de validar o no las normas y los procedimientos que las organizaciones debían seguir con respecto al correcto uso de los sistemas de información.

Los registros de auditoría eran propios de los años 70, para reconocer qué actividades se habían desarrollado en el sistema.

Hoy, la realidad de unas aplicaciones más elaboradas y con alta integración con diferentes componentes, tanto de hardware como de software, nos exige ir más allá de los registros de auditoría y pensar en infraestructuras de computación que generen rastros ahora propios de esta nueva interactividad. Para eso, es necesario pensar en el diseño de la auditabilidad de los sistemas desde el diseño de las mismas, como un elemento formal dentro del desarrollo y la puesta en producción de los mismos.

Pensar en el diseño de las auditorías de un sistema, en el contexto actual, es pensar primero en las necesidades del negocio, las cuales son las que definen los puntos de control y rastro requeridos por la organización para probar o validar la existencia de una acción en el sistema.

Pensar en el diseño de las auditorías de un sistema es pensar primero en las necesidades del negocio.

Dentro de los principios de diseño de sistemas de seguimiento y control basado en aplicaciones, podemos detallar, entre otros, el control de errores propios de los componentes de las aplicaciones (servidor de

aplicaciones, servidores Web, protocolos de seguridad como ssl), los registros de excepción de las intercomunicaciones entre procesos, los catálogos de reglas de negocio y su cumplimiento, los registros de los mecanismos de seguridad de la información, los cuales establecen un cúmulo de información que está disponible para desentrañar los eventos que se suceden en el uso (autorizado o no) de las aplicaciones.

Iniciemos detallando el diseño de las estrategias de seguimiento y control basado en aplicaciones. Estos sistemas se determinan por una necesidad de negocio asociada con la noción de cumplimiento (en inglés *compliance*). Esta noción exige que la gerencia de la organización mantenga un estricto seguimiento de las actividades de negocio, cuidando el cumplimiento de las estrategias definidas con la alta gerencia y asegurando que los demás componentes de las mismas se comporten conforme lo requerido para lograr los objetivos.

Estos sistemas son generalmente alertas o indicadores de logro corporativo, inmersos en las aplicaciones y fruto de cruces de información generada por las diferentes áreas, que permiten a los directivos ver cómo sus proyecciones se van materializando o saliendo de curso, de acuerdo con lo planeado. Las aplicaciones de este estilo procesan continuamente los datos generados por otras aplicaciones para dar respuesta a los interrogantes que plantean los ejecutivos de la compañía frente a las consideraciones y planes de la organización. Las estrategias de seguimiento y control, basadas en aplicaciones, son implementaciones de alto nivel que generan un registro de actividades que debe ser confiable y suficiente para soportar las decisiones de la alta gerencia.

Las estrategias de seguimiento y control, basadas en aplicaciones, son elementos clave en la gestión de tecnologías de Información.

El control de errores en las aplicaciones es una práctica generalmente aceptada en el desarrollo de software; sin embargo, con frecuencia los desarrolladores y programadores no la consideran formalmente dentro de la construcción de las piezas de programación.

El control de errores permite acotar y registrar las fallas de los componentes del programa.

El control de errores permite acotar y registrar las fallas de los componentes del programa, para establecer las condiciones en las cuales se presentan las mismas. El no hacer este control abre la puerta a la incertidumbre de la confiabilidad de los programas diseñados, y la pérdida de confianza de la alta gerencia frente a la toma de decisiones.

El manejo de los errores es igualmente una manera de evitar que terceros se enteren y descubran detalles de la infraestructura de la organización, los cuales pueden ser utilizados para tomar ventaja de las fallas documentadas y no documentadas de la misma. Los errores son la fuente de aprendizaje del área de tecnología para descubrir y administrar la complejidad propia de las aplicaciones integradas y convergentes, pues mientras mayores sean las conexiones que se efectúen entre sistemas, más efectos inesperados se pueden presentar, bien sea por situaciones propias asociadas con el desconocimiento de la nueva conexión, por la falta de conocimiento profundo de las tecnologías utilizadas o por eventos inciertos que son propios de esta nueva integración.

Un registro del estado, las fallas y actividades de los procesos establece un paradigma de seguimiento dentro de las aplicaciones corporativas, denominadas el monitor de procesos.

Complementario a lo anterior, los registros de conexión entre procesos son una parte fundamental del control de las aplicaciones. Existen múltiples procesos que interactúan para darle la funcionalidad requerida al software aplicativo. En este sentido, tener un registro del estado, las fallas y actividades de los procesos, establece un paradigma de seguimiento dentro de las aplicaciones corporativas, que podemos denominar el monitor de procesos.

El monitor de procesos, al igual que en un sistema operacional, mantiene un registro en línea de las actividades y el estado de los procesos, sugiere acciones y alarmas que pueden advertir al operador del sistema o al usuario sobre las acciones que deben tomarse para ajustar lo que sea pertinente. Extrapolar el concepto que actualmente se implementa en los sistemas operativos al mundo de las aplicaciones, exige de los dueños de las aplicaciones repensar la auditabilidad de las aplicaciones más allá de los registros normales exigidos por el negocio,

hacia una actividad más elaborada, conceptualizada en el diseño de los aplicativos, una forma como el desarrollador ofrece a su cliente una manera de ver lo que ocurre entre la interfaz gráfica y la interacción con las bases de datos (*gráfico 3.8*).

Gráfico 3.8

Estructura base de la gestión de logs

Sin descuidar los registros tradicionales de actividades generados por los mecanismos de seguridad, es importante advertir que las propuestas de rastros reseñadas exigen una conciencia en el área de tecnología por el cumplimiento de sus mejores prácticas y la visibilidad real de la complejidad de las aplicaciones, en un tablero de control y seguimiento que le diga tanto al negocio como al área de tecnología que las piezas de software interactúan y generan valor, pero también fallas que esperan comprender mejor en este contexto, que sin él.

Las propuestas de rastros reseñadas exigen una conciencia en el área de tecnología.

Finalmente, el turno de los registros propios de los mecanismos de seguridad de la información son la evidencia real de que existe o no un intento de acceso o uso de un recurso en una aplicación o un servidor. Al igual que los años 70, los detalles de cómo se configuran y detallan son propios de cada proveedor y práctica empresarial, pero lo importante con ellos es que deben desarrollar al menos las características siguientes: disponibilidad, integridad y control de acceso, para que las conclusiones que de ellos se obtengan sean pertinentes, conducentes y relevantes para los propósitos de las investigaciones que se adelanten.

3.4 AUDITABILIDAD Y TRAZABILIDAD

3.4.1 Auditabilidad

La computación ha sugerido novedosas formas de enfrentar la complejidad de las organizaciones y hacer sus procesos más eficientes.

Desde sus inicios, la computación ha sugerido novedosas formas de enfrentar la complejidad de las organizaciones y hacer sus procesos más eficientes. De igual forma, la capacidad de cómputo y las facilidades que ésta brinda han sido (y seguirán siendo) fuente de estrategias para vulnerar o para socavar los sistemas de información.

No se requiere mucho conocimiento tecnológico para sobrepasar posibles controles o limitaciones de los sistemas informáticos.

No se requiere mucho conocimiento tecnológico para sobrepasar posibles controles o limitaciones de los sistemas informáticos. Pero de manera contraria, se podría sugerir que se requiere contar con un detalle importante del sistema para tener acceso o manipular los registros de eventos del sistema o los denominados logs (término tomado del inglés, relacionado con la acción de logging o registro de operaciones o acciones de los sistemas de información), o registros de auditoría, dado que generalmente éstos están asociados con uso de permisos y accesos por parte de los usuarios (aunque para los realmente intrusos no es una limitación, sino un reto).

En este sentido, podemos establecer la auditabilidad como aquella propiedad de todo sistema o tecnología de información para registrar, de manera clara, completa y efectiva, los eventos de una acción en particular con el propósito de:

- Mantener la historia de los eventos
- Realizar el seguimiento y el control de los mismos.

Entendiendo la claridad como la correcta lectura y uso del formato en el que se registran los hechos auditados; la completitud, como el conjunto de variables requeridas para identificar las acciones particulares de los usuarios y la efectividad, como el registro real y correcto de los eventos en los archivos o los dispositivos previstos para el almacenamiento de los mismos.

Los registros de auditoría, dependiendo de la estrategia que se utilice, pueden estar a la vista del usuario o ubicados de manera especial en el sistema de archivos con controles de acceso a los mismos. Los logs (Weber 1999) representan la historia y la evolución de los sistemas de información, son la memoria vigente del sistema operacional, del hardware o de la aplicación o las aplicaciones, que le permite tanto al programador como a la organización conocer el comportamiento de éstos, así como la interacción de los usuarios en el desarrollo de sus funciones.

Los registros de auditoría hacen parte de la historia del sistema mismo.

Sin embargo, es común encontrar que si se pregunta sobre los registros de auditoría, bien sea de las aplicaciones o el sistema operacional, se encuentra que éstos sólo se revisan o se observan cuando existe una falla. Luego, si previamente no hemos visto el registro e identificado qué es un comportamiento normal allí, ¿cómo vamos a identificar lo anormal? Así mismo, cuando la falla se manifiesta, ¿cómo sabemos qué puede estar pasando si no hemos mirado cómo el sistema registra sus acciones normales? O, como muchas veces no sabemos, ¿cómo está diseñado el registro de auditoría? O, lo que es más grave, existen múltiples formatos de logs que pueden tener mayor o menor detalle sobre lo ocurrido en el sistema, lo que puede ocasionar conceptos o diagnósticos incompletos.

Todas las preguntas anteriores nos advierten que mucha parte de la evidencia que se tiene sobre posibles actividades, no autorizadas o autorizadas, puede estar comprometida, por falta de controles sobre las mismas, por falta de conciencia de los administradores o de los encargados de los sistemas de información, o sencillamente por el conocimiento limitado y la capacidad de análisis de estos registros.

En razón de lo anterior, pese a que se cuente con estrategias de registro antes de, después de y de transacción o de operación del dispositivo (hardware o software), el solo registro no asegura que se vaya a contar con elementos suficientes de evidencia para determinar la veracidad de las posibles acciones no autorizadas o autorizadas. Por

El registro detallado de las organizaciones se debe complementar con una estrategia corporativa que permita administrar los logs: la Gestión de logs (Gelogs).

tanto, el registro detallado y formal de las organizaciones se debe complementar con una estrategia corporativa que permita una administración de los logs: la Gestión de logs (Gelogs).

La Gestión de logs implica reconocer en los registros de auditoría una herramienta gerencial que le permita a la organización valorar sus activos y los recursos utilizados, así como una manera de mantener la memoria del comportamiento de los dispositivos o las aplicaciones, atendiendo a los principios fundamentales de la seguridad informática: confidencialidad, integridad y disponibilidad (*gráfico 3.9*).

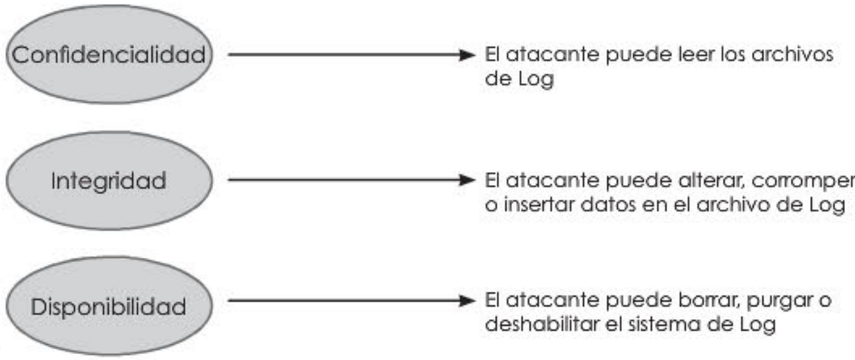


Gráfico 3.9

Ataques a los logs o registros de auditoría

Este concepto, que si bien no es nuevo en las organizaciones, pues constantemente éstas desarrollan ejercicios de seguimiento y gestión sobre sus actividades del negocio, busca llamar la atención sobre la función de la tecnología y la responsabilidad de contar con una adecuada estrategia de Gelogs, que le permita tanto al encargado de esa función como a la organización contar con una manera clara de recuperar, revisar y analizar la evolución del sistema (hardware o software).

La Gelogs es una manera de reconocer la importancia del registro de auditoría, no por su registro en sí mismo que es importante, sino por las implicaciones de análisis y la toma de decisiones que de él se desprenden. Por ejemplo, se puede considerar un incremento de capacidad de cómputo o de memoria

de un servidor, dado que el análisis de registros de log muestra que sistemáticamente, pese a los ajustes de rendimiento efectuados por el administrador, el software o el hardware no presentan los niveles de servicio requeridos. Por otra parte, si se presenta un incidente de seguridad o un intento no autorizado en la aplicación o el dispositivo, y se cuenta con una adecuada Gelogs, se puede contar con una estadística previa de comportamiento del sistema que sugiere elementos de análisis puntales y focalizados, sin perder tiempo valioso de investigación tratando de identificar qué podría haber pasado.

En razón de lo anterior, el contar con registros de auditoría en los dispositivos o las aplicaciones es un factor clave para mantener la historia del sistema, pero sin una Gelogs solamente es un conjunto de datos de eventos (posiblemente no relacionados) que se almacenan "por si son necesarios", y no lo que realmente representan, material de análisis y orientación para la gerencia en temas de arquitectura tecnológica y posible carga probatoria ante eventos que atenten contra la seguridad informática.

En este sentido, una Gelogs debería desarrollar proyectos que busquen adecuar las arquitecturas de cómputo actuales para mantener un registro centralizado, asegurado y correlacionado de los eventos (Cano 2003), que son de interés para la organización, con el fin de preparar a las organizaciones para enfrentar situaciones adversas o procesos legales que se presenten en un futuro. Sin una adecuada Gelogs, las organizaciones estarán limitadas para contar con elementos suficientes para validar o verificar sucesos en sus sistemas, pues, entre otros interrogantes, la duda sobre la integridad de los mismos podrá ser cuestionada y resuelta a favor del posible intruso.

Sin una adecuada Gelogs, no habra espacios para validar o verificar sucesos en los sistemas de información.

Finalmente, los logs, generalmente tratados como archivos de "segunda", poco consultados por los administradores y/o usuarios, están esperando su oportunidad para incorporarse dentro de las actividades formales de las áreas de tecnología, no como una carga más de la función de tecnología, sino como parte fundamental de la atención de incidentes de seguridad (Cano 2002).

3.4.2 Trazabilidad

La trazabilidad implica revisar definiciones y reflexiones previamente establecidas alrededor de la auditoría de las tecnologías de información (TI).

Establecer que significa la *trazabilidad*, implica revisar definiciones y reflexiones que previamente se han establecido alrededor de la auditoría de las tecnologías de información (TI). Si bien el registro de las operaciones electrónicas es un factor fundamental en los procesos de las organizaciones, la reconstrucción de eventos obedece tanto a la formalidad de los registros de auditoría, como a las características técnicas y administrativas que las organizaciones deben adoptar si quieren contar con estrategias y escenarios para rastrear situaciones particulares. Por reconstrucción de eventos se entiende la asociación que pueda existir entre las transacciones de una aplicación o un sistema, teniendo en consideración sus posibles interfaces.

Trazabilidad es la capacidad de una organización o un sistema para rastrear, reconstruir o establecer relaciones entre objetos monitoreados, a fin de identificar y analizar situaciones específicas en estos mismos.

Trazabilidad es la *capacidad* que tiene una organización o un sistema para *rastrear, reconstruir o establecer* relaciones entre *objetos monitoreados*, para identificar y analizar situaciones específicas o generales en los mismos[1]. Para aclarar esta definición se procede a profundizar en las palabras en itálica o cursiva, brindándole un sentido práctico de aplicación que será revisado más adelante en el documento.

- *Capacidad:* Esta palabra sugiere la definición de acciones y estrategias específicas por parte de la organización o el sistema que permita, bajo lineamientos establecidos, desarrollar una actividad específica.
- *Rastrear, reconstruir o establecer:* Este conjunto de verbos hacen referencia a la esencia misma del concepto que especifican. Son las acciones que se busca efectuar cuando de trazabilidad se habla.

[1] Definición adaptada de: *IEEE Standard Computer Dictionary: A compilation of IEEE Standard Computer Glossaries*. New York, 1990

- *Objetos monitoreados:* La trazabilidad sin una adecuada definición de pistas de auditoría no logra alcanzar sus objetivos *(rastrear, reconstruir o establecer)*. El monitoreo es un prerrequisito para darle sentido a la trazabilidad como capacidad en un sistema. Es importante aclarar que es posible no tener monitoreo definido formalmente, pero sí tener registros propios de los sistemas o procesos que pueden ser útiles para rastrear, reconstruir o establecer relaciones. Así mismo, es fundamental la capacidad de relacionar esa información de auditoría, entre los diversos niveles y componentes de una infraestructura informática. Estas relaciones se establecen siempre y cuando los registros de auditoría generados y la arquitectura de cómputo se adhieran a las características básicas descritas más adelante.

Niveles de trazabilidad

Es importante aclarar que la trazabilidad exige algunas características básicas en la infraestructura para lograr "rastrear, reconstruir o establecer", como lo son (Cano 2002)[2]:

- Sincronización
- Control y aseguramiento de registros de monitoreo
- Confiabilidad de la generación de registros de monitoreo

Es necesario establecer una clasificación básica para la trazabilidad en las infraestructuras corporativas.

Con base en estas características presentadas, es necesario establecer una clasificación básica para la trazabilidad en las infraestructuras corporativas de acuerdo con el nivel de importancia y criticidad en el cumplimiento de su misión (*ver cuadro 3.2*).

[2] *Sincronización:* Esta característica requiere que la arquitectura presente unos mecanismos de tiempo centralizado que sean utilizados por las máquinas que soportar las aplicaciones.
Control y aseguramiento de registros de monitoreo: Esta característica exige que los registros de monitoreo están configurados de tal manera que se conozca dónde se generan, quién tiene acceso a ellos y si ocurren cambios, queden documentados con fecha, hora y responsable. Esto permitiría además el uso de esta información como sustento legal en caso de requerirse.
Confiabilidad de la generación de registros de monitoreo: Este elemento hace referencia a la efectividad y eficiencia de las características del registro de eventos (logs de auditoría) en los sistemas de información. Es decir, verificar que el registro de los eventos realizados está conforme a la definición de monitoreo establecida para el sistema de información.
Este documento fue realizado en el contexto del curso Introducción a la Informática Forense, bajo la supervisión del Profesor Jeimy J. Cano, Ph.D. FCE.

Características requeridas				
Nivel de trazabilidad	Definición de pistas de autoría	Confiabilidad en la generación de los registros de monitoreo	Control y aseguramiento de los registros de monitoreo	Sincronización de la arquitectura de computo
ALTA	X	X	X	X
MEDIA	X	X	X	
BAJA	X	X		

Cuadro 3.2

Propuesta de niveles de trazabilidad

El nivel de trazabilidad alta se asocia con la necesidad que tiene la organización de crear, almacenar y recuperar información confiable.

El nivel de *trazabilidad alta* está asociado con la necesidad que tiene la organización de crear, almacenar y recuperar información confiable que sea reconocida como evidencia digital válida en cualquier proceso judicial que se adelante alrededor de las aplicaciones que requieran este nivel. Contar con este nivel de trazabilidad exige que la organización mantenga un conjunto de prácticas organizacionales alrededor de la definición y el control de registros de auditoría, como base fundamental para fortalecer los esquemas probatorios a futuro, los cuales deben estar fundados en las directrices de seguridad de la información de la organización.

El nivel de *trazabilidad media* está relacionado con el requisito de las organizaciones por mantener evidencia de las acciones realizadas por usuarios, o por procesos en el uso de los sistemas de información y las posibles relaciones entre ellos. Si bien esta información se puede requerir para procesos de investigación interna de las empresas, hay que considerar que la sincronización no es un requisito formal de la misma. Es decir, la generación de registros de auditoría no está asociada a un sistema centralizado de tiempo que verifique la hora y la fecha de su creación. Se confía en el manejo del tiempo interno para los dispositivos de hardware o de software. Los registros generados con nivel de trazabilidad media obedecen a políticas y formalidades establecidas por la organización.

El aplicar un nivel de *trazabilidad baja* es una decisión que toma una organización consciente de que los registros de los eventos en los sistemas no requieren mayores exigencias, más allá del debido registro de las acciones de los usuarios para efectos de estadísticas y proyecciones de uso. Los registros generados o las relaciones establecidas bajo este nivel no pueden ser considerados evidencia confiable de hechos acontecidos.

El aplicar un nivel de trazabilidad baja es una decisión que toma una organización consciente de que los registros de los eventos en los sistemas no requieren mayores exigencias.

Es importante tener en cuenta que el nivel de detalle que alcance la investigación está asociado con el nivel de granularidad definido para las pistas de auditoría del sistema investigado. Es decir, mientras el diseño de las pistas de auditoría no responda una definición formal de lo que se requiere registrar para revisión posterior, los resultados de la investigación podrían resultar menos detallados o inclusive inconclusos.

3.5 CONSIDERACIONES JURÍDICAS Y ASPECTOS DE LOS RASTROS EN LAS PLATAFORMAS TECNOLÓGICAS

Si bien los rastros o las evidencias electrónicas son cada vez más invisibles en las infraestructuras de cómputo, también es un hecho que los procesos legales y los procedimientos judiciales no cuentan con la experiencia y la técnicas jurídicas requeridas para armonizar las actuaciones y sentencias de los jueces. En esta encrucijada se hace necesario un "pare y reflexione" que invite a todas las partes para buscar propuestas interdisciplinarias que permitan comprender las diferentes variables de un fenómeno que no es exclusivamente jurídico, ni técnico, ni procedimental, ni gubernamental, sino sistémico: el delito informático.

La evidencia digital, representada en todas las formas de registro magnético u óptico generadas por las organizaciones, debe avanzar hacia una estrategia de formalización que ofrezca un cuerpo formal de evaluación y análisis que deba ser observado por el ordenamiento judicial de un país. En general, las legislaciones y las instituciones judiciales han fundado sus reflexiones sobre la

La evidencia digital debe avanzar hacia una estrategia de formalización.

admisibilidad de la evidencia en cuatro (4) conceptos (Sommer, P. 1995, Ioce 2000, Casey 2001, cap. 6):

1. Autenticidad
2. Confiabilidad
3. Completitud[3] o suficiencia
4. Conformidad con las leyes y regulaciones de la administración de justicia

A continuación revisamos brevemente cada uno de ellos, analizando estrategias de implementación técnica que sugieran el cumplimiento de la característica legal planteada en medios digitales (*gráfico 3.10*).

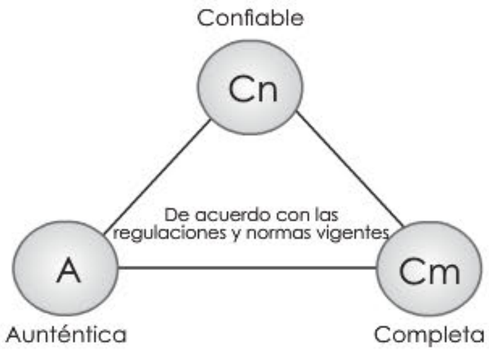


Gráfico 3.10

Características legales de la evidencia

3.5.1. Autenticidad

La autenticidad de la evidencia sugiere ilustrar a las partes de que esa evidencia se ha generado y registrado en los lugares o los sitios relacionados con el caso.

La autenticidad de la evidencia nos sugiere ilustrar a las partes de que esa evidencia ha sido generada y registrada en los lugares o los sitios relacionados con el caso, particularmente en la escena del posible ilícito, o en los lugares establecidos en la diligencia de levantamiento de evidencia. Así mismo, la autenticidad, entendida como aquella característica que muestra la no alterabilidad de los medios originales, busca confirmar que los registros aportados corresponden a la realidad identificada en la fase de identificación y recolección de evidencia.

[3] Por este término se entiende la compleción o suficiencia, para hacer referencia a que se aportan todas las evidencias pertinentes al caso. (N. del E.)

En medios no digitales, la autenticidad de las pruebas aportadas no será refutada, de acuerdo por lo dispuesto por el artículo 11 de la Ley 446 de 1998: "Autenticidad de los documentos. En todos los procesos, los documentos privados presentados por las partes para ser incorporados a un expediente judicial con fines probatorios, se reputarán auténticos, sin necesidad de presentación personal ni autenticación. Todo ello sin perjuicio de lo dispuesto en relación con los documentos creados por terceros". En este sentido, todas las pruebas que se aporten por las partes se entenderán como válidas y sólo vía una demostración de hecho y científica podrán ser refutadas.

En los medios digitales resulta complicado aplicar lo expuesto en el párrafo anterior, dada la volatilidad y la alta capacidad de manipulación que se presenta en los medios de almacenamiento electrónico. Si bien éstas características también son de alguna manera inherentes a los medios tradicionales, el detalle se encuentra en que existe una serie de procedimientos asociados con el manejo y el control de los mismos en las organizaciones, mientras que para los registros magnéticos aún no se tiene con la misma formalidad.

Para algunos casos "sirven como pruebas la declaración de la parte, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez", los archivos digitales podrían verse involucrados dado que harían parte de "otros medios" presentados para aportar al caso en estudio, pero la forma como sean identificados, generados y recogidos puede influir en la manera como sean valorados por la corte.

En este sentido, verificar la autenticidad de los registros digitales requiere, de manera complementaria a la directriz general establecida por la organización sobre éstos registros, el desarrollo y la configuración de mecanismos de control de integridad de archivos. Es decir, al satisfacer la característica de autenticidad se requiere una infraestructura tecnológica que exhiba mecanismos que aseguren la integridad de los archivos y el control de cambios en los mismos.

Para verificar la autenticidad de los registros digitales se requiere desarrollar y configurar mecanismos de control de integridad de archivos.

Luego, al establecer una arquitectura de cómputo donde se fortalezca la protección de los medios digitales de registro y el procedimiento asociado para su verificación, aumentan sustancialmente la autenticidad y la veracidad de las pruebas recolectadas y aportadas. En consecuencia, la información que se identifique en una infraestructura con estas características tendrá mayor fuerza y solidez, no sólo por lo que su contenido ofrezca, sino por las condiciones de generación, control y revisión de los registros electrónicos.

Con mecanismos y procedimientos de control de integridad se disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada.

O sea, al contar con mecanismos y procedimientos de control de integridad se disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada, y el proceso se concentra en los hechos y no en errores técnicos de control de la evidencia digital bajo análisis.

3.5.2 Confiabilidad

De otro lado, la confiabilidad de la evidencia es otro factor relevante para asegurar la admisibilidad de la misma. La confiabilidad nos dice si efectivamente los elementos probatorios aportados provienen de fuentes que son creíbles y verificables, y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue.

En medios digitales, podríamos relacionar el concepto de confiabilidad con la configuración de la infraestructura de computación. ¿Cómo se diseñó la estrategia de registro? ¿Cómo se diseñó su almacenamiento? ¿Cómo se protegen? ¿Cómo se registran y se sincronizan? ¿Cómo se recogen y analizan? Éstas son preguntas cuyas respuestas buscan demostrar que los registros electrónicos poseen una manera confiable para ser identificados, recolectados y verificados.

Cuando logramos que una infraestructura tecnológica ofrezca mecanismos de sincronización de eventos y una centralización de registros de sus actividades, los cuales, de manera complementaria, soportan estrategias de control de integridad, hemos avanzado en la formalización de la confiabilidad de la evidencia digital. Así mismo, en el desarrollo de software o el diseño de programas es necesario incluir, desde las primeras fases de la creación de aplicaciones, un momento para la configuración de los registros de auditoría del sistema, ya que,

de no hacerlo, se corre el riesgo de perder la trazabilidad de las acciones de los usuarios en el sistema y, por tanto, crear un terreno fértil para la ocurrencia de acciones no autorizadas y la pérdida de capacidad probatoria posterior.

Es decir, se sugiere que la confiabilidad de la evidencia en una infraestructura tecnológica estará en función de la manera como se sincronice el registro de las acciones de los usuarios, y de un registro centralizado e íntegro de los mismos. Todo eso reitera la necesidad de un control de integridad de los registros del sistema, para mantener la autenticidad de los mismos.

Se sugiere que la confiabilidad de la evidencia en una infraestructura tecnológica esté en función de la manera como se sincronice el registro de las acciones de los usuarios

3.5.3 Suficiencia

La completitud o la suficiencia de la evidencia o, más bien, la presencia de toda la evidencia necesaria para adelantar el caso, es una característica que, al igual que las anteriores, es factor crítico de éxito en las investigaciones adelantadas en procesos judiciales. Frecuentemente la falta de pruebas o la insuficiencia de elementos probatorios ocasionan la dilación o la terminación de procesos que podrían haberse resuelto. En este sentido, los abogados reconocen que mientras mayores fuentes de análisis y pruebas se tengan, habrá más posibilidades de avanzar en la defensa o en la acusación en un proceso judicial.

La falta de pruebas o la insuficiencia de elementos probatorios ocasionan la dilación o la terminación de procesos que podrían haberse resuelto.

Desarrollar estas características en infraestructuras de tecnología requiere afianzar y manejar destrezas de correlación de eventos en registros de auditoría. Es decir, contando con una infraestructura y unos mecanismos de integridad, sincronización y centralización, se pueden establecer patrones de análisis que muestren la imagen completa de la situación bajo revisión.

La correlación de eventos, definida como el establecimiento de relaciones coherentes y consistentes entre diferentes fuentes de datos,

para establecer y conocer eventos ocurridos en una infraestructura o en unos procesos, sugiere una manera de probar y verificar la suficiencia de los datos entregados en un juicio. Si analizamos esta posibilidad, es viable establecer relaciones entre los datos y eventos presentados, canalizando las inquietudes y afirmaciones de las partes sobre comportamientos y acciones de los involucrados, sustentando esas relaciones con hechos o con registros que previamente han sido asegurados y sincronizados.

Con esto en mente, la correlación se convierte en factor aglutinante de las características anteriores referenciadas para integridad y confiabilidad de la evidencia, sugiriendo un panorama básico requerido en las infraestructuras de cómputo para validar las condiciones solicitadas por la ley en relación con la evidencia.

Es decir, la correlación de eventos, como una función entre la centralización del registro de eventos y el debido control de integridad de los mismos, se soporta en una sincronización formal de tiempo y eventos que deben estar disponibles en la infraestructura de cómputo, para asegurar la suficiencia del análisis de la información presente en ella.

3.5.4 Conformidad con las leyes y las regulaciones de la administración de la justicia

La conformidad de las leyes y regulaciones de la administración de justicia se refiere a los procedimientos aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital.

Finalmente, lo relacionado con la conformidad de las leyes y regulaciones de la administración de justicia hace referencia a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien en los códigos de procedimiento civil y penal se han previsto las actividades mínimas requeridas para aportar evidencia a los procesos, en medios digitales existen iniciativas internacionales como las de la IOCE (International Organization of Computer Evidence (2002)), la Convención de Cibercrimen presentada por la Comunidad Europea, el Digital Forensic Research Workshop, HB-171 2003 Management of IT Evidence –Australia Standards, British Standard Institute–, Code of practice for legal admissibility and evidential weight

of information stored electronically, entre otros, donde se establecen lineamientos de acción y parámetros que cobijan el tratamiento de la evidencia en medios electrónicos, los cuales deben ser revisados y analizados en cada uno de los contextos nacionales para su posible incorporación.

Cuando se tiene acceso a evidencia digital por medios no autorizados, y no existen medios para probar su autenticidad, confiabilidad y suficiencia, los elementos aportados carecerán de la validez requerida y podrán ser tachados de falsos. Esta evidencia, obtenida de este modo, no ofrece maneras para comprobar las posibles hipótesis que sobre el caso se hayan efectuado, dadas las irregularidades que enmarcan su presentación.

Resumen

La administración de una infraestructura de tecnologías de información no puede pasar inadvertida en el contexto de la gerencia de tecnologías actual. Pese a que en el pasado el administrador estaba acotado por las precisiones de los proveedores de los sistemas informáticos, hoy la realidad es muy diferente. El administrador de un sistema no sólo debe conocer de la configuración del objeto que maneja y coordina, sino que debe entender las relaciones y la dinámica que ese objeto exhibe en el contexto de la dinámica de negocio.

En este sentido, la seguridad de la información, en el sistema que se administra, debe ser el resultado de una serie de actividades previamente planeadas y diseñadas, con el fin de mantener limitados los efectos de borde en la infraestructura gestionada. Si bien estas acciones que el administrador adelante no serán completamente efectivas, dada la presencia de los riesgos propios de los objetos tecnológicos, sí deberán contar con procesos y procedimientos que les permitan una posición proactiva frente a fallas en la continuidad y la denegación de servicio que el sistema pudiese presentar en el desarrollo normal de sus funciones.

Considerando lo anterior y sabiendo que una falla puede ocurrir en cualquier momento, bien sea por razones propias de la infraestructura tecnológica o por intentos no autorizados de intrusos, el administrador debe establecer aquellos puntos del

sistema que son susceptibles de vulnerabilidades, y tratar de contar con registros de auditoría y control que puedan ser utilizados para comprender mejor las mismas.

Esos registros de auditoría y control requieren características propias para mejorar la confiabilidad de los mismos, y así los análisis que sobre ellos se adelanten sean consistentes y coherentes con las situaciones que los han generado. El control de integridad, la sincronización y el control de acceso a estos archivos son características básicas que esos registros deben tener, pues, de no ser así, la probabilidad de manipulación y distorsión de la información será parte de la duda razonable que rodee la presentación de los mismos.

La auditabilidad y la trazabilidad son dos características que los sistemas de información y las infraestructuras de tecnología deben tener frente a un ambiente altamente interconectado y de negocios electrónicos, entre múltiples participantes. En este contexto, contar con los rastros y las evidencias de las transacciones se convierte en un factor fundamental para animar la confianza de los clientes y el correcto registro de las operaciones, para poder reconstruir en cualquier momento, de manera parcial o total, todas las actividades realizadas por los usuarios.

Estudiando las responsabilidades y los procedimientos que debe atender el administrador del sistema, el investigador forense en informática debe establecer el conjunto de buenas prácticas de seguridad y control, de atención de incidentes y manejo de crisis, las cuales le indicarán elementos de análisis en el desarrollo de una investigación y una orientación sobre las evidencias que puede recabar del hecho analizado.

Preguntas y ejercicios

Esta sección busca reforzar los elementos conceptuales presentados en este capítulo; para eso le sugerimos al lector revisar sus reflexiones y anotaciones para plantear respuestas a los interrogantes propuestos en esta sección.

1. ¿Existe actualmente consenso sobre cuál debe ser la descripción del cargo de una persona como administrador de un sistema?

2. ¿Para qué sirven un firewall y un sistema de detección de intrusos? ¿Ambos son lo mismo o complementarios?
3. Si un registro de auditoría en sus fechas de creación no coincide con la fecha registrada por el sistema, ¿puede sugerirse que el archivo ha sido alterado?
4. ¿Todo sistema de información que es auditable, es trazable?
5. ¿Cuáles son las características que se requieren para que un registro o log de auditoría sea admisible en un proceso jurídico?
6. Si fuese a diseñar un registro de auditoría, ¿cuáles son los datos mínimos que usted considera deben estar registrados en este archivo?
7. ¿Cómo debería actuar un administrador del sistema, cuando ocurre un incidente de seguridad en sus dominios?

Apéndice

Para profundizar

Los IDS y los IPS: Una comparación práctica

Córdoba Jonathan, Laverde Ricardo, Ortiz Diego, Puentes Diana

Debido al carácter interdependiente entre la información y la tecnología en las organizaciones actuales y la criticidad de la fidelidad, integridad, disponibilidad y confidencialidad de la información, han surgido y evolucionado técnicas que permiten acceder a dicha información de manera ilegítima por medio de la explotación de vulnerabilidades o debilidades de las plataformas tecnológicas.

En respuesta a lo anterior, nacieron y se han desarrollado arquitecturas, técnicas y sistemas (en particular los IDS y los IPS) en pos de detectar y prevenir el acceso indebido a la información organizacional, asegurando de este modo los atributos de la información recién mencionados.

Históricamente los IDS surgen antes que los IPS, con la función principal de detectar situaciones anómalas y usos indebidos de los recursos y servicios de la infraestructura tecnológica. Como consecuencia de la dificultad para reaccionar oportunamente a las alertas de intrusión generadas por los IDS, nacen los IPS que se encargan de reaccionar proactivamente a las intrusiones detectadas por el IDS tan pronto se identifican.

Con el fin de caracterizar las diferencias entre los IDS y los IPS, Para profundizar los compara desde una perspectiva teórica y práctica en un ambiente controlado de pruebas.

1. IDS: SISTEMAS DE DETECCIÓN DE INTRUSOS (Intrusion Detection Systems)

A. *Definición*

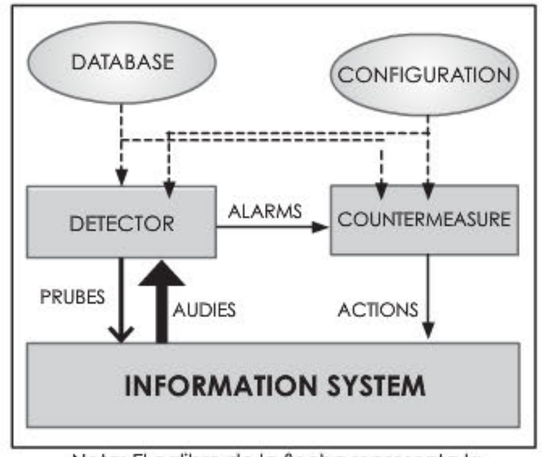
La detección de intrusos consiste en un conjunto de métodos y técnicas para revelar la actividad sospechosa sobre un recurso o conjunto de recursos computacionales. Es decir, eventos que sugieran comportamientos anómalos, incorrectos o inapropiados sobre un sistema (D. Lehmann); entendido como el ente que está siendo monitoreado (v. gr., estación de trabajo, dispositivos de red, servidores, firewalls, etc.).

B. *Descripción*

Un IDS puede ser descrito como un detector que procesa la información proveniente del sistema monitoreado. Es una herramienta de apoyo en procesos de auditoría, entendida como el control del funcionamiento de un sistema a través del análisis de su comportamiento interno (H. ºDebar) como se ilustra en el gráfico A3.1.

Para detectar intrusiones en un sistema, los IDS utilizan tres tipos de información: la recopilada tiempo atrás que tiene datos de ataques previos, la configuración

actual del sistema y finalmente la descripción del estado actual en términos de comunicación y procesos (H. ºDebar) (*gráfico A3.1*).



Nota: El calibre de la flecha representa la catidad de información que fluye desde un componente hasta el otro.

Gráfico A3.1

Un sistema de detección de instrusos simplificado. (H. ºDebar)

C. *Criterios de evaluación de los IDS*

Para definir la bondad de un IDS existen varios criterios. Según P. Porras y A. Valdés (marzo 1998), hay tres criterios para evaluar esta clase de sistemas: la precisión, el rendimiento y la completitud.

La *precisión* tiene que ver con la efectividad de la detección y la ausencia de falsas alarmas.

Por otra parte, el *rendimiento* de un IDS es la tasa de eventos procesados por unidad de tiempo; lo ideal es que el IDS reconozca los ataques en tiempo real.

Finalmente, la *completitud* es la capacidad del IDS para detectar la mayor cantidad de ataques posibles.

Aparte de los anteriores, H. ºDebar menciona otros dos criterios: tolerancia a fallas y rapidez. El IDS es *tolerante a fallas* si es inmune a ataques que comprometan la fiabilidad y la integridad de los análisis y es rápido si tiene la capacidad de informar en el menor tiempo posible una intrusión, lo cual implica realizar todas las actividades de análisis precedentes en tiempo real.

Por su parte, Axelsson (S. Axelsson (Mayo 20 de 1999)) reconoce como criterios de bondad la interoperabilidad (capacidad que tiene el IDS

para comunicarse y operar con otros IDS), y la facilidad de uso (el nivel de claridad que ofrece el IDS a los usuarios para su administración y análisis de alarmas).

Adicionalmente existen los siguientes indicadores estadísticos que permiten cuantificar la bondad del IDS, como se muestra en el *gráfico A3.2*.

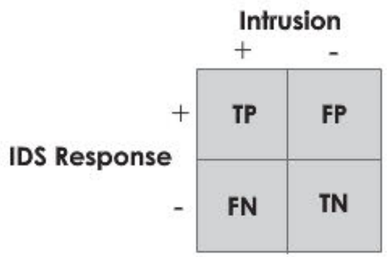


Gráfico A3.2

Cuantificación estadística de los IDS. (Chuvakin y C. P.)

Tales indicadores (sensibilidad, especificidad y precisión) se basan en los conceptos siguientes:

- *Verdaderos positivos (TP):* Intrusión existente y correctamente detectada.
- *Falsos positivos (FP):* Intrusión no existente e incorrectamente detectada.
- *Falsos negativos (FN):* Intrusión existente y no detectada.
- *Verdaderos negativos (TN):* Intrusión no existente y no detectada

A partir de los anteriores conceptos, los indicadores se definen como:

- Sensibilidad= (#TP/(#TP+#FN)). Mide la efectividad de las detecciones cuando existe alguna intrusión.
- Especificidad= (#TN/(#TN+#FP)). Mide la efectividad de las detecciones cuando no existe intrusión.
- Precisión= (#TP+#TN)/(#TP+#TN+#FP+#FN).Mide la efectividad de las detecciones cuando existe o no existe intrusión.

D. *Taxonomía*

La clasificación de los IDS puede guiarse por la metodología empleada (firmas o anomalías), o por las características inherentes al sistema, como se detalla a continuación.

1.1 Clasificación por la metodología empleada

(*Ver cuadro A3.1*) (S. Axelsson (Mayo 20 de 1999); R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash (2004)).

Anomaly	**Self - learning**	non time series
		time series
	Programmed	descriptive stat
		default derry
Signature	**Programmed**	state - modeling
		expert - system
		string - matching
		simple rule - based
Signature Inspired	**Self - learning**	automatic feature set

Cuadro A3.1

Clasificación de principios de detección
(P. Porras y A. Valdés (Marzo 1998))

En primer lugar, se tiene la *detección de anomalías* que consiste en analizar la información del sistema monitoreado, en busca de cualquier anormalidad; es decir, una señal característica de ataque. Para determinar la normalidad o anormalidad en el comportamiento en un sistema (fase de entrenamiento), existen dos aproximaciones: los sistemas de autoaprendizaje y los sistemas de detección programada.

Los sistemas de autoaprendizaje funcionan generando modelos de lo que se constituye normal a partir de la observación del comportamiento del sistema, por largos períodos de tiempo. Éstos a su vez se dividen en (S. Axelsson (Mayo 20 de 1999)):

- *Modeladores de reglas:* Autogeneran reglas que definen la normalidad en el comportamiento del sistema.
- *Analistas estadísticos:* Recolectan información estadística descriptiva, a partir de la cual crean vectores de distancia entre el comportamiento normal y anormal.

Por otro lado, en los sistemas de *detección programada* el sistema no es el que aprende, sino que existe un ente externo que programa lo que es considerado anormal. Existen dos representantes de este tipo de sistemas (S. Axelsson (Mayo 20 de 1999)):

- *Analistas estadísticos:* Construyen perfiles estadísticos de comportamiento de las anormalidades, a partir de parámetros obtenidos del ejercicio estadístico.
- *Denegación por defecto:* Se fijan explícitamente las circunstancias en las cuales el sistema opera en forma normal o aceptable, identificando como situación anormal las desviaciones a tales circunstancias.

En último lugar, se tiene la *detección por firma (detección por regla)* que se basa en la asociación de la actividad en el sistema con un patrón previamente definido en forma de reglas (S. Axelsson (Mayo 20 de 1999)).

Los sistemas basados en detección de anomalías se caracterizan por su buen desempeño a la hora de detectar nuevos tipos de intrusiones, ya que éstas usualmente difieren de los patrones normales de comportamiento del sistema.

Sin embargo, estos sistemas presentan dificultades para adaptarse a nuevos comportamientos normales, ya que la única forma de hacerlo es reiniciando el IDS en fase de entrenamiento.

Adicionalmente, vale la pena notar que la fase de entrenamiento debe cubrir todos los eventos aceptables posibles en el sistema, de tal manera que se reconozcan como normales y consecuentemente se reduzca la cantidad de falsos positivos. Es importante tener en cuenta que el costo en tiempo y recursos de esta fase es alto, excepto en el caso de la *denegación por defecto*.

Por otro lado, los sistemas basados en reglas se caracterizan por su facilidad de adaptación al entorno cambiante, ya que basta definir la regla escribiéndola u obteniéndola de un tercero.

Empero, los sistemas basados en reglas son potencialmente vulnerables a ser comprometidos por medio del uso de nuevas tácticas, para las cuales no se han definido las reglas correspondientes o todavía no es posible crear la regla, debido al desconocimiento del funcionamiento del ataque.

1.2 Clasificación por características intrínsecas del sistema

(*Ver gráfico A3.4*) (H. °Debar; R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash (2004)) (*gráfico A3.3*).

Existen tres parámetros de clasificación a partir de las características intrínsecas del sistema: método de detección, ubicación de la fuente auditada, y paradigma de detección.

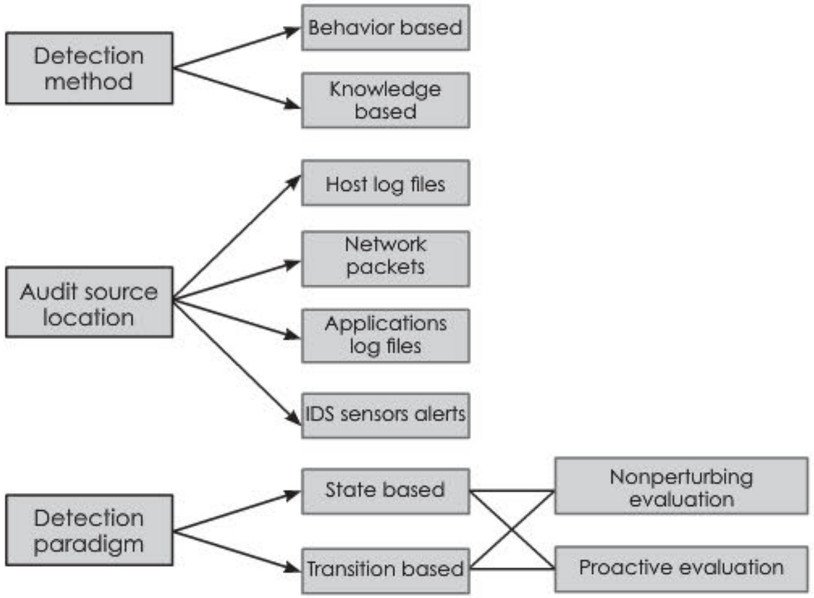


Gráfico A3.3
Clasificación por características intrínsecas

La división por método de detección se basa en las características de funcionamiento del IDS. Las basadas en comportamiento comparan contra comportamientos normales; mientras que las basadas en conocimiento crean patrones que identifican los ataques y las intrusiones.

La división por ubicación de la fuente auditada discrimina el tipo de información que es analizada y el punto físico en el que se realiza la auditoría de datos. Según esta clasificación, existen cuatro tipos de IDS (H. °Debar):

Los IDS basados en el host (HIDS) solamente procesan información de las actividades de los usuarios y servicios en una máquina determinada; por ejemplo, la creación de archivos, los llamados al sistema operativo y los llamados a las interfaces de red.

Los IDS basados en la red (NIDS) hacen sniffing sobre algún punto de la red, y analizan el tráfico capturado en busca de intrusiones.

En caso de que el NIDS se encuentre distribuido (DIDS), disponiendo de varios puntos de recolección y análisis de datos (sensores), usualmente se consolida un banco de datos centralizado que contiene la información procesada por los diferentes sensores.

Finalmente, los IDS basados en logs procesan los archivos de log en búsqueda de información relacionada con eventos de intrusión; este tipo de detección se caracteriza por su completitud y precisión.

Para terminar, la división por paradigma de detección se refiere al mecanismo de detección de intrusos (H. °Debar):

Los basados en estado reconocen situaciones peligrosas, cuando éstas ya han ocurrido, mientras que los basados en transiciones están en capacidad de reconocer actividades sospechosas que son potencialmente parte de una intrusión.

E. *Snort*

Snort es uno de los NIDS basados en firmas más populares. Inicialmente fue desarrollado por Martin Roesch, quien los bautizó basado en su rol como "sniffer and more" (R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash (2004)). Actualmente Snort es software de código abierto por SourceFire (SourceFire (s.f.)).

2. IPS: SISTEMAS DE PREVENCIÓN DE INTRUSOS (INTRUSION PREVENTION SYSTEMS)

A. *Definición y características generales de los IPS*

Los IPS son dispositivos de hardware o de software, encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. La respuesta usualmente consiste en descartar los paquetes involucrados en el ataque o modificarlos (scrubbing), de tal manera que se anule su propósito. Es claro que este comportamiento los clasifica como dispositivos proactivos, debido a su reacción automática a situaciones anómalas (R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash (2004)).

De alguna manera el comportamiento de los IPS semeja el comportamiento de los firewalls, ya que ambos toman decisiones con respecto a la aceptación de un paquete en un sistema. Sin embargo, la diferencia radica en el hecho de que los firewalls basan sus decisiones en los encabezados del paquete entrante, en particular los de las capas de red y de transporte, mientras que los IPS basan sus decisiones tanto en los encabezados como en el contenido de datos (payload) del paquete (M. DeShon (s.f.)).

B. *Los IPS como evolución de los IDS*

Para varios autores los sistemas de prevención de intrusos son la evolución de los sistemas de detección de intrusos (R., J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash (2004); M. DeShon (s.f.); T. Doty (Enero 23 de 2002)), particularmente, se clama que los primeros ofrecen un manejo más efectivo

de las intrusiones al tiempo que superan las dificultades inherentes de los IDS, en particular, la permisividad de los IDS ante las intrusiones.

El IDS se limita a detectar y notificar la intrusión a la persona encargada de recibir y responder las alertas (p. e.,: el administrador de la red o el operador del IDS), quien debe tomar la acción correctiva pertinente, lo que es análogo a darse cuenta de un robo en un banco y limitarse a notificarle a la policía (M. DeShon (s.f.)).

Por su parte, una vez el IPS detecta la intrusión la detiene de algún modo. En el caso de la analogía del robo, el IPS representa un guardia armado que reacciona de forma instintiva al ataque.

Vale la pena mencionar que el nivel de alertas de un IPS es considerablemente menor que el nivel de alertas producido por un IDS, puesto que el IPS se encarga de manejar la situación y sólo genera alertas si se le configura explícitamente para tal fin, o cuando la criticidad de los eventos y circunstancias lo amerite.

Es importante tener en cuenta que entre los IDS y los IPS hay una categoría especial de IDS que se denominan IDS con respuesta activa, que cumplen la función de detener las intrusiones, descartando los paquetes relacionados con el ataque.

Según R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash, la diferencia principal entre los IDS con respuesta activa y los IPS es que estos últimos están en capacidad de inutilizar los paquetes involucrados en el ataque, modificando su contenido, pero tal distinción parece no estar muy difundida y la mayor parte de la bibliografía cataloga los IDS con respuesta activa como un tipo particular de IPS.

La propiedad inherente a los IPS de reaccionar automáticamente a las intrusiones (o lo que ellos determinan como tales) ciertamente disminuye de manera significativa el tiempo de reacción al ataque, pero también puede desencadenar eventos inesperados e inconvenientes cuando se reacciona ante un falso positivo (FP). Lo anterior indica que es indispensable la disminución de estas caracterizaciones para que el IPS sea más preciso. (R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash).

Las consecuencias de la intervención inoportuna e inesperada del IPS, en caso de un falso positivo, pueden ir desde la negación del servicio a los clientes hasta el aislamiento total de la máquina. En R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash, se comenta el caso de un IPS que erróneamente determinó que el servidor DNS de la empresa estaba haciendo un scan de puertos de la red, y tomó la decisión de bloquear todo acceso a éste, produciendo un colapso en los aplicativos de red en la organización.

Por otro lado, las arquitecturas actuales para los IPS centralizan su funcionamiento en un solo punto, lo que facilita su operación y administración; sin embargo, la centralización disminuye la escalabilidad del sistema

y convierte al IPS en un punto crítico, cuyo mal funcionamiento impacta negativamente a nivel de uso y de desempeño en la red sobre la que opera (R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash; N. Desai (Febrero 27 de 2003)).

Finalmente, es importante notar que los IPS no son la "bala de plata" que hace desaparecer los problemas de seguridad, ni soluciona las falencias de los IDS; por ejemplo, los IPS no están en capacidad de detectar y mucho menos de detener intrusiones sobre comunicaciones cifradas, o de detener intrusiones que ni siquiera son capaces de detectar.

De lo anterior se deduce que los IPS son un elemento en la arquitectura de seguridad, y no se les puede considerar como una arquitectura per se. Por esto se recomienda adoptar un esquema de seguridad por capas o una estrategia de defense in depth (M. DeShon (s.f.)), cuya discusión sobrepasa los límites de este escrito.

C. *La evolución y las categorías de los IPS* (N. Desai (Febrero 27 de 2003))

Es posible distinguir dos generaciones históricas de los IPS: los primeros, al detectar un ataque proveniente de una dirección IP determinada, descartaban todos los paquetes provenientes de dicha dirección, estuvieran o no relacionados con el ataque (IPS de primera generación).

Posteriormente se refinó la estrategia anterior, de tal manera que el IPS descartara únicamente los paquetes relacionados con el ataque identificado, permitiendo el tráfico de otros paquetes provenientes de la IP del atacante, siempre y cuando no estuvieran relacionados con el ataque (IPS de segunda generación) (M. DeShon (s.f.)).

Por otro lado, es posible distinguir cinco categorías de IPS, dependiendo de su funcionamiento, sus capacidades y su ubicación en la arquitectura de la red; tales categorías se describen a continuación (N. Desai (Febrero 27 de 2003)).

2.1 Los IPS inline

Estos IPS usualmente se despliegan en algún punto de la red como un bridge de nivel dos, de tal manera que media entre los sistemas que protege y el resto de la red, como se muestra en el *gráfico A3.4*.

En adición a la funcionalidad típica de un *bridge*, el IPS inline revisa todos los paquetes en busca de la firma que define alguno de los ataques que está configurado para identificar. En caso de que el paquete esté "limpio", el IPS le permite el paso (como un bridge normal), en caso contrario, lo descarta registrándolo en un log. El IPS inline puede incluso permitir el paso de un paquete sospechoso, modificando su contenido, de tal manera que el propósito del ataque se frustre sin que el atacante sepa que sus paquetes están siendo modificados.

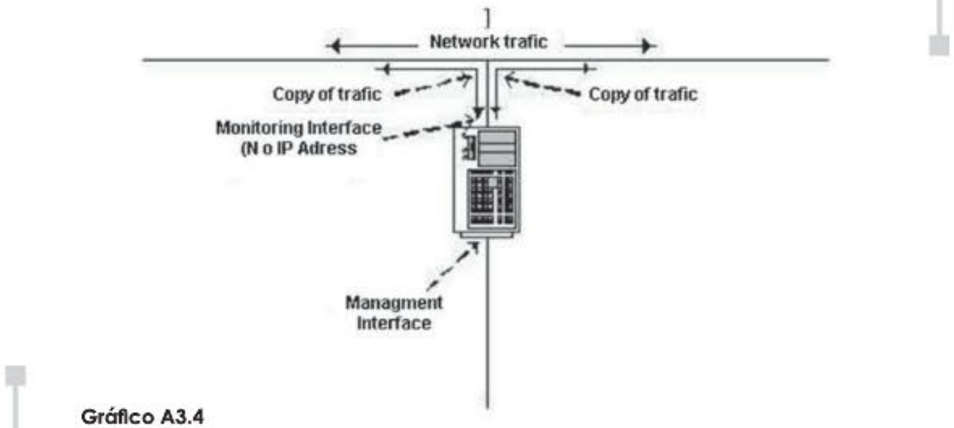


Gráfico A3.4

Los IPS inline. (N. Desai (Febrero 27 de 2003))

Existen implementaciones de los IPS inline más elaboradas que pueden llegar a realizar consultas DNS reversas y traceroutes sobre la identidad del atacante, consignando los resultados obtenidos en un log, de tal modo que se obtenga automáticamente información adicional sobre el autor del ataque (R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash).

Es importante tener en cuenta que los IPS inline son una evolución de los NIDS, en particular, de los NIDS basados en reglas (firmas). Debido a lo anterior, los IPS inline heredan las mismas limitaciones de éstos, mencionadas en la primera parte de este Para profundizar.

2.2 Switches de nivel de aplicación (McClellan Consulting)

Últimamente ha aumentado la tendencia a utilizar switches en la capa de aplicación, que funcionan de forma independiente a otros dispositivos de red, y en su propio hardware optimizado para manejar grandes volúmenes de tráfico (entre uno y varios gigabits).

La tarea principal de los switches de nivel siete (también conocidos como switches de contenido) es balancear las cargas de las aplicaciones distribuidas entre varios servidores, tomando decisiones de enrutamiento o conmutación a partir del payload de información de nivel siete, como se ve en el *gráfico A3.5*.

El modus operandi recién descrito se adapta de forma precisa a lo que se espera del IPS, ya que revisa el contenido de datos del paquete, y es posible configurarlo para que lo analice y descarte de forma eficiente en caso de que su contenido concuerde con alguna firma preestablecida en el IPS.

Debido a lo anterior, los switches de aplicación son los más efectivos (aunque usualmente costosos) a la hora de prevenir intrusiones, particularmente de negación del servicio (*gráfico A3.5*).

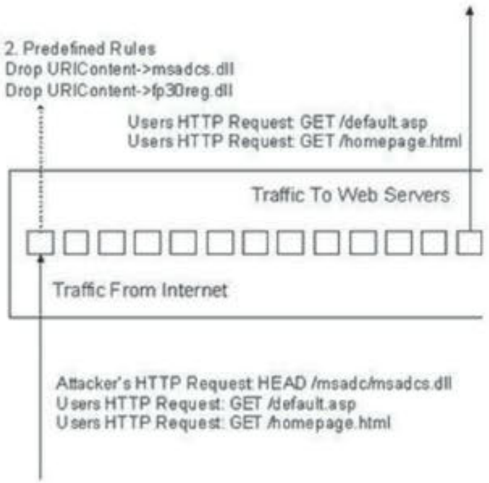


Gráfico A3.5

Los switches de nivel de aplicación.
(N. Desai.)Febrero 27 de 2003))

2.3 Firewalls de aplicación / IDS

A diferencia de los enfoques precedentes, los firewalls de aplicación/ IDS no funcionan al nivel de paquete. Éstos se instalan en cada host que se desea proteger, adaptándose íntimamente con las aplicaciones que corren en el host que protegen. Para lograr lo anterior es necesario que antes de comenzar la fase de protección se ejecuten en modalidad de entrenamiento, de forma análoga a los HIDS mencionados en la segunda sección de Para profundizar.

La modalidad de entrenamiento consiste en el proceso de identificación de patrones de comportamiento normales en el host. En particular, se crea un perfil de relaciones frecuentes entre las aplicaciones y varios componentes del sistema, como: el sistema operativo, otras aplicaciones, la memoria y los usuarios. Tales relaciones se ilustran en el *gráfico A3.6*.

Una vez se han establecido los patrones de comportamiento normal, el IPS se comporta de forma similar a los IDS basados en detección de anomalías a la hora de detectar las intrusiones.

Lo anterior hace de esta categoría de IPS los más efectivos a la hora de detectar y prevenir vulnerabilidades generadas por errores en la

programación de las aplicaciones. Además, debido a que se apoyan en la detección de comportamientos anómalos y no en la coincidencia de firmas, es posible prevenir intrusiones muy recientes para las cuales todavía no existe la definición de sus firmas específicas (W. Jackson (Febrero 16 de 2005)).

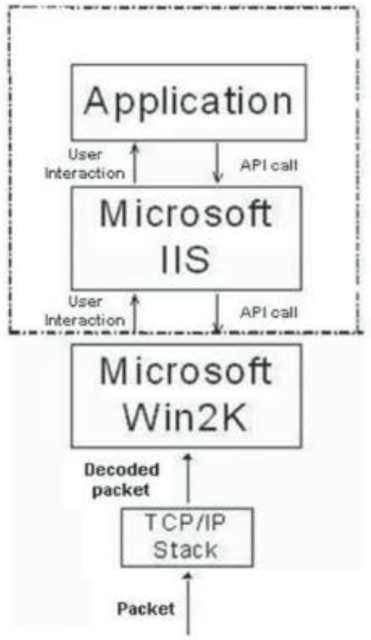


Gráfico A3.6

Los firewalls de aplicación.
(N. Desai. (Febrero 27 de 2003))

Por su parte, la desventaja principal de este tipo de IPS –al igual que los IDS basados en detección de anomalías– es que la fase de entrenamiento debe comprender absolutamente todos los comportamientos válidos, a fin que ningún comportamiento normal no aprendido se catalogue como anormal. Lo anterior puede traer graves consecuencias, como se discutió al final del literal B de esta sección.

2.4 Switches híbridos

Los switches híbridos son una combinación entre los firewall de aplicación / IDS y los switches de nivel de aplicación. Al igual que estos últimos, funcionan sobre dispositivos de hardware dedicados y optimizados para la inspección y el manejo de paquetes, pero a diferencia de éstos se basan en políticas de aceptación de tráfico (comportamiento) válido, de manera similar a los firewall de aplicación/IDS, como se aprecia en el *gráfico A3.7*.

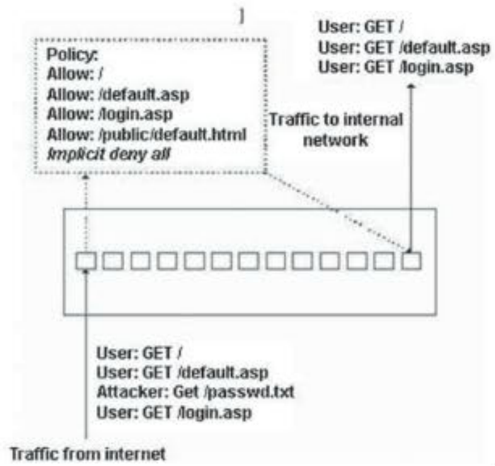


Gráfico A3.7

Los switches híbridos

La fortaleza de esta aproximación radica en el conocimiento detallado del tráfico que debe aceptar y, por consiguiente, el que debe rechazar una aplicación o un host determinado.

2.5 Aplicaciones engañosas (deceptive)

Al igual que los *firewalls* de aplicación/IDS, las aplicaciones engañosas aprenden el comportamiento de los servicios ofrecidos por cada uno de los host que protege. Una vez se detecta algún tipo de comportamiento sospechoso sobre un servicio/host existente o no, el IPS suplanta al servicio en caso de que exista o lo simula en caso contrario, respondiendo al atacante y marcándolo de tal forma que sea posible identificarlo y bloquearlo posteriormente.

2.6 Una comparación práctica entre un IDS y un IPS

Para ilustrar las diferencias a nivel práctico entre los IDS y los IPS, se llevó a cabo un experimento con el fin de evaluar el impacto en el comportamiento y el desempeño en una red de tres máquinas ante la presencia de un IDS o de un IPS (*gráfico A3.8*).

A. *Configuración del experimento: la red* (*gráfico A3. 8*)

Desde la máquina de monitoreo (M) se estableció una sesión SSH (OpenSSH 4.0) con la máquina víctima (V), a fin de verificar la accesibilidad de esta última y monitorear su estado. La máquina física M simultáneamente ejecutaba Linux Fedora Core 3 (Fedora Core 3) sobre una máquina virtual VMWare (VMWare Inc. (s.f.)), con el único propósito de atacar la máquina V.

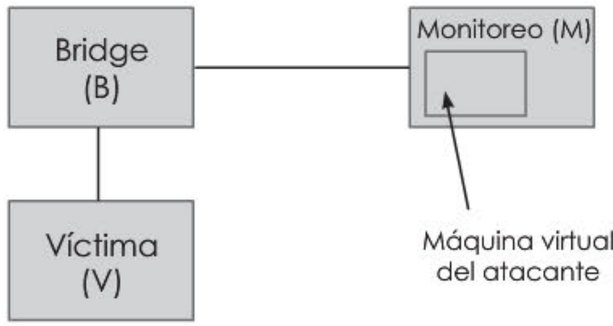


Gráfico A3.8

Diagrama de la red para el experimento

La máquina *bridge*, para la primera parte del experimento, funcionaba como IDS: analizando y reenviando (*bridging*) el tráfico entre la máquina de monitoreo/ataque (MA) y la máquina víctima.

En el caso de la segunda parte del experimento, la misma máquina funcionaba como IPS, es decir, no reenviaba el tráfico entre las máquinas MA y V, sino que, dependiendo del análisis del tráfico, lo reenviaba o rechazaba.

B era una máquina con procesador Pentium II @ 333 MHz., memoria RAM de 192 MB y sistema operativo Linux-Fedora Core 3, instalado por defecto.

Finalmente, V era un computador portátil con procesador AMD Mobile Athlon XP 2600+, 512 MB de memoria RAM y el mismo sistema operativo que las máquinas B y A.

La máquina B únicamente tenía abiertos los puertos TCP 22, 80 y 443 (los dos últimos sobre los que corría el servidor HTTP Apache 2.0.52 (Apache (s.f.)).

B. *Configuración del experimento: el software*

Como IDS, se utilizó Snort 2.3.0 (SourceFire (s.f.)), el cual fue brevemente comentado al final de la segunda sección Para profundizar.

Snort es un NIDS basado en detección de firmas relativamente liviano y altamente configurable. Su instalación no es compleja, requiriendo únicamente la instalación previa de la librería de captura de paquetes Libpcap (Tcpdump/Libpcap), y la librería de expresiones regulares PCRE (P. Hazle (s.f.); SourceFire (s.f.)) y el capítulo 3 de R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash (s.f.) son fuentes claras y completas en lo referente al proceso de instalación de Snort.

La configuración de Snort está concentrada principalmente en el archivo snort.conf, ubicado usualmente en la carpeta etc del sistema o de la instalación. En este archivo se definen todas las variables correspondientes a la red sobre la que opera el IDS, y se referencian todos los archivos de reglas para el motor de detección (uno de los componentes arquitectónicos de Snort para la detección de intrusiones (R. Rehman, R. (2003) Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash)).

En particular, en snort.conf, se definen las variables $External_Net (direcciones de las redes externas), $Home_Net (dirección CIDR de la Intranet), $Http_Servers (direcciones de los Servidores Web en la Intranet), entre otras. Para una descripción detallada de este archivo de configuración, es posible consultarlo ya que se encuentra cuidadosamente documentado, o en su defecto, remitirse a R. Alder, J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash; W. Metcalf (s.f.).

Por su lado, como IPS se utilizó Snort_inline 2.3.0 RC1 (W. Metcalf), un IPS inline cuya instalación fue más complicada que la del IDS.

Es preciso tener en cuenta que en su principio Snort_inline fue un desarrollo independiente de Snort, que se basó en este último para procesar el tráfico de red (SourceFire (s.f.); W. Metcalf).

Desde su versión 2.3.0, Snort incorporó la funcionalidad *inline* como parte integral del proyecto. Para activar el modo IPS basta usar el modificador `--enable-inline` a la hora de configurar el script de instalación antes de compilar el código fuente de la aplicación (W. Metcalf).

Adicionalmente, Snort_inline, a diferencia de Snort, debe operar en modo *bridge*, lo que requiere activar esta funcionalidad antes de poder ejecutar el IPS. La mayoría de las fuentes consultadas recomiendan el uso del programa Bridge, disponible en S. Hemminger, para configurar el *bridging* anteriormente descrito.

Por otro lado, Snort_inline no toma los paquetes directamente de la NIC *(Network Interface Card)* por medio de Libpcap (Tcpdump/Libpcap) como lo hace Snort, sino de la cola de salida del *firewall* de Linux (IPTables (O. Andreasson)). Por esto es necesario configurar IPTables, de tal manera que enfile los paquetes entrantes en la susodicha cola para que puedan ser procesados por Snort_inline.

Finalmente, el *kernel* de Linux no permite ejecutar simultáneamente IPTables y Bridge, por lo que es necesario parcharlo con EBTables (EBTables) que es una herramienta de filtrado para *firewalls en modo bridge*.

C. El experimento: DoS (negación del servicio) sobre Apache 2.0.52

El ataque consistió en una negación de servicio sobre el servidor Apache 2.0.52, a partir del envío de mensajes HTTP con peticiones (request) mal formadas de la siguiente manera:


```
GET / HTTP/1.0\n
(espacio) x 8000\n
(espacio) x 8000\n
(espacio) x 8000\n
```

La información sobre el ataque se obtuvo de (C. Trivedi) y (D. Guido), y la prueba de concepto de (D. Guido), cuyo código está escrito en C y utiliza varios hilos para aumentar la cantidad de tráfico enviado a la víctima.

2.6.1 Detección del ataque con el IDS

A partir de la descripción del ataque presentada anteriormente, se compuso la siguiente regla con el fin de detectarlo en el IDS:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (pcre:"/\x20{6000}/";msg:"6000 espacios contiguos detectados";)
```

Esta regla tiene como función alertar sobre cualquier datagrama IP, que provenga de cualquier dirección IP, hacia cualquiera de los servidores HTTP (en el caso del experimento, la dirección IP de V: 192.168.0.105), sobre los puertos HTTP definidos en la variable $Http_Ports en snort.conf (80 y 443). El payload de datos debe contener 6.000 espacios seguidos para que se cumpla la regla y se alerte sobre la posible intrusión.

Una vez se escribió la regla y se ejecutó el IDS en B, se inició el ataque desde A, monitoreando desde M el estado de V, en particular, su uso de memoria RAM.

Entre 03/16-00:51:02.609266 y 03/16-01:02:53.836897 se ejecutó el ataque con los resultados siguientes:

El IDS se ejecutó de tal manera que almacenó un registro detallado de los paquetes capturados, encontrándose que la víctima recibió 101463 peticiones HTTP mal formadas en el lapso de tiempo en el que se ejecutó el ataque. La captura de una petición se muestra a continuación:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/16-00:51:02.611854 192.168.0.125:32771 -> 192.168.0.105:80
TCP TTL:64 TOS:0x0 ID:58731 IpLen:20 DgmLen:67 DF
***AP*** Seq: 0x916637C2 Ack: 0xC0BCFFCC Win: 0x5B4 TcpLen: 32
TCP Options (3) => NOP NOP TS: 512761 1220540
47 45 54 20 2F 20 48 54 54 50 2F 31 2E 30 0A  GET / HTTP/1.0.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/16-00:51:02.613799 192.168.0.125:32771 -> 192.168.0.105:80
TCP TTL:64 TOS:0x0 ID:58733 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x916637D1 Ack: 0xC0BCFFCC Win: 0x5B4 TcpLen: 32
TCP Options (3) => NOP NOP TS: 512763 1220540
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
…(Siguen 87 líneas con 16 espacios (0x20))
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

En la anterior captura se ve claramente la petición HTTP (GET / HTTP/1.0), seguida por una cantidad elevada de espacios (0×20).

Por su parte, el motor de detección del IDS detectó y clasificó los datagramas involucrados con las peticiones mal formadas, generando una entrada por cada uno de ellos en el log de alertas (ubicado usualmente en

```
(**) (1:0:0) 6000 espacios contiguos detectados (**)
(Priority: 0)
03/16-00:53:14.044895 192.168.0.125:32771 -> 192.168.0.105:80
TCP TTL:64 TOS:0x0 ID:60225 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x9AB88C02 Ack: 0xc0EEF748 Win: 0x5B4 TcpLen: 32
TCP Options (3) => NOP NOP TS: 177101 526711
```

/var/log/snort/alert). Una de tales alertas se muestra a continuación:

Al ejecutarse el ataque, el consumo de memoria RAM aumentó considerablemente en V, como se muestra en el *gráfico A3.9*.

Luego de varios minutos de ejecución del ataque desde A (*gráfico A3.10*), no fue posible acceder al servidor Web, como se ve en el *gráfico A3.11*, ni seguir verificando el estado de uso de la memoria de V vía SSH.

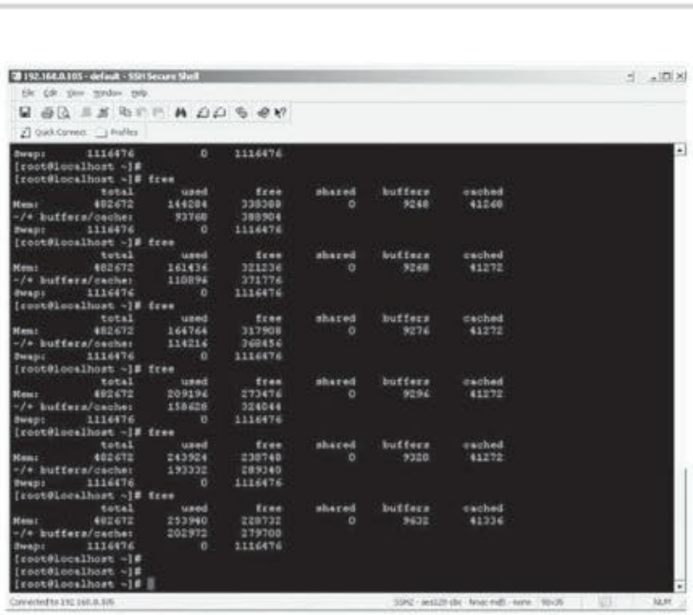


Gráfico A3.9

Estado de uso de memoria V

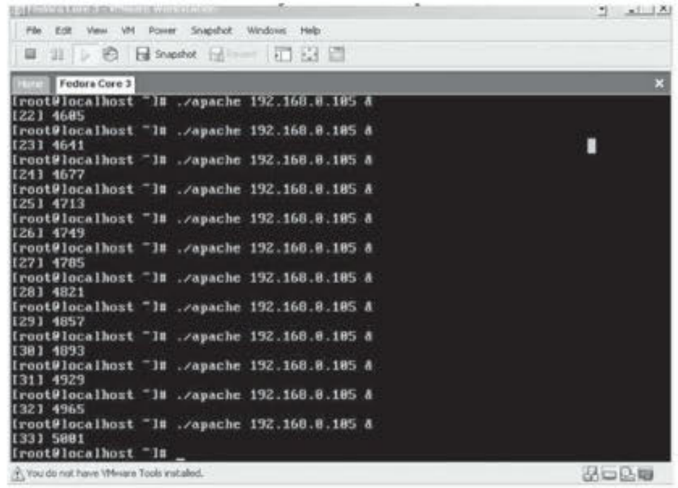


Gráfico A3.10

Ejecución del ataque desde A

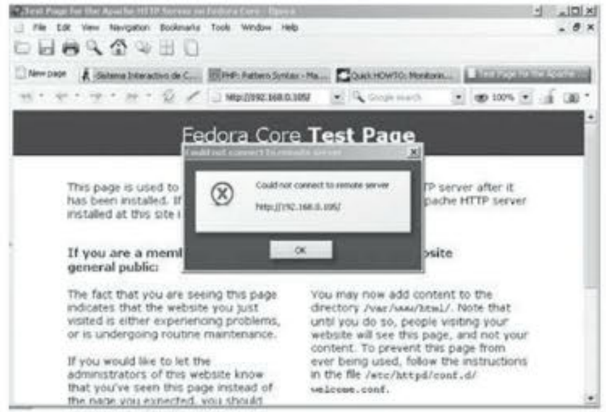


Gráfico A3.11

Error en el acceso al servidor Web

Finalmente, se capturó directamente la información de uso de memoria de V (*gráfico A3.12*), donde se aprecia que el ataque logró consumir 400.484 MB - 190.020 MB = 210.646 MB en alrededor de 10 minutos, logrando el objetivo de la negación del servicio no sólo sobre el servidor Web, sino sobre todos los servicios de red activos en V.

```
[root@localhost ~]# free
             total       used       free     shared    buffers     cached
Mem:        482672     292644     190028          0       9520      41380
-/+ buffers/cache:     241816     240856
Swap:      1116476          0    1116476
```

Gráfico A.12
Error en el acceso al servidor Web

2.6.2. Detección del ataque con el IPS

Dado que el IPS permite descartar los paquetes que concuerdan con determinada regla, se modificó la acción de la regla usada por el IDS para detectar el ataque, de tal manera que se descartaran los datagramas relacionados con éste, así:

```
drop tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS pcre:"/\
x20{6000}/";msg:" 6000 espacios contiguos detectados -> Da-
tagrama descartado!";)
```

Al probar dicha regla, se vio con sorpresa que el IPS no descartaba el paquete sino que lo reenviaba a la víctima. Después de revisar las posibles causas para tal comportamiento, se concluyó que la aplicación de la regla, en particular, de la expresión regular era muy pesada y el IPS no alcanzaba a procesar los paquetes oportunamente.

Debido a lo anterior, y en aras de probar el IPS, se modificó la regla, como sigue:

```
drop tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(pcre:"/\x20{100}/";msg:"100 espacios contiguos detectados ->
Conexión reestablecida!";)
```

Con la anterior regla, los paquetes del ataque eran debidamente descartados y nunca llegaban a V. Tales paquetes se registraban en el log de alertas de la manera siguiente:

```
(**) (1:0:0) 100 espacios contiguos detectados -> Datagrama descartado! (**)
(Priority: 0)
03/16-11:43:57.018220 192.168.0.125:32909 -> 192.168.0.105:80
TCP TTL:64 TOS:0x0 ID:39544 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x5CA13670 Ack: 0xDA343090 Win: 0x5B4 TcpLen: 32
TCP Options (3) => NOP NOP TS: 205048 534950
```


Usando esta regla se encontró, mediante el uso de un analizador de tráfico de red en V, que los paquetes hostiles no lograron llegar; debido a lo anterior, el uso de memoria no presentó aumentos significativos (*gráfico A3.13*).

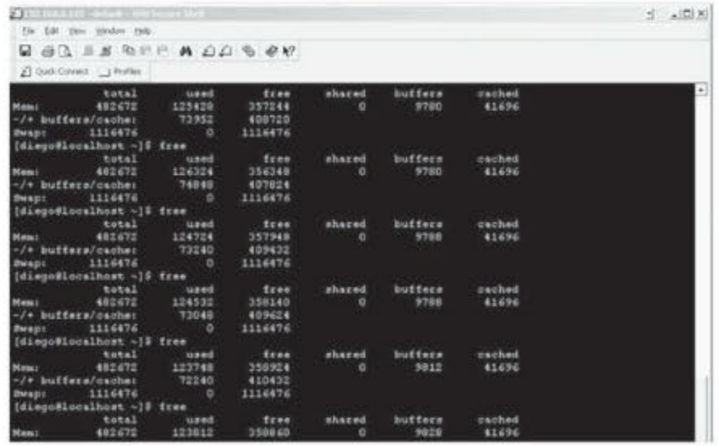


Gráfico A3.13
Error en el acceso al servidor Web

Sin embargo, al ejecutar el ataque desde varios procesos simultáneos, el IPS no estuvo en capacidad de analizar y, por ende, descartar los paquetes involucrados en el ataque, permitiéndoles el paso hacia V.

Finalmente, se probó la siguiente regla alternativa:

```
reject tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(pcre:"/\x20{100}/";msg:" 100 espacios contiguos detectados
-> Conexión restablecida!";)
```

El propósito de esta regla es descartar los paquetes comprometidos en el ataque y restablecer (reset) la conexión con el atacante, mediante el envío de de un segmento TCP con las banderas FIN y ACK encendidas.

Sin embargo, a la hora de ejecutar el IPS con la regla de reject, se desplegaron innumerables errores de Libpcap (Tcpdump/Libpcap) relacionados con la imposibilidad de escribir la respuesta, como se ve en el *gráfico A3.14*.

Gráfico A3.14

Errores al invocar la acción reject

Conclusiones

A nivel teórico la diferencia entre los IDS y los IPS radica en la forma como reaccionan ante las intrusiones: los primeros se limitan a detectar y notificar de la intrusión, mientras que los segundos toman acciones de algún tipo frente a tales eventos.

Debido a lo anterior el uso de los IDS implica un corto lapso de tiempo para enterarse, analizar y determinar la acción correctiva a adoptar frente a la intrusión, para finalmente reaccionar manualmente al ataque.

Por esta razón, la fortaleza de los IDS radica en su utilidad a posteriori, ya que ayudan a la reconstrucción del ataque para su posterior análisis.

Sin embargo, muchas veces es deseable detener el ataque de manera oportuna, campo en el cual los IPS son la solución adecuada, siempre y cuando estén debidamente configurados y puestos a punto con el fin de maximizar su nivel de precisión.

Finalmente, a partir del experimento fue posible determinar que la efectividad de los IDS/IPS está altamente ligada a la cantidad de recursos destinados para su operación.

Por esto, es preciso calibrar las reglas de acuerdo con el ambiente de hardware en que opera el sistema, ya que pueden exigir un alto nivel de procesamiento, incluso uno mayor al ofrecido por la infraestructura de hardware.

✓ ***Resumen:*** Para profundizar se presenta una introducción a los Sistemas de Detección y Prevención de Intrusos (IDS e IPS respectivamente), mostrando las principales características, clasificación y diferencias.

A fin de contrastar ambos sistemas se realiza un ejercicio práctico que muestra y analiza diferencias de comportamiento ante el mismo estímulo (ataque).

✓ ***Términos claves:*** IDS, IPS, detección de intrusos, prevención de intrusos, Snort.

Enlaces en el Web

http://csrc.nist.gov –Documentos del Nacional Institute of Standards and Technology– NIST norteamericano.
http://dfrws.org/ –Digital Forensic Research Workshop– Conferencia internacional de avances en investigaciones forenses en informática.
http://www.cccure.org/Documents/HISM/ewtoc.html –Handbook of Information Security Management.
http://www.cert.org/work/organizational_security.html –CERT Organizational Security.
http://www.cisco.com/webWeb/about/ac123/ac147/archived_issues/ipj_10- 4/104_standards.html –Security Standards for Information Security Management– Dr. William Stallings. CISCO IP Journal, Vol. 10, No. 4 de 2007
http://www.cisecurity.org –Center for Internet Security– Documentos de aseguramiento de infraestructuras de computación.
http://www.digital-evidence.org/ –Página desarrollada por el Dr. Brian Carrier, sobre avances en temas de evidencia digital.
http://www.isecom.org/projects/soma.shtml –SOMA– Security Operations Maturity Architecture.
http://www.loganalysis.org/ –Página dedicada al análisis de diferentes tipos de archivos de auditoría en diferentes sistemas operativos y herramientas de seguridad.
https://www.securityforum.org/index.htm –Information Security Forum– Buenas prácticas en seguridad de la información.

Referencias*

Alder, R., J. Babbin, A. Doxtater, J. Foster, T. Kohlenberg, M. Rash. (2004). "*Snort 2.1 Intrusion Detection*", Second Edition, Syngress.
Andreasson, O. (s.f.). "*Iptables Tutorial 1.1.19*". Disponible en: http://www.linuxsecurity.com/resource_files/firewalls/IPTables-Tutorial/iptables-tutorial.html

* Referencias de la sección Para profundizar. (N. del E.).

Apache. (s.f.). Apache HTTP Server Project. Disponible en: http://httpd.apachet.org.
Axelsson, S. (Mayo 20 de 1999). *"The Base-Rate Fallacy and its Implicatios for the Difficulty of Intrusion Detection"*. Disponible en: http://www.raid-symposium.org/raid99/PAPERS/Axelsson.pdf.
Bruneau, G. (s.f.). *"The History and Evolution of Intrusion Detection"*. Disponible en: http://www.sans.org/rr/whitepapers/detection/344.php
Chuvakin, A. y C. P. Bruneau. (2004). *"Security Warrior"*. O Reilly. [No está citado en el contenido]
[0]Debar, H. (s.f.). *"An introduction to Intrusion-Detection Systems"*. IBM Research, Zurich Research Laboratory.
Desai, N. (Febrero 27 de 2003). *"Intrusion Prevention Systems: the Next Step in the Evolution of IDS"*. Disponible en: http://www.securityfocus.com/printable/infocus/1670
DeShon, M. (s.f.). *"Intrusion prevention versus intrusion detection"*. Disponible en: http://www.secureworks.com/en/html/printer/internet/techResourceCenter/Intrusion-prevention-versus-intrusion-detection.html
Doty, T. (Enero 23 de 2002). "New Approach To Intrusion Detection: Intrusion *Prevention"*. Disponible en: http://www.itsecurity.com/papers/doty1.htm
"EBTables". (s.f.). Disponible en: http://ebtables.sourceforge.net/.
"Fedora Core 3". (s.f.). Disponible en: http://fedora.redhat.com.
Guido, D. (s.f.). *"Apache Multiple Space Header DoS (Multi-Threaded Exploit)"*. Disponible en: http://www.securiteam.com/exploits/6O00G2ABPS.html
Hazle, P. (s.f.). *"PCRE –Perl Compatible Regular Expressions"*. Disponible en: http://www.pcre.org/
Hemminger, S. (s.f.). *"Bridge –Linux Ethernet bridging"*. Disponible en: http://bridge.sourceforge.net/
Jackson, W. (Febrero 16 de 2005). *"Intrusion prevention systems provide an active line of defense"*.. Disponible en: http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcndaily2&story.id=35069
Lehmann, D. (s.f.). *"Intrusion Detection FAQ"*. Disponible en: http://www.sans.org/resources/idfaq/what_is_id.php
McClellan Consulting. (s.f.). *"Layer 4 through Layer 7 Switching"*. Disponible en: http://www.mcclellanconsulting.com/whitepapers/Layer4through7.pdf
Metcalf, W. (s.f.). *"Snort Inline"*. (s.f.). Disponible en: http://snort-inline.sourceforge.net/
"OpenSSH 4.0". (s.f.). Disponible en: http://www.openssh.com/
Porras, P. y A. Valdés. (Marzo 1998). *"Live traffic analysis of TCP/IP gateways"*. En *"Proceedings of the 1998 ISOC Symposium on Network and Distributed System Security"*, San Diego, CA.
Rehman, R. (2003). *"Intrusion detection with SNORT: Advanced IDS techniques using Snort, Apache, MySQL, Php and ACID"*. Prentice Hall PTR.
"Snort_inline". (s.f.). Disponible en: http://snort-inline.sourceforge.net/
SourceFire. (s.f.). Snort.org. Disponible en: http://www.snort.org.
«Tcpdump/Libpcap". (s.f.). Disponible en: http://www.tcpdump.org/
The Honeynet Project. (s.f.). *"Tools for Honeynets"*. Disponible en: http://www.honeynet.org/tools/
Trivedi, C. (s.f.). *"FullDisclosure: DoS in Apache 2.0.52?"*. Disponible en: http://seclists.org/lists/fulldisclosure/2004/Nov/0022.html
VMWare Inc. (s.f.). *"VMWare"*. Disponible en: http://www.vmware.com.

Bibliografía

Cano, J. (2002). Conceptos y retos de la atención de incidentes y la evidencia digital. *Revista Electrónica de Derecho Informático*. Junio 2002. http://www.alfa-redi.org
Cano, J. (2003). Admisibilidad de la evidencia digital. De los conceptos legales a las implementaciones técnicas. Universidad de Los Andes. Facultad de Derecho.
Cano, J. (Mayo 2004). Inseguridad informática. Un concepto dual en seguridad informática. *Revista de Ingeniería*. Universidad de Los Andes. Facultad de Ingeniería. ISSN: 0121-4993.
Casey, E. (2001). *Handbook of Computer Crime Investigation*. Academic Press. CERT (2002). Overview of attack trends. http://www.cert.org/archive/pdf/attack_trends.pdf
Council of Europe. (2001). Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
Digital Evidence: Standards and Principles. Scientific Working Group on Digital
Evidence (Swgde). International Organization on Digital Evidence (IOCE). (2000). http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm. Forensic Science Communication, Vol. 2, No. 2.
Digital Forensic Research Workshop –Dfrws. (2001). A road map for Digital Forensic Research. Technical Report. http://www.dfrws.org
Farmer, D. y Venema, W. (2000). Forensic Computer Analysis: An Introduction. *Dr. Dobb's Journal*. September. http://www.ddj.com/documents/s=881/ddj0009f/0009f.htm
Farmer, D. y Venema, W. (Abril 2001). Being Prepared for Intrusion. *Dr. Dobb's Journal*. http://www.ddj.com/documents/s=868/ddj0104f/0104f.htm
International Organization on Computer Evidence –IOCE. (2002). Guidelines for best practice in the forensic examination of digital technology. http://www.ioce.org/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf
Sommer, P. (1995). Forensic Computing –CSRC Research Project. http://csrc.lse.ac.uk/People/sommerp/forensic.htm
Weber, R. (1999). *Information Systems Control and Audit*. Prentice Hall.

4 El investigador y la criminalística digital

Objetivos

- ✓ Revisar el concepto emergente de la criminalística digital.
- ✓ Analizar los roles y las responsabilidades del investigador forense en informática.
- ✓ Describir los modelos y algunos procedimientos para adelantar una investigación forense en informática.
- ✓ Detallar algunas de las credenciales de los investigadores forenses en informática.
- ✓ Presentar la estructura de los informes de investigación y la presentación de pruebas informáticas.

INTRODUCCIÓN

"Frecuentemente, lo que todo el mundo sabe es un error. Es un error porque las personas suponen una o más cosas que no son verdad y luego todo el mundo queda convencido de ellas. (…)". Estas frases acuñadas por Cohen (p. 50), en su libro *En clase con Drucker*, nos indican que muchas veces lo que escuchamos o vemos no es lo que se ajusta a lo que se observa en la realidad. En este sentido, los investigadores tienen un papel fundamental para recabar en los hechos de lo que ocurre o ha ocurrido, las pistas y los rastros que nos conduzcan a lo que realmente está sucediendo o ha sucedido.

En medios electrónicos, la verdad de lo que ha ocurrido puede ser tan escurridiza como lo es en el mundo de las investigaciones normales que conocemos. Los atacantes y los delincuentes, al utilizar las tecnologías de información para materializar sus acciones punibles,

saben que en la actualidad las instituciones de la administración de justicia tienen limitaciones para comprender las mismas, y que cuentan con recursos técnicos y profesionales restringidos para valorar las evidencias en formato de mensajes de datos (*léase información almacenada electrónicamente* INALE). Adicionalmente, a la fecha los jueces no cuentan con el entrenamiento suficiente para enfrentar procesos donde la INALE sea parte fundamental de la diligencia, lo que ofrece una ventaja particular al crimen informático para continuar desafiando el mundo *offline* desde el mundo *online*.

> Los atacantes y delincuentes saben que las instituciones de la administración de justicia tienen limitaciones. A la fecha los jueces no cuentan con el entrenamiento suficiente para enfrentar procesos donde la INALE sea parte de la diligencia.

En este contexto abierto e informático, es necesario que se desarrolle una nueva disciplina auxiliar, científica y evolutiva que, basada en el concepto general de la criminalística, como lo es "procurar elementos probatorios identificadores y reconstructores que conduzcan a establecer la verdad de los hechos que se investigan" (López Calvo, P. y Gómez Silva, P. 2003, p. 154), establezca un conjunto de habilidades, herramientas y conocimientos que permitan a estos nuevos investigadores enfrentar las conductas exigentes y desafiantes de los delincuentes, ahora en sistemas de computación, dispositivos electrónicos o tecnologías emergentes.

Este nuevo investigador no puede ser la extensión de los investigadores actuales formados en las ciencias de la criminalística tradicional, sino un nuevo profesional que actuando bien sea como perito o criminalista digital o informático, es capaz de comprender la evolución de las nuevas tecnologías de la información, reconocer y analizar la inseguridad informática emergente en los sistemas, así como recorrer la mente del criminal informático, no sólo desde la lógica natural de los delincuentes tradicionales, sino desde la imaginación y la destreza de los intrusos informáticos, mal llamados "hackers".

En consecuencia, en este capítulo se revisan algunos conceptos básicos de una disciplina emergente denominada *criminalística digital*, las estrategias y responsabilidades de los investigadores forenses en informática, así como algunas ideas sobre su formación, los modelos frecuentemente utilizados, así como reflexiones y propuestas sobre los

informes que se rinden luego de las diligencias o las investigaciones que adelantan en un escenario informático.

4.1 INTRODUCCIÓN A LA CRIMINALÍSTICA DIGITAL

De acuerdo con el reporte del Instituto Australiano de Criminalística, denominado "Future directions in technology-enable crime: 2007-09" (Raymond Choo, K.K., Smith, R.y McCusker, R. 2007, p. 3), se vienen incrementando las actividades de los intrusos por medio de las tecnologías de información, haciéndose cada vez más sofisticadas e imperceptibles, lo cual implica que pueden evidenciarse impactos económicos severos y mayores que los que se presentan con los crímenes tradicionales.

En este sentido, los intrusos y delincuentes encuentran en las tecnologías emergentes una estrategia "confiable" para materializar sus acciones, con una alta probabilidad de evitar cualquier tipo de proceso o de investigación que logre asociarlos con los hechos. En este contexto, estos representantes del "lado oscuro de la fuerza" establecen un nuevo desafío para la criminalística tradicional, pues su perfil criminal, esa "técnica psicológica que, basada en los aspectos psicosociales del comportamiento humano, establece, a partir de la escena del crimen, las características sociales y psicológicas de la víctima y los hallazgos forenses y criminalísticos, la motivación del autor (…)" (Soria 2006, p. 365), encuentra dificultades para distinguir aquellos posibles delincuentes con inclinación al uso de las tecnologías, de otros con problemas por adicción al tema tecnológico.

> Los intrusos y delincuentes encuentran en las tecnologías emergentes una estrategia "confiable" para materializar sus acciones.

Los criminales informáticos o tecnológicos responden a diferentes tipos de perfiles de individuos o grupos que tienen en común un gusto y pasión por las tecnologías y sus posibilidades, y que aprovechando mucho el desconocimiento mismo de los ciudadanos comunes, diseñan estrategias para lograr sus objetivos ilícitos, vulnerando los derechos y garantías propias de los nacionales en el uso de las tecnologías de información.

> Cualquier persona puede llegar a ser un delincuente informático, solamente hace falta una motivación, una creencia racionalizada, el medio y el momento para actuar.

No existe una definición concreta o perfil exacto sobre los delincuentes tecnológicos (según afirma Rogers 2001) en su tesis doctoral inédita, titulada *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study* –2001. University of Manitoba. Manitoba. Canadá). Se habla de características como solitarios, orientados por la tecnología y sus avances, inestabilidad emocional y con problemas para definir los límites de sus actuaciones e impactos. En este sentido, cualquier persona puede llegar a ser un delincuente informático, solamente hace falta una motivación, una creencia racionalizada, el medio (generalmente tecnológico) y el momento para actuar.

La dificultad existente para perseguir la criminalidad informática[1] radica en varias razones como el entendimiento de las tecnologías y las vulnerabilidades inherentes por parte de los Cuerpos de Seguridad del Estado y la Administración de Justicia, la comprensión y análisis de la evidencia digital y los rastros electrónicos, la información y su valor en los mercados internacionales y la falta de precisión en el perfil de un delincuente tecnológico, como elementos que exigen de la academia, el gobierno y las instituciones de la justicia un esfuerzo conjunto para avanzar en las construcción de caminos que confronten a los nuevos y organizados criminales.

En los medios electrónicos, la realidad de la inseguridad de la información y la materialización de la delincuencia nos debe llevar a mirar en perspectiva lo que la justicia requiere para enfrentar el desafío de un atacante anónimo, que se mimetiza en la red, que manipula evidencias, que elimina rastros y que conoce en los detalles las herramientas de apoyo y soporte de las investigaciones informáticas.

En este contexto, el Nacional Intitute of Justice –NIJ– del Departamento de Justicia de los Estados Unidos (Stambaugh, H., Beaupre, D., Icove, D., Baker, R., Cassaday, W y Williams, W. 2001)

[1] *Criminalidad Informática:* Cuando en este capítulo se hable de este término se hará referencia a todas aquellas acciones que un individuo o grupo de individuos desarrolla para vulnerar las características fundamentales de la información: confidencialidad, integridad y disponibilidad, que el Estado estima como importantes y, por tanto, desea proteger. El bien fundamental es la información.

adelantó un estudio que establece aquellos elementos y consideraciones que se hacen necesarios para apoyar tanto táctica como operacionalmente a la administración de justicia, para enfrentar el reto de la criminalidad informática y de las telecomunicaciones.

La inseguridad de la información y la delincuencia nos deben llevar a mirar en perspectiva lo que la justicia requiere para enfrentar el desafío de un atacante.

Los resultados del estudio establecen 10 temas críticos donde se debe trabajar para avanzar en el fortalecimiento de las habilidades de la administración de justicia y su relación con las nuevas armas de delincuencia informática.

1. Concienciación del público
2. Estadísticas y datos sobre delitos informáticos
3. Entrenamiento uniforme y cursos de certificación para investigadores
4. Asistencia en sitio para las unidades de lucha contra el delito informático
5. Actualización del marco normativo
6. Cooperación con los proveedores de alta tecnología
7. Investigaciones y publicaciones especializadas en crímenes de alta tecnología
8. Concienciación y soporte de la gerencia
9. Herramientas forenses y de investigación criminal informática
10. Estructuración de Unidades de lucha contra el delito informático

Como se puede observar en el resultado del estudio del NIJ, el combate del cibercrimen requiere toda una estrategia de formación y articulación que permita a la sociedad contar con una administración de justicia moderna y acorde con los retos que la criminalidad le impone. El no considerar algunos de los elementos planteados por la investigación implica debilitar el modelo de administración de justicia, en el escenario de una sociedad

El combate del cibercrimen requiere toda una estrategia de formación y articulación que permita a la sociedad contar con una administración de justicia moderna.

de la información, y generar un espacio de acción más amplio para los artificios jurídicos que utilizarán los delincuentes para evadir las sanciones que deben tener por sus acciones.

La criminalística digital, como resultado nativo de una sociedad digital, es una práctica emergente que busca articular las prácticas generales de la criminalística tradicional para indagar, reconocer y presentar un análisis científico y formal de la evidencia digital disponible en una escena del crimen. Los delitos informáticos o las situaciones donde los derechos y libertades individuales son vulnerados mediante elementos digitales, se convierten en la especialidad de los nuevos investigadores que deben estar entrenados para confrontar y demostrar que comprenden la nueva dinámica de una sociedad de la información, y con un uso creciente de tecnologías de información y comunicaciones.

Sin un adecuado entendimiento de los temas tecnológicos, la probabilidad de una persecución y una judicialización de un posible criminal informático es limitada. Con base en esta preocupación se planteó una investigación detallada en los Estados Unidos, en 2000 (Jay Myers 2000, p. 11) que buscaba determinar los conocimientos requeridos para detectar, investigar y perseguir crímenes de alta tecnología. Este estudio revisó los programas de pregrado disponibles en justicia criminal, y cómo éstos se estaban formando en los temas de alta tecnología.

Los resultados de esta investigación encontraron que los currículos de los programas revisados debían ser actualizados para preparar a sus egresados frente a un tipo diferente de criminalidad, ahora mediante tecnologías de información. Adicionalmente, la pluralidad de enfoques y formas de comprender los delitos, a través de medios computarizados, hacía que los enfoques curriculares cambiaran y no hubiese uniformidad de las enseñanzas en los programas objeto del estudio.

Además, el estudio detectó que no existía un número suficiente de profesionales con una apropiada combinación de conocimiento de investigaciones y habilidad en tecnologías de información, para combatir el problema creciente de los cibercrímenes. En este contexto, se sugiere que la formación de los nuevos profesionales en la lucha de los cibercrímenes debe comprender al menos tres áreas, a saber: Justicia Criminal y Criminología, Principios de Contabilidad y Auditoría y,

Administración y Operación de Tecnologías de Información (en el documento originalmente se tiene *computer operations and tecnology*).

De manera semejante en Latinoamérica se adelantó un estudio (Cano 2005) sobre la formación de profesionales en este mismo sentido. Este estudio exploratorio realizado con la colaboración y el apoyo de la red de especialistas en derecho informático, Alfa-Redi (http://www.alfa-redi.org) establece conclusiones semejantes, y ofrece una propuesta complementaria a las expuestas en el estudio norteamericano.

La formación de los nuevos profesionales en la lucha de los cibercrímenes debe comprender tres áreas: Justicia Criminal y Criminología, Principios de Contabilidad y Auditoría, y Administración y Operación de Tecnologías de Información.

Dentro de los hallazgos del estudio, se tiene:

1. No existe una definición clara de qué es un perito informático.
2. No es clara la formación de estos profesionales híbridos, a quienes no les son indiferentes las ciencias jurídicas ni su área de formación.
3. "Mientras la justicia no considere la formación de este profesional plural y criminalista digital, los delincuentes, intrusos o agresores en el entorno digital, estarán planeando nuevas estrategias y artimañas para poner en aprietos a la justicia, que deberá fallar posiblemente con pocas y limitadas fuentes de información y análisis integrales" (Cano 2005, p. 11).
4. "(…) se requiere la formación de un perito informático integral que, siendo especialista en temas de tecnologías de información, se quiera formar en las disciplinas jurídicas, criminalísticas y forenses" (Cano 2005, p. 9).
5. "El perito informático, que podemos contextualizar como criminalista digital, es la evolución natural de los instrumentos de la justicia para establecer un nuevo referente frente al rápido avance de las tecnologías de información, y así preparar y ajustar los instrumentos científicos, técnicos y legales, para decirles a los litigios y problemas en el entorno digital que estamos preparados para asumir el reto y confrontar el desafío de la inseguridad informática con argumentos, técnicas y procedimientos que aseguren la transparencia y la confianza de los procesos y sus resultados" (Cano 2005, p. 11).

Con base en este contexto, la criminalística digital, como la ciencia auxiliar de la administración de justicia ahora, en una sociedad de la información y del conocimiento, se apoya en los avances técnicos-científicos asociados con las tecnologías de información y desarrollos tecnológicos emergentes, con el fin de recabar, analizar, custodiar y detallar elementos probatorios basados en mensajes de datos y sistemas de información que procuren la identificación y la reconstrucción de la verdad de los hechos que se investigan.

Si lo anterior es correcto, la formación de los criminalistas actuales exige una nueva especialidad que, adicionalmente al conocimiento detallado de las diferentes disciplinas científicas y las ciencias naturales, detalle las nuevas amenazas en temas informáticos, los diferentes riesgos emergentes derivados de la inseguridad informática, las prácticas y los estándares del manejo de la tecnología de información y el reconocimiento y el estudio de la evidencia digital, como referente natural de las investigaciones en entornos electrónicos e informáticos.

El nuevo criminalista digital debe reconocer su nuevo papel en el escenario de una verdad procesal informática.

En consecuencia de lo anterior, el nuevo criminalista digital debe reconocer su nuevo papel en el escenario de una verdad procesal informática; cómo debe adelantar sus investigaciones, sus procedimientos y actuaciones, cómo descifrar las nuevas motivaciones y tendencias de los intrusos informáticos, y reconocer sus responsabilidades frente a la realidad que le imponen una conducta punible en medios informáticos.

4.2 ROLES Y RESPONSABILIDADES DEL INVESTIGADOR FORENSE EN INFORMÁTICA

Adaptando la propuesta de Ieong (2007, p. 5), en un proceso de investigación forense en informática se identifican ocho roles que participan del mismo: *líder del caso, el propietario del sistema o negocio, el asesor legal, el auditor/ingeniero especialista en seguridad de la información, el administrador del sistema, el especialista en informática forense, el analista en informática forense y el fiscal.* Esos roles tienen un papel fundamental en el desarrollo de la investigación, y en la medida en que se comprendan

los alcances de cada uno de ellos, mejores serán los resultados de las diligencias que se adelanten en el contexto del caso en estudio.

El *líder del caso* es la persona que planea y organiza todo el proceso de investigación digital. Éste, al coordinar todas las actividades que se desarrollan, puede establecer si se avanza o no en la investigación. Generalmente, este rol lo asume la persona designada por la organización o por la administración de justicia para administrar el proceso de investigación, cuidando que los objetivos de la investigación se lleven a cabo. Este rol establece y solicita la investigación inicial, la naturaleza de los eventos investigados, identifica el lugar en donde se llevará a cabo la investigación, establece quiénes serán los participantes iniciales y el marco de tiempo requerido para la misma.

El líder de la investigación deberá tener una visión sistémica de la investigación, para lo cual, cada vez que se avance en el establecimiento de los nexos causales, deberá relacionar cada uno de los hechos del caso para comprender la relación entre el sospechoso, la víctima y la escena del crimen. El líder debe construir la imagen integrada y general del caso, con el fin de evidenciar si lo que se investiga tiene el sustento y el soporte requeridos para verificar o no las conclusiones de la investigación.

El *propietario del sistema o negocio* es por lo general la víctima, la persona natural o jurídica que ha efectuado la denuncia de los hechos y quien está interesado en que se esclarezcan los hechos que lo afectan. El propietario del sistema debe tener un compromiso firme y una voluntad real para invertir tiempo, esfuerzos y recursos para apoyar al equipo que trabaja en la investigación. Es importante anotar que, en algunas ocasiones, este rol puede ser sospechoso dentro del caso.

El *asesor legal* es el abogado litigante líder del caso con el que se cuenta para tener la orientación necesaria a fin de avanzar en los aspectos jurídicos de la investigación en curso. Este rol está en contacto permanente con el líder del caso para mantenerlo enterado de las consideraciones legales que se deben tener en cuenta en las diligencias especiales que se emitan, o los conceptos que se identifiquen en los diferentes momentos de la investigación.

El propietario del sistema o negocio suele ser la víctima, la persona natural o jurídica que ha hecho la denuncia de los hechos.

El abogado litigante es el garante de las condiciones del proceso: los procedimientos aplicados, los aspectos positivos o negativos de la teoría del caso, entre otras, de tal forma que pueda representar con claridad los intereses, bien sea de la defensa o del ente acusador, según corresponda.

El asesor legal deberá conocer en detalle los elementos del derecho procesal, del sistema penal acusatorio y del tema probatorio en el contexto informático, de tal manera que pueda sugerir estrategias de acción que controviertan las pruebas, correlacionen hechos y construyan nexos causales en la búsqueda de la verdad del caso en estudio. Se resalta el hecho de que este rol es el garante de los derechos individuales y colectivos del proceso, en la medida en que custodia el cumplimiento de los deberes de los participantes de la investigación, en el lado de la defensa o de la parte que acusa.

El asesor legal deberá conocer en detalle los elementos del derecho procesal, del sistema acusatorio y del tema probatorio en el contexto informático.

El *auditor/ingeniero especialista en seguridad de la información* conoce el escenario en donde se desarrolla la investigación. Tiene el conocimiento del modelo de seguridad y control donde se materializaron los hechos, conoce los diseños y las implementaciones de las tecnologías de seguridad, y el nivel de confiabilidad de los mismos, validado mediante pruebas de vulnerabilidades y evaluaciones de auditoría, que muestran la confiabilidad de la infraestructura de tecnologías de información.

El *auditor/ingeniero especialista en seguridad de la información* conoce los usuarios definidos, las acciones adelantadas por éstos y los perfiles asociados. En una investigación forense este rol provee información sensible y crítica para los investigadores forenses, pues ellos previamente (si han sido formales en sus diseños) han configurado las pistas de auditoría sobre los objetos de misión crítica, y sobre aquellos de interés de la gerencia de la organización.

El administrador del sistema es el cargo que apoya al especialista en informática forense, para detallar las características del sistema que ha sido comprometido del ataque que se ha materializado y de los posibles rastros que haya dejado el intruso en el sistema. Por su

posición y conocimiento del sistema, el administrador puede ser al tiempo una herramienta muy útil para identificar las acciones de los atacantes, pero al mismo tiempo, el principal sospechoso de los hechos, dado que por lo general es el usuario con todos los privilegios en el sistema y no cuenta con medidas de monitoreo y control formales.

El *especialista en informática forense* es el líder del proceso de investigación de campo en el lugar de los hechos. Es el criminalista digital que tiene como finalidad recabar la INALE, e identificar los diferentes elementos probatorios informáticos vinculados al caso, procurando determinar la relación directa entre los elementos encontrados y los hechos (descubrir el autor, si es posible, demostrar su presencia en el lugar y su presunta responsabilidad) (López Calvo, P. y Gómez Silva, P. 2003, p. 22).

El especialista en informática forense prepara y detalla el modelo de la investigación de campo que se adelantará y desarrollará, en conjunto con el analista en informática forense, para detallar los hallazgos y las relaciones que de éstos surjan para establecer con claridad los móviles de los hechos investigados.

El especialista en informática forense es el líder del proceso de investigación de campo en el lugar de los hechos.

El analista en informática forense examina en detalle los datos, los elementos informáticos o de hardware que se recogieron en la escena del crimen, con el fin de extraer toda la información relevante para el caso, siguiendo para ello procedimientos de aseguramiento de la evidencia, control de los elementos probatorios, herramientas de hardware y software certificadas y las normas y regulaciones pertinentes al análisis en profundidad que debe desarrollar.

El analista en informática forense es un profesional técnico especializado, que conoce de los avances tecnológicos, de las tendencias en ataques y técnicas de los intrusos, así como de la evolución de las técnicas forenses en informática, que le permitan adelantar sus análisis de la forma más concreta y profesional posible. Sabe que la probabilidad de error siempre estará presente, por lo cual documentará todas sus acciones para su análisis y consulta posterior.

Finalmente tenemos el *fiscal del caso*. El fiscal es el ente acusador quien tiene a su cargo controvertir y comprometer los argumentos de la defensa, para lograr la condena de

El fiscal es el ente acusador encargado de controvertir y comprometer los argumentos de la defensa.

la persona acusada. El fiscal es ese personaje que representa por lo general al Estado, que busca la recuperación de los derechos de los ciudadanos y ejercer el orden constitucional que rige la nación (*gráfico 4.1*).

Gráfico 4.1

Roles en las investigaciones forenses en informática

Cada uno de estos roles interactúan dentro del proceso de una investigación forense en informática, con el fin de recabar los elementos probatorios, analizar sus relaciones con los hechos y procurar el esclarecimiento de la verdad sobre lo investigado.

Reconocer los alcances de los roles y sus responsabilidades permite comprender con mayor claridad los elementos de un proceso de investigación forense en informática, y así seguir la pista del desarrollo del caso, y cómo sus participantes suman en la dinámica técnico-jurídica que proponen esta clase de investigaciones.

Es importante anotar que los roles presentados previamente responden a un proceso estructurado y formal donde existen recursos disponibles para contar con personal en cada uno de ellos. En este sentido, pueden existir procesos en los cuales una misma persona puede asumir varios de ellos, manteniendo la formalidad del proceso que se adelanta. Aun cuando una investigación sea de carácter interno o judicial, la formalidad del proceso se debe mantener, a pesar de que un mismo profesional pueda asumir varios papeles en el proceso, claro está considerando los posibles conflictos de interés que se pudieran presentar.

4.3 MODELOS Y PROCEDIMIENTOS PARA ADELANTAR INVESTIGACIONES FORENSES EN INFORMÁTICA

El incrementar los niveles de formalidad de las investigaciones forenses en informática implica , por un lado, fortalecer los programas académicos en esta disciplina y, por otro, afianzar y mejorar los modelos y procedimientos para adelantar las investigaciones donde la información almacenada electrónicamente sea parte del acervo probatorio bajo análisis.

En este contexto, en esta sección se revisa la evolución de los modelos de investigaciones forenses en informática basados en la investigación realizada por Pollitt (2007), complementada por las recientes propuestas desarrolladas por Abdalla, Hazem y Hashem (2007), con el fin de establecer referentes básicos sobre procedimientos generales de aplicación sobre investigaciones forenses en informática, que habrá que afinar y ajustar según las necesidades de cada caso. De igual forma, se comentará brevemente sobre algunas de las herramientas actuales, tanto de código abierto como aquellas sujetas a proveedores que materializan los análisis y extracciones que se detallan en los procedimientos forenses en informática.

De acuerdo con Bishop y otros (2007), existen cinco (5) principios generales para adelantar un análisis forense en informática:

- Considere el sistema completo
- Registre la información a pesar de las fallas o de los ataques que se generen
- Considere los efectos de los eventos, no sólo las acciones que los causaron
- Considere el contexto, para asistir en la interpretación y el entendimiento de los eventos
- Presente los eventos de manera que puedan ser analizados y entendidos por un analista forense

Estos cinco principios deben ser transversales a los modelos de investigaciones y procedimientos de análisis forense, de tal modo que los profesionales en esta disciplina, al adelantar sus acciones sobre las evidencias recabadas en la escena del delito, mantengan la formalidad de sus resultados y la documentación requerida para defender sus informes.

4.3.1 Algunos modelos de investigaciones forenses en informática[2]

Uno de los primeros modelos reportados para adelantar investigaciones forenses en informática fue el desarrollado por Pollitt en 1995, que establecía que las investigaciones contaban con cuatro fases: adquisición, identificación, evaluación y admisión de las pruebas como evidencia. Estas cuatro fases exigían de los investigadores procedimientos formales que permitieran, entre otros puntos, mantener la formalidad de la cadena de custodia, la integridad del medio original, el análisis de los datos y los soportes técnicos y científicos para sustentar la admisibilidad de la prueba para su valoración por parte de juez.

Uno de los primeros modelos reportados para adelantar investigaciones forenses en informática fue el desarrollado por Pollitt, en 1995.

En este contexto, Pollitt establece que la admisibilidad de los elementos materiales probatorios, como evidencia formal, debía revisarse en los contextos físico, lógico y legal. Tres variables que permitieran evidenciar lo efectuado sobre el medio, lo registrado en los medios y lo requerido para soportar el caso, respectivamente.

El modelo jerárquico de tres niveles sugiere una estructura base para el desarrollo de guías, para adelantar investigaciones forenses en informática.

Luego en el año 2000, Noblett, Pollitt y Presley establecieron un modelo jerárquico para el desarrollo de guías para adelantar investigaciones forenses en informática. Este modelo surge como una respuesta a la necesidad de comenzar a estructurar los temas de la práctica de diligencias forenses informáticas, para lo cual sugiere una estrategia para desarrollar un cuerpo formal de conocimiento en los temas de investigaciones forenses en informática (*gráfico 4.2*).

Ese cuerpo de conocimiento establece tres niveles de análisis: procedimientos y técnicas, política organizacional y prácticas y principios de revisión. Basados en estas tres variables, los autores establecen focos de investigación y aplicación, que permitan contar con desarrollos posteriores ordenados y consecuentes con las necesidades de las investigaciones forenses en informática.

[2] Resumen de Pollitt 2007.

Gráfico 4.2

Un modelo jerárquico de tres niveles para desarrollar guías de apoyo a las investigaciones forenses en informática. (Traducido de: Pollitt, M. 2007, p. 3).

En 2001, el *Digital Forensic Research Workshop* –Dfrws (http://www.dfrws.org), organización sin ánimo de lucro y basada en el voluntariado, dedicada a compartir conocimiento y difundir ideas sobre las investigaciones forenses en informática, desarrolló un trabajo conjunto con diversos investigadores y analistas del tema, para establecer un modelo general de investigaciones forenses en informática que cubre siete (7) etapas, a saber: identificación, preservación, recolección, examen, análisis, presentación y decisión.

Cada una de esas etapas cuenta con una serie de prácticas para tener en cuenta, con el fin de que el investigador cuente con un conjunto de elementos formales de aplicación al efectuar su diligencia forense, y aumentar así la formalidad y la credibilidad de sus análisis y conclusiones. Para mayor información sobre este particular, revisar: http://www.dfrws.org/2001/dfrws-rm-final.pdf.

En 2003, los investigadores Carrier y Spafford desarrollaron un nuevo modelo de investigaciones forenses en informática, que combina lo que ocurre en las investigaciones forenses físicas tradicionales con lo que se desarrolla en las investigaciones forenses en informática. Esta combinación sugiere la revisión de los procedimientos de análisis establecidos hasta el momento en los temas informáticos, a la luz de lo que se tiene definido para los temas de ciencias forenses tradicionales, lo cual permite organizar las actividades realizadas hasta hoy en la aplicación científica de los procedimientos forenses en medios informáticos.

En 2003, Carrier y Spafford desarrollaron un modelo conceptual de análisis basado en entradas y salidas.

Durante el mismo año 2003, Carrier desarrolla un modelo de abstracción para adelantar el examen forense en informática. Su modelo establece dos entradas y dos salidas, tal como se presenta a continuación. Ese modelo sostiene que para tener el examen de un objeto se requieren datos base del análisis de objeto; por ejemplo, el sistema de archivos, la metadata, la aplicación que lo genera, entre otras. Este escenario define unas reglas de aproximación y revisión que luego de reconocidas y aplicadas sobre el objeto, se tienen datos de salida de esta operación, y el margen de error basado en las herramientas utilizadas (*gráfico 4.3*).

Gráfico 4.3

Modelo de nivel de abstracción para adelantar un examen forense en informática. (Traducido de Pollitt 2007, p. 6).

Cada uno de los modelos presentados anteriormente establece referentes conceptuales que les permiten a los investigadores forenses en informática consideraciones formales, en cuanto a las fases que deben seguir las investigaciones para que en la práctica se fortalezcan los resultados de los procedimientos aplicados a los casos que se adelanten.

Recientemente Abdalla, Hazem y Hashem (2007), retomando y analizando estos modelos de investigaciones y otros que por extensión de los mismos se omiten en esta sección, han propuesto un discurso metodológico de investigaciones forenses en informática que cubre muchos de los aspectos requeridos, cuando se trate de una investigación de un cibercrimen.

Esta propuesta consta de cinco fases: preparación, forensia física e investigación, forensia digital, reporte y presentación, cierre

o clausura. Es importante anotar que esta propuesta metodológica se alinea con los roles y las responsabilidades del investigador forense en informática presentados anteriormente (Abdalla, Hazem y Hashem 2007, pp. 57-58).

En la fase de *preparación* se adelantan los procedimientos de atención y manejo de incidentes, los cuales se deben aplicar en cualquier investigación. El propósito de esta fase es hacer confiable tanto la operación como la infraestructura que soporta la investigación. Esta fase, a su vez, se divide en prepreparación, evaluación del caso, preparación de los detalles para el caso, preparación de plan de la investigación y determinación de los recursos requeridos. En esta fase intervienen el líder del caso y el asesor legal.

En la fase de preparación se adelantan los procedimientos de atención y manejo de incidentes.

En la fase de *investigación y forensia* física se recolecta, preserva y analiza la evidencia física, así como la reconstrucción de que ocurrió en la escena del crimen. Esta etapa se compone, a su vez, de otros momentos, como son: preservación física, examen preliminar de la escena del crimen, evaluación de la escena física, documentación inicial, fotografía y narración, búsqueda y recolección de evidencia física y examen final de la escena física del crimen. Durante esta etapa pueden estar participando el propietario del sistema, el especialista en seguridad y el administrador del sistema.

En la etapa de *forensia digital* se busca identificar y recolectar los eventos electrónicos e informáticos que han ocurrido en el sistema y analizarlos, de tal manera que los resultados puedan ser utilizados con los resultados anteriores en la reconstrucción de los eventos. Este paso incluye actividades, como la evaluación y la valoración, adquirir la evidencias digitales, el examen de la escena digital, la revisión y el análisis de la evidencia digital, la reconstrucción y el análisis de los datos extraídos y las conclusiones. Generalmente, en esta fase participan el especialista y el analista en informática forense.

En la fase de investigación y forensia física se recolecta, preserva y analiza la evidencia física.

Seguidamente tenemos la fase de *reporte y presentación*, en donde se exhiben las conclusiones y la correspondiente evidencia sobre la investigación adelantada. En casos de investigaciones empresariales, la audiencia típicamente incluye al abogado representante, al área de recursos humanos y los ejecutivos de la compañía. Lo que se revisa en este contexto son las directrices corporativas y la reglamentación interna de la organización. En el caso de un proceso legal, la audiencia son el juez, el jurado (si aplica), el abogado de la defensa, la fiscalía o el ente acusador, considerando que los elementos materiales probatorios entregados deben ser entregados previamente para su evaluación, antes de ser considerados evidencia formal en el caso. Esta fase cuenta con la participación del líder del caso, el asesor legal y el especialista en informática forense.

En la fase de reporte y presentación se exhiben las conclusiones y la evidencia.

Finalmente, se tiene la fase de *clausura o cierre del caso*, en la cual se detalla la revisión de todos los procedimientos aplicados en la investigación, se revisa qué tan bien se adelantaron tanto las investigaciones físicas como digitales, cómo se desarrolló la recolección de la evidencia y la suficiencia de los análisis realizados para resolver el caso. Así mismo, se asegura el retorno de la evidencia física y digital a sus dueños, siempre y cuando hacerlo no constituya ninguna contravención o violación de restricciones previamente impuestas por el juez sobre ésta.

A manera de resumen, se presenta un gráfico que detalla algunas de las acciones previstas en cada uno de los pasos del discurso metodológico presentado anteriormente (*gráfico 4.4*).

En la medida en que los investigadores forenses en informática profundicen y analicen los modelos actuales de investigaciones forenses digitales, es posible revisar la práctica misma de las diligencias, para que se mejoren aspectos que a la fecha no se han contemplado. Es claro que si bien estos modelos presentados son fruto de años de investigación y práctica de la disciplina, son fuente permanente de actualización, dada la dinámica propia de la inseguridad informática en los avances de las tecnologías de información.

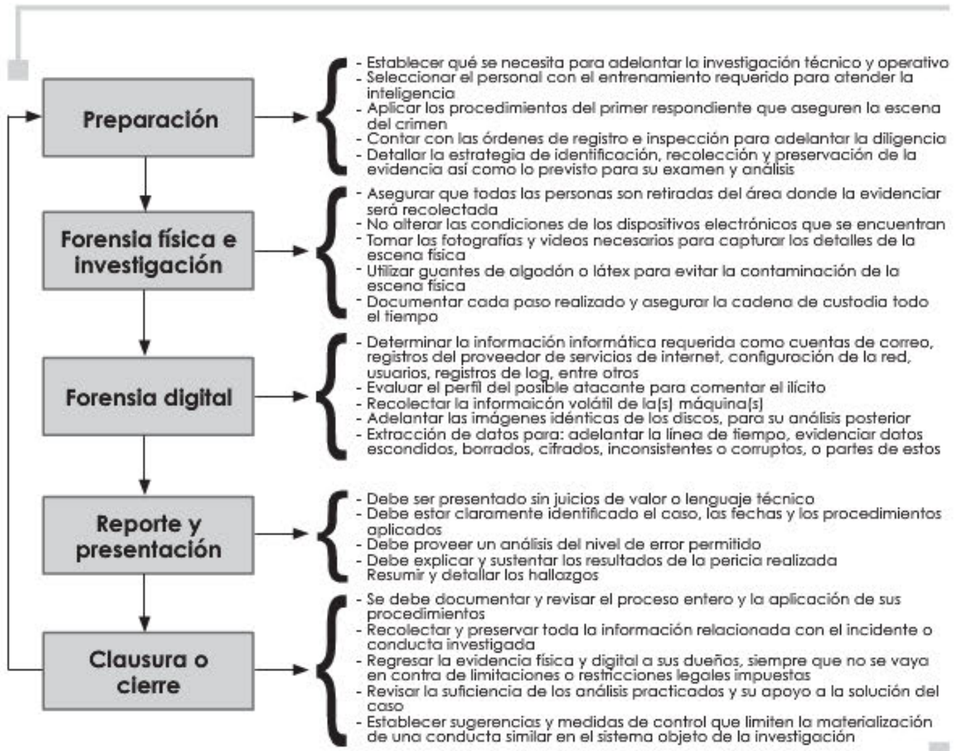


Gráfico 4.4

Modelo de investigación forense digital. (Adaptado y traducido de: Abdalla, Hazem y Hashem 2007, pp. 57-58).

4.4 CREDENCIALES PARA LOS INVESTIGADORES FORENSES EN INFORMÁTICA

Es un hecho que durante la última década las intrusiones y los incidentes de seguridad han crecido de manera exponencial, estableciendo un escenario oscuro sobre la seguridad de las infraestructuras de computación. En este sentido, las organizaciones han adelantado esfuerzos en el mejoramiento de su seguridad, instalando diferentes mecanismos de protección y efectuado múltiples pruebas, con el fin de optimizar las condiciones de seguridad existentes en cada uno de sus entornos de negocio. Sin embargo, dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre permanece; por tanto, cuando éste se presenta, las organizaciones son puestas a prueba para validar su capacidad de respuesta y atención a los mismos.

Las intrusiones y los incidentes de seguridad han crecido de manera exponencial, durante la última década.

El atender un incidente exige que la organización destine recursos importantes para contar con un equipo que entre en acción cuando esto ocurre. Un equipo que no debe conocer exclusivamente de elementos tecnológicos, sino tener habilidades gerenciales que le permitan comprender en los procesos de negocio cómo se ha materializado la inseguridad para, por un lado, contener los posibles avances y los impactos de la misma y, por otro, detallar en profundidad las implicaciones de los posibles daños en el contexto del negocio.

Los investigadores forenses en informática, profesionales que contando con un conocimiento de los fenómenos técnicos en informática, son personas preparadas para aplicar procedimientos legales y técnicamente válidos para establecer evidencia en situaciones en las cuales se vulneran o se comprometen sistemas, utilizando métodos y procedimientos científicamente probados y claros que permitan establecer posibles hipótesis sobre el hecho, y contar con la evidencia requerida que sustente esas hipótesis.

Con el fin de desarrollar este perfil forense en informática, se han adelantado esfuerzos importantes en el mundo para contar con documentación, entrenamiento y procedimientos de aplicación generalmente aceptada que permitan validar actuaciones y valoraciones de profesionales forenses en informática de manera estándar en el mundo. Es importante referir que los esfuerzos internacionales de la industria representan una iniciativa que busca afrontar el reto de la formación de un especialista en informática forense.

Los esfuerzos internacionales de la industria son una iniciativa para afrontar el reto de la formación de un especialista en informática forense.

En este sentido, la Iacis –International Association of Computer Investigative Specialist (http://www.cops.org)–, la HTCN (http://www.htcn.org) –High Technology Crime Network, la Iisfa –International Information Systems Forensics Association (http://www.iisfa.org/)–, la Isfce –International Society of Forensic Computer Examiners (http://www.isfce.com/)– y el SANS Institute (http://www.sans.org/

about/sans.php), cinco asociaciones internacionales (generalmente denominadas neutrales ante los proveedores; es decir, no están orientadas a productos o servicios específicos), han desarrollado programas de certificación forenses en informática, que permiten detallar algunas habilidades requeridas y capacidades deseables en los investigadores forenses informáticos.

4.4.1 IACIS

La Iacis ofrece la certificación internacional denominada External CFCE –*Certified Forensic Computer Examiner*, la cual se encuentra diseñada tanto para personas que no pertenezcan a instituciones judiciales o de policía, para los cuales el programa cuenta con algunas diferencias, dada su función, como para oficiales o personas con funciones de policía judicial activos. Este proceso externo está abierto para aquellos informáticos forenses que consideran que tienen el entrenamiento necesario y la experiencia para convertirse en CFCE.

Para adelantar este proceso, las personas interesadas deben aplicar y cancelar el valor de la aplicación, la cual será revisada y analizada por el cuerpo directivo de la Iacis. Si la aplicación es rechazada, el valor pagado previamente le será devuelto al aplicante.

La IACIS ofrece la certificación internacional denominada External CFCE –Certified Forensic Computer Examiner.

El proceso de certificación externo (para aquellos que aun habiendo tomado el curso anual de dos semanas coordinado por la Iacis no lograron la certificación) consiste en tres problemas relacionados con disquetes, uno con una imagen de una USB, otro problema de "Wildcard" o palabra comodín en la formulación de búsquedas, un análisis de un disco duro, un análisis de un CD y un examen final escrito. Cada problema debe ser revisado, resolver el problema técnico planteado y generar un reporte formal de sus análisis y resultados. Luego de evaluados sus resultados por el personal de la Iacis dispuesto para esta evaluación y, si es satisfactoria, se le entrega al candidato el siguiente ejercicio. Es importante acotar que existe un período de tiempo limitado para la entrega de los reportes en inglés de cada uno de los problemas.

4.4.2 HTCN

La HTCN ofrece diversas certificaciones en la línea forense en informática. En particular revisaremos el CCCI –Certified Computer Crime

Investigator–, nivel básico y avanzado. Cada una de las certificaciones requiere que el aplicante cuente con un curso de entrenamiento, con un número de horas y exámenes escritos debidamente aprobados, en centros de entrenamiento autorizados, con el fin de contar con las destrezas requeridas para otorgar la certificación.

El propósito de la certificación es desarrollar un alto nivel de profesionalismo y entrenamiento continuo, que soporte investigaciones de crímenes de alta tecnología en la industria y las organizaciones. El pago del costo de la certificación se utiliza para evaluar el documento de aplicación y analizar la experiencia del aspirante, así como para cubrir los gastos relacionados con el registro ante notaría de la experiencia certificada y los títulos adjuntos.

La certificación CCCI nivel básico requiere del aplicante:

- Tres años de experiencia directamente relacionada con la investigación de incidentes técnicos o crímenes informáticos (como agente de policía judicial o como investigador interno organizacional).
- Haber completado satisfactoriamente un curso de 40 horas sobre delitos informáticos o computación forense, ofrecido por una agencia, organización o empresa.
- Entregar un reporte narrativo, detallando su experiencia derivada de investigaciones, de al menos 10 casos relacionados con delitos informáticos.

La certificación CCCI nivel avanzado requiere del aplicante:

- Cinco años de experiencia directamente relacionada con la investigación de incidentes técnicos o crímenes informáticos (como agente de policía judicial o como investigador interno organizacional).
- Haber completado satisfactoriamente un curso de 80 horas sobre delitos informáticos o computación forense, ofrecido por una agencia, organización o empresa.
- Haber sido investigador líder en al menos veinte casos y haber participado en al menos cuarenta casos adicionales, bien sea como líder, supervisor o como profesional especializado de apoyo. El total de casos donde haya participado debe ser como mínimo de sesenta.

- Entregar un reporte narrativo, detallando su experiencia derivada de investigaciones, de al menos 15 casos relacionados con delitos informáticos.

4.4.3 IISFA

La Iisfa ofrece la certificación denominada CIFI –Certified Information Forensics Investigador–, la cual exige conocimiento en múltiples áreas (técnicas y jurídicas), experiencia práctica y demostración de habilidades y entendimiento de la informática forense, para lo cual somete a sus candidatos a un examen.

De acuerdo con lo expuesto en su sitio Web durante el año 2005 (http://Web.archive.org/Web/20050617073432/www.iisfa.org/certification/certification.asp), el cuerpo de conocimiento de evaluación de los profesionales que aplican a esta certificación consideraba aspectos de auditoría, atención de incidentes, ley e investigaciones, herramientas y técnicas, seguimiento de rastros y contramedidas o controles. A la fecha, en el sitio Web actual no hay mayor información sobre esta certificación. Para obtener mayor información al respecto, a los lectores les recomendamos regresar frecuentemente a la página de esta asociación.

4.4.4 ISFCE

A diferencia de otras asociaciones, la Isfce es una entidad privada, fundada en conjunto con una compañía norteamericana dedicada a los temas de computación forense, denominada Key Computer Service, LLC. Esta asociación ofrece la certificación CCE –Certified Computer Examiner–, la cual se otorgó por primera vez en el año 2003.

Hasta la fecha, la certificación CCE tiene varios niveles: básico y avanzado o maestro. Las habilidades requeridas para el nivel básico son:

La certificación CCE tiene varios niveles: básico y avanzado o maestro.

- Buen entendimiento de las reglas de la evidencia, particularmente lo relacionado con:
  - Identificación y adquisición de medios magnéticos
  - Manejo, etiquetado y almacenamiento de evidencia digital
  - La cadena de custodia
  - El derecho a la privacidad

- Buen entendimiento de cómo eliminar, verificar y validar medios de almacenamiento de información.
- Buen entendimiento de cómo proteger el medio original de escrituras accidentales.
- Buen entendimiento de cómo hacer y verificar copias exactas de medios de almacenamiento de información.
- Un entendimiento básico del hardware del PC.
- Un buen entendimiento básico de las redes de computadores.
- Un buen entendimiento de las aplicaciones de Microsoft Office, y cómo acceder a la metadata almacenada en estos archivos.
- Un entendimiento básico de formatos de datos y sus encabezados.
- Un entendimiento básico de cómo quebrar contraseñas.
- Un entendimiento básico de los aspectos de Internet, como son el "who is", entre otros servicios.
- Habilidad para escribir claramente reportes.
- Habilidad para organizar y presentar gráficas y análisis de resultados en reportes.

La asociación anuncia que tendrá disponible la certificación Master Certified Computer Examiner –MCCE–, para aquellos que ya son CCE y quieren avanzar en un nivel superior de habilidad y reconocimiento de sus actividades, para lo cual deben tomar cursos especializados.

4.4.5 SANS Institute

El Instituto de Administradores de Sistemas, Auditoría, Redes y Seguridad (SANS, por sus siglas en inglés de SysAdmin, Audit, Network, Security), es una institución creada en 1989, para formación, entrenamiento y generación de conocimiento en temas de seguridad de la información. En este empeño ha creado una serie de certificaciones en diferentes temas; particularmente en el tema de informática forense se tiene la Global Information Assurance Certification Certified Forensics Analyst, conocida como GCFA por sus siglas en inglés.

Esta certificación buscar formar individuos responsables de investigaciones y análisis forenses, aquellos encargados del manejo y del control de incidentes, que finalmente adelantan investigaciones formales de los mismos. Para alcanzar esta certificación se requiere tomar un examen supervisado de 150 preguntas en 4 horas. La certificación se debe renovar cada cuatro años.

Dentro del conjunto de temas que se revisan en esta certificación, tenemos:

- Estructura de sistemas de archivos y su metadata
- Característica de los sistemas de archivos FAT/NTFS/Ext2/Ext3
- Mejores prácticas en el manejo de evidencia e integridad de la misma
- Adquisición de evidencia de discos duros y datos volátiles
- String Searching Utilizing Dirty Word Lists
- Análisis de tiempo sobre sistemas de archivo
- Recuperación de datos utilizando cadenas y encabezados de archivos
- Comparación de hash de archivos contra bases de datos de hash
- Análisis del registro del sistema, rastros en Internet y metadata de archivos
- Análisis de huellas de las aplicaciones
- Análisis forense de USB
- Análisis forense de Windows XP y Vista

Con las certificacones presentadas anteriormente se pretende mostrar un conjunto base de conocimientos y experiencia requerida para la formación de investigadores forenses en informática, y no recomendar alguna de ellas como la más valiosa o importante en el tema. En este sentido, las certificaciones son una interesante carta de presentación de un profesional en informática forense; sin embargo, es necesario que la academia adelante esfuerzos para establecer programas de formación en estos temas, que permitan un desarrollo complementario y científico en esta naciente disciplina derivada de las ciencias forenses tradicionales (*cuadro 4.1*).

	Técnica	Jurídica	Procedimientos	Comentarios
IACIS	X	X	X	Ofrece una certificación balanceada y basada en el ejercicio práctico de los investigadores en el área. Se verifica actividad permanente en el sitio Web.
HTCN	-	-	-	Se basan en la validación de la experiencia de los aplicantes y los cursos que han tomado en el tema de informática forense. Se ha reactivado el sitio Web recientemente, así como la membresía.
IISFA	X	-	X	Ofrece una certificación orientada a los aspectos técnicos y de procedimiento. Su sitio Web no se encuentra actualizado a la fecha.
ISFCE	X	X	X	Ofrece una certificación semejante a lo que se tiene en Iacis, dado que su fundador fue miembro del cuerpo directivo de esa asociación. Es una entidad privada, soportada por una empresa particular en temas de computación forense en EE.UU.
SANS GIAC	X	-	X	Ofrece una certificación fuertemente orientada a los elementos técnicos informáticos. Es ideal para aquellos que quieren profundizar en los detalles de la implementación de las tecnologías.

Cuadro 4.1

Análisis de certificaciones en informática forense

En consecuencia con lo anterior, se tienen algunas iniciativas académicas internacionales que mencionamos a continuación, como ejemplos que se vienen desarrollando para formar en la academia los especialistas en informática forense. Una lista parcial de programas académicos formales en temas de informática forense, computación forense y temas conexos con seguridad de la información se puede encontrar en: http://www.e-evidence.info/education.html.

Bachelor of Science (B.S) in computers and digital forensic (http://digitalforensics.champlain.edu/index.html), programa de pregrado de cuatro años desarrollado por el College de Champlain en el estado de Vermont en los Estados Unidos. Este programa busca responder a la creciente demanda de especialistas en temas de computación forense en este país, con el fin de contar con un profesional formado en la academia en los temas de ciencias forenses aplicadas a la informática.

Master of Science (M.S) in Forensic Computing (http://www.comp.brad.ac.uk/courses/courses.php/pg/mscfc/struct), programa de maestría en computación forense desarrollado por la Universidad de Bradford en el Reino Unido, el cual es parte de la tradición de formación que en esta parte del mundo se ha venido dando en los temas de persecución de criminales a través de medios informáticos.

Master of Science (M.S) in Digital Forensic (http://msdf.ucf.edu/), programa de maestría en forensia digital, desarrollado por la Universidad Central de Florida, es un de los esfuerzos académicos en Norteamérica que busca especializar a los profesionales que se han venido desempeñando en temas de investigaciones forenses en informática. Este programa ofrece áreas de formación tanto para los profesionales en ejercicio como para aquellos que quieran continuar con una formación de investigación científica en el área.

Por último detallamos una propuesta de formación de un profesional en informática forense, desarrollado a la luz de una investigación (Cano 2005), realizada en Latinoamérica con el apoyo de la red latinoamericana de especialistas en derecho informático Alfa-Redi (http://www.alfa-redi.org). El autor establece cinco áreas de formación, a saber: tecnologías de información y electrónica, seguridad de la información, jurídica, ciencias forenses y criminalística e informática forense.

Área de Tecnologías de Información y Electrónica:

- ❒ Lenguajes de programación
- ❒ Teoría de sistemas operacionales y sistemas de archivo
- ❒ Protocolos e infraestructuras de comunicación
- ❒ Fundamentos de circuitos eléctricos y electrónicos
- ❒ Arquitectura de computadores
- ❒ Fundamentos de bases de datos

Área de Seguridad de la Información:

- ❒ Principios de seguridad de la información
- ❒ Políticas, estándares y procedimientos en seguridad de la información
- ❒ Análisis de vulnerabilidades de seguridad informática
- ❒ Análisis y administración de riesgos informáticos
- ❒ Recuperación y continuidad de negocio
- ❒ Clasificación de la información

- ❒ Técnicas de Hacking y vulneración de sistemas de información
- ❒ Mecanismos y tecnologías de seguridad informática
- ❒ Concienciación en seguridad informática

Área Jurídica:

- ❒ Teoría general del Derecho
- ❒ Formación básica en delito informático
- ❒ Formación básica en protección de datos y derechos de autor
- ❒ Formación básica en convergencia tecnológica
- ❒ Formación básica en evidencias digital y pruebas electrónicas
- ❒ Análisis comparado de legislaciones e iniciativas internacionales

Área de Criminalística y Ciencias Forenses:

- ❒ Fundamentos de conductas criminales
- ❒ Perfiles psicológicos y técnicos
- ❒ Procedimientos de análisis y valoración de pruebas
- ❒ Cadena de custodia y control de evidencias
- ❒ Fundamentos de Derecho Penal y Procesal
- ❒ Ética y responsabilidades del perito
- ❒ Metodologías de análisis de datos y presentación de informes

Área de Informática Forense:

- ❒ Esterilización de medios de almacenamiento magnético y óptico
- ❒ Selección y entrenamiento en software de recuperación y análisis de datos
- ❒ Análisis de registros de auditoría y control
- ❒ Correlación y análisis de evidencias digitales
- ❒ Procedimientos de control y aseguramiento de evidencias digitales
- ❒ Verificación y validación de procedimientos aplicados en la pericia forense

El establecer un programa que cubra las áreas propuestas en esta investigación requiere un esfuerzo interdisciplinario y voluntad de cooperación entre la academia, el gobierno y la industria, para iniciar la formación de un profesional que eleve los niveles de confiabilidad y formalidad exigidos para que, en un entorno digital, la justicia ofrezca las garantías requeridas en los procesos donde la evidencia digital es la protagonista.

4.5 INFORMES DE INVESTIGACIÓN Y PRESENTACIÓN DE PRUEBAS INFORMÁTICAS

Complementario a lo anterior es necesario desarrollar una sección especial para detallar las estrategias y los modelos de informes de investigaciones realizadas, así como aspectos prácticos requeridos para ilustrar los resultados de las diligencias adelantadas en el contexto de las pruebas informáticas o digitales identificadas y analizadas en un caso.

4.5.1 Teoría básica de la preparación de informes

Antes de iniciar el desarrollo de los informes, revisaremos la teoría base de la presentación de informes como contexto general y orientación al lector sobre este tema. Desarrollar un informe debe ser una tarea con propósito, que exige de su creador el análisis de su público objetivo, redacción, ortografía, claridad y oportunidad en su entrega.

Los informes pueden ser escritos por muchas razones; entre otras (Forsyth, P. 2003, p. 21), tenemos:

Para que un informe sea bien recibido, su creador debe tener claras las expectativas de sus lectores.

- Informar
- Recomendar
- Motivar
- Influir o tomar parte en una discusión
- Persuadir
- Impresionar
- Registrar
- Reforzar o extender situaciones o creencias presentes
- Instruir
- Validar y verificar una situación

Para que un informe sea bien recibido por sus lectores, su creador debe tener claras las expectativas de los mismos. Estudiar quién será el receptor de este documento y el propósito del mismo son elementos clave que los investigadores forenses en informático deben contemplar a la hora de elaborar su informe. No es solamente detallar los procedimientos y hallazgos de su diligencia, sino presentar, de la mejor forma, los hechos y las acciones adelantadas, para que la audiencia siga, de manera clara y precisa, lo que se quiere ilustrar en el documento. Es claro que en este informe, como se aplica

en algunos casos, en los cuales "...la prueba pericial es procedente para efectuar valoraciones que requieran conocimientos científicos, técnicos, artísticos o especializados", se presentan modelos y prácticas académicas, técnicas y científicas especializadas con el fin de analizar los elementos materiales probatorios entregados para su estudio.

En un informe no se admiten palabras superlativas o diminutivas, que expresen o motiven emociones más allá de lo que las pruebas o los modelos científicos sugieran.

En este contexto, un informe que puede llegar de manera más agradable al lector (Forsyth, P. 2003, p. 23), debe tener las características de ser:

- **Breve:** Un informe que diga lo necesario, vaya directamente a los hechos investigados y presente las teorías base de sus análisis. Ser breve no implica poco número de páginas, pero sí un importante esfuerzo del creador para lograr su propósito.
- **Claro**: Un informe se debe comprender en su lectura, con lenguaje apropiado según su audiencia, libre de jerga propia de grupos o profesiones, ajustado a los hechos presentados.
- **Preciso:** Un informe no debe desviarse de su objetivo, ni adornarse con el lenguaje. Esto le permite al lector mantenerse concentrado en lo que corresponde.
- **Simple:** Un informe no debe sugerir estructuras complejas del documento, múltiples secciones o subdivisiones que hagan perder al lector en su objetivo. Las secciones deben ser las mínimas requeridas, animadas con párrafos introductorios que le den continuidad al documento.
- **Bien estructurado:** Un informe debe sugerir una secuencia de presentación que muestre el objetivo del mismo y oriente al lector en su búsqueda y comprensión del mismo.

Si bien un informe pericial tendrá un grado importante de especialidad, no quiere decir que dicho documento no pueda ser revisado por una persona del común sin la especialidad requerida. En particular, un informe pericial debe ser lo suficientemente concreto de modo que el objetivo perseguido por su creador se verifique tanto en el personal especializado como en la persona sin el conocimiento

propio de su especialidad. Es importante recordar que pueden existir al menos dos tipos de documentos. Uno de carácter eminentemente técnico, con detalles tecnológicos concretos y explícitos y otro de corte preferencialmente gerencial, que contendrá el resumen de los hechos y las implicaciones propias para la organización.

Recordemos que el lector del informe pericial tiene su propio interés y quiere que el informe sea tan conciso como lo hemos presentado anteriormente; sólo lo considerará realmente útil si lo encuentra comprensible, interesante y relacionado con su propia situación o realidad. Sin embargo y dado que este informe presenta análisis realizados por una persona especializada en un tema, la lectura de un tercero será focalizada; es decir, si es la parte de la defensa, buscará los elementos que le sean más favorables, y otro tanto hará la fiscalía o la parte acusadora.

Tomando como base lo anterior, el creador del informe pericial debe considerar algunos elementos que es preciso evitar en la redacción del mismo, tales como enviar un mensaje equivocado a sus lectores. Entre otros aspectos (Forsyth, P. 2003, pp. 76-78), al redactar un informe hay que tener en cuenta:

- **Parcialidad:** Un informe pericial no debe sugerir o inclinarse siguiendo intereses propios o ajenos, esto le resta credibilidad y formalidad. El creador debe construir su documento ajustado a los formalismos científicos y pruebas realizadas, con lo cual deberá concluir y verificar sus resultados.
- **Juicios de valor:** Las palabras superlativas o diminutivas, que expresen o motiven emociones más allá de lo que las pruebas o los modelos científicos sugieran, no son admisibles. Además de cuestionar al creador del documento, no muestran la imparcialidad del evaluador de los elementos materiales probatorios. Conviene aclarar que un juicio de valor bien fundado, puede ser un elemento importante en el informe.

> El objetivo de un informe pericial es entregar y revelar la opinión de un perito, sobre un tema específico de su especialidad.

- **Inconsistencia:** Un informe con inconsistencia o inconsistente es aquel que en su estructura y redacción contradice su posición, o

que, relacionado con otros documentos previos del autor, descalifica la posición de éste en el mismo. Es importante que el creador del documento, mantenga una posición clara de sus hallazgos y, basado en ellos, detalle sus conclusiones.

4.5.2 Consideraciones básicas sobre los informes periciales

Siguiendo lo establecido por Babitsky, S. y Mangraviti, Jr, J. (2002), un informe pericial persuasivo, comprensivo y formal debe considerar las pautas siguientes, que son complementarias a las prácticas presentadas anteriormente. En particular, las recomendaciones de los autores buscan darle mayor profundidad, credibilidad y poder al informe que se presenta:

- No especule o trate de adivinar cosas.
- Evite el uso de universales o absolutos como "siempre", "nunca", "para todos los casos".
- Evite expresiones que sugieran vaguedad, aspectos equívocos o incertidumbre.
- Evite el uso de lenguaje empático, signos de exclamación, uso de formatos, como negrita, itálicas y mayúsculas para enfatizar los hallazgos o lasconclusiones.
- Use lenguaje preciso sin jerga.
- Use un lenguaje seguro, sin adornos literarios y evite las palabras como "se ve como", "podría", "aparentemente", "yo creo", "es probable que", entre otras.
- Defina todo término técnico propio del informe.
- Use un lenguaje concreto sobre los hechos, y evite caracterizaciones subjetivas para describir la investigación, los hallazgos y las conclusiones.
- Explique cualquier abreviatura utilizada.
- Evite lenguaje argumentativo que pueda sugerir que el autor se inclina por un interés particular.
- Evite comentarios sobre la credibilidad de los testigos y las pruebas.

- Mantenga presente validar la consistencia de su informe, tanto dentro de su contenido, como su relación con otros casos donde usted haya participado.
- Evite cualquier sesgo en su informe.
- Numere las líneas de su informe para que en caso de requerirse alguna revisión de sus resultados, se remitan de manera rápida al sitio en el mismo.

4.5.3 Estructura base de un informe pericial

Un informe pericial tiene como objetivo entregar y revelar la opinión de un perito[2], sobre un tema específico de su especialidad. Esta diligencia de análisis y detalle de los objetos propios del caso puede ser solicitada por la defensa o sugerida por la fiscalía. En este caso, si fue solicitada por la defensa, el perito será de parte, posiblemente pagado por el representante del acusado. Si la pericia es solicitada por la fiscalía, generalmente el Estado provee los peritos de oficio, quienes son parte de la administración de justicia, los cuales no reciben remuneración adicional por adelantar estas diligencias, dado que es parte de su trabajo como servidor de la Justicia.

Si bien cada informe pericial tiene su propia dinámica, a continuación presentamos a manera de ejemplo de estructura general de un informe pericial orientado particularmente a temas de informática forense.

A la fecha no hay programas de estudio o de formación especializada para educar y entrenar formalmente a los nuevos criminalistas.

[2] Definición tomada del Diccionario de la Real Academia Española: Persona que, poseyendo determinados conocimientos científicos, artísticos, técnicos o prácticos, informa, bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia. Disponible en: http://buscon.rae.es/draeI/SrvltObtenerHtml?origen=RAE&LEMA=perito&SUPIND=0&CAREXT=10000&NEDIC=No#0_3

4.5.4 Estructura general

1. *Encabezado del informe* (*cuadro 4.2*).

Fecha	Fecha en la que se entrega el informe
No. caso interno	Se sugiere numeración anual, con reinicio los años siguientes.
Analistas o peritos	Nombres de los peritos asignados
Solicitante	Manuel Vargas (con su cargo)
Oficio o documento que autoriza la pericia:	Documento donde se autoriza a adelantar la diligencia
Tipo de solicitud	Detalle de lo que se requiere adelantar con la evidencia que se entrega
Clasificación documento	Etiqueta de seguridad que se le asigna al documento: confidencial, sensible, circulación restringida
Cifra control de este documento	Cálculo de la cifra de control del documento que generalmente se tiene en un archivo aparte.

Cuadro 4.2

Encabezado del informe

Este encabezado identifica, de manera clara y concreta, qué se requiere hacer, quiénes participan, la identificación del caso, la clasificación del informe según su nivel de seguridad requerido y los investigadores participantes en el caso.

2. *Introducción*
En la introducción se detallan los aspectos base del caso que se investiga, basado en el expediente del mismo y en los datos que se ofrecen por parte bien sea de la fiscalía o de la defensa. En esta sección se describen la conducta que se investiga y los alcances de la pericia que se adelanta, con el fin de limitar los análisis y exploraciones a lo que se requiere para el caso particular.
3. *Validación y verificación de la cadena de custodia*
En esta sección se detalla y registra la evidencia con su formato de cadena de custodia, donde se especifica, qué se recibe, de quién, en qué fecha, las características de los objetos, sus marcas y seriales, los nombres de los peritos que reciben, la identificación del caso, entre otros aspectos.
4. *Procedimientos de preparación y adecuación de la evidencia recibida*
En esta sección se detallan los procedimientos relacionados con los medios informáticos que se tienen para adelantar las copias

idénticas del material recibido, los programas informáticos requeridos para esta labor y su posterior análisis, las verificaciones de las copias y los detalles de los análisis que se van a realizar según lo especificado en la introducción.

5. *Análisis de la evidencia*
   En esta sección de adelanta en el análisis detallado de las copias de la evidencia, utilizando los recursos de software y hardware disponibles, los cuales previamente han sido validados y verificados en la etapa anterior, según se requiera para evidenciar la confiabilidad y la calidad de los resultados que se van a obtener. Es importante, detallar las técnicas utilizadas para identificar y extraer la información de los medios entregados para el análisis.

6. *Hallazgos o hechos identificados*
   En esta sección se presenta, luego de la exploración de la evidencia realizada en la sección, lo que se encontró relevante para la materia de investigación. Se presenta tal como se indica en las herramientas, sin análisis ni opiniones al respecto. Ésta es la exposición de los resultados de las herramientas que generalmente hablan de archivos, sitios en los medios, calidad de la información recuperada, entre otros aspectos.

7. *Conclusiones*
   En esta sección se presentan los análisis de los hallazgos en el contexto del caso investigado, basados en las formalidades científicas y técnicas que puedan ser validadas por un tercero si así se requiere. Las afirmaciones que se hagan en esta sección deben corresponder a lo que la formalidad técnica establece, a las características de los objetos analizados y los hechos investigados.

8. *Firma de los analistas o peritos*
   Esta sección es tan importante como las anteriores. Corresponde al momento en que el perito refrenda su ejercicio técnico y científico con su rúbrica, haciéndose responsable del contenido de informe y todo lo que allí se encuentre. Se recomienda que este profesional firme con una pluma con tinta especial y de color diferente al negro. Así mismo, es recomendable que el perito o analistas firmen todas las hojas, como medida de confiabilidad sobre el informe, que permita identificar con mayor certeza su informe, por si un tercero quisiera alterar el contenido del mismo, sin autorización.

Resumen

En este capítulo hemos desarrollado el concepto de criminalística digital, como esa disciplina emergente de la criminalística tradicional, que busca darles a estos nuevos profesionales una particular especialidad, la cual recae sobre los medios informáticos o tecnológicos, que los intrusos utilizan actualmente para materializar conductas punibles.

A la fecha no se encuentran programas de estudio o formación especializada para educar y entrenar formalmente a los nuevos criminalistas, representados en los informáticos forenses, lo que establece un reto técnico y legal, que una sociedad digital y del conocimiento debe asumir, para enfrentar la criminalidad informática y sus efectos conexos. Sin este requisito, el mensaje que se les envía a los nuevos ciudadanos de un estado digital, desestima la confianza y el buen desarrollo de la sociedad, marginando la competitividad y las posibilidades que las tecnologías de información abren a los estados y sus individuos.

Los informáticos forenses en este contexto adquieren una responsabilidad con el Estado y con la administración de justicia, de tal forma que se convierten en garantes de la verdad procesal en el contexto digital. Esto es, al desarrollar una diligencia informática en el escenario de un caso, deben desempeñar roles y aplicar actividades que le permitan a los interesados del proceso ver con claridad lo que se hace, cómo se hace, quién lo hace y las conclusiones a las que llega. Por tanto y complementario con lo anterior, la formación requerida de éstos es parte de lo exigible por las partes para procurar un nivel de confiabilidad en el desarrollo de las diligencias del proceso.

De otra parte y no menos importante, los modelos y procedimientos que los informáticos forenses utilicen son parte fundamental de la apreciación de la calidad y la formalidad de éstos. Un informático forense que no procure la continua actualización de sus conocimientos y el estudio permanente de los modelos de investigaciones informáticas será marginado de nuevos casos, los cuales son, en últimas, la manera como aumenta su visión y la habilidad para reconocer y presentar nuevas conductas punibles a través de medios informáticos o tecnológicos.

Finalmente, todos estos elementos se materializan en un informe final de la pericia que debe manifestar la formalidad, la calidad, la educación, la experiencia y la oportunidad del informático forense en el desarrollo del caso. El informe es la carta de presentación del informático forense, pues allí se exhiben el profesionalismo, la fortaleza técnica y la imparcialidad de sus análisis y conclusiones, características que son clave para soportar la presentación del mismo ante las instancias judiciales pertinentes.

Preguntas y ejercicios

Esta sección busca reforzar los elementos conceptuales presentados en este capítulo, para eso le sugerimos al lector revisar sus reflexiones y anotaciones para plantear respuestas a los interrogantes propuestos en esta sección.

1. ¿Qué es la criminalística digital?
2. ¿Qué papeles o roles puede desempeñar un informático forense?
3. ¿Qué certificaciones o estudios se requieren para denominarse un informático forense?
4. ¿Quién puede ser un perito? ¿Se puede extrapolar la definición para perito informático?
5. ¿Qué consideraciones debe tener un modelo de investigaciones en informática forense?
6. ¿En qué no se puede equivocar un informático forense al aplicar un modelo de investigaciones forenses en informática?
7. ¿Qué características son deseables en los informes de pericia de los profesionales en informática forense?

Apéndice

Para profundizar

Análisis de datos: Una propuesta metodológica y su aplicación en The Sleuth y EnCase

Córdoba Jonathan, Laverde Ricardo, Ortiz Diego, Puentes Diana

Como consecuencia del aumento de la capacidad de los dispositivos de almacenamiento, al igual que el incremento en la heterogeneidad de la información en ellos contenida, la labor del investigador en computación forense se ha tornado cada vez más compleja.

Debido a lo anterior, existe una necesidad imperiosa de construir herramientas y concebir guías metodológicas adecuadas que apoyen y sistematicen esta labor.

De hecho, esta problemática se presenta en M. Reith, C. Carr, G. Gunsch, que a su vez plantea un modelo abstracto de nueve etapas para desarrollar el proceso forense digital, que se define como "el uso científico de métodos probados hacia la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de la evidencia digital obtenida de cualquier fuente digital, con el propósito de facilitar la reconstrucción de los eventos criminales o ayudar a anticipar acciones no autorizadas que trastornen las operaciones normales".

Las etapas de este modelo: identificación preparación, estrategia de aproximación, preservación, recolección, examen, análisis, presentación y reintegro de la evidencia (en los casos legalmente permisibles), en conjunto, están encaminadas a satisfacer la definición recién mencionada (M. Reith, C. Carr, G. Gunsch (s.f.)).

Este documento se centra en las fases de examen y análisis, en particular, propone una guía metodológica que a partir de la imagen binaria de datos –un resultado específico de la etapa de recolección– permite hallar de forma sistemática la evidencia digital relacionada con el caso que se investiga.

Seguidamente, se presentan y describen dos herramientas relacionadas con el ejercicio de la computación forense: EnCase ("Guidance Software". (s.f.)) y Sleuth Kit / Autopsy (B. Carrier. (s.f.)), [B. Carrier. (s.f.)] y finalmente se ilustra la metodología en acción usando tales herramientas sobre un caso específico.

1. METODOLOGÍA DE EXAMEN Y ANÁLISIS DE DATOS

Para realizar un análisis de datos forense es necesario seguir una serie de pasos para la obtención de la evidencia. A continuación se propone una guía metodológica que reúne y organiza una serie de actividades conducentes a la obtención de tal evidencia (*gráfico A4.1*) (M. Reith, C. Carr, G. Gunsch. (s.f.); E. Casey. (s.f.); E. Casey. (2002); J. Morris. (Febrero 11 de 2003); M. Janiczek. (2004); R. Lee. (2004); J. Morris. (s.f.); US. Department of Justice. (Abril 2004) y T. Gluzinski, J. Kida. (s.f.)). En el caso de la guía metodológica propuesta, es necesario definir un conjunto de elementos requeridos que constituyen la información inicial para seguirla. Estos elementos son:

- Imágenes binarias de los dispositivos de almacenamiento digital comprometidos en el caso con sus respectivos compendios criptográficos.
- Descripción del caso ilustrando el marco circunstancial.
- Metadatos de cada una de las imágenes, es decir, todo tipo de información necesaria para determinar las características de la imagen, en particular, la existencia de un HPA (Host Protected Area) 21, concepto que se explicará más adelante.

El objetivo de esta guía metodológica es obtener un informe de hallazgos que describa la evidencia hallada y la forma como se obtuvo.

A. Descripción de los pasos

1. *Creación del archivo de hallazgos*

Consiste en la creación y el aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado (*gráfico A4.1*).

2. *Imagen de datos*

Consiste en la recepción de las imágenes de datos que conciernen al caso en investigación.

3. *Verificación de integridad de la imagen*

Para cada imagen suministrada se debe calcular su compendio criptográfico (MD5), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.

4. *Creación de una copia de la imagen suministrada*

En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada, sino sobre su copia.

5. *Aseguramiento de la imagen suministrada*

Se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

6. *Revisión antivirus y verificación de la integridad de la copia de la imagen*

Una vez se ha obtenido la copia de la imagen, es necesario asegurar que no tenga ningún tipo de virus conocido.

Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original (paso 2). De hecho, esta actividad es transversal en la metodología, es decir, debe realizarse periódicamente durante el proceso de análisis de datos, de modo tal que se garantice la integridad de los datos desde el comienzo, hasta el fin de la investigación.

7. *Identificación de las particiones actuales y anteriores (las que sea posible recuperar)*

La identificación de las particiones en un dispositivo es de vital importancia, ya que reconocerlas implica la identificación de su sistema de archivos, mediante el cual se pueden reconocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.

8. *Detección de información en los espacios entre las particiones*

Cuando se detectan datos en estas zonas de la imagen, se debe proceder a hacer un análisis para determinar si representan algún tipo de información relevante para la investigación. En caso de estar protegidos, estos archivos serán tenidos en cuenta en la fase de la identificación de archivos protegidos, de lo contrario, se incluirán en el conjunto de archivos potencialmente analizables.

9. *Detección de un HPA*

Este paso debe realizarse sólo si en los metadatos se indica la existencia del HPA (B. Carrier. (Noviembre 15 de 2004)), ya que de otro modo es imposible de identificar. En el caso en que exista, se debe seguir el mismo procedimiento del paso anterior.

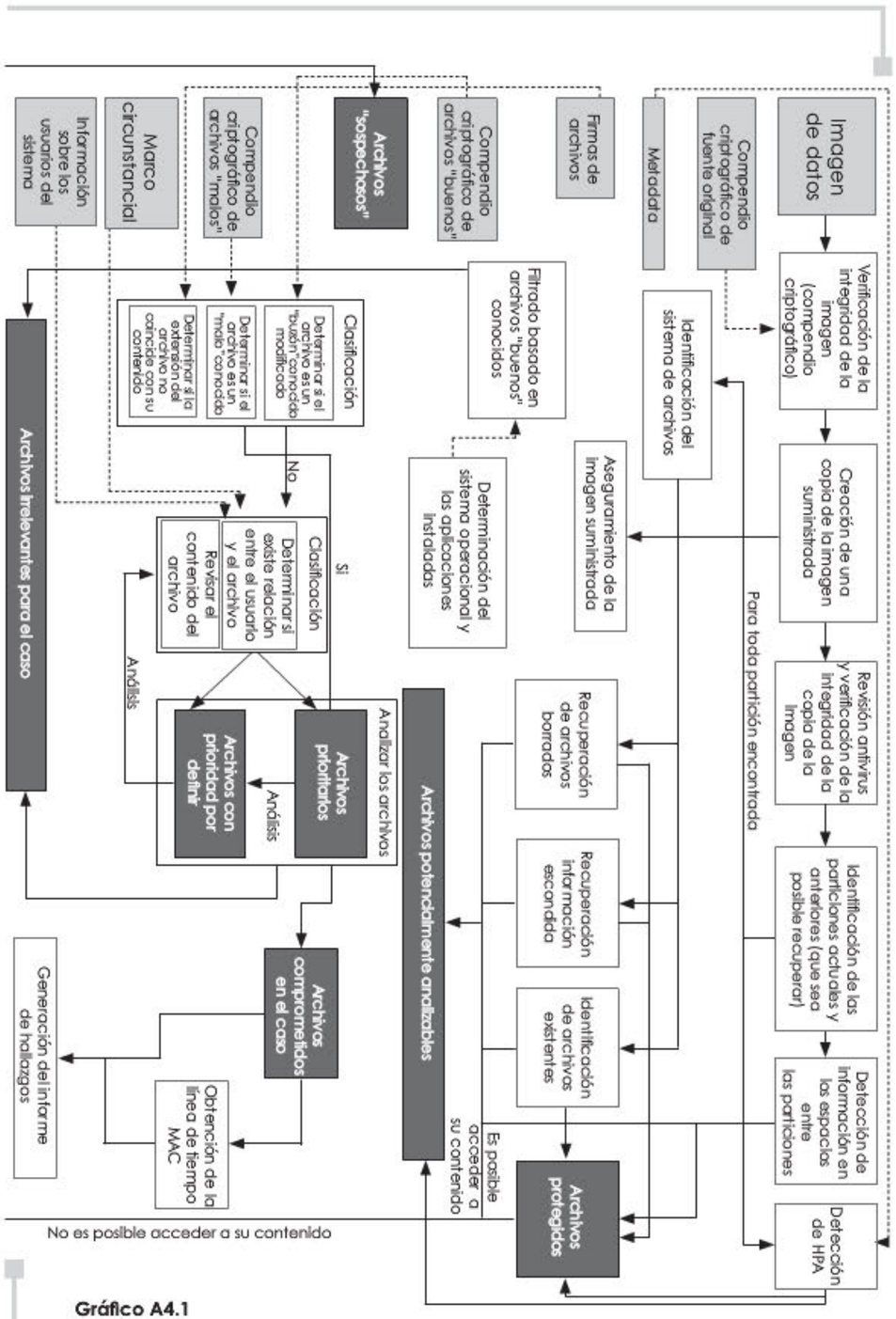


Gráfico A4.1

Metodológica de examen y análisis de datos Guía

10. *Identificación del sistema de archivos*

Para cada una de las particiones identificadas en el paso 6, debe identificarse su sistema de archivos, con el fin de escoger la forma de realizar las actividades posteriores del análisis de datos.

11. *Recuperación de los archivos borrados*

Durante esta actividad se debe tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente, dado el frecuente el borrado de archivos para destruir evidencia.

Dependiendo de las características técnicas y del estado del sistema de archivos, puede no ser posible la recuperación de la totalidad de los archivos eliminados; por ejemplo, si éstos han sido sobresescritos, o si se han utilizado herramientas de borrado seguro para eliminarlos.

Los archivos recuperados exitosamente formarán parte de los archivos potencialmente analizables, exceptuando los archivos identificados como protegidos que serán tenidos en cuenta durante la fase de identificación de archivos protegidos.

12. *Recuperación de información escondida*

En esta etapa se deben examinar exhaustivamente el slack space, los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

Al igual que en la fase 10, los archivos protegidos también se tendrán en cuenta durante la fase de análisis de éste tipo de archivos.

13. *Identificación de archivos existentes*

Seguidamente, se clasifican los archivos restantes entre protegidos y no protegidos, donde estos últimos harán parte de los archivos potencialmente analizables, mientras los primeros harán parte la fase de análisis de archivos protegidos.

14. *Identificación de archivos protegidos*

Esta es la fase de consolidación de archivos protegidos identificados en las fases anteriores. Durante esta fase se pretende descifrar o romper tal protección en estos archivos, con el fin de adicionarlos al conjunto de archivos potencialmente analizables. Los archivos cuya protección no pudo ser vulnerada formarán parte del conjunto de archivos sospechosos.

15. *Consolidación de archivos potencialmente analizables*

Durante esta fase se reúnen todos los archivos encontrados durante las fases de: recuperación de archivos borrados, recuperación de información escondida, identificación de archivos no borrados e identificación de archivos protegidos.

16. *Determinación del sistema operativo y las aplicaciones instaladas*

Al determinar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de estos archivos de encontrarse en la imagen sometida a análisis.

17. *Filtrado basado en archivos buenos conocidos*

Con la lista de compendios criptográficos obtenida en el paso anterior, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, éste se considera "bueno" y, por lo tanto, es descartado del proceso de análisis.

18. *Consolidación de archivos sospechosos*

Como resultado del filtrado de "buenos" conocidos, se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamará archivos sospechosos.

19. *Primera clasificación*

Divide los archivos sospechosos en:

- *Archivos "buenos" modificados:* Son identificados en la fase de filtrado como archivos buenos cuya versión original (descrita por la lista obtenida en el paso 15) ha sido modificada.
- *Archivos "malos":* Se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos "malos" relacionados con el sistema operativo particular. Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o se ejecutan, por ejemplo: troyanos, backdoors y virus, entre otros.
- *Archivos con extensión modificada:* Aquellos cuya extensión no es consistente con su contenido.

Los archivos que cumplen alguna de las anteriores características se convierten en archivos prioritarios para el análisis. Los que no cumplen con estas características se someten a la siguiente etapa de clasificación.

20. *Segunda clasificación*

Esta clasificación toma archivos que no han sido considerados de máxima prioridad, los examina y los evalúa respecto a dos criterios: relación de los archivos con los usuarios involucrados en la investigación y contenido relevante para el caso, derivado del marco circunstancial.

El resultado de esta clasificación es seleccionar como prioritarios para el análisis los archivos que sean identificados bajo los anteriores criterios.

21. *Analizar los archivos*

Este proceso se basa en la discriminación de los archivos prioritarios con respecto a su relevancia con el caso y el criterio del investigador.

Es importante resaltar que los procesos de la segunda clasificación y análisis, pueden ser iterativos con el fin de obtener más cantidad de evidencia pertinente. En cada iteración cada archivo de alta prioridad puede ser descartado o catalogado como archivo comprometido en el caso, y los archivos con poca prioridad son sometidos a una nueva iteración.

Este proceso cesa cuando el investigador, a partir de su criterio y experiencia, considera suficiente la evidencia recolectada para resolver el caso, o porque se agotan los datos por analizar.

22. *Archivos comprometidos con el caso*

Es el conjunto de archivos que forman parte de la evidencia del caso.

23. *Obtención de la línea de tiempo definitiva*

Se procede a realizar la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permite correlacionarlos enriqueciendo la evidencia.

Es importante resaltar que es algunas ocasiones, y dependiendo del sistema de archivos del volumen analizado, puede ser imposible realizar un análisis temporal, situación que, como todos los hallazgos, debe ser consignada en el informe.

24. *Generación del informe*

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados, apoyándose en la documentación continua de la aplicación metodológica.

2. INTRODUCCIÓN A ENCASE

EnCase ("Guidance Software". (s.f.)) surgió en 1998 como una herramienta de apoyo integral al ejercicio forense, rompiendo el esquema de trabajo

de los investigadores ya que operaba sobre Windows, en una época en la que no se usaba este sistema operativo para las investigaciones forenses (E. Casey. (2002, 2004)).

En su versión 4.20, EnCase es un software comercial que apoya las actividades del investigador forense, ofreciendo funcionalidades como: generación de imágenes binarias de discos duros, discos flexibles y otros dispositivos electrónicos de almacenamiento.

Tales imágenes pueden ser analizadas de diversas formas, mediante búsquedas de cadenas de caracteres, recuperación de datos borrados, establecimiento de líneas de tiempo de uso del sistema de archivos, verificación de la relación entre los contenidos de los archivos y su extensión (verificación de la firma de tipo de archivo), entre otras descritas a continuación (J. Morris. (Febrero 11 de 2003)).

A. Descripción de funcionamiento

EnCase realiza el análisis forense desde un dispositivo virtual de sólo lectura (archivo de trabajo), que construye internamente a partir del dispositivo o la imagen original su sistema de archivos, asegurando la integridad de los datos contenidos en la imagen o el dispositivo (E. Casey. (2002, 2004)).

Con antelación a la creación del archivo de trabajo, EnCase calcula el compendio criptográfico *(message digest)* MD5 de la imagen original, obtenida o generada, comparándola con la del archivo de trabajo para verificar la integridad de los datos (Guidance Software. (Julio de 2004)). Posteriormente, el resultado del compendio se utiliza para verificar periódicamente la integridad de los datos en el archivo de trabajo durante el proceso forense, ya que el compendio calculado del archivo de trabajo no debe variar durante el proceso de análisis.

A continuación se describen las principales funcionalidades de EnCase en lo concerniente al tema central de Para profundizar.

1. *Recuperación de archivos borrados en EnCase*

Como se presentó en la metodología de análisis de datos, una de las primeras actividades a realizar es la recuperación de archivos borrados y datos en el espacio no asignado por el sistema de archivos (E. Casey. (2002, 2004)).

EnCase (*gráfico A4.2*) muestra y reconstruye los archivos borrados cuya información descriptiva residual es suficiente para tal fin (solamente en sistemas de archivos FAT 16/32), mostrándolos como parte del árbol de archivos en la carpeta Recovered Files (R. Keightley. (s.f.)).

El árbol de archivos es una estructura visual generada por EnCase a partir del archivo de trabajo y sin mediación del sistema operativo subyacente, que además permite visualizar los datos en el *file slack*, en los archivos de intercambio/paginación *(swap files)*, de impresiones previas

(contenidas en el anterior) y en el espacio no asignado por el sistema de archivos (Guidance Software. (Julio de 2004)).

2. *Verificación de firmas de tipo de archivo*

Una de las actividades más comunes para esconder información, es el cambio de extensión de los archivos para que éstos pasen desapercibidos; por ejemplo, cambiando "chicas.bmp" por "ventas.xls" (Cmdr. D. Pettinari. (Julio 2 de 2000)) (gráfico A4.2).

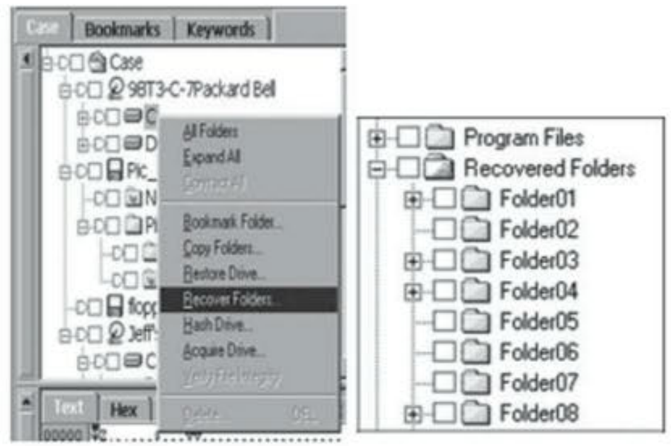


Gráfico A4.2

Recuperando archivos borrados y espacio no asignado del disco (R. Keightley (s.f)).

Para identificar estas actividades, EnCase emplea una base de datos que contiene patrones característicos de tipos de archivos conocidos (firmas). Con base en lo anterior, se valida la correspondencia entre la extensión del archivo y su contenido, notificando cuando hay inconsistencia entre tales elementos (Guidance Software. (Julio de 2004)).

Cabe resaltar que Guidance Software refiere que: "Most files contain a few bytes at the beginning of the sector that constitute a unique "signature" of the file". Consideramos que lo anterior es impreciso, porque basados en la observación de varios archivos del mismo tipo, se puede afirmar que la firma es simplemente un patrón que se puede dar a lo largo de todo el archivo (no sólo en sus primeros 'bytes'), o que EnCase no verifica la coincidencia del patrón sobre la totalidad del mismo, lo que se constituye en una limitación operacional destacable.

3. *Ponderación de archivos (gráficos A4.3 y A4.4)*

EnCase le provee al examinador forense la capacidad de buscar, filtrar y organizar los archivos según diferentes criterios, lo que le permite alcanzar una visión más clara del caso.

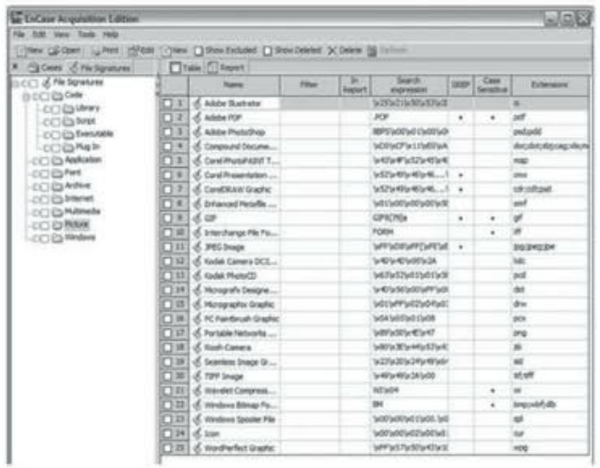


Gráfico A4.3

Galería de firmas conocidas por EnCase

Por medio de la herramienta de búsqueda, EnCase permite buscar cadenas alfanuméricas o patrones por medio de la herramienta grep, que permite identificar archivos que eventualmente constituyen evidencia de algún tipo (gráfico A4.4).

EnCase permite además destacar los archivos que se consideran relevantes para el caso mediante marcadores *(bookmarks)*, con el fin de facilitar las búsquedas, el ordenamiento y el filtrado de tales archivos (gráfico A4.5).

4. *Reconstrucción temporal*

EnCase genera 'líneas de tiempo' () que reconstruyen temporalmente los hechos ocurridos sobre los datos (a nivel de archivos) contenidos en el archivo de trabajo (E. Casey. (2002, 2004)).

La línea de tiempo (gráfico A4.6) provee información de las fechas de creación, modificación y último acceso a los archivos en cuestión (tiempos MAC (M. Janiczek. (2004) y Guidance Software. (Julio de 2004)).

Gráfico A4.4

Búsqueda de patrones Grep en EnCase (R. Keightley (s.f.))

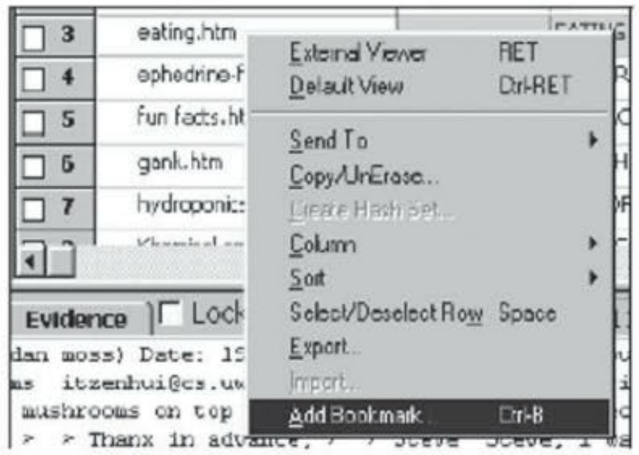


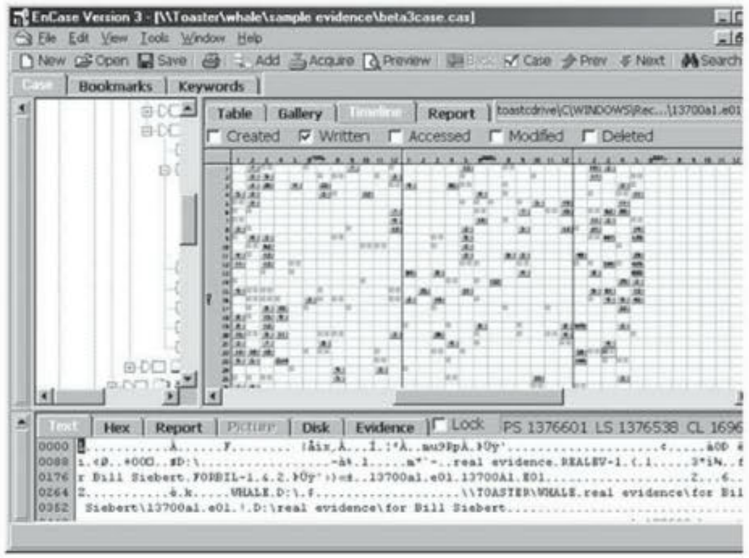
Gráfico A4.5

Marcado de archivos en EnCase (R. Keightley (s.f.))

Adicionalmente, despliega gráficamente la anterior información, marcando la creación con gris oscuro, la última modificación en gris medio y el último acceso en gris oscuro (R. Keightley (s.f.)).

5. *Otras funcionalidades*

EnCase presenta otras características relevantes que se describen a continuación.



Nota: La línea de tiempo puede ser vista en diferentes escalas, para profundizar o generalizar los detalles.

Gráfico A4.6

Un ejemplo de vizualización de la linea de tiempo (Guidance Software)

a. *Recuperación de particiones NTFS* (B. Carrier. (s.f.))

EnCase proporciona una herramienta de reconstrucción de sistemas de archivos NTFS sobre volúmenes que han sido formateados. Lo anterior, a partir de la búsqueda de información sobre la partición, y luego, sobre el sistema de archivos NTFS. En caso de que la información se encuentre en un estado recuperable, esto es que no haya sido sobrescrita, o que no haya sido borrada del disco con herramientas de borrado seguro, la reconstrucción despliega automáticamente la estructura de directorios e identifica los archivos borrados (Guidance Software. (Julio de 2004)).

b. *Apoyo en el análisis de logs* ("Guidance Software". (s.f.))

El componente de análisis y búsqueda archivos de EnCase integra logs heterogéneos, consolidándolos en un repositorio común con un formato uniforme que posteriormente puede ser analizado por medio de la herramienta (Guidance Software. (Julio de 2004)).

c. *Toolkit de análisis para Internet* (B. Carrier. (s.f.))

EnCase provee herramientas de reconocimiento y análisis de archivos de correo, archivos generados por los navegadores de Internet y archivos que sugieran la existencia de aplicaciones P2P (Peer to Peer) o mensajería instantánea.

3. INTRODUCCIÓNA A SLEUTH KIT (B. Carrier. (s.f.). Y AUTOPSY (B. Carrier. (s.f.))

'The Sleuth Kit' (TSK) es una colección de herramientas para el análisis forense de los datos hallados en un sistema sospechoso (B. Carrier. (s.f.)). Éste surge de 'The Coroner's Toolkit' (TCT) ("The Coroner's Toolkit". (s.f.)). como solución a tres limitaciones particulares de este grupo de herramientas (B. Carrier. (Febrero 15 de 2003)). Solamente funciona para sistemas de archivos de tipo Unix, no tiene noción de nombres de archivos ni directorios, pues opera a nivel de bloques e I-nodos y requiere que la plataforma de análisis sea igual a la del sistema analizado (B. Carrier. (Febrero 15 de 2003)).

TSK tuvo sus orígenes en 'Tctutils', un módulo de extensión desarrollado por Brian Carrier que le permitió a TCT manejar la noción de nombres de archivos y directorios. Después de un tiempo se desarrollaron otras herramientas de análisis de datos ejecutables vía línea de comandos en sistemas tipo Unix, que se agruparon en 'The @stake Sleuth Kit' (TASK), hoy en día conocido como TSK.

Paralelamente, Autopsy apareció como una interfaz gráfica de usuario escrita en Perl que ofrecía acceso a la funcionalidad de Sleuth Kit a través de un cliente Web [B. Carrier. (s.f.)], añadiéndole de esta manera un manejo ordenado, menos complejo y centralizado de las actividades de análisis forense de datos (B. Carrier. (Marzo 15 de 2003)).

A. The Sleuth Kit

TSK está compuesto por 21 herramientas de acceso a la información no volátil (imágenes) almacenada en el sistema examinado (B. Carrier. (s.f.)). Taxonómicamente, se basa en un modelo de cinco capas que describe los datos contenidos en un sistema de archivos. Este modelo propuesto por Carrier, al igual que las herramientas de TSK que funcionan sobre cada una de sus capas, se describen a continuación.

1. *Capa de datos* (Data Unit) (B. Carrier. (s.f.); B. Carrier. (Febrero 15 de 2003); B. Carrier. (2005) y B. Carrier. (s.f.))

Está compuesta por el agregado de los datos de los archivos y directorios contenidos en una imagen binaria de datos, en particular, por sus ubicaciones de almacenamiento o unidades de datos, que reciben diferentes nombres de acuerdo con el sistema de archivos en uso; por ejemplo, clusters en FAT y NTFS, o fragmentos en Ext2/3 y UFS. Sin embargo, en el caso de FAT, TSK

siempre utiliza los sectores como unidad de datos (B. Carrier. (Enero 15 de 2005)).

Existen cuatro herramientas que comienzan con la letra 'd' relacionadas con esta capa: [B. Carrier. (s.f.)] dcat, dls, dstat y dcalc, descritas a continuación:

- `dcat:` Muestra los contenidos de una o más unidades de datos consecutivas.
- `dls:` Permite extraer una imagen de los datos contenidos en el espacio no asignado por el sistema de archivos.
- `dstat:` Despliega los detalles relacionados con una unidad de datos, en particular, su estado de asignación.
- `dcalc:` Crea una biyección entre las unidades de datos no asignadas en la imagen original y las de la imagen de datos generada con dls.

2. *Capa de metadatos (metadata)* (B. Carrier. (s.f.); B. Carrier. (Febrero 15 de 2003); B Carrier. (2005) y B. Carrier. (s.f.))

Contiene los datos descriptivos de la información almacenada en el sistema de archivos; por ejemplo, las entradas de directorio raíz en FAT, los registros en la MFT de NFTS y los I-nodos en ExtX y UFS. Por este motivo las herramientas relacionadas con esta capa comienzan con la letra 'i'.

Dependiendo del sistema de archivos, la metadata de un archivo está compuesta de información sobre sus permisos, estampillas de tiempo, tamaño y apuntadores a las unidades de datos que lo contienen, entre otros.

La información contenida en esta capa puede ser accedida por medio de las siguientes cuatro herramientas de TSK (B. Carrier. (s.f.)):

- `icat:` Extrae las unidades de datos de un archivo a partir de la dirección de sus metadatos.
- `ils:` Genera una lista de las entradas de metadatos del sistema de archivos y sus contenidos.
- `istat:` Muestra los detalles de una entrada de metadatos en un formato fácilmente legible.
- `ifind:` Dado un nombre de archivo o una dirección de una unidad de asignación, encuentra la estructura de metadatos con la que se relaciona. En algunos casos, la unidad de asignación puede estar no asignada y aun así relacionarla con la información de metadatos.

3. *Capa de nombre de archivo (File Name)* (B. Carrier. (s.f.); B. Carrier. (Febrero 15 de 2003); B. Carrier. (2005) y B. Carrier. (s.f.)).

Si bien la metadata determina al archivo, usualmente tiene una dirección numérica difícil de recordar, lo que da origen a la capa de nombre de archivo, que se encarga de almacenar el nombre de los archivos y relacionarlos con las estructuras de metadatos que los describen. Cabe decir que, en el caso del sistema de archivos FAT, las capas de metadatos y nombre de archivo son los mismos.

TSK contiene dos herramientas cuyo nombre comienza con la letra 'f' destinadas a los datos de ésta capa:

- `ffind:` Busca el nombre de archivo o directorio a partir de la dirección de una estructura de metadatos.
- `fls:` Genera un listado de los nombres de archivo asignados y algunos borrados en una imagen de datos.

4. *Capa de sistema de archivos (File System)* (B. Carrier. (s.f.)); B. Carrier. (Febrero 15 de 2003)); B. Carrier. (2005)) y B. Carrier. (s.f.)).

Como su nombre indica, almacena la información característica de un sistema de archivos, permitiendo diferenciarlo de otros del mismo tipo. Las estructuras de administración (como los Bitmaps), de asignación y de distribución pertenecen a esta categoría.

La herramienta correspondiente a esta capa es fsstat (el prefijo para esta capa es 'fs'), cuya función es desplegar la información del sistema de archivos.

5. *Capa de aplicación* (B. Carrier. (s.f.); B. Carrier. (Febrero 15 de 2003); B. Carrier. (2005) y B. Carrier. (s.f.))

Actualmente existen otras estructuras de datos encargadas de almacenar información sobre las estructuras a nivel de datos y metadatos comprometidas en los cambios que se hacen sobre el sistema de archivos (*Journals*) (B. Carrier. (s.f.)). Éstas constituyen la capa de aplicación que completa el modelo de datos propuesto por Carrier.

Las herramientas relacionadas con el *Journal* tienen el prefijo 'j', y actualmente se trata de las siguientes (soportando únicamente Ext3):

- `jcat:` Muestra el contenido de un bloque (unidad de datos) del Journal.
- `jls:` Enumera las entradas del Journal del sistema de archivos.

Por otro lado, existen otros grupos de herramientas que permiten desarrollar el análisis forense a partir de la información contenida en la imagen del disco, en particular.

6. *Herramientas de manejo de medios (Media Management)* (B. Carrier. (s.f.) y (B. Carrier. (s.f.))

Este grupo de herramientas (prefijo 'mm') están encaminadas a analizar la estructura de las particiones (tabla de particiones y etiquetas) de un disco o su imagen, con el objeto de identificar datos ocultos entre las particiones así como los desplazamientos (offsets) de los sistemas de archivos requeridos por varias herramientas de TSK.

Actualmente la única herramienta disponible de manejo de medios es mmls, que muestra la distribución (layout) del disco incluyendo los espacios no asignados entre particiones.

7. *Herramientas de archivo de imagen (Image File Tools)* (B. Carrier. (s.f.); B. Carrier. (s.f.))

La herramienta img_stat permite conocer los detalles de un archivo de imagen siempre y cuando sea soportado por TSK [B. Carrier. (Marzo 15 de 2005)], en particular, su formato, que puede ser raw o split.

8. *Herramientas de disco (Disk Tools)* (B. Carrier. (Febrero 15 de 2003)]-B. Carrier. (Noviembre 15 de 2004)-B. Carrier. (s.f.))

Este grupo de herramientas tiene como objetivo detectar y remover las Áreas Protegidas de Máquina (*Host Protected Areas, HPA*) que son una porción al final del algunos discos duros, no direccionable para el sistema operativo empleada por los fabricantes de computadores para almacenar información de configuraciones e instalaciones, y muchas veces empleado para ocultar información.

Lamentablemente la única forma de adquirir el HPA es directamente sobre el disco que la contiene, comparando el número máximo de direcciones del disco, con la máxima dirección accesible por el usuario; si hay una diferencia se puede determinar que el disco tiene una HPA (B. Carrier. (Noviembre 15 de 2004)); por lo tanto, una vez se ha hecho la adquisición de la imagen del disco es muy tarde para accederla.

Para leer los contenidos de la HPA es necesario remover su configuración en el disco duro, de tal forma que éste reporte la HPA como parte del área direccionable de datos del disco duro, con el agravante de que se requiere la modificación de la información en la evidencia potencial.

Actualmente se han desarrollado dos herramientas para Linux que apoyan ésta tarea (prefijo 'disk_') (B. Carrier. (s.f.)).

- `disk_sreset:` Temporalmente remueve la HPA de un disco (si existe), de tal forma que el disco entero pueda ser plasmado en la imagen. Una vez el disco se apaga, la HPA vuelve a existir.
- `disk_stat:` Determina si existe o no una HPA en el disco.

9. *Otras herramientas (Other Tools)* (B. Carrier. (s.f.); B. Carrier. (Febrero 15 de 2003) y B. Carrier. (s.f.))

Este grupo está compuesto de las siguientes herramientas:

- `hfind:` Permite buscar un valor de compendio criptográfico en un repositorio de valores de compendios criptográficos preestablecidos. Puede utilizarse para filtrar un archivo que se considera normal y sin valor para la investigación, o determinar si se trata de un archivo sospechoso.
- `mactime:` Usa fls e ils para generar una línea de tiempo de actividad de los archivos basada en los tiempo de modificación, acceso y creación (MAC times) (M. Janiczek (2004)).
- `sorter:` Clasifica los archivos contenidos en una imagen de acuerdo con su tipo, verificando que sus extensiones coincidan con su categoría, excluyendo los archivos incluidos en las listas de archivos normales (por medio de hfind) y mostrando los archivos sospechosos (B. Carrier. (Abril 15 de 2003); B. Carrier. (Mayo 15 de 2003) y B. Carrier. (Junio 15 de 2003)).
- `sigfind:` Busca una cadena binaria en un archivo suministrado. Es útil para hallar sectores perdidos, super-bloques y tablas de particiones.

Finalmente, se muestra un resumen de las categorías de herramientas de TSK (*gráfico A4.7*).

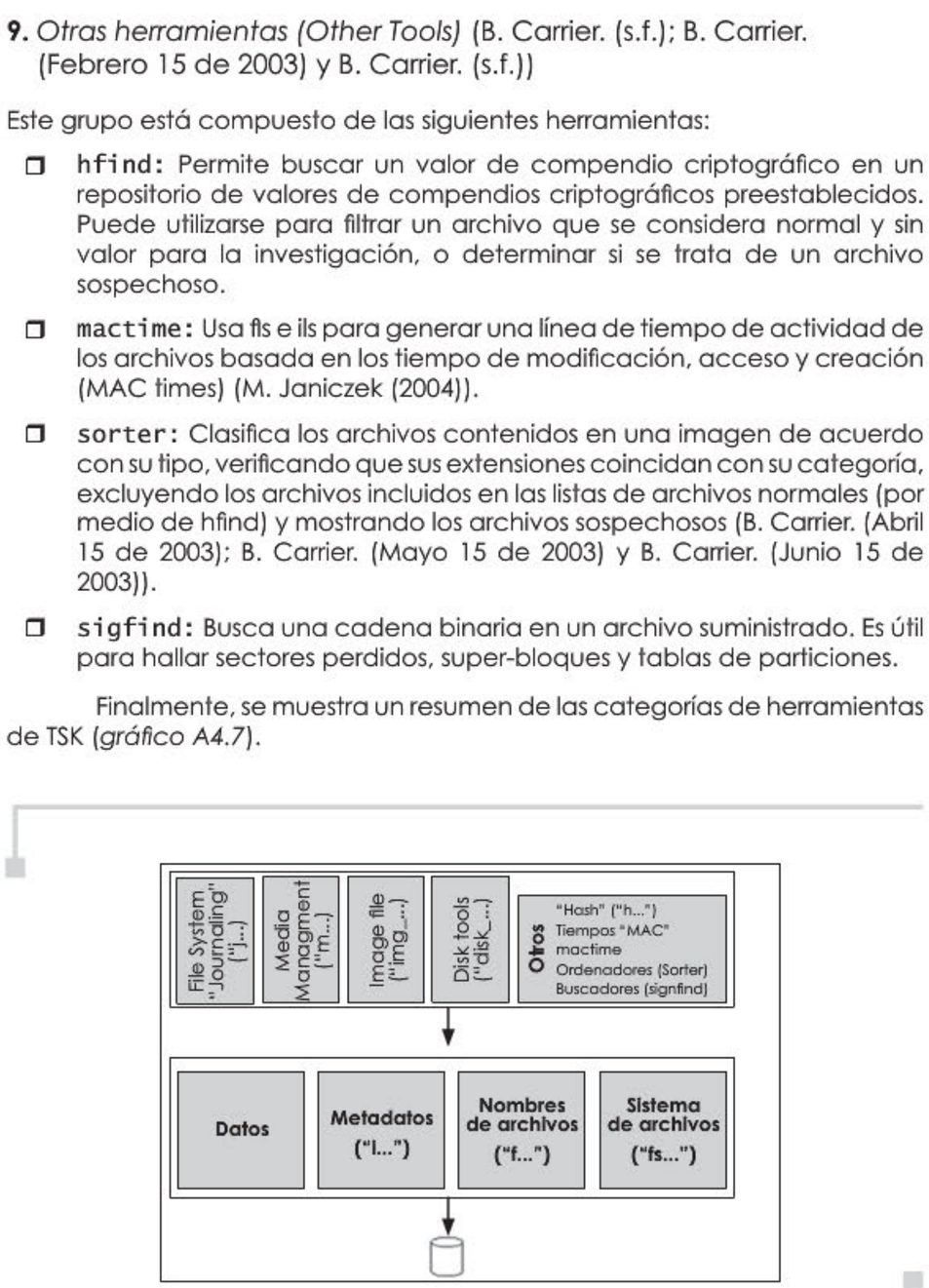


Gráfico A4.7

Taxonomía de herramientas de TSK

B. Autopsy

TSK y Autopsy (B. Carrier. (Febrero 15 de 2003); B. Carrier. (Marzo 15 de 2003) y R. Lee. (2004)) son aplicaciones independientes y las herramientas de TSK pueden ser ejecutadas sin necesidad de Autopsy; de hecho, Autopsy se limita a usar las herramientas proveídas por TSK y, salvo su existencia, sus parámetros y el formato de su retorno, no conoce nada más sobre ellas (B. Carrier. (Febrero 15 de 2003)).

El valor agregado de Autopsy sobre TSK es que organiza el manejo de la investigación forense, en casos que pueden contener más de un sistema (host) involucrado (una ventaja funcional sobre EnCase). A su vez, para cada host se almacena su nombre, zona de horaria, desfase de tiempo y una o más imágenes que corresponden a un sistema de archivos (B. Carrier. (Marzo 15 de 2003)). El *gráfico A4.8* ilustra la sistematización de casos empleada por Autopsy.

Además, Autopsy tiene la noción de investigador, a quien relaciona con uno o más casos, permitiéndole tomar notas y generar resultados y reportes con base en sus investigaciones en el caso. (B. Carrier. (Marzo 15 de 2003)).

Por otro lado, Autopsy mantiene logs sobre todas las actividades realizadas por cada uno de los investigadores en cada uno de los casos, documentando automáticamente los pasos seguidos en el análisis forense (B. Carrier. (Marzo 15 de 2003)).

A nivel de la interfaz de usuario, Autopsy permite navegar por los archivos que se encuentran en cada una de las imágenes (incluso aquellos borrados que logran ser recuperados), permitiendo ver su contenido en representación *ASCII* o directamente en hexadecimal. También es posible realizar búsquedas directamente sobre la imagen (incluyendo el espacio no asignado por el sistema de archivos), haciendo uso de grep, strings y sstrings, organizar los archivos (haciendo uso de sorter), crear y visualizar una línea de tiempo (utilizando mactime) y recuperar archivos borrados (basándose en dls) (R. Lee. (2004)).

C. Algunas limitaciones

Las herramientas de análisis del *Journal* en TSK solamente se encuentran implementadas para los sistemas de archivo Ext3. (B. Carrier. (s.f.)), siendo necesaria su presencia para los sistemas de archivo NTFS, lo que permitiría encontrar una mayor cantidad de archivos borrados y establecer con mayor precisión las líneas de tiempo.

Además, TSK no provee ninguna herramienta que facilite la búsqueda de información en el *slack space*, lo cual obliga al investigador a desarrollar este tedioso proceso de forma manual.

En el caso de Autopsy, existe una limitación al efectuar búsquedas de cadenas, ya que no se realizan en los archivos sino en las unidades de datos.

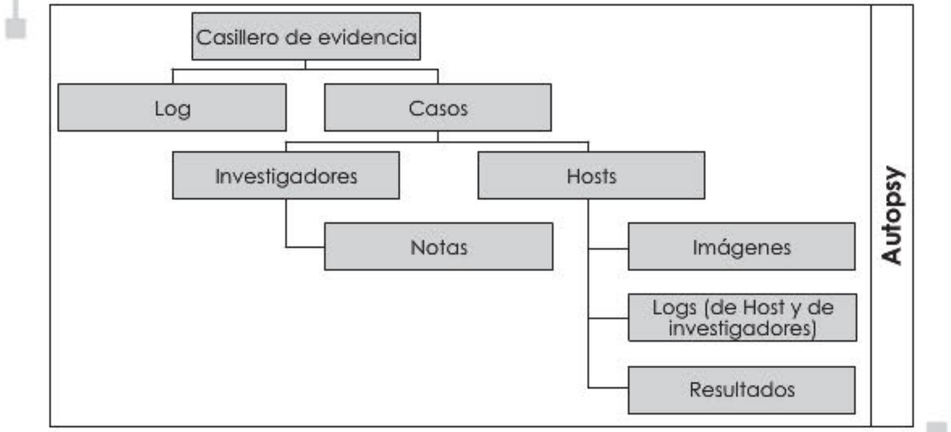


Gráfico A4.8

Manejo de casos en Autopsy

Lo anterior imposibilita el eventual hallazgo de las cadenas si se encuentran justamente entre unidades de datos no contiguas en el caso de archivos fragmentados.(B. Carrier. (Septiembre 15 de 2003)).

Por otro lado, el entender la imagen como 'un sistema de archivos en el sistema sospechoso'.(B. Carrier. (Marzo 15 de 2003)), puede dar pie a obviar potenciales datos relevantes a la investigación, ya que tales datos pueden estar 'ocultos' en el espacio entre los sistemas de archivos (imágenes).

Finalmente, las líneas de tiempo basadas en los tiempos MAC deberían ser presentadas, haciendo uso de algún tipo de representación gráfica que facilite su compresión, basándose en la facilidad humana de procesar paralelamente este tipo de información (R. Erbasher, K. Walker, D. Frincke. (s.f.)).

4. CASO DE PRUEBA

A. Presentación

Para ilustrar la guía metodológica previamente planteada, se propone el análisis del caso propuesto en *The Honeynet Project* (The Honeynet Project. (s.f.)). Es importante resaltar que no se busca solucionarlo exhaustivamente, sino encontrar mostrar cómo se aplica la metodología mediante cada una de las herramientas.

En general, el caso plantea una situación de venta de marihuana, en el cual se ve implicado Jimmy Jungle, quien aparentemente es el traficante. El caso requiere el análisis de la imagen de un disco flexible de 3½, para identificar archivos que incriminen a este personaje con la venta de drogas en colegios (The Honeynet Project. (s.f.)).

Para solucionar el caso, se utilizaron las herramientas de análisis forense anteriormente descritas; la solución detallada por medio de la aplicación de la metodología se describe en los dos literales siguientes.

Para ambas soluciones, el primer paso consistió en bajar la imagen comprimida, descomprimirla y comprobar su integridad como se ve en el *gráfico A4.9*.

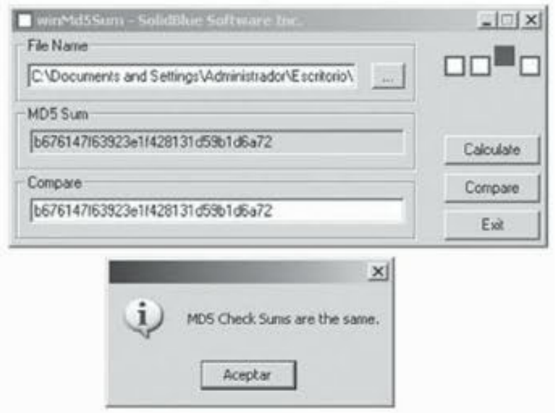


Gráfico A4.9

Verificación de integridad de la imagen

B. Desarrollo con EnCase

1. *Imagen de datos*

La imagen de datos del caso fue proveída junto a su marco circunstancial (The Honeynet Project. (s.f.)).

2. *Verificación de integridad de la imagen*

Previamente se realizó la verificación de integridad del archivo proveído con el caso. Es importante tener en cuenta que la verificación de integridad se hizo frente a una imagen y no contra la fuente original.

3. *Creación de una copia de la imagen suministrada*

En el momento de adquirir una imagen EnCase genera el archivo de trabajo; por lo tanto, en este caso no se requiere realizar ninguna copia adicional.

A continuación se crea un nuevo caso (*gráfico A4.10*), que requiere un nombre para el investigador y para el archivo de trabajo.

Luego se agrega al caso la imagen adquirida por medio de la herramienta de adquisición de imágenes. Posteriormente se adquieren de ésta los archivos que la contienen (*gráfico A4.11*).

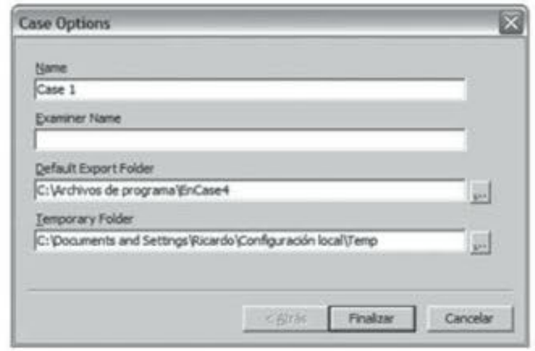


Gráfico A4.10

Creación del caso de prueba

Gráfico A4.11

Adquisición de la imagen

4. *Aseguramiento de la imagen suministrada*

Debido a que en este punto se está trabajando sobre una copia segura de sólo lectura, se puede asegurar la imagen original ubicándola en una ubicación segura del disco del investigador, o copiándola en algún dispositivo de almacenamiento electrónico. Para este caso, la imagen se almacenó en una carpeta asignada al caso, con permisos limitados.

5. *Revisión antivirus y verificación de la integridad de la copia de la imagen*

La primera actividad de esta fase es generar una copia de la imagen a la cual se le puede aplicar un análisis de detección de virus. Para este caso específico, se realizará una proyección en un disquete, usando dd en Linux, para después hacer la revisión antivirus sobre Windows, usando Norton antivirus (Symantec. (s.f.)).

Posteriormente, se realiza el cálculo del compendio criptográfico (*gráfico A4.12*) del archivo de trabajo para compararlo con el compendio inicial de la imagen obtenida para el caso.

Gráfico A4.12

Cálculo del compendio criptográfico de la copia de la imagen

6. *Identificación de las particiones actuales y anteriores (las que sea posible recuperar)*

Según Guidance Software (Julio de 2004), EnCase identifica las particiones del disco (*gráfico A4.13*), por medio de la búsqueda del carácter 0×55AA, y las enumera como partes no usadas del disco.

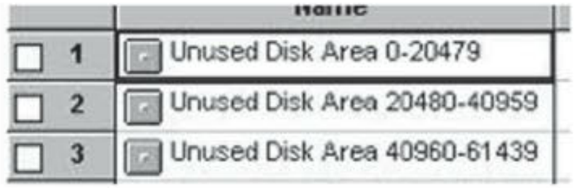


Gráfico A4.13

Cómo identificar las particiones

En este caso, EnCase no identificó ninguna partición en el disco (*gráfico A4.14*); por lo tanto, podemos asumir que solamente existe una partición.

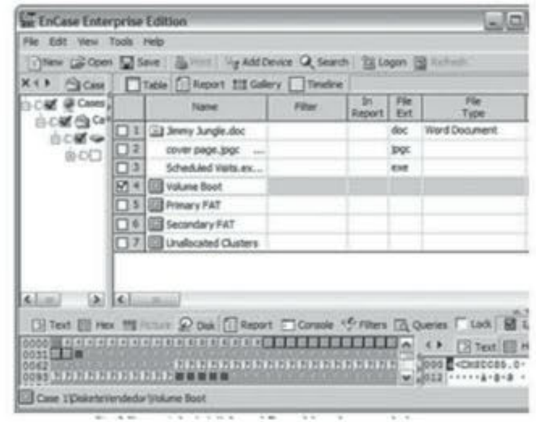


Gráfico A4.14

Identificación de particiones

7. *Detección de información en los espacios entre las particiones*

Al no haber particiones, no existe espacio entre particiones que pueda ser analizado

8. *Detección de HPA*

En este caso no aplica, debido a que se está trabajando sobre la imagen de un disquete.

9. *Identificación del sistema de archivos*

Aunque EnCase identifica automáticamente el sistema de archivos de la imagen, y por esta razón puede mostrar de manera ordenada sus archivos; se debe realizar una búsqueda en el sector de boot de la imagen para identificar el tipo de sistema de archivos, ya que EnCase no muestra este dato como muestra el *gráfico A4.15*

10. *Recuperación de los archivos borrados*

En la recuperación inicial de la imagen, EnCase reconoce algunos clusters no asignados, y archivos eliminados, mostrándolos, en el árbol de archivos (*gráfico A4.16*).

Sin embargo, para tener la certeza de que no había más archivos escondidos, se realizó un proceso de recuperación de carpetas, que no

arrojó ningún resultado, indicios que hacen concluir que únicamente existe un archivo borrado cuyo nombre es Jimmy Jungle.doc.

Gráfico A4.15

Recuperación del sistema de archivos

11. *Recuperación de información escondida* (gráficos A4.16 y A4.17)

Esta fase se concentra en el estudio de los clusters de la imagen, particularmente los marcados como dañados, con el fin de tratar de recuperar la información que contienen.

La descripción de los clusters de la imagen se presenta en el *gráfico A4.17*, donde se ve que solamente no existen clusters dañados (color negro), sino que se pueden identificar clusters perdidos, que pueden tener información relevante para el caso. Por ejemplo, en el último cluster perdido de la imagen se pudo encontrar una palabra sospechosa: "pw=goodtimes", que puede constituirse en evidencia para el caso en cuestión.

Adicionalmente, mediante un proceso de carving (escarbar) se logró identificar que en el espacio de clusters perdidos estaba escondida una imagen a la cual se hace referencia al archivo borrado encontrado en el paso anterior (*gráfico A4.18*).

12. *Identificación de archivos existentes*

Con base en el análisis de clusters y en la recuperación de archivos proveída por EnCase, se pueden identificar dos archivos: Schedule Visits.exe y coveredPage.jpgc.

Gráfico A4.16

Recuperación de archivos borrados

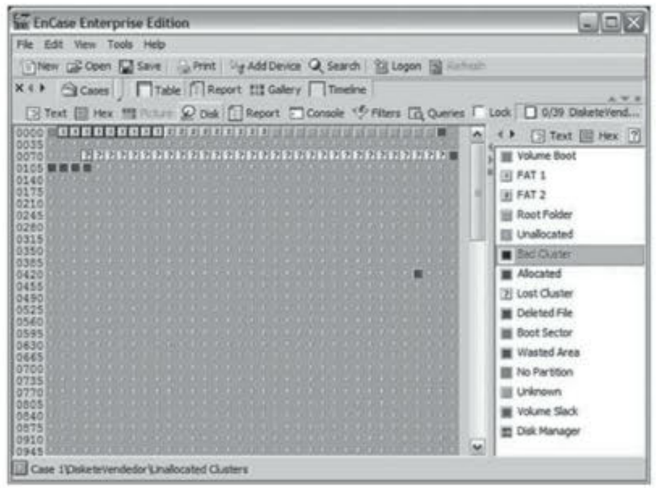


Gráfico A4.17

Recuperación de información escondida

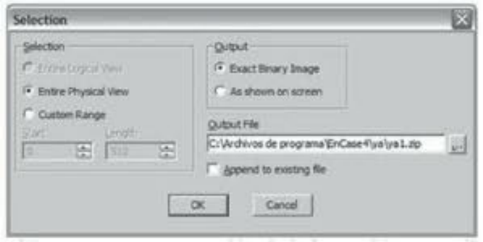


Gráfico A4.18

Recuperación de información escondida

13. *Identificación de archivos protegidos*

Durante esta fase, en particular, no se identifica ningún archivo protegido con contraseña.

14. *Consolidación de archivos potencialmente analizables*

En este punto del análisis se reúnen los archivos dispuestos a ser analizados.

15. *Determinación del sistema operativo y las aplicaciones instaladas*

En este caso no aplica, debido a que se está trabajando sobre la imagen de un disquete.

16. *Filtrado basado en archivos buenos conocidos*

En este caso tampoco aplica, debido a que se está trabajando sobre una imagen de un disquete.

17. *Consolidación de archivos sospechosos*

Al encontrarse tan pocos archivos en la imagen, no es necesario realizar un filtrado. Esto implica que todos los archivos son potencialmente sospechosos.

18. *Primera clasificación*

Durante este paso, se debe hacer una ponderación de los archivos, teniendo en cuenta diferentes criterios. En este caso, uno de los archivos con más prioridad es el archivo de Word que se encuentra eliminado, aunque también se debe realizar el análisis de firmas de los otros archivos existentes.

EnCase no arrojó ninguna inconsistencia entre los archivos y su extensión; sin embargo, se identificó manualmente que el contenido de dos de los archivos no correspondía a su extensión: coverpage.jpgc y Schedule Visits.exe.

19. *Segunda clasificación*

Durante esta fase, se analiza el archivo de Word identificando el paso de recuperación de archivos borrados, lo que revela datos concretos relevantes en la investigación.

20. *Analizar los archivos*

Al correlacionar el marco circunstancial, el archivo encontrado en el paso 18 y la información obtenida en el paso anterior, se pudo determinar que el contenido de este archivo estaba posiblemente protegido con una contraseña, que resultó ser la palabra sospechosa identificada en el paso 11.

Es importante notar que el proceso de recuperación del archivo zip se hizo mediante el mismo procedimiento de exportación de contenido por clusters empleado en el paso 11, debido a que el archivo leído por EnCase tenía información errada de su tamaño en su entrada de directorio.

EnCase proporcionó información suficiente para determinar la cantidad real de clusters del archivo y poder reconstruirlo.

21. *Archivos comprometidos con en el caso*

A partir del análisis se identificaron tres archivos comprometidos:

- CoverPage.jfif
- Schedule Visits.xls
- Jimmy Jungle.doc

22. *Obtención de la línea de tiempo definitiva*

En este caso no es necesario hacer una línea de tiempo, ya que el caso se resolvió completamente mediante los archivos encontrados y sus relaciones.

C. DESARROLLO CON SLEUTH KIT Y AUTOPSY

1. *Imagen de datos*

Suministrada junto al marco circunstancial del caso.

2. *Verificación de integridad de la imagen*

Se realizó la verificación de la integridad del archivo comprimido que tenía la imagen original; sin embargo, dado que el compendio criptográfico de la fuente original no fue suministrado, no fue posible validar la integridad de la imagen con respecto a su fuente.

3. *Creación de una copia de la imagen suministrada*

Se hizo una copia (image-copy) de la imagen original (image).

4. *Aseguramiento de la imagen suministrada*

El archivo original de imagen (el archivo comprimido) fue almacenado en un sitio seguro.

5. *Revisión antivirus y verificación de la integridad de la copia de la imagen*

Como no se contaba con ningún programa antivirus para Linux, fue necesario realizar este proceso en un sistema operativo Windows, usando una proyección de image-copy sobre un disco flexible de 3½, haciendo uso del comando:

- `dd if=/home/diego/FORENSICS/caso-paper/image of=/devfloppy`

Luego de comprobar la ausencia de virus, se realizó la verificación del compendio criptográfico de los dos archivos, para asegurar la equivalencia bit a bit entre image e image-copy como se muestra a continuación:

- ```
  # md5sum image
  ac3f7b85816165957cd4867e62cf452b image
  ```
- ```
  # md5sum image-copy
  ac3f7b85816165957cd4867e62cf452b image-copy
  ```

6. *Identificación de las particiones actuales y anteriores (las que sea posible recuperar)*

Se utilizó el comando mmls para descubrir las particiones en la imagen, pero el resultado indicó que solamente había una partición.

7. *Detección de información en los espacios entre las particiones*

Debido a los resultados del paso anterior, esta actividad fue omitida.

8. *Detección de HPA*

Dado que se trata de la imagen de un floppy, este paso no aplica.

9. *Identificación del sistema de archivos*

Antes de continuar con el análisis, es necesario agregar el caso, los investigadores, el host y la imagen a Autopsy como se ve en el *gráfico A4.19*.

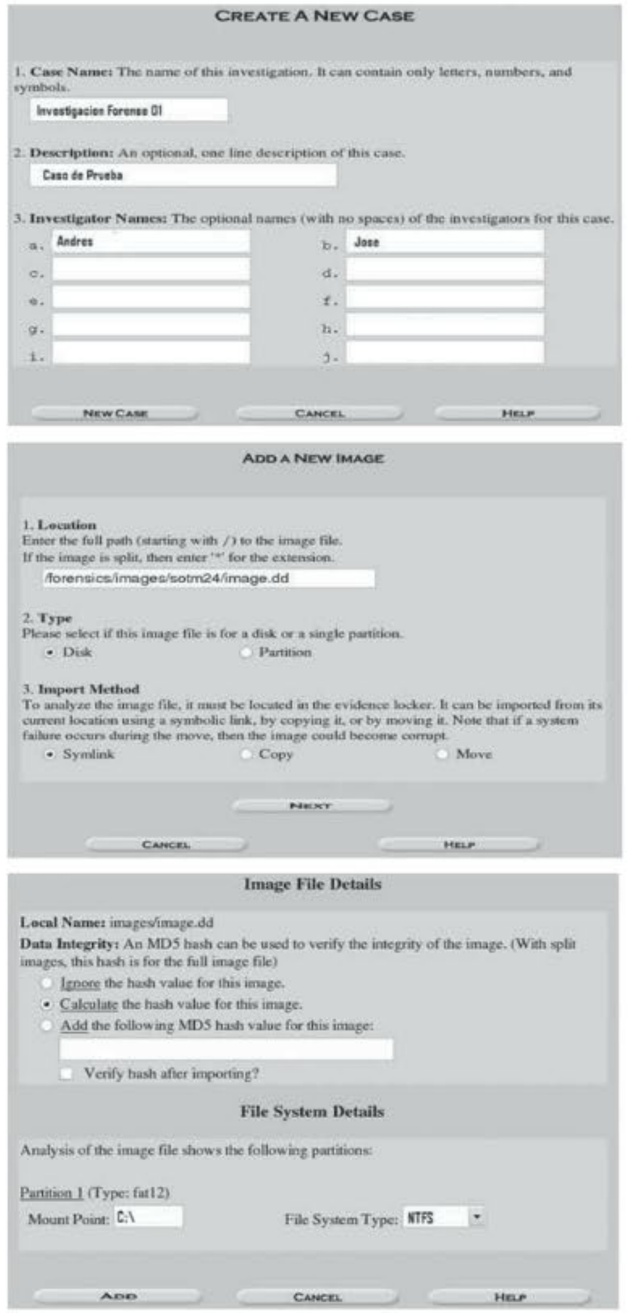


Gráfico A4.19

Proceso de adición de casos, host, investigadores e imagen en Autopsy

Posteriormente, se procede a revisar el sistema de archivos de la imagen. Lo anterior se logra desde la pantalla central del host, por medio del botón details -> FileSystem, que despliega la misma información que el comando fsstat, como se muestra a continuación:

```
# ../sleuthkit-2.01/bin/fsstat image-copy FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT12
OEM Name: MSDOS5.0
Volume ID: 0xc4b1cdcf
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory:
File System Type Label: FAT12
Sectors before file system: 0
File System Layout (in sectors)
Total Range: 0 - 2879
* Reserved: 0- 0
** Boot Sector: 0
* FAT 0: 1 - 9
* FAT 1: 10 - 18
* Data Area: 19 - 2879
** Root Directory: 19 - 32
** Cluster Area: 33 - 2879

METADATA INFORMATION
--------------------------------------------
Range: 2 - 45554
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 2848

FAT CONTENTS (in sectors)
--------------------------------------------
73-103 (31) -> EOF
104-108 (5) -> EOF
```

La información anteriormente presentada indica que se trata de un sistema de archivos FAT12 (lo esperado para un floppy), con dos fragmentos de archivo asignado.

10. *Recuperación de los archivos borrados*

En Autopsy, en la pantalla del host se selecciona Analyse -> File Analysis, para visualizar todos los archivos contenidos en la imagen, incluyendo los que han sido borrados y que fue capaz de recuperar, como se ve en el *gráfico A4.19*. Los archivos encontrados fueron adicionados al conjunto de archivos potencialmente analizables.

11. *Recuperación de información escondida*

A través del uso de Autopsy (Data Unit -> Allocation List) se buscaron los sectores asignados sin metadatos (sectores perdidos). Con base en la revisión del primer sector perdido se determinó que en él probablemente comenzaban los datos de una imagen (JPEG W3C. (s.f.)] image data, JFIF Standard 1.01). A continuación se realizó un recorrido por los sectores contiguos hasta encontrar su final, determinado por el principio de otro archivo.

Con esta información se procedió a extraer los datos de la imagen que se adicionaron al grupo de archivos potencialmente analizables.

12. *Identificación de archivos existentes*

La pestaña File Analysis de la interfaz de Autopsy lista los archivos contenidos en la imagen (gráfico A4.20).

Gráfico A4.20

Proceso de adición de casos, host, investigadores e imagen en Autopsy

13. *Identificación de archivos protegidos*

Uno de los archivos identificados en el paso anterior estaba comprimido. Se procedió a tratar de accederlo pero aparentaba estar corrupto. A continuación se notó, por medio de la lista de sectores asignados, que el

tamaño notificado por la metadata del archivo (File Analysis -> Metadata) no coincidía con el número de sectores continuos asignados. Por lo anterior hubo que extraerlo en su totalidad por medio de dcat, logrando recuperarlo más no accederlo, ya que éste estaba protegido con contraseña. Por esta razón, fue incluido en la lista de archivos sospechosos.

14. *Consolidación de archivos potencialmente analizables*

Tomando como base los archivos encontrados durante las fases anteriores, se procede a realizar una agrupación de los archivos que se analizarán durante el proceso.

15. *Determinación del sistema oprativo y las aplicaciones instaladas*

Debido a que se está trabajando sobre la imagen del disquete. No se requiere hacer este paso.

16. *Filtrado basado en archivos buenos conocidos*

Debido al reducido número de archivos comprometidos en la investigación, los dos últimos pasos fueron obviados en el proceso.

17. *Consolidación de archivos sospechosos*

Para este caso, este conjunto equivale al de los archivos potencialmente analizables.

18. *Primera clasificación*

Se encontró una inconsistencia entre el contenido de un archivo y su extensión, el cual tendrá una máxima prioridad al momento de realizar el análisis. Lo anterior se logró en Autopsy por medio de File Analysis -> File Types -> Extension Mismatches, que mostró:

Extension Mismatch

```
A:/Scheduled Visits.exe
 Zip archive data, at least v2.0 to extract (Ext: exe )
  Image:  /home/diego/EVIDENCE_LOCKER/PaperAnalisisDatos/
Floppy/images/image-copy Inode: 11
```

19. *Segunda clasificación*

No fue posible determinar una relación entre los archivos y el usuario, debido a que el sistema de archivos particular no mantiene este tipo de información. A su vez, se determinó que todos los archivos encontrados tienen alta prioridad.

20. *Analizar los archivos*

A la hora de analizar los archivos, se encontró un documento que proveía información sobre el proveedor del inculpado. Además, referenciaba la existencia de un archivo que contenía la contraseña del archivo protegido.

A continuación, se tomó el otro archivo (la imagen) y se procedió a buscar en él la firma de terminación de los archivos JPEG, la cual, se halló por medio de la aplicación de grep sobre el volcado hexadecimal de dichos archivo. Una vez se identificó la posición de la firma en el archivo, se descubrió un espacio de varios sectores, de los cuales se extrajo una cadena sospechosa que resultó ser la contraseña del archivo protegido que se encontró en el paso 13, cuyos contenidos se constituyeron en evidencia.

21. *Archivos comprometidos con en el caso*

Este grupo de archivos es igual al de los archivos sospechosos, más el archivo de Excel que logró ser accedido dentro del archivo comprimido.

22. *Obtención de la línea de tiempo definitiva*

Dado que la información de tiempo de los archivos no estaba disponible, no fue posible desarrollar este paso de la metodología.

Conclusiones

En Para profundizar se ha presentado una metodología para el análisis de datos en el marco de una investigación forense. Para aplicarla se han descrito y empleado dos herramientas particulares: EnCase y Sleuth Kit.

Lo anterior ha evidenciado que si bien el investigador forense tiende a seguir una metodología, frecuentemente las herramientas no permiten su seguimiento estricto. Esto se concluyó durante la realización del trabajo práctico, ya que se siguió el mismo proceso y la secuencia de hallazgos fue diferente.

Por otro lado, debido a que cada herramienta de análisis de datos es diferente, presentan características particulares, que facilitan o dificultan algunas actividades del proceso de análisis de datos. Por ejemplo, mientras EnCase está en capacidad de mostrar gráficamente el estado de los clusters asignados, Autopsy muestra estos datos sin formato gráfico, dificultando su interpretación.

Adicionalmente, se encontró que, a pesar de la gran utilidad que presentan las herramientas, el investigador forense muchas veces se ve en la necesidad de analizar los datos a nivel binario, debido a que gran cantidad de indicios se encuentran en esta capa y no son detectados por las aplicaciones.

✓***Resumen:*** Este apéndice propone una guía metodológica para realizar análisis forense a partir de una imagen de datos, independientemente del sistema de archivos, la plataforma y la herramienta de análisis utilizada. Dicha metodología se aplicó para un caso particular utilizando dos herramientas (EnCase y Sleuth Kit), las cuales se describen brevemente a partir de sus principales funcionalidades.

✓***Términos clave:*** Análisis de datos, Autopsy, EnCase, Forense, Sleuth Kit, TSK.

Enlaces en el Web

http://www.cerias.purdue.edu/research/forensics/ –Página del Grupo de Investigación en Computación Forense de Purdue University.
http://www.cert.org/forensics/ –Página del CERT de Carnegie Mellon University sobre computación forense.
http://www.cftt.nist.gov/ –Computer Forensic Testing Tools Program.
http://www.digital-evidence.org/ –Sitio Web del Dr. Brian Carrier con información y artículos sobre computación forense.
http://www.e-evidence.info –Sitio donde se tiene acceso a una gran cantidad de información en temas de informática forense.
http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm –Digital Evidence: Principles and Standards.
http://www.forensics.nl/links –Enlace a artículos y presentaciones sobre computación forense.
http://www.ijde.org –*Internacional Journal of Digital Evidence.*
http://www.jdfsl.org/index.htm –*Journal of Digital Forensics, Security, and Law.*
http://www.porcupine.org/forensics/ –Página de los Drs. Wietse Venema y Dan Farmer sobre análisis forense.
http://www.simson.net/cv/pubs.php –Publicaciones del Dr. Simson Garfinkel en temas de seguridad informática y computación forense.
http://www.swgde.org/ –Scientific Working Group on Digital Evidence.

Referencias*

Carrier, B. (Marzo 15 de 2005). "New Image File Support" en "The Sleuth Kit Informer Issue #19".. Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-19.html.
Carrier, B. (2005). "File System Forensics Analysis". Addison
Carrier, B. (Abril 15 de 2003). "Sorting Out The Sorter (Part 1 of 3)" en "The Sleuth Kit Informer Issue #3".. Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-3.html.
Carrier, B. (Enero 15 de 2005). "Description of the FAT fsstat Output" en "The Sleuth Kit Informer Issue #18".. Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-18.html.

* Referencias de la sección Para profundizar. (N. del E.).

Carrier, B. (Febrero 15 de 2003). "A High-Level Design Overview of Autopsy and TASK" en "The Sleuth Kit Informer Issue #1".. Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-1.html.
Carrier, B. (Junio 15 de 2003). "Sorter Internals (Part 3 of 3)", en "The Sleuth Kit Informer Issue #5". Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-5.html.
Carrier, B. (Marzo 15 de 2003). "Autopsy 1.70 Case Management", en "The Sleuth Kit Informer Issue #2". Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-2.html.
Carrier, B. (Mayo 15 de 2003). "Creating Custom Sorter Rule Sets" en "The Sleuth Kit Informer Issue #4". Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-4.html.
Carrier, B. (Mayo 15 de 2004). "TSK FAT File Recovery" en "The Sleuth Kit Informer Issue #14".. Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-14.html.
Carrier, B. (Noviembre 15 de 2004). "Detecting Host Protected Areas (HPA) in Linux" en "The Sleuth Kit Informer Issue #17".. Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-17.html.
Carrier, B. (s.f.). "Autopsy Forensic Browser". Disponible en: http://www.sleuthkit.org/autopsy.
Carrier, B. (s.f.). "Sleuth Kit Manual Pages". Disponible en: http://www.sleuthkit.org/sleuthkit.
Carrier, B. (s.f.). "TCTUTILs v1.01". Disponible en: http://www.porcupine.org/forensics/tct.html.
Carrier, B. (s.f.). "The Sleuth Kit". Disponible en: http://www.sleuthkit.org/sleuthkit.
Carrier, B. (Septiembre 15 de 2003). "Locking in on Keywords" en "The Sleuth Kit Informer Issue #8".. Disponible en: http://www.sleuthkit.org/informer/sleuthkit-informer-8.html.
Casey, E. (2002, 2004). Handbook of Computer Crime Investigation. Forensic Tools and Technology. First Edition, 2004 Reprint. Elsevier Academic Press 2002.
Casey, E. (s.f.). "Error, uncertainty and loss in digital evidence". Disponible en: http://www.sleuthkit.org/autopsy.
Cmdr. D. Pettinari. (Julio 2 de 2000). "EnCase Forensic Evidence Acquision and Analysis", Investigative and Technical Protocols, Pueblo High-Tech Crimes Unit,.
Erbasher, R. Walker, K. Frincke, D. (s.f.). "Intrusion and Misuse Detection in Large Scale Systems".
Gluzinski, T. Kida J. (s.f.). " Managing your Evidence your Evidence Problems associated with proper collection procedures". Disponible en: http://www.paladintek.com/WhitePaper/Managing_Your_Evidence.pdf.
Guidance Software. (Julio de 2004). "EnCase® Enterprise Edition Detailed Product Description". Disponible en: http://www.EnCase.com/corporate/whitepapers/downloads/EEEDetailed.pdf
Guidance Software. (s.f.). "EnCase Forensic Edition Visual Guide".
Guidance Software". (s.f.). Disponible en: http://www.EnCase.com http://www.sleuthkit.org/sleuthkit/man/
Janiczek, M. (2004). "Principios Básicos del Análisis Forense" en "Hackin9", Vol. 3. pp. 62-79.

Keightley R. (s.f.). Guidance Software, "EnCase versión 3.0 Manual". Revision 3.18.
Lee, R. (2004). "Windows Computer Forensics" en "Know Your Enemy. Learning About Security Threats". 2a. edición. Addison Wesley. 2004.
Morris, J. (Febrero 11 de 2003). "Forensics on the Windows Platform Part Two". Disponible en: http://www.securityfocus.com/infocus/1665
Morris, J. (s.f.). "Fcrensics on the Windows Platform, Part One", Disponible en: http://www.securityfocus.com/infocus/1661.
"Problems associated with proper collection procedures". Disponible en: http://www.paladintek.com/WhitePaper/Managing_Your_Evidence.pdf.
Reith, M. Carr, C. Gunsch, G. (s.f.). "An Examination of Digital Forensic Models". Disponible en: http://www.ijde.org/archives/02_fall_art2.html.
Symantec. (s.f.). "Norton Antivirus". Disponible en: http://www.symantec.com/nav/nav_9xnt/
The Coroner's Toolkit". (s.f.). Disponible en: http://www.porcupine.org/forensics/tct.html.
The Honeynet Project. (s.f.). "Scan of the Month 24". Disponible en: http://www.honeynet.org/misc/files/sotm.tar.gz
US Department of Justice. (Abril 2004). "Forensic Examination of Digital Evidence: A Guide for Law Enforcement".
W3C. (s.f.). "JPEG JFIF". Disponible en: http://www.w3.org/Graphics/JPEG/
Williams, C. (2001). "Ext3 Journaling File System". Disponible en: http://www.cs.umd.edu/projects/shrug/ppt/5-Oct-2001.ppt

Bibliografía

Abdalla, S., Hazem, S. y Hashem, S. (2007). Guideline model for Digital forensic Investigation. *En Proceedings of Conference on Digital Forensics, Security and Law.* Pp. 55-75.
Babitsky, S. y Mangraviti, JR, J. (2002). *Writing and defending your expert report.* SEAK, Inc.
Bishop y otros (2007). Toward models for forensic analysis. *Proceedings of Second International Workshop on systematic approaches to Digital Forensic Engineering.* IEEE.
Cano, J. (2005). Estado del arte del peritaje informático en Latinoamérica. Comunidad Alfa-Redi. Disponible en: http://www.alfa-redi.com/ar-dnt-documento.shtml?x=728. (Consultado: 2-03-2008).
Cano, J. (2007). Inseguridad informática y computación antiforense: Dos conceptos emergentes en seguridad de la información. Disponible en: http://www.virusprot.com/Archivos/Antifore07.pdf (Consultado: 28/04/2007).
Cohen, W. (2008). *En clase con Drucker*. Diecisiete lecciones magistrales. Editorial Norma.
Forsyth, P. (2003). *Presente informes y propuestas eficaces*. Ed. Gedisa.
Gavin, M. (2006). *CSI: Cyberspace*. Forrester Research.
Homeland Security –USA (2007). *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development.*
Ieong, R. (2007). FORZA –Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. Número 35, pp. 29-36.

Jay Myers, L. (2000). *High technology crime investigation: A curricular needs assessment of the largest criminal justice and criminology programs in the United States*. Tesis doctoral no publicada. Texas A&M University. Texas, Estados Unidos de Norteamérica.
López Calvo, P. y Gómez Silva, P. (2003). *Investigación criminal y criminalística.* Segunda edición. Temis.
Nelson, S., Olson, B. y Simek, J. (2006). *The electronic evidence and discovery handbook*. Forms, checklist and guidelines. ABA Law Practice Management Section.
Osterburg, J. y Ward, R. (2000). *Criminal investigation*. Third Edition. Anderson Publishing.
Pollitt, M. (2007). An ad hoc review of Digital Forensic Models. *Proceedings of Second International Workshop on systematic approaches to Digital Forensic Engineering*. IEEE.
Raymond Choo, K.K., Smith, R. y McCusker, R. (2007). Future directions in technology-enabled crime: 2007-09. Australian Institute of Criminology. Research and Public Policy Series. Número 78. Disponible en: http://www.aic.gov.au/publications/rpp/78/rpp78.pdf (Consultado: 20-04-2008).
Rice, D. (2008). *Geekonomics. The real cost of insecure software.* Addison Wesley.
Riofrío, J. C. (2004). *La prueba electrónica.* Temis.
Rogers, M. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study. Unpublished Doctoral Thesis. University of Manitoba. Manitoba. Canadá. Disponible en: http://homes.cerias.purdue.edu/~mkr/cybercrime-thesis.pdf (Consultado: 20-04-2008).
Saferstein, R. (2001). *Criminalistic. An introduction to forensic science*. Seventh Edition. Prentice Hall.
Schmalleger, F. y Pittaro, M. (2009). *Crimes of the Internet*. Pearson-Prentice Hall.
Soria Verde, M. A. y Sáiz Roca, D. (coordinadores). (2006). *Psicología criminal*. Pearson-Prentice Hall.
Soria, M. (2006). La psicología de investigación criminal: perfiles psicológicos criminales y hallazgos criminológicos forense. En Soria, M. y Sáiz, D. (coordinadores). (2006). *Psicología criminal*. Pearson-Prentice Hall.
Stambaugh, H., Beaupre, D., Icove, D., Baker, R., Cassaday, W y Williams, W. (2001). Electronic Crime Needs Assessment for State and Local Law Enforcement. National Institute of Justice. *Research Report*. Disponible en: http://www.ncjrs.gov/pdffiles1/nij/186276.pdf (Consultado: 2-03-2008).
Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E. y Liederbach, J. (2006). *Digital crime and digital terrorism.* Pearson- Prentice Hall.
Walden, I. (2007). *Computer Crimes and digital investigations*. Oxford Press

5 RETOS Y RIESGOS EMERGENTES PARA LA COMPUTACIÓN FORENSE

Objetivos

- ✓ Revisar y analizar la formación de especialistas en informática forense.
- ✓ Presentar algunos desafíos propios de la confiabilidad de las herramientas forenses en informática.
- ✓ Presentar avances en el desarrollo de las técnicas antiforenses y sus implicaciones para las investigaciones.
- ✓ Analizar las tendencias emergentes, como el cibercrimen y el ciberterrorismo.
- ✓ Ilustrar algunos de los retos tecnológicos más sobresalientes para los investigadores forenses en informática: archivos cifrados, esteganografía en video, rastros en ambientes virtuales, evidencias en memoria volátil y análisis de sistemas en vivo.

5.1 LA FORMACIÓN DE ESPECIALISTAS EN INFORMÁTICA FORENSE

La evolución actual de los negocios y de las posibilidades, que día a día se abren con el uso de las tecnologías de información y comunicaciones, establece retos interesantes tanto para las organizaciones como para los profesionales en telecomunicaciones e informática. En este contexto, esa evolución aprovechada de manera positiva ofrece a los ciudadanos nuevas opciones y oportunidades para conectarse y compartir información,

La evolución de los negocios establece retos para las organizaciones y los profesionales en telecomunicaciones e informática.

productos o servicios más allá de las fronteras nacionales, generando relaciones multilaterales que lleven a las personas, empresas y naciones a competir en un escenario global.

Esta realidad positiva se contrasta con la evolución natural de delincuencia tradicional, y organizada ahora en medios electrónicos (Parker y Nycum 1984, Parker 2007b), en donde han encontrado un nuevo nicho para desarrollar sus actividades criminales, sabiendo que tendrán ventajas comparativas frente a lo que hacían en el mundo *offline*. Los nuevos criminales informáticos (Knetzger y Muraski 2008) reconocen en los medios tecnológicos una manera fácil para materializar sus acciones, económicamente favorable (poca inversión con ganancias superiores), moralmente menos exigente (atacar o inhabilitar a una máquina no tiene el mismo componente moral que hacerlo a una persona), y una manera fácil de llamar la atención, dados los impactos de las acciones sobre objetivos conocidos.

Los delincuentes informáticos son una nueva generación de criminales.

Los delincuentes informáticos son una nueva generación de criminales que, utilizando sus técnicas naturales en el mundo físico, renuevan y afinan las mismas para producir acciones punibles de mayores impactos, con alta efectividad en el logro de sus objetivos y limitadastrazasparaserrastreadosodetectados. Si bien los crímenes perfectos son difíciles de lograr en el mundo virtual, esta teoría se hace menos evidente, porque los rastros propios de las acciones de los delincuentes pueden ser y serán alterados, manipulados, escondidos o eliminados (Peikari y Chuvakin 2004, Cano 2007) según la habilidad de estos últimos.

En este escenario, donde tenemos un enemigo que se mimetiza en los tejidos de la red de los bits y los bytes, es necesario desarrollar una nueva raza de investigadores, de acuerdo con el reto que exige seguir un delincuente en medios tecnológicos (Yasinac, A., Erbacher, R., Marks, D., Pollitt, M. y Sommer, P. 2003). Este nuevo investigador debe saber que siempre estará a un paso atrás del atacante, que sus técnicas se pondrán a prueba en cada caso, y que sus razonamientos lógicos podrán ser controvertidos por la constante evolución del atacante para tratar de evadir las investigaciones. Este investigador debe reconocer

en el criminal informático un blanco móvil, generalmente invisible y altamente técnico que hará que sus técnicas y procedimientos (Andrew 2007) se actualicen constantemente y se ajusten, según la realidad de la inseguridad en las tecnologías de información y comunicaciones.

El *cibercrimen* (basado en las potencialidades de la inseguridad informática), como elemento emergente en el escenario de un mundo interconectado, tiene elementos que lo hacen imperceptible y característico de una "sorpresa predecible" (Bazerman, M. y Watkins, M. 2004).

El cibercrimen tiene elementos que lo hacen imperceptible y característico de una "sorpresa predecible".

- La gente piensa que eso es un invento de "los paranoicos" y que si pasara, no sería tan grave.
- Se tienen datos y noticias relacionados con este tema, pero dispersos y poco difundidos.
- Los gobiernos no tienen tiempo para mirar esto, porque existen otros temas más prioritarios para sus naciones.

Adicionalmente a estos elementos planteados, se suman las falsas alarmas, las cuales crean inmunización y fatiga en los analistas, que disminuyen su atención en los problemas potenciales emergentes, generando una falla estructural en el sistema de inteligencia de las naciones que no permite reconocer una amenaza real cuando ésta llega.

La inseguridad informática es una sorpresa predecible, algo con lo cual se convive y, aún así, sus manifestaciones, cada vez más silenciosas y estratégicamente concebidas, no nos alertan sobre los efectos que puede traer al adecuado funcionamiento de las organizaciones (Parker 2007). Esta situación genera una resistencia natural a estar atentos por algo que no podemos evitar, pero que sí podemos intentar comprender, y no sólo identificar.

Por tanto, la formación de investigadores forenses en informática, como esos garantes de la justicia ahora en los medios digitales e informáticos, requiere atención especial para establecer los referentes mínimos del plan de estudios que lleve a la profesionalización de

La formación de investigadores forenses en informática requiere atención especial para establecer los referentes mínimos del plan de estudios.

estos nuevos investigadores. A continuación se presentan algunas de las iniciativas en este sentido.

Los estudios realizados por Myers (2000), para establecer los conocimientos requeridos para detectar, investigar y perseguir crímenes de alta tecnología, así como sus análisis de los programas de justicia criminal en los Estados Unidos, en el año 2000, concluyen con una propuesta de formación del especialista investigador en crímenes de alta tecnología, que incluye tres áreas de conocimiento: justicia criminal y criminología, principios de contabilidad y auditoría y, finalmente, tecnologías de información y operaciones en computadores (*gráfico 5.1*).

Gráfico 5.1

Investigación de crímenes de alta tecnología. (Traducción libre de: Myers 2000, p.132).

De otra parte, las investigaciones realizadas por Taylor, Endicott-Popovsky y Phillips (2007) establecen que existen cuatro (4) componentes de excelencia que deben estar presentes en programas de formación en forensia digital (digital forensics), los cuales permiten que dichos programas desarrollen profesionalmente a los especialistas en estos temas. Los cuatro componentes son: contenido multidisciplinario, ejercicios prácticos en el laboratorio (hands-on), instructores calificados y con amplio conocimiento en el tema, y ejemplos del mundo real (*gráfico 5.2*).

Gráfico 5.2

Componentes fundamentales de los programas en forensia digital.
(Traducción libre de: Taylor, Endicott-Popovsky y Phillips 2007, p. 6)

El contenido multidisciplinario debe permitir la formación no sólo de un analista técnico en temas de tecnologías de información, sino el conocimiento y el manejo de temas en criminalística, criminología, delitos informáticos, seguridad de la información, cumplimiento de normas y estándares, entre otros elementos. El especialista debe estar entrenado para abordar la problemática que se le proponga con amplia perspectiva, de tal manera que sepa presentar sus argumentos técnicos en escenarios no técnicos.

Los ejercicios prácticos en el laboratorio, con herramientas tecnológicas (licenciadas o de código abierto), deben procurar diferentes niveles de dificultad de análisis de los especialistas: información volátil, información de redes, información en micros, nuevos dispositivos de almacenamiento, dispositivos móviles, entre otros, que pongan a prueba los conocimientos técnicos y sus procedimientos para una adecuada identificación, manejo y control de la evidencia digital.

Los instructores calificados, y con amplio conocimiento del tema, son pieza fundamental de los programas en temas de forensia digital; dado que no existe un cuerpo de conocimiento formal, la experiencia de éstos, su visión acerca de los casos que han desarrollado, les permite ofrecer a los estudiantes un escenario de análisis y revisión que enriquece el contenido de las materias que se ofrecen en el currículo que se plantee.

Finalmente, los ejemplos del mundo real buscan darle mayor autenticidad y profundidad al aprendizaje planteado a lo largo de los cursos. Los casos reales le muestran al estudiante la problemática real, la habilidad de los atacantes y los impactos que éstos pueden causar con sus acciones en infraestructuras de computación, organizaciones o naciones.

Si bien estas dos iniciativas no son las únicas que a la fecha existen sobre la formación de investigadores en informática forense (Craiger, Ponte, Whitcomb, Pollitt y Eaglin 2007, Collins y McGuire 2008), sí plantean elementos clave para considerar en futuras iniciativas en estos temas, para enfrentar el desafío curricular para capacitar y entrenar a los nuevos detectives informáticos que, conscientes de la evolución permanente de la criminalidad, puedan advertir, confrontar y perseguir las novedosas acciones punibles ahora en medios tecnológicos.

5.2 CONFIABILIDAD DE LAS HERRAMIENTAS FORENSES EN INFORMÁTICA

Para la computación forense, otro reto es validar la confiabilidad de las herramientas forenses utilizadas en sus investigaciones.

Para la computación forense, otro reto emergente son las herramientas tecnológicas que los investigadores utilizan para adelantar sus pericias (Adams 2007). Por un lado, las herramientas licenciadas, propiedad de firmas desarrolladoras de software para forensia digital, establecen un nicho de negocio que exige de los investigadores forenses en informática importantes inversiones, tanto en hardware como en software, para darles mayores formalidad y certeza a las partes involucradas en un caso de la evidencia digital.

Dichas inversiones no sólo son en la adquisición, sino en el mantenimiento y la actualización de las mismas, lo que hace que los especialistas forenses deben constantemente reforzar sus habilidades en el uso de estos programas y mantenerse notificados de posibles errores, propios de las mismas y sus maneras de mitigarlos, pues saben que un caso basado en la confiabilidad de las mismas se puede o no decidir (McDonald, Kim y Yasinsac 2008).

De otra parte, se encuentran las herramientas forenses de código abierto (llamadas software libre), las cuales aún son cuestionadas en muchos tribunales y poco se recomiendan como herramientas de uso formal para presentar en audiencias, por su condición de herramientas revisadas y analizadas por una comunidad de la cual poco se conoce de sus pruebas, de las personas que adelantan las mismas, ni del control de los errores. Sin embargo, otra corriente defiende estas herramientas (Carrier 2003) frente a las licenciadas, diciendo que en el mundo de código abierto todo está para el escrutinio de un tercero, que las pruebas se pueden adelantar con mayor confianza que en las abiertas, y que el nivel de confiabilidad es mayor, dado que son muchos "ojos" los que están tratando de mejorarla (*gráfico 5.3*).

Las herramientas forenses de código abierto (software libre) aún son cuestionadas en muchos tribunales.

ALGUNAS HERRAMIENTAS LICENCIADAS		ALGUNAS HERRAMIENTAS DE CÓDIGO ABIERTO
ENCASE - guidance software FORENSIC TOOL KIT - Access data WINHEX FORENSICS -X- Ways Software technology AG PRODISCOVER TOOLS - technology pathways COMPUTER FORENSICS SOFTWARE TOOL SUITE - New technology, Inc	VS.	THE SLEUTH KIT THE CORONER TOOL KIT DCFL-DD LIVEVIEW NETCAT CRYPTCAT PASCO

Gráfico 5.3

Herramientas forenses en informática: licenciadas versus código abierto

Mientras esta disyuntiva continúa, se adelantan importantes esfuerzos formales para probar las herramientas forenses como lo es el proyecto de *Nacional Institute of Standards and Technology* norteamericano, NIST, denominado, *NIST Computer Forensic Tool Testing Program,* cuyo objetivo es "establecer una metodología para probar aplicaciones forenses en informática a través del desarrollo de la especificación

general de herramientas, procedimientos de prueba, criterios de prueba, conjuntos de pruebas y pruebas de hardware. En este sentido, los resultados de esta iniciativa proveerán la información necesaria a los proveedores para mejorar sus aplicaciones; elementos de juicio y análisis a los usuarios de las mismas en el momento de adquirir y utilizar estas herramientas, así como criterios a terceras partes interesadas para comprender las capacidades y limitaciones de las aplicaciones forenses en informática" (traducción libre de: NIST IR –*Interagency Report* 7490. *Digital Forensics at NIST.* http://www.cftt.nist.gov/NISTIR_7490.pdf, p. 3).

Las pruebas efectuadas por centros de investigación especializados a los programas y dispositivos de hardware son útiles para dar cumplimiento a las exigencias propias del test de Daubert.

En este contexto, las pruebas que se realicen a los programas y dispositivos de hardware serán útiles para dar cumplimiento a las exigencias propias del *test de Daubert,* prueba de referencia generalizada para establecer la confiabilidad de las herramientas en computación forense.

El test de Daubert (Dixon y Gill 2001) es un conjunto de reglas extraídas de la sentencia de la Corte Suprema de Justicia Estadounidense, en el caso de Daubert *versus* Merrell Dow Pharmaceutics, Inc., 509 U.S. 579 de 1993, donde se clarifican los estándares que los jueces federales deben tener en cuenta a la hora de admitir o no la evidencia entregada por expertos en un caso. Si bien no es un estándar universalmente seguido, sí se ha considerado en muchas iniciativas normativas sobre el tema a nivel internacional. Las reglas que establece la prueba de Daubert son:

- La técnica o el programa utilizados han sido probados en condiciones reales y no sólo en los laboratorios.
- La técnica o el programa han sido sometidos a revisión de pares académicos o científicos y publicaciones especializadas.
- Se conoce el nivel de error potencial del programa o técnica.
- Existe un estándar o un referente para el control y la revisión del programa o técnica.

- La técnica o el programa son generalmente aceptados dentro de la comunidad científica relevante a la misma.

En este sentido, los programas o las herramientas de computación forense requieren estudios y análisis detallados para contar con un nivel de aceptación de los mismos, bien sean licenciados o de código abierto. Mientras más pruebas formales se tengan, mayor exposición a la verificación de sus niveles de error, mejores condiciones habrá para el fortalecimiento de las mismas tanto a nivel jurídico en un caso, como a nivel profesional en el uso de la misma.

Los programas o las herramientas de computación forense requieren estudios y análisis detallados.

Considerando lo anterior y que el indiciado o imputado cuenta con todas las garantías constitucionales durante el desarrollo de un caso, el investigador forense en informática deberá seguir rigurosamente todos sus procedimientos y asegurarse de que la herramienta o las herramientas utilizadas pueden soportar el escrutinio del test de Daubert, y así no tener problemas al sustentar los informes de pericia que tenga que desarrollar. En este contexto, recuerde que cualquier duda que se identifique en la presentación de resultados o la utilización de las herramientas forenses, si no es absuelta satisfactoriamente bajo las exigencias del test, será resuelta siempre a favor del procesado.

Cualquier duda no verificada satisfactoriamente en el desarrollo de un proceso será resuelta siempre a favor del procesado.

5.3 TÉCNICAS ANTIFORENSES Y SUS IMPLICACIONES PARA LAS INVESTIGACIONES ACTUALES Y FUTURAS

Los atacantes evolucionan tan rápido como la inseguridad de la información (Raymond Choo, Smith y McCusker 2007). Cuando un nuevo desarrollo tecnológico hace su aparición, más se demora la industria en promocionarlo, que evidenciarse una vulnerabilidad propia del diseño del dispositivo o aplicación. En este sentido,

Los atacantes evolucionan tan rápido como la inseguridad de la información.

tanto los especialistas en seguridad de la información como los investigadores en informática forense deben avanzar en el reconocimiento de esa tecnología y estudiar sus ventajas y limitaciones, para estar tan cerca como sea posible de la explotación de las vulnerabilidades que pudiesen presentarse (*gráfico 5.4*).

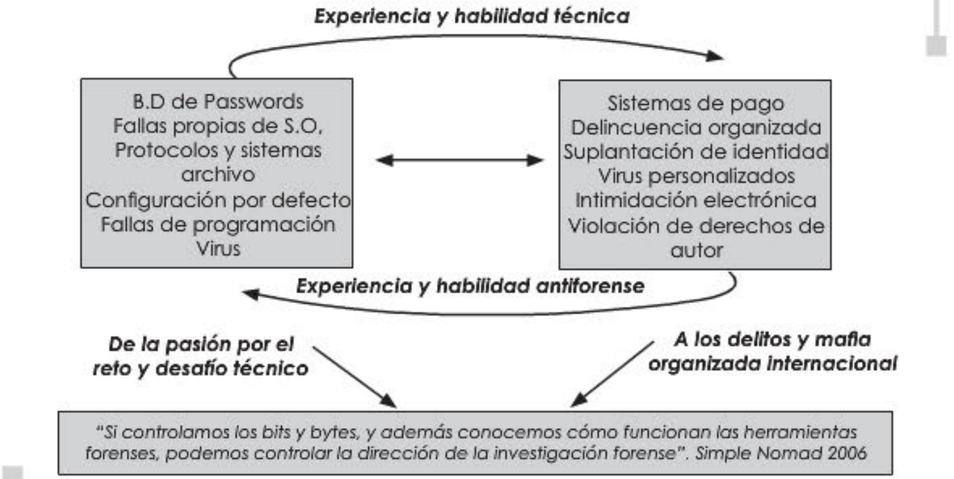


Gráfico 5.4

Evolución de los atacantes. ¿Para dónde vamos?

Las técnicas antiforenses no cuentan con un marco de referencia compartido para su estudio o análisis.

A la fecha, las técnicas antiforenses no cuentan con un marco de referencia compartido para su estudio o análisis, pero revisándolas desde la perspectiva de las vulnerabilidades informáticas podríamos ver una oportunidad para comprender mejor su funcionamiento. En este sentido, las técnicas antiforenses retan a los investigadores para hacer fallar las herramientas forenses disponibles y afinar las mismas (Schneier, B. 2003, p. 8).

Si bien, la madurez de las herramientas forenses disponibles hasta la fecha es tema de investigación actual, de igual forma y con

mayor preocupación, están las técnicas antiforenses, como ese factor crítico de éxito para ajustar los procedimientos forenses que se adelanten en las investigaciones. Es claro que los procedimientos estándar que actualmente se tienen para asegurar la escena del incidente o delito podrían no tener cambios significativos, pero sí requieren ser repensados y analizados a la luz de la imaginación de los atacantes para disminuir la capacidad de identificación, recolección, análisis y presentación de evidencia en un proceso.

La madurez de las herramientas forenses disponibles a la fecha es tema de investigación actual.

Las técnicas antiforenses genéricas (Peikari y Chuvakin 2004, cap. 22), como las técnicas forenses específicas en informática, evolucionan y se perfeccionan; en este sentido, los conceptos base para la comprensión de sistemas de archivo, sistemas de comunicaciones, sistemas inalámbricos, medios de almacenamiento, sistemas operacionales, protocolos de comunicaciones, manejo de dispositivos electrónicos recientes, como los asociados con Radio Frequency Identification, *RFID*, se vuelven críticos para la formación y la práctica de los investigadores forenses, pues, sin un conocimiento claro de los mismos, el atacante tendrá mayores oportunidades para confundir y distorsionar la realidad de los hechos. Es importante aclarar que no se pretende que el investigador tenga un conocimiento total de todos los conceptos base comentados, sino la conciencia y la experiencia requeridas para que en el trabajo de campo futuro sepa qué puede hacer, qué no y dónde puede aportar para reconocer posibles estrategias de evasión que los intrusos utilizan.

En este escenario de constante evolución, las técnicas forenses requieren un protocolo diferente de estandarización y ajuste para estar tan cerca como las nuevas vulnerabilidades que se presenten tanto en sus herramientas como en las infraestructuras de las empresas. En este contexto, los encargados del mejoramiento de las prácticas forenses (institutos internacionales, organismos gubernamentales, universidades e investigadores de campo) deben dedicar parte

Las técnicas forenses requieren una actualización y ajuste permanente basado en el entendimiento de las nuevas vulnerabilidades.

de su tiempo para mirar cómo los eventos del entorno son relevantes para la práctica de las investigaciones forenses. No solamente es la regulación del ejercicio práctico y procedimental, que es necesario para generar mayor confiabilidad de los resultados (Ieong 2006), sino la capacidad para desarrollar nuevas formas de fortalecer las herramientas y técnicas utilizadas en favor del avance de la disciplina como tal y, por ende, de la administración de justicia.

Para desarrollar un marco conceptual de análisis de las estrategias antiforenses (Harris 2006, pp. 44 y 45), revisamos algunas definiciones disponibles sobre las mismas:

1. "(…) métodos usados para prevenir (o actuar en contra de) la aplicación de la ciencia, por parte de las agencias de policía, como apoyo a las leyes penales y civiles en un sistema de administración de justicia".
2. "(…) limitar la identificación, recolección y validación de datos electrónicos (…)".
3. "(…) cualquier intento para limitar la cantidad y calidad de la evidencia forense".
4. "(…) cualquier intento para comprometer la disponibilidad o utilidad de la evidencia en un proceso forense (…)".

Revisando estas definiciones, observamos que cada una de ellas hace énfasis en diferentes realidades de las investigaciones forenses. La primera está orientada al proceso formal en el cual se fundan la criminalística y el ejercicio formal de los criminalistas, para apoyar a la administración de justicia en su búsqueda de la verdad en cada uno de los procesos. La segunda y tercera están enfocadas al proceso mismo de la investigación que procura la mejor evidencia posible para probar lo ocurrido. Finalmente, la cuarta, trata de cubrir todas las anteriores, combinando lo requerido en el proceso formal forense y la utilidad de la evidencia identificada, recuperada y analizada.

Estrategia antiforense es "Cualquier intento exitoso... que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital..."

Si tratamos de modificar la cuarta definición, podríamos expandirla de tal forma que oriente a los investigadores forenses en la práctica. La propuesta sería: "Cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la

identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense".

Considerando lo anterior, las estrategias antiforenses aplicadas en la escena del posible ilícito o incidente buscan, entre otros objetivos (Garfinkel 2007, p. 77), los siguientes:

- Limitar la detección de un evento que haya ocurrido.
- Distorsionar la información residente en el sitio.
- Incrementar el tiempo requerido para la investigación del caso.
- Generar dudas en el informe forense o en el testimonio que se presente.
- Engañar y limitar la operación de las herramientas forenses informáticas.
- Diseñar y ejecutar un ataque contra el investigador forense que realiza la pericia.
- Eliminar los rastros que pudiesen haber quedado luego de los hechos investigados.

En consecuencia, las estrategias antiforenses establecen un nuevo capítulo en las investigaciones científicas tanto en seguridad de la información como en las ciencias forenses, pues, considerando los objetivos planteados anteriormente, se requiere conocer detalladamente los procedimientos forenses establecidos a la fecha, para desvirtuarlos uno a uno, y así generar confusión e incertidumbre para todos los actores del proceso.

Si lo previamente planteado es correcto, es necesario profundizar en los métodos previstos para materializar esas estrategias antiforenses. Investigaciones recientes (Harris 2006, p. 45) proponen la siguiente clasificación de métodos evasivos, como: destrucción de la evidencia, eliminación de la fuente de la evidencia, ocultar la evidencia y la falsificación de la evidencia.

> Las estrategias antiforenses establecen un nuevo capítulo en las investigaciones científicas en temas informáticos.

5.3.1 Destrucción de la evidencia (Cano 2007)

Este método busca modificar físicamente el objeto que contiene la evidencia requerida, de tal forma que no sea posible conseguirla de manera confiable o real. Cuando se habla de *eliminar la fuente de la evidencia*, significa neutralizar el sistema o la técnica utilizada por el sistema para dejar los rastros (Hoglund y Butler 2006); al controlar esta técnica o proceso no existirá la evidencia y, por tanto, no habrá trazas que seguir en una investigación (ídem).

Si el atacante no ha podido materializar los dos métodos anteriores, puede optar por esconder *la evidencia o falsificarla*. En la primera, la evidencia se dispersa en el medio que la contiene, se oculta en el mismo, o en el sistema donde se encuentra, limitando los hallazgos del investigador en su proceso. En la segunda, crea o invalida la evidencia residente en el sistema para limitar las conclusiones y análisis que adelante el investigador (ídem).

A manera de resumen y como elemento de análisis, se adjunta (con la autorización de su autor) un cuadro resumen y analítico de las técnicas antiforenses desarrollada y ajustada por Andrés Almanza, M.Sc. en Seguridad de la Información, de la Universidad Oberta de Cataluña, en España (*cuadro 5.1*).

Propósito	Tipo	Nivel de esfuerzo requerido
Destrucción	Lógica: borrado seguro de datos	Bajo
	Física: desmagnetizador (degausser)	Alto
Ocultar	Aplicaciones: criptografía, esteganografía, rootkits	Medio
	Sistemas de archivos: unidades de datos, metadata, archivos cifrados	Medio
	Medios de almacenamiento: HPA (Host Protected Area)	Alto
Eliminar la fuente	Memoria física	Medio
	Desactivar sistemas de monitoreo	Medio
Falsificar	Sistema de archivos: metadata	Medio
	Sistemas de logs y auditoría	Medio

Cuadro 5.1

Taxonomía de técnicas antiforenses

Complementando la propuesta efectuada por Harris, Garfinkel (Garfinkel 2007, pp. 78-80) detalla algunas técnicas tradicionalmente utilizadas para materializar los métodos previamente presentados, entre los cuales mencionamos la sobrescritura de datos y metadatos, así como la utilización de técnicas criptográficas y esteganográficas.

La sobrescritura de datos y metadatos está asociada con la modificación física de la información residente en los medios de almacenamiento, y sus sistemas de archivo. Es una manera para dejar inconsistente una posible recuperación de información, o una forma de construir entradas falsas en las tablas de asignación de archivos que generen la aparición de archivos inexistentes.

Como podemos observar en este segmento, las técnicas antiforenses están evolucionando para confrontar los procedimientos y esfuerzos en informática forense, de tal forma que los atacantes tengan a su favor la duda razonable, y la impunidad haga su aparición en los procesos vinculados con informática. En este contexto, se requiere un compromiso decidido de la industria, de la academia, del gobierno y de todos los actores sociales para abrir nuevas posibilidades de colaboración y construcción conjunta frente a esta realidad de la delincuencia informática organizada, no sólo para enfrentar la amenaza planteada, sino para edificar relaciones de cooperación organizada de largo plazo.

5.4 CIBERCRIMEN Y CIBERTERRORISMO: AMENAZAS ESTRATÉGICAS Y TÁCTICAS DE LAS ORGANIZACIONES MODERNAS

5.4.1 Ciberterrorismo

De acuerdo con Denning (2000), el ciberterrorismo es la convergencia entre el terrorismo y el ciberespacio, una conjunción de fuerzas que, utilizando las ventajas y capacidades del terrorismo físico, ahora basado en fallas y vulnerabilidades tecnológicas, logran intimidar o presionar a un estado y sus ciudadanos.

De otra parte, Nelson, Choi, Iacobucci, Mitchell y Gagnon (1999) establecen que el ciberterrorismo está asociado con las vulnerabilidades asociadas con las infraestructuras críticas de una nación: energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, sistemas de suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales, aquellos sistemas que hacen parte de la dinámica de la economía de una nación y el bienestar de los ciudadanos. Si bien las vulnerabilidades no son sinónimo de amenazas, dado que ellas son debilidades que se presentan en un sistema, las amenazas requieren un actor con motivación, recursos y deseos de explotar la misma.

Gordon y Ford (2003) comentan que las acciones ciberterroristas son actividades terroristas llevadas a cabo en el mundo virtual.

De igual forma, Gordon y Ford (2003) comentan que las acciones ciberterroristas son actividades terroristas llevadas a cabo completamente (de manera preferente) en el mundo virtual. En este contexto, los investigadores mencionados establecen un modelo base para comprender el ciberterrorismo, como una extensión del terrorismo, para lo cual establecen siete elementos de análisis, a saber:

- Quién es el perpetrador?: un grupo o un individuo;
- El sitio donde se adelanta la acción;
- La acción misma realizada;
- La herramienta o estrategia utilizada: violencia, secuestro, bomba, etc.;
- El objetivo de la acción: el gobierno, una organización particular;
- La afiliación a la que pertenece el perpetrador y finalmente
  La motivación.

No hay un consenso sobre lo que se debe entender por ciberterrorismo.

Como se puede observar, no hay un consenso sobre lo que se debe entender por ciberterrorismo; sin embargo, la definición sugerida por Pollitt, mencionada en Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E. y Liederbach, J. (2006, p. 23) muestra una forma interesante de comprender el mismo, la cual conjuga los aspectos mencionados por los autores anteriores: "El ciberterrorismo es un ataque premeditado, política o ideológicamente motivado o una amenaza de ataque contra la información, los sistemas de información, programas de computadores y datos que puede llevar una acción violenta contra objetivos civiles".

Cuando entendemos el ciberterror como esa fuerza emergente que reconoce en las vulnerabilidades propias de los sistemas, y en la tendencia convergente de la tecnologías de información, la manera de ocasionar el mayor daño, con el menor esfuerzo y el mayor impacto en

las infraestructuras de misión crítica de una nación, sabemos que está en un margen de acción que escribe una nueva historia de los intrusos, que ahora no conocen límites para demostrar que han aprendido a explotar la ventajas de la tecnología para intimidar y desafiar a los estados en un mundo donde no existen fronteras, y cuyo límite no está en las instituciones, sino en la imaginación del ser humano.

En este sentido, el ciberterrorismo abarca cuatro (4) variables que deben ser parte del análisis de esta nueva amenaza, la cual se confunde con las fallas mismas de los sistemas de información, y deja sin argumentos tanto a los profesionales de la seguridad, como a los analistas de inteligencia.

Las variables propias del ciberterrorismo son:

- Ataques a la infraestructura de tecnologías de información, TI,
- Ataques a la información,
- Utilización de las TI para labores de coordinación de los planes terroristas, y
- La promoción y difusión de sus consignas ideas, así como del entrenamiento de sus grupos de acción (*gráfico 5.5*).

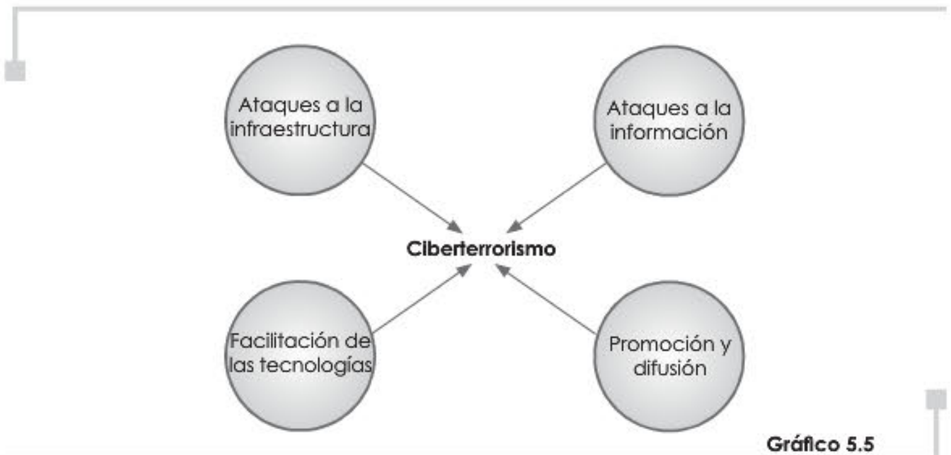


Gráfico 5.5
Variables del ciberterrorismo

Al estudiar como mínimo estas cuatro variables y las relaciones entre ellas, podemos ver comportamientos emergentes que nos permitirán ver cómo las naciones, las organizaciones y los individuos

deben cerrar sus filas para que el terror en línea no se convierta en esa amenaza invisible y predecible que todos advertimos pero no queremos enfrentar (Council of Europe 2007, Rollins y Wilson 2007). Si esta tendencia actual persiste, estaremos allanando el camino para eventos de mayor magnitud, que le permitirán al atacante demostrar que puede atemorizar a un estado, que ha faltado a su deber de protección de sus ciudadanos ahora en un mundo *online*.

5.4.2 Cibercrimen: viejos hábitos del mundo *offline*, nuevas armas en el mundo *online*

Para la UIT (2008), la ciberseguridad consiste en "(…) proteger contra el acceso no autorizado y la manipulación y destrucción de recursos y activos esenciales (…)".

Para la UIT (2008), la ciberseguridad consiste en "(…) proteger contra el acceso no autorizado y la manipulación y destrucción de recursos y activos esenciales (…)", definición que si bien establece un lineamiento concreto para los gobiernos e interesados, limita un entendimiento profundo del concepto de seguridad informática, pues considera a la inseguridad de la información, causante de los riesgos identificados, como la enemiga de la sociedad.

Cuando comprendemos que el estudio de la inseguridad de la información nos permite ver el otro lado de la distinción de la seguridad, podemos alimentar un modelo de estrategias más consistente y real frente a las fallas emergentes de un sistema y no frente a los controles que se diseñan para protegerlo. Es decir, pensando como "el atacante": puedo ver aquello que desde la cotidianidad del uso del sistema no puedo ver.

La realidad de la inseguridad de la información y la materialización de la delincuencia, en medios electrónicos, nos debe llevar a mirar en perspectiva lo que la justicia requiere para enfrentar el desafío de un atacante anónimo, que se mimetiza en la red, que manipula evidencias, que elimina rastros y que conoce en los detalles las herramientas de apoyo y soporte de investigaciones informáticos (Shmallerger y Pittaro 2009).

Los constantes avances tecnológicos y los altos niveles de conocimientos técnicos involucrados en los nuevos desarrollos electrónicos y computacionales (Howard 1997, Raymond Choo, K.

K, Smith, R. y McCusker 2007), establecen un reto para presentar una definición general de lo que puede denominarse un *computer crime* o delito por computador o semejante. En este sentido, existen múltiples interpretaciones y sugerencias que buscan modelar esta naciente y conflictiva área para el derecho y las tecnologías de información (*cuadro 5.2*).

Computer Abuse *Parker, 1976*	• El computador es el objeto, o los datos en el computador son los objetos, del acto. • El computador crea un entorno único o una única forma para los activos • El computador es el instrumento o la herramienta del acto • El computador representa un símbolo utilizado para la intimidación o el engaño.
Computer Crime *Taylor, 2006*	• El computador es el objeto de la conducta • El computador es el instrumento para cometer la conducta • El computador facilita la consumación de la conducta • Conductas asociadas contra la industria informática

Cuadro 5.2

Conceptualizando el cibercrimen

El no contar con una definición concreta sobre el tema desestima los esfuerzos para una adecuada detección, investigación y judicialización de este tipo de conductas en medios electrónicos y computacionales. A pesar de que las estadísticas actuales nos muestran un importante incremento de eventos relacionados con explotación de vulnerabilidades informáticas en diferentes ramos y campos, dejando pérdidas millonarias para las organizaciones y grandes vacíos en la sociedad sobre las acciones que el Estado toma al respecto, no se han experimentado avances significativos ni estrategias, desde el punto de vista jurídico, que articulen los limitados esfuerzos sugeridos desde la perspectiva de la administración de la seguridad de la información.

Para perseguir la criminalidad informática, la dificultad existente radica en varias razones, como el entendimiento de las tecnologías y las vulnerabilidades inherentes por parte de los cuerpos de seguridad del Estado y la administración de justicia, la comprensión y el análisis de la evidencia digital y los rastros electrónicos, la información

Para perseguir la criminalidad informática, la dificultad radica en varias razones, como el entendimiento de las tecnologías y las vulnerabilidades inherentes por parte de los cuerpos de seguridad del Estado.

y su valor en los mercados internacionales y la falta de precisión en el perfil de un delincuente tecnológico, como elementos que exigen de la academia, el gobierno, la industria y las instituciones de la justicia un esfuerzo conjunto para avanzar en las construcción de caminos que confronten a los nuevos y organizados criminales (Knetzger, M. y Muraski 2008).

5.4.3 Retos tecnológicos para los investigadores forenses en informática

Los atacantes establecen un reto para los investigadores forenses en informática, por los alcances y las habilidades técnicas requeridas para alcanzar sus objetivos criminales.

Como hemos venido revisando a lo largo de este capítulo, los atacantes establecen un interesante reto para los investigadores forenses en informática, no por sus acciones en sí mismas, sino por los alcances y las habilidades técnicas requeridas para alcanzar sus objetivos criminales.

En este sentido, el atacante natural ha evolucionado y ha descubierto en las tecnologías de información no sólo un incentivo y motivación para materializar sus acciones, sino también maniobras para evadir las investigaciones, como lo hemos revisado en la sección sobre técnicas antiforenses.

En razón de lo anterior, se requiere revisar y analizar algunos de esos elementos emergentes que pueden ser aprovechados por los criminales informáticos para entorpecer las investigaciones en curso, a través del estudio de nuevas técnicas y estrategias tecnológicas recientes, que requieren mayor investigación formal y análisis científico para comprenderlas en profundidad.

5.4.4 Archivos cifrados

Una de las técnicas que más utilizan los atacantes es cifrar la información residente en el dispositivo de almacenamiento con algoritmos de cifra, utilizando llaves de cifrado generalmente largas (512, 1.024, 2.048 bits).

Una de las técnicas más utilizadas por los atacantes, como parte de sus actividades delictivas, es cifrar la información (Casey y Stellatos 2008) residente en el dispositivo de almacenamiento con algoritmos de cifra conocidos, utilizando llaves de cifrado generalmente largas (512, 1024, 2048 bits), que limiten un ataque de fuerza bruta que intente descifrar lo que se encuentra allí.

Esta estratagema establece una importante limitación para los investigadores forenses en informática, ya que mucha parte de esa información cifrada posiblemente contenga elementos valiosos para la investigación y, al no tener la posibilidad de acceso de manera legible, no podrá ser aportada en el proceso. En muchas ocasiones un caso se desvanece por la falta de herramientas para descifrar información, pues cuando el investigador se enfrenta a este reto debe conocer, entre otras cosas: el algoritmo de cifra: DES, 3DES, RSA, AES, entre otros, el tamaño de la llave de cifra, y si está con mucha suerte la palabra de paso o clave para descifrar.

Hasta la fecha, los archivos cifrados representan un gran reto para la computación forense, pues, de lograr descifrar cualquier tipo de información cifrada, estaríamos poniendo en tela de juicio la formalidad de los algoritmos de cifra utilizados, y abriendo una falla estructural en el tema de privacidad e integridad de la información. De otra parte, de no poder conocer información adicional sobre los archivos cifrados, cerramos la posibilidad de avanzar en las investigaciones y los atacantes tendrán mayores elementos de defensa para exhibir, haciendo valer su derecho natural a no autoincriminarse.

Los archivos cifrados son un gran reto para la computación forense.

5.4.5 Esteganografía en video (*ver* sección Enlaces en el Web)

La *esteganografía* es una técnica a través de la cual, manipulando la estructura interna de un archivo inicial, logramos esconder otro en éste. Nótese que hablamos de esconder y no de cifrar. En este sentido, este artificio es posible gracias a que los archivos tienen segmentos de su estructura que pueden ser recompuestos sin perder muchas de sus características originales.

La *esteganografía* en video consiste en manipular el flujo de video en línea y lograr esconder la información allí, para luego en el receptor interpretar la secuencia embebida en el flujo.

Si bien este engaño tecnológico ha sido ampliamente utilizado en la actualidad y ya existen múltiples herramientas que buscan detectar el uso del mismo, estamos advirtiendo una interesante evolución del tema ahora en flujos de video a través de Internet. La técnica consiste

en manipular el flujo de video en línea y lograr esconder la información allí, para luego en el receptor interpretar la secuencia embebida en el flujo, y extraer la información remitida por este medio.

En este escenario, la detección de esta clase de estrategia se vuelve compleja, porque en el momento de ejecución habría que reconocer el patrón o el engaño esteganográfico para identificar la información allí insertada. Si hablamos de herramientas comerciales para adelantar esta detección, aún se encuentran en laboratorios académicos algunas iniciativas que deberán madurar para avanzar en este nuevo desafío.

5.4.6 Rastros en ambientes virtuales[1]

Si lo anterior es un reto tecnológico exigente, el rápido incremento de las plataformas virtuales, la virtualización de servidores y almacenamiento nos muestra un futuro más demandante de reflexiones y análisis para comprender ahora, en un entorno dominado por la memoria y archivos residentes en disco, lo que significa un rastro en una infraestructura virtualizada.

Los entornos virtualizados son escenarios de alta volatilidad en el manejo de memoria.

Los entornos virtualizados son escenarios de alta volatilidad, en el manejo de memoria, múltiples referencias a archivos en disco que soportan las operaciones en memoria dinámica, redefinición de lo que significa un sistema de archivos y, por tanto, los elementos de seguridad propios del acceso a sus objetos. Si bien la virtualización busca aislar un sistema operativo de otro en el contexto de la ejecución de su entorno en la máquina que lo contiene, es probable que comparta segmentos de memoria en conjunto de otras instancias de otros sistemas operativos en ejecución, lo cual puede hacerlo vulnerable a una falla generalizada de la máquina original que lo contiene.

En este escenario virtual encontrar los rastros de un ataque o incidente de seguridad exige del investigador forense comprender en

[1] Garfinkel y Rosenblum 2005.

detalle el funcionamiento de las máquinas virtuales, su utilización de la memoria y el disco, los archivos que ayudan al manejo de cada entorno y sus relaciones entre sí. Luego de esto, sí establecer qué tipo de rastros podrían haber quedado en las máquinas virtuales, la identificación de los usuarios y las posibles estrategias que ha utilizado el atacante para desvirtuar las trazas identificadas.

Hasta la fecha, los ambientes virtuales son uno de los referentes más exigentes para la computación forense, pues la definición de lo que puede ser un rastro y su materialización, en el contexto real de la máquina que lo contiene, requiere mayor análisis e investigación.

Los ambientes virtuales son uno de los referentes más exigentes para la computación forense.

5.4.7 Información almacenada electrónicamente en memoria volátil

Al igual que el punto anterior, la información que se halle en memoria es insumo fundamental para cualquier investigación. Tal es la importancia de este hecho, que, por lo general, a los investigadores se les recomienda que no apaguen la máquina si la encuentran encendida, dado que la información volátil disponible, particularmente lo residente en memoria, es pieza clave de lo que pudo haber ocurrido (Hewardt y Pravat 2008).

Estudios recientes muestran que es posible capturar lo que hay en memoria de un computador encendido, y que es viable exportar el resultado del mismo a un archivo para su análisis posterior. Sin embargo, por lo general, las herramientas disponibles para ello pertenecen, como es natural, al proveedor del sistema operativo quien es el que sabe cómo se comporta su sistema operativo con el hardware. En este sentido, es necesario adelantar, con los proveedores de tecnologías de información, investigaciones sobre una manera forense válida y consistente de captura de la información en memoria, de tal manera que pueda ser sujeto de revisión vía el test de Daubert, y así fortalecer la idoneidad de la prueba que se presente.

Estudios recientes muestran que es posible capturar lo que hay en memoria de un computador encendido, y que es viable exportar el resultado del mismo a un archivo para su análisis posterior.

Por otro lado, se adelantan esfuerzos en el campo del hardware (Carrier, B. y Grand, J. 2004), para contar con tarjeta de recolección de información volátil en memoria de un equipo ante un incidente, la cual se instala en el computador en una de las ranuras disponibles en modalidad deshabilitada. Una vez ocurre el incidente, se abre la máquina y se activa el dispositivo para que capture lo que se encuentra en memoria, lo almacene y resguarde en la tarjeta, y luego proceder a retirarlo para revisar esa información en el laboratorio. Esta técnica se encuentra disponible en el mercado; sin embargo, sus costos actuales no permiten una difusión masiva de la misma. Se espera que en un futuro cercano se tenga mayor acceso a esta clase de estrategias de seguridad y control de información volátil en una máquina.

5.4.8 Análisis de sistemas en vivo

Cuando el investigador forense se enfrenta al análisis de un sistema en vivo, sabe que la modificación de variables o de archivos en el sistema revisado siempre será el riesgo a mitigar.

Finalmente y no menos importante, cuando el investigador forense se enfrenta al análisis de un sistema en vivo (Carrier 2006, Ieong y Leung 2007), sabe que la modificación de variables o de archivos en el sistema revisado siempre será el riesgo a mitigar. En este contexto, las técnicas que se utilicen para este trabajo deberán considerar procedimientos formales y probados que limiten la modificación involuntaria de la escena del crimen.

Las herramientas actuales disponibles tratan de evitar cualquier tipo de modificación o de contacto con los elementos del sistema analizado en vivo; sin embargo, la probabilidad de modificación de elementos en memoria o incluso de archivos abiertos en disco es alta, lo que exige del investigador conocer con claridad los posibles cambios que se pueden dar en la máquina analizada, para documentarlo y mantener la fidelidad de sus análisis.

En este sentido, es necesario que tanto los proveedores como las experiencia de los investigadores forenses en informática se unan para conocer de primera mano las especificaciones de las herramientas y sus alcances tecnológicos, así como las vivencias de los casos de los investigadores, donde se ven avocados a probar que no hubo modificaciones importantes en la evidencia o dispositivo tecnológico analizado.

El análisis de sistemas en vivo es, por tanto, un reto tecnológico crítico para los investigadores forenses actuales, pues saben que un atacante informado y tan conocedor como él, lo pondrá a prueba para poner en duda sus procedimientos y el uso de sus herramientas, para favorecerse de la incertidumbre, y así controvertir los resultados de la aplicación del procedimiento de identificación, recolección, control, análisis y presentación de información almacenada electrónicamente.

El análisis de sistemas en vivo es un reto tecnológico crítico para los investigadores forenses.

Resumen

Como disciplina naciente, la computación forense establece un escenario de análisis y retos emergentes, que sugieren a todos aquellos interesados en ella una ruta de aprendizaje, desaprendizaje y renovación permanente, que hace de los profesionales que se dedican a ella investigadores y científicos en formación constante, para descubrir y avanzar conforme la criminalidad lo hace.

Negar la existencia del crimen organizado (Branigan 2005, Walden 2007), o ignorarlo es condenar el desarrollo de la informática forense, pues en la medida en que la inseguridad de la información se materializa y avanza, podemos ver nuevas posibilidades y actividades para conocer con mayor detalle la tecnología y sus posibilidades. Se podría decir que estamos ante una paradoja en computación forense: "Mientras más conocemos el lado oscuro de la tecnología, más nos acercamos a los mecanismos y estrategias que nos permitan reconocerla y mejorarla".

Los ataques frecuentes a los sistemas informáticos, la inteligencia notable de los intrusos y su habilidad para invalidar sus rastros son algunas de la motivaciones para reconocer, en las ciencias forenses aplicadas a la informática y la telecomunicaciones, oportunidades de crecimiento y desarrollo profesional, tecnológico y jurídico (Kovacich 2000, Casey 2001).

En lo profesional, se establece una nueva caracterización de los investigadores forenses en informática, el desafío de su formación y

la aceptación de los mismos como los nuevos garantes de la verdad procesal (Riofrío 2004). Los investigadores forenses en informática, peritos informáticos o forenses digitales, son la nueva raza de profesionales que, reconociendo su formación multidisciplinaria e interdisciplinaria, formalizan los procedimientos forenses en medios tecnológicos, no como especialistas en temas técnicos, sino como profesionales forenses integrales que conocen los impactos jurídicos, las implicaciones procesales de la evidencia digital y los detalles tecnológicos que los soportan.

En lo tecnológico, la computación forense debe estar atenta a los cambios y avances de la tecnología para conocerla, analizarla y detallarla (Sammes y Jenkinson 2007), porque sabe que tarde o temprano tendrá que enfrentarse al reto de investigarla, cuando un evento o un hecho punible se materialice en ella.

En lo jurídico, es una oportunidad para descubrir y analizar las connotaciones propias de los derechos de las personas, los lineamientos procesales y probatorios que hacen real una evidencia en un proceso, las características de los sistemas penales y sus implicaciones, en pocas palabras la estrategia perfecta para fortalecer su papel como fuente de pruebas y credibilidad en los casos y las investigaciones con componentes tecnológicos.

Si bien en este capítulo se proponen algunos de los retos más sobresalientes y propios de los procesos en computación forense, existen muchos otros que por limitaciones de espacio y tiempo no se van a mencionar. Lo importante es reconocer que tenemos un amplio espectro de conocimiento para cubrir y que la lucha contra el lado oscuro continúa, para ser consecuentes y formales con lo que dice la sabiduría popular: "El crimen nunca duerme", y poder responder "Nosotros tampoco".

Preguntas y ejercicios

Esta sección busca reforzar los elementos conceptuales presentados en este capítulo; para eso le sugerimos al lector revisar sus reflexiones y anotaciones para plantear respuestas a los interrogantes propuestos en esta sección.

1. ¿Cuáles serían los elementos fundamentales en la formación de especialistas en informática forense?
2. ¿Qué es lo que hace que una herramienta que se utilice en computación forense sea confiable?
3. ¿Qué son las técnicas antiforenses?
4. Mencione y analice por lo menos tres (3) técnicas antiforenses y sus impactos en las investigaciones
5. A la fecha, ¿cómo ha evolucionado el perfil del criminal informático?
6. ¿Qué es el ciberterrorismo? ¿Qué estrategias sugiere para enfrentarlo?
7. ¿Cómo podría definir el cibercrimen?

Apéndice

Para profundizar

Recuperación de información: NTFS vs. FAT

Daniel Castro, Camilo Cuesta, Leonardo Rodríguez, Sonia Vivas

El objetivo de este documento es explicarle al lector las posibilidades de recuperar información que pudo ser considerada perdida en los sistemas de archivos NTFS y FAT.

La información confidencial es un bien invaluable, y como tal debe ser celosamente protegido. Con esto en mente y teniendo en cuenta las posibilidades que se presentan actualmente, borrar un archivo confidencial puede no ser seguro, de modo que esta información puede estar vagando libremente y puede ser recuperada por una persona con acceso a la máquina. A pesar de que existen muchas técnicas de borrado seguro, aún es un procedimiento poco implementado, y existen herramientas que recuperan parte de esta información, si el borrado no es suficiente. Los sistemas de archivos FAT y NTFS son de uso bastante común. Sin embargo, la forma como funcionan no es conocida por los usuarios comunes, y por ello se tiende a generar ideas erróneas sobre las posibilidades de estos sistemas. Una de las ideas más comunes, en cuanto a la información, es que una vez borrada de la papelera de reciclaje esta información es irrecuperable. No obstante, esto no es cierto, y la información puede ser fácilmente recuperada. Con el conocimiento suficiente, es posible ser más cuidadoso con la información, y entender cómo recuperarla en caso de que sea necesario.

¿QUÉ ES UN MEDIO MAGNÉTICO?

El término "medio magnético" se usa para describir cualquier formato en el que la información sea guardada y recolectada en la forma de una señal magnética. Las cintas magnéticas (casetes de audio, de video y de computador), los discos duros y los disquetes) son formas comunes de medios magnéticos (Smith, Jan. (Agosto 27 de 2003)).

Diversos tipos de soportes magnéticos han sido usados con el correr de los años. En los primeros grabadores se usó alambre ferroso (wire recorder); sin embargo, en los equipos modernos se usa una delgada capa de material ferromagnético que es soportada por un sustrato no magnético. La capa magnética puede estar formada de partículas magnéticas en una matriz polimérica (Introducción a VCR. (Marzo 20 de 2004)).

Estos soportes magnéticos suelen diferenciarse para medios duros y medios blandos. Los medios duros requieren campos aplicados grandes para lograr el magnetismo permanente y, una vez magnetizados, otros campos

intensos son requeridos para revertir la magnetización y borrar el material. Estos medios tienen gran aplicación en computadoras y almacenamiento de datos. Los medios blandos requieren relativamente bajos campos para lograr la magnetización, y son apropiados para aplicaciones de audio (Introducción a VCR. (Marzo 20 de 2004)).

Los disquetes de 3½ y 5¼ están hechos de un plástico delgado y maleable (de allí el nombre *floppy*), con un recubrimiento de óxido, que provee la cualidad magnética al disco. Los discos Zip también son medios magnéticos (Smith, Jan. (Agosto 27 de 2003)).

Los discos duros consisten en uno o más platos de metal guardados en una caja sellada. El metal es magnético, y la unidad del disco duro utiliza este magnetismo para almacenar y eliminar datos (Smith, Jan. (Agosto 27 de 2003)).

El deterioro de los medios magnéticos puede producirse de diferentes formas; por ejemplo, las partículas que conservan la información cifrada en la capa magnética pueden llegar a ser inestables, conduciendo a una pérdida gradual de calidad de la señal y eventual pérdida de la información (Smith, Jan. (Agosto 27 de 2003)).

Información sobre el manejo correcto de medios magnéticos puede encontrarse en (Smith, Jan. (Agosto 27 de 2003) y Roosa, Mark. (s.f.)).

¿CÓMO SE GUARDA LA INFORMACIÓN?

Los sistemas de archivos tienen un 'índice'; por ejemplo, el caso de la tabla de asignación de archivos, lugar en donde se guarda información sobre el archivo (más adelante se explica en detalle cómo funcionan los sistemas de archivos; sin embargo, es importante entender cómo se guardan los archivos en el disco). Parte de esta información consiste en un apuntador al cluster donde se encuentra guardado el archivo, si éste es muy grande puede estar dividido en varias partes del disco, por lo que cada parte tendrá a su vez apuntadores al siguiente cluster. La información es magnéticamente grabada en el disco, codificada por diferentes métodos, según el tipo de unidad (Disk Geometry. (s.f.)). La geometría de los discos es un tema interesante y denso, pero no es el centro de esta investigación. Al lector se le recomienda estudiar el tema, para una comprensión más precisa sobre la forma como se guarda la información físicamente, y la ilusión que se genera para el usuario final (cuadro A5.1).

1. SISTEMAS DE ARCHIVOS

En esta sección del paper se pretende dar al lector una visión global de los sistemas de archivos FAT y NTFS, de modo que sea posible compararlos y diferenciarlos en cuanto a recuperación de información, que es el tema principal de este documento. El *cuadro A5.1* es una lista comparativa de estos sistemas de archivos (NTFS.com. (Marzo 21 de 2004)).

Criteria	NTFS5	NTFS	FAT32	FAT16
Operating System	Windows 2000 Windows XP	Windows NT Windows 2000 Windows XP	Windows 98 Windows ME Windows 2000 Windows XP	DOS All versions of Microsoft Windows
Limitations				
Max Volume Size	2TB	2TB	2TB	2GB
Max Files on Volume	Nearly Unlimited	Nearly Unlimited	Nearly Unlimited	~65000
Max File Size	Limit Only by Volume Size	Limit Only by Volume Size	4GB	2GB
Max Clusters Number	Nearly Unlimited	Nearly Unlimited	268435456	65535
Max File Name Length	Up to 255	Up to 255	Up to 255	Standard - 8.3 Extended - up to 255
File System Features				
Unicode File Names	Unicode Character Set	Unicode Character Set	System Character Set	System Character Set
System Records Mirror	MFT Mirror File	MFT Mirror File	Second Copy of FAT	Second Copy of FAT
Boot Sector Location	First and Last Sectors	First and Last Sectors	First Sector	First Sector
File Attributes	Standard and Custom	Standard and Custom	Standard Set	Standard Set
Alternate Streams	Yes	Yes	No	No
Compression	Yes	Yes	No	No
Encryption	Yes	No	No	No
Object Permissions	Yes	Yes	No	No
Disk Quotas	Yes	No	No	No
Sparse Files	Yes	No	No	No
Reparse Points	Yes	No	No	No
Volume Mount Points	Yes	No	No	No
Overall Performance				
Built-In Security	Yes	Yes	No	No
Recoverability	Yes	Yes	No	No
Performance	Low on small volumes High on Large	Low on small volumes High on Large	High on small volumes Low on large	Highest on small volumes Low on large
Disk Space Economy	Max	Max	Average	Minimal on large volumes
Fault Tolerance	Max	Max	Minimal	Average

Cuadro A5.1.
NTFS vs FAT

1.1 NTFS

En la década de los años 90, Microsoft quiso desarrollar un sistema operativo que tuviera un alto desempeño, una alta confiabilidad, que fuera seguro, y de buena calidad. Su primer intento fue MS-DOS, y Windows 3.x. Ninguno de estos dos intentos lograba competir con los mejores sistemas operativos de la época, entre los cuales encontramos a Unix. Uno de sus principales limitantes se basó en el sistema de archivos que utilizaron, el cual era FAT, del que también hablamos en este documento. Más adelante, Microsoft quiso desarrollar un nuevo sistema operativo, mucho más confiable, y con nuevas características. Para ello, tenían que cambiar, entre algunas otras cosas, su sistema de archivos. El sistema de archivos que desarrollaron se llamó New Technology File System, o NTFS (Kozierok, Charles M. (Abril 3 de 2004)).

Es un sistema de archivos más avanzado que FAT; sobre él se pueden montar servicios que administra el sistema operativo; algunos de estos servicios son: Puntos de Repase, Estructura Nativa de Almacenamiento, Cuotas en Disco, Cadenas de Objetos Identificables, Diario de Operaciones, Número Único de Secuencia, y cifrado (Kozierok, Charles M. (Abril 3 de 2004)). De éstos sólo el diario de operaciones y el número único de secuencia son de nuestro interés, ya que aquí es donde se centra el gran potencial de NTFS.

NFTS no es, como su nombre indica, completamente nuevo, ya que está basado en otro sistema de archivos PSF (Kozierok, Charles M. (Abril 3 de 2004)), en el cual estuvo trabajando Microsoft algún tiempo, en asociación con la IBM, para crear el sistema operativo OS/2 (Kozierok, Charles M. (Abril 3 de 2004)). NTFS fue diseñado para satisfacer un número especifico de objetivos, entre los cuales encontramos: *Confiabilidad, Seguridad y Control de Acceso, Romper la Barrera Tamaño, Eficiencia de Almacenamiento, Nombres de Archivos Largos, Trabajo en Red, entre otros* (Kozierok, Charles M. (Abril 3 de 2004)). El desarrollo de NFTS no se detuvo en la versión utilizada inicialmente por Windows NT, sino que ha sido mejorada a medida que pasa el tiempo.

Microsoft le ha realizado cambios a NTFS, por diferentes razones, entre las cuales se encuentran la corrección a problemas del sistema de archivos, para dar soporte a nuevo hardware, y para habilitar nuevas características de los sistemas operativos (Kozierok, Charles M. (Abril 3 de 2004)). De NTFS existen 2 versiones: NTFS 1.1 o como también es conocida NTFS 4.0 (Kozierok, Charles M. (Abril 3 de 2004)) y, por último, NTFS 5.0 (Kozierok, Charles M. (Abril 3 de 2004)). El cambio más grande que ha tenido NTFS ocurrió con la salida al mercado de Windows 2000, el cual tiene unas características nuevas, las cuales debían ser soportadas por el sistema de archivos (Kozierok, Charles M. (Abril 3 de 2004)).

El diario de operaciones es un conjunto de caracteres que crean un log persistente de las operaciones que ha realizado en volumen; éstas son: adición, modificación, borrado, por cada volumen NTFS (Microsoft Windows 2000 server. (2000)).

El número único de secuencia provee un log persistente de los cambios hechos a los archivos de un volumen. Así, cuando un archivo es modificado por un controlador de dominio, éste llena una tabla con un USN que se le asigna. Este número aumenta secuencialmente por cada cambio realizado. Esto se explica con más detalle más adelante.

1.1.1 *Estructura de NTFS*

NTFS proporciona una combinación de desempeño, seguridad y confiabilidad que no se encuentra presente en FAT. NTFS tiene una arquitectura especial que, además de sus habilidades avanzadas, anteriormente mencionadas, utiliza un esquema conceptual simple, el cual facilita la introducción de nuevas características, realizando un mínimo de cambios. Esta última característica fue utilizada, en la versión 5.0 (Kozierok, Charles M. (Abril 3 de 2004)).

Virtualmente, todas las estructuras en NTFS son registros, incluyendo las estructuras que se utilizan para manejar la partición y mantener las estadísticas y el control de información acerca de ella misma. La información de control es almacenada en un grupo de archivos especiales que se crean, cuando la partición NFTS es creada. Estos archivos son llamados Metadata Files, e incluyen la lista de archivos presentes en la partición, y la ubicación de los clusters (Kozierok, Charles M. (Abril 3 de 2004).). La única parte de la arquitectura de NTFS, que no puede considerarse un archivo (cuadro A5.2), es la zona de Boot Sector, la cual se encarga de operaciones básicas, como cargar el sistema operativo (28 Kozierok, Charles M. (Abril 3 de 2004)).

Boot Sector	System Files "Metadata"	Master File Table	File Area

Cuadro A5.2

(Kozierok, Charles M. (Abril 3 de 2004))

El diseño de NTFS es sencillo y con mucho potencial. Como dijimos antes, todo dentro de una partición de NTFS es un récord, y todo dentro de un archivo es una colección de atributos, incluso la información (datos), del archivo, es sólo uno de muchos atributos (Kozierok, Charles M. (Abril 3 de

2004)). Este sistema es muy parecido a una base de datos, cada archivo es un elemento de una tabla, al cual se le pueden agregar más atributos en un futuro si es necesario (Kozierok, Charles M. (Abril 3 de 2004)).

Internamente, NTFS almacena todos los archivos, incluyendo los archivos de metadata, usando un sistema de clusters. NTFS, al igual que FAT, no manejan sectores individuales de 512 bytes; en lugar de esto estos sectores son agrupados en bloques llamados clusters, o también *allocation units*. La principal razón para utilizar *clusters* es el desempeño, ya que, de lo contrario, se requeriría una gran cantidad de recursos para mantener el rastro de un archivo, y adicionalmente la fragmentación del disco se convertiría en un problema mucho más serio. NTFS utiliza un tamaño por defecto del cluster, dependiendo del tamaño de la partición. El *cuadro A5.3* muestra el tamaño por defecto para los clusters, dependiendo del tamaño de la partición (Kozierok, Charles M. (Abril 3 de 2004)).

NTFS utiliza dos diferentes sistemas de asignación para el tamaño de los clusters, y éste depende de la versión del sistema operativo. Si es una versión de Windows NT 3.5 o anterior, el sistema de archivos utiliza el cuadro A5.3 completo. Si se está utilizando una versión de Windows NT 3.51 o posterior, el sistema de archivos utiliza únicamente las primeras cuatro filas del cuadro; por lo tanto, el tamaño máximo del cluster es de 4kB, para todas las particiones por encima de 2.0 GB (Kozierok, Charles M. (Abril 3 de 2004)).

La razón por la cual existen estos dos sistemas de selección del tamaño del cluster es la capacidad de trabajar con archivos basados en compresión en NTFS. La compresión no está soportada para sistemas de archivos con un tamaño de cluster de más de 4 kB. La versión de Windows 3.5 y las anteriores no soportaban los archivos basados en compresión; por eso utilizan el *cuadro A5.3* en su totalidad (Kozierok, Charles M. (Abril 3 de 2004)). La compresión de los archivos utiliza una de las características de la mayoría de los datos, la cual es la presencia de patrones repetitivos. Utilizando programas que implementan algoritmos de compresión y descompresión, se pueden almacenar datos, ocupando menos espacio, que el que normalmente ocuparían. Una de las características más útiles que tiene NTFS es la posibilidad de tener archivos basados en compresión. Esta característica es manejada directamente por el sistema operativo, el cual se encarga de comprimir los datos, en el momento de la escritura, y la descompresión es automática, en el momento en que una aplicación necesita leer el archivo (Kozierok, Charles M. (Abril 3 de 2004)).

En ese cuadro se muestran los tamaños por defecto que utiliza NTFS para los clusters. Este tamaño por defecto puede ser modificado al momento de realizar el formato, al utilizar el parámetro "/A (tamaño)", en el comando FORMAT. El tamaño de los clusters tiene un efecto importante

Tamaño de partición (GB)	Número de sectores por cluster	Tamaño del cluster (kB)
< = 0,5	1	0,5
> 0,5 a 1,0	2	1
> 1,0 a 2,0	4	2
> 2,0 a 4,0	8	4
> 4,0 a 8,0	16	8
> 8,0 a 16,0	32	16
> 16,0 a 32,0	64	32
> 32,0	128	64

Cuadro A5.3

(Kozierok, Charles M. (Abril 3 de 2004))

en el desempeño del sistema, ya que al aumentar el tamaño del cluster, además de poder perder la capacidad de realizar compresión de archivos de NTFS, el tamaño del Slack también aumenta. El Slack es la porción de un cluster que es desperdiciado por un archivo, que no ocupa en su totalidad el cluster (*cuadro A5.4*) (Kozierok, Charles M. (Abril 3 de 2004).

En ese cuadro se muestran los tamaños por defecto que utiliza NTFS para los clusters. Este tamaño por defecto puede ser modificado al momento de realizar el formato, al utilizar el parámetro "/A [(tamaño])", en el comando FORMAT. El tamaño de los clusters tiene un efecto importante en el desempeño del sistema, ya que al aumentar el tamaño del cluster, además de poder perder la capacidad de realizar compresión de archivos de NTFS, el tamaño del *Slack* también aumenta. El *Slack* es la porción de un cluster que es desperdiciado por un archivo, que no ocupa en su totalidad, todo el cluster (*cuadro A5.4*) (Kozierok, Charles M. (Abril 3 de 2004)).

1.1.2 *Sector de arranque*

Cuando se crea una partición NTFS, el primer bloque de información que es creado es el *Boot Sector* o Sector de Arranque. Esta estructura es fundamental para NTFS, y se encarga de manejar información que no se almacena en la *Master File Table* de la cual hablamos más adelante. Este sector está compuesto por 16 sectores de 512 bytes, para un total 8 kB. El Boot Sector empieza en el primer sector de la partición, y está conformado por dos estructuras, las cuales son el bloque de parámetros de la BIOS, y el código de arranque, o *bootstrap*. De éstos hablamos a continuación.

Offset	Length	HEX	DEC	Descripción
0Bh	Word	0200h	512	Tamaño de sector (bytes)
0Dh	Byte	Ver cuadro 20	Ver cuadro 20	Número de sectores por cluster
0Eh	Word	0000h	0	Sectores reservados
10h	Byte	00h for NTFS	0 for NTFS	Número de partición FAT
11h	2 bytes	0000h for NTFS	0 for NTFS	Max Root Directory Entries FAT12/16
13h	2 bytes	0000h not used by NTFS	0 for FAT32	Small Sector Count for FAT 12/16
15h	Byte	F8h Hard Disk	Hard Disk	Media Descriptor ID. Win 2k/XP don't use it
16h	2 bytes	0000h for NTFS	0 for NTFS	Sectores por FAT, lo usa FAT 12/16
18h	Word	003Fh Depende del disco	63	Sectors per track
1Ah	Word	Depende del disco	X	Número de cabezas
1Ch	Double Word	Depende de # de partición	0 si no hay partición	Número de sectores ocultos (Cyl=0, Head=0) Los que preceden esta partición NTFS
20h	4 bytes	0h Not used by NTFS	0	Número de sectores en un volumen de FAT32
24h	4 bytes	80008000	El primer byte es el número del drive	El SO que usa NTFS siempre coloca el valor de 80008000
28h	Long Word 8 bytes	Depende de la partición	X, X, X	Sectores totales en el volumen
30h	Long Word 8 bytes	Depende de la ubicación del MFT	X	Número del cluster donde empieza el $MFT en esta partición
38h	Long Word 8 bytes	Depende de dónde está la copia del MFT	X	Número del cluster donde empieza la copia de $MFT en esta partición ($MFTMirror)
40h	Signed Double Word	Varía	Varía	Clusters o bytes por MFT Récord Segment
44h	Double Word	Varía	Varía	Clusters por Index Block o récord
48h	Long Word 8 bytes	Varía	Varía	NTFS Volume Serial Number
50h	Double Word	00000000 Parece que no se usa	0	Checksum

Cuadro A5.4

(Kozierok, Charles M. (Abril 3 de 2004); NTFS.com. (Abril 3 de 2004) y Sedory, Daniel B. (Abril 3 de 2004))

El bloque de parámetros de la BIOS contiene información fundamental de la partición. Este bloque identifica la partición como una NTFS, y contiene información, como el *volume label*, y su tamaño; también se encuentra información adicional sobre la partición, como la ubicación de los archivos de metadata. El código de boot es un bloque de instrucciones de programa, que le indican al sistema cómo hacer para cargar el sistema operativo. Las instrucciones de programa son específicas para el tipo de sistema operativo. Este código normalmente carga el N.T.L.D.R. (bootstrap); una vez cargado, se le transfiere el control para que éste cargue el resto del sistema operativo. La estructura de NTFS Boot Sector se muestra en el cuadro A5.5.

En el cuadro A5.5 se ve la configuración general del primer sector de NTFS Boot Sector. Es importante especificar que el *bootstrap* code, para un volumen NTFS, es más grande de 426 bytes, como está especificado en el cuadro anterior. Cuando se da formato a un disco con NTFS, los primeros 16 sectores de la partición son asignados para el Partition Boot Sector, y para el Bootstrap Code (Kozierok, Charles M. (Abril 3 de 2004); NTFS.com. (Abril 3 de 2004); Lynch, Michael. (Abril 3 de 2004); Mikhailov, Dmitrey. (Abril 3 de 2004); Sedory, Daniel B. (Abril 3 de 2004); Active @ Data Recovery Software. (Abril 3 de 2004) y Russon, Richard. (Abril 3 de 2004)).

Byte Offset	Longitud del campo	Nombre del campo
0x00	3 bytes	Jump Instruction
0x03	8 bytes	OEM ID
0x0B	25 bytes	Bios Parameter Block
0x24	48 bytes	Extended BPB
0x54	426 bytes	Bootstrap Code
0x01FE	2 bytes	End of Sector Marker

Cuadro A5.5

(Kozierok, Charles M. (Abril 3 de 2004))

Los primeros 3 bytes son llamados *Jump Instruction*, pero en realidad únicamente los 2 primeros bytes, 0xEB, 0x52, se usan para formar la instrucción en assembler de JMP (Jump). El tercer byte 0x90, en lenguaje de máquina, es un NOP, no operation. Los siguientes 8 bytes son el nombre del sistema de archivos, o OEM ID; para NTFS, estos bytes tienen el siguiente valor "4E 54 46 53 20 20 20 20", que corresponde a "NTFS"; esto es, el nombre del sistema de archivos, seguido de cuatro espacios en blanco. Los siguientes 73 bytes corresponden al BPB y al extended BPB (Bios Parameter Block). Para un

mejor entendimiento de este bloque, el *cuadro A5.6* especifica cada uno de los campos (*ver* referencias (Kozierok, Charles M. (Abril 3 de 2004); NTFS.com. (Abril 3 de 2004); Lynch, Michael. (Abril 3 de 2004); Mikhailov, Dmitrey. (Abril 3 de 2004); Sedory, Daniel B. (Abril 3 de 2004); Active @ Data Recovery Software. (Abril 3 de 2004); Russon, Richard. (Abril 3 de 2004)).

Una vez terminado el bloque de BPB, y el Extended BPB, comienza la estructura llamada bootstrap code. Normalmente la bootstrap code ocupa 8 sectores. Los restantes 8 sectores del Boot Sector están totalmente llenos con ceros. En el primer sector normalmente se encuentra código en lenguaje de máquina hasta un offset de 0x182, desde el inicio del sector (para mayor información sobre este segmento, consultar las referencias (Sedory, Daniel B. (Abril 3 de 2004)); éste tiene la traducción a código en assembler, y comentarios sobre su funcionamiento. Comúnmente, los últimos 125 bytes del primer sector del Boot Sector contienen mensajes de error; también tienen el número de bytes de offset de cada uno de los mensajes, y el *signature ID* o *End of Sector Marker*. Normalmente, los mensajes de error empiezan a un offset del inicio del sector de 0x183. Todos los mensajes de error empiezan con los bytes 0x0D, y 0x0A. El primero es un *Carriage Return* y el segundo en un *Line Feed*. Y todos terminan con el byte 0x00, que usualmente es conocido por muchos lenguajes de programación como el terminador de una cadena de caracteres, como el '\0' en el lenguaje C. El número de bytes de offset de los mensajes, empieza siempre a un offset del inicio del primer sector de 0x1F8, y está compuesto normalmente por cuatro bytes; esto claro, si hay cuatro mensajes de error. La diferencia entre los valores de cada uno de estos bytes nos da el número de bytes que hay entre los mensajes correspondientes. Finalmente, el *Signature ID* siempre debe tener el valor de 0x55AA, hay que tener en cuenta que en la arquitectura Intel x86 siempre se almacena primero la parte baja de la palabra, por lo que en realidad en el disco duro queda almacenada es la siguiente secuencia de bytes "AA 55" (Sedory, Daniel B. (Abril 3 de 2004)).

Los seis sectores siguientes, que están después del Boot Record (Primer Sector), contienen el código del bootstrap o código de arranque, que hace interfaz con el archivo NTDLR, si este existe, para iniciar el SO en la partición. El segundo sector siempre tiene en sus primeros 16 bytes lo siguiente: "05 00 4E 00 54 00 4C 00 44 00 52 00 04 00 24". Entre el tercero y décimoctavo bytes, se puede leer N.T.L.D.R. El resto del sector es código de máquina. Del tercero al sexto sectores, solamente hay código de máquina. Recordemos que el código del bootstrap es dependiente del sistema operativo, ya que cada sistema necesita realizar rutinas diferentes para cargar los distintos componentes necesarios, porque todos los SO tienen una arquitectura relativamente diferente. El séptimo sector tiene sus últimos 300 bytes en cero, al igual que los 9 sectores restantes (Sedory, Daniel B. (Abril 3 de 2004)). NTFS

hace una copia de seguridad del Boot Sector, y su ubicación depende del sistema operativo. Windows NT 3.51 y las versiones anteriores almacenan esta copia en el centro lógico del volumen, mientras que las versiones posteriores almacenan esta copia al final del volumen (Lynch, Michael. (Abril 3 de 2004); Sedory, Daniel B. (Abril 3 de 2004) y NTFS.com. (Abril 3 de 2004)). Exactamente después de que terminan los 16 sectores correspondientes al Boot Sector, empieza otra importante estructura llamada *Master File Table*.

1.1.3 *Tabla Maestra y Metadata*

La Master File Table es, en esencia, una tabla de una base de datos relacional, la cual contiene varios atributos para cada uno de los archivos que existen dentro de la partición. Como habíamos dicho, todo dentro del sistema de archivos NTFS es considerado un récord, con sus excepciones, el cual está compuesto por varios atributos, entre los cuales los datos son solamente uno de los muchos atributos de ese registro (Lynch, Michael. (Abril 3 de 2004); Mikhailov, Dmitrey. (Abril 3 de 2004); NTFS.com. (Abril 3 de 2004); Kozierok, Charles M. (Abril 3 de 2004)).

Cuando la partición es creada, el programa que da el formato a la partición crea un grupo de archivos que contienen la metadata que se usa para implementar la estructura del sistema de archivos. El sistema de archivos NTFS reserva los primeros 16 récords de la MFT (para la información relacionada con esos archivos de metadata (*ver* Lynch, Michael. (Abril 3 de 2004); NTFS.com. (Abril 3 de 2004); Kozierok, Charles M. (Abril 3 de 2004)).

El primer récord tiene información que describe el funcionamiento la MFT, y una lista con todo el contenido del volumen NTFS; el segundo registro a metadata es una copia imagen del primer registro. Si el primer registro se corrompe, es utilizado el segundo registro para restaurar al primero.

El tercer registro de matadata es un registro de log, que almacena todas las transacciones de los archivos, y es muy útil para restauración de archivos y del sistema. Siempre que el sistema se ha corrompido, este log es usado para la restauración. Este registro tiene un tamaño máximo de 4 MB.

Los siguientes 8 registros almacenan información sobre el sistema (NTFS.com. (Abril 3 de 2004); (Kozierok, Charles M. (Abril 3 de 2004)). Estos registros son el *Descriptor del Volumen*, el cual tiene información sobre el volumen, como el nombre, y la fecha de creación, entre otros. El registro de la *Tabla de Definición de Atributos*, el cual contiene el nombre y la descripción de los atributos usados en la partición NTFS. También se encuentra el registro del *Root Directory/Folder*, el cual es un apuntador al directorio o carpeta raíz de la partición. Otro registro muy importante es el *Cluster Allocation Bitmap*, el cual contiene un mapa lógico de los clusters de la partición, mostrando cuáles están ocupados y cuáles están libres. De estos registros, el más

importante para esconder información es el décimo registro llamado *Bad Cluster File*, el cual tiene la información sobre todos los clusters defectuosos dentro del volumen. Otro registro llamado el *Volume Boot Code*, el cual tiene una copia del código de arranque de la partición. También se halla el registro llamado Quota Table, el cual contiene información de la cuota, si ésta es usada en la partición. Por último, se encuentra el registro llamado *Upper Case Table*, el cual contiene la información para convertir los nombres de los archivos al sistema de nombres de archivos *Unicode*. Los restantes 5 registros de metadata están reservados para un uso futuro, pero es posible utilizar estos 5 registros para ocultar información, aunque NTFS no lo utiliza.

NTFS usa los registros de MFT para definir los archivos a los cuales corresponden. Toda la información de un archivo, ya sea fechas, horas, permisos y contenido, se guardan en la MFT o en un lugar externo pero descrito por la MFT.

Si un archivo es pequeño, típicamente 1,5 kB o menos, puede ser almacenado en su correspondiente registro dentro del MFT. Si un archivo es muy grande o está altamente fragmentado, es necesario que la MFT contenga más de un registro del archivo; en este caso, el primer registro, el registro base, contiene la ubicación de los otros registros. Si un registro de una carpeta o un archivo es muy grande para ser almacenada dentro del MFT, son organizados en árboles –B, donde el registro, dentro de la MFT, guarda apuntadores a clusters fuera del MFT. La arquitectura anterior se encuentra expresada en el *gráfico A5.1* (NTFS.com. (Abril 3 de 2004); Kozierok, Charles M. (Abril 3 de 2004)).

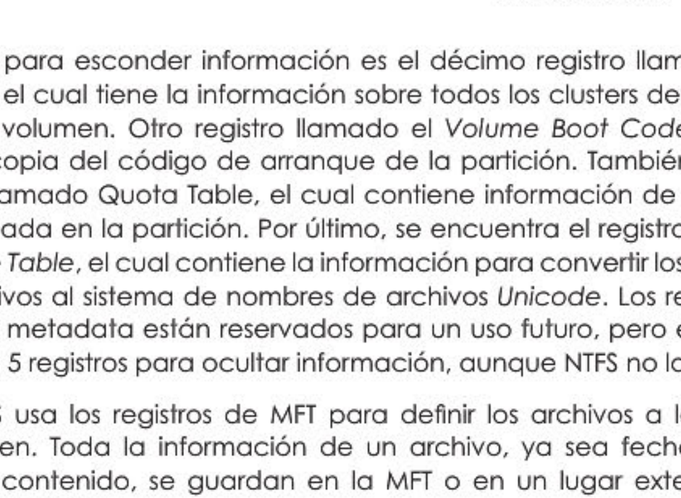


Gráfico A5.1

MFT

1.1.4 *Atributos de archivos*

Todo sector diseccionado por NTFS, en una partición, corresponde a archivos. Para NTFS, un archivo o un directorio son un conjunto de atributos. Los elementos, como nombre, permisos y demás, son atributos (NTFS.com. (Abril 3 de 2004) y Kozierok, Charles M. (Abril 3 de 2004)).

Un código identifica un atributo; cuando un atributo está en la MFT se llama atributo residente; el nombre y la estampilla de tiempo siempre son residentes. Si el conjunto de atributos es muy grande, algunos de éstos son no residentes; entonces NTFS direcciona estos atributos a un espacio reservado en un grupo de clusters en algún lugar del volumen. Y se crea una lista de atributos que describen los registros de los atributos (NTFS.com. (Abril 3 de 2004) y Kozierok, Charles M. (Abril 3 de 2004)).

Existen diferentes tipos de atributo. Están los de información estándar, como las estampillas de tiempo. Otro tipo es la lista de atributos externos al MFT, el cual tiene la ubicación de todos los clusters con los atributos no residentes. Los permisos son otro atributo que le brinda seguridad a este sistema de archivos; se puede especificar una lista de acceso al archivo, propietarios. Los datos son otro de los atributos. Si éstos son lo suficientemente pequeños, pueden ser almacenados dentro del MFT; de lo contrario, lo que se almacena es un grupo de apuntadores, a los clusters externos al MFT que contienen los datos.

Uno de los atributos más importantes es el Object ID, el cual es único dentro del volumen para cada archivo, pero hay algunos archivos que no tienen o no usan este identificador. También hay un atributo, el cual se encarga de asignar diferentes acciones al archivo.

El *cuadro A5.6* contiene los atributos externos de un archivo de NTFS (NTFS. (2002)).

NTFS también cuenta con un sistema de criptografía de archivos llamado EFS, el cual protege la información, de personas sin autorización. Esta característica es transparente para el usuario.

Algo que de gran importancia para nosotros es cómo maneja NTFS los clusters, ya que no son diseccionados de una manera física, él lo hace de una manera lógica, así NTFS cuenta con un conjunto de clusters disponibles, y otro conjunto que son utilizados; así se direcciona de una manera que los archivos están en clusters virtuales continuos, y se agrupan por archivos y por directorios. Esto es de gran importancia para recuperar archivos, ya que en ese conjunto de clusters disponibles es donde están los archivos que se desea recuperar (Russinovich, Mark. (Noviembre 19 de 2000)).

Un sistema de archivos basado en un diario de operaciones tiene muchas ventajas; entre ellas, la más importante es brindar la posibilidad de recobrar el sistema de indexado del sistema de archivos cuando ocurre una falla en el volumen. NTFS maneja su sistema de archivos utilizando índices, de tal forma que se puede saber dónde está almacenada toda la información dentro del volumen. En sus primeras versiones, NTFS no manejaba un diario de operaciones o log de persistencia, por lo que la restauración del sistema era muy complicada y demorada. Con la versión 5.0, NTFS se convirtió en un sistema de archivos basado en un diario de operaciones (NTFS Change Journal (Adams, Blake C. (s.f.) y Richter, Jeffrey. (Abril 3 de 2004)).

Tipo de atributo	Descripción
Información estándar	Información, como estampilla de tiempo y fechas.
Lista de atributos	En caso de no residir en la MTF, da la ubicación de la lista de los atributos foráneos.
Nombre del archivo	Atributo siempre presente, que puede tener una longitud de 255 caracteres Unicode.
Descriptor de seguridad	Describe quién tiene permisos y quién es el dueño.
Data	Contiene los datos del archivo. NTFS permite varios atributos DATA, cada cual con sus específicos, según los requerimientos.
ID del objeto	Número único para el archivo, que se usa en el USN, pero no todos los archivos tienen uno.
Herramienta de logeo	Usado por el EFS, para poner entradas en log del sistema de archivos.
Punto de restauración	Usado para rastrear puntos de restauración del sistema junto con el log del sistema de archivos.
Índice de raíz	Usado para implementar carpetas.
Índice de colocación	Usado para implementar carpetas.
Bitmap	Usado para implementar carpetas.
Información del volumen	Contiene la versión del sistema de archivos
Nombre del volumen	Contiene el nombre del volumen.

Cuadro A5.6

Atributos externos de un archivo de NTFS (NTFS (2002)).

NTFS tiene un diario de operación por cada volumen presente en el sistema. El sistema de diario de operaciones crea un registro para cada cambio que experimente un archivo o carpeta. Estos cambios son creación, modificación y borrado. Cada registro almacena el tipo del cambio realizado y el nombre del objeto cambiado y una estampilla de tiempo, pero la información cambiada en si no es almacenada (Richter, Jeffrey. (Abril 3 de 2004)). Este sistema de diario de operaciones permite rastrear la historia y demás información sobre todos los archivos y carpetas existentes. Si hay varias particiones o varios volúmenes, los registros son adicionados a todos

los volúmenes y particiones a las cuales se tenga acceso (Adams, Blake C. (s.f.); Richter, Jeffrey. (Abril 3 de 2004)). Por infortunio, este sistema de diario de operaciones no tiene la capacidad de retroceder los cambios realizados a los archivos y carpetas, pero es una gran herramienta determinar qué operaciones ha realizado determinado archivo (Adams, Blake C. (s.f.) y Richter, Jeffrey. (Abril 3 de 2004)). El diario de operaciones de un archivo, que cuando es creada la partición de NTFS, inicialmente está vacío. Este archivo está oculto, para que los usuarios no tengan acceso directo a él. Cada vez que ocurre un cambio en un archivo se agrega un registro al final del diario de operaciones. A cada registro se le asigna un identificador de 64 bits, llamado Update Secuence Number (USN). Cada vez que un USN es generado éste incrementa su valor.

Una característica algo extraña es que estos números de secuencia no son consecutivos, ya que los que implementaron este sistema escogieron utilizar el offset del registro, como el USN (Richter, Jeffrey. (Abril 3 de 2004)). Como los registros contienen el nombre del archivo que ha sido "alterado", el tamaño del registro también varía. Esta es la razón por la cual los USN no son consecutivos. El sistema escribe en el diario en bloques de 4 kB, los cuales contienen entre 30 y 40 registros. Si un registro no cabe en el bloque, el espacio restante del bloque es rellenado con ceros, y se inicia un nuevo paquete, donde se introduce el registro. Todos los registros que se encuentran en la MFT almacenan diferentes atributos sobre los archivos que hay en el sistema; estos registros también almacenan el último valor del USN, que se le ha asignado a su respectivo archivo (Richter, Jeffrey. (Abril 3 de 2004)). El archivo del diario tiene un tamaño máximo, el cual, al alcanzar su máxima capacidad, empieza a descartar los primeros registros almacenado en él (Richter, Jeffrey. (Abril 3 de 2004).). El diario de operaciones se puede deshabilitar en cualquier momento. Resulta curioso que siendo ésta una útil y gran herramienta, está deshabilitada por defecto (Richter, Jeffrey. (Abril 3 de 2004)).

A. FAT

La FAT, siglas de File Allocation Table, se refiere a la Tabla de Asignación de Archivos (File Allocation Table, por sus siglas en inglés). Su característica principal son sus dos copias por volumen: Si se pierde la primera se recupera de la segunda. La FAT primaria está en un corrimiento específico para que siempre la encuentre, y la secundaria al final del volumen. La FAT16 funciona igual en todos los sistemas operativos Windows, al igual que la FAT32.

FAT 16

Se organiza por sectores, cada sector es de longitud igual a 521 bytes. Es la unidad más pequeña usada por el Sistema Operativo. Aunque el cluster

es la unidad que se utiliza para direccionar los archivos en un volumen FAT16. El tamaño del cluster lo determina el volumen de la unidad, teniendo un tamaño máximo de 64 kB (Microsoft Windows 2000 server. (2000)).

Se utiliza la FAT12 en caso de que el volumen sea muy pequeño, teniendo en cuenta que cada entrada de la FAT sea más pequeña, como resultado se tiene una FAT pequeña y así se optimiza el espacio (Microsoft Windows 2000 server. (2000)).

En un volumen FAT16 se tiene un directorio raíz. A diferencia de los directorios comunes, el directorio raíz es de tamaño fijo, 512 registros por volumen lógico. El número de registros en un disco extraíble depende del tamaño del volumen (*cuadro A5.7*) (Microsoft Windows 2000 server. (2000)).

Boot Sector
FAT
FAT 12
Root Folder
Datos

Cuadro A5.7

(Microsoft Windows 2000 server. (2000))

Los directorios tienen entradas de 32 bytes por cada archivo y directorio que contiene el directorio. En el cuadro *cuadro A5.8* se muestran los componentes de un archivo o directorio (Microsoft Windows 2000 server. (2000)).

Entrada	Bits
Nombre	8.3
Atributo	8
Hora de creación	24
Fecha de creación	16
Último acceso	16
Última hora de modificación	16
Última fecha de modificación	16
Número del primer cluster	16
Tamaño del archivo	32

Cuadro A5.8

(Microsoft Windows 2000 server. (2000))

No existe una organización para los directorios. Se asigna el primer cluster libre en el volumen a un archivo. El campo de primer cluster corresponde a la dirección del primer cluster usado por el archivo. Al final de cada cluster contiene un fin de archivo (0xFFFF) o un apuntador al siguiente cluster. Esta organización de la FAT es usada por todos los sistemas operativos que tienen soporte para FAT (Siyan, Karanjit S. (1996)).

Debido a que las entradas de un directorio son iguales en tamaño, el byte de atributo para cada entrada de un directorio es usado para describir qué tipo de entrada es. Es decir, un byte indica que se trata de un subdirectorio, y otra entrada marca qué es la etiqueta de un volumen. Normalmente sólo el sistema operativo usa este método (Siyan, Karanjit S. (1996)).

Hay 4 atributos posibles:

- Archivo
- Archivo del sistema
- Archivo oculto
- Sólo lectura

Como la FAT16 tiene un tamaño máximo para el volumen, y el tamaño del cluster está determinado por el tamaño del volumen, entonces, a continuación se muestra el *cuadro A5.9* con el tamaño normal del cluster para diferentes tamaños de volúmenes y con los posibles tamaños de particiones (Microsoft Windows 2000 server. (2000)).

Tamaño de la partición	Sectores por cluster	Tamaño del cluster
0 – 32 MB	1	512 bytes equivalente al tamaño del sector de la partición
33 – 64 MB	2	1.024 bytes
65 – 128 MB	4	2.048 bytes
129 – 256 MB	8	4.096 bytes
256 – 512 MB	16	8.192 bytes
512 – 1.024 MB	32	16 kB
1024 – 2.048 MB	64	32 kB
2048 – 4.096 MB	128	64 kB

Cuadro A5.9

(Microsoft Windows 2000 server. (2000))

FAT32

La ventaja de FAT32 es poder manejar particiones más grandes que FAT16, FAT 16 solamente maneja particiones hasta 4 GB, mientras que FAT 32 puede manejar particiones de hasta 2.047 GB (Microsoft Windows 2000 server. (2000)).

Estructura de la partición

FAT32 puede manejar archivos de 4 GB menos 2 bytes. La diferencia es que FAT32 maneja 4 bytes por cluster contra 2 bytes de FAT16. Una partición de FAT32 debe tener por lo menos 65.527 clusters y el tamaño de la partición no puede aumentar (*cuadro A5.10* (Microsoft Windows 2000 server. (2000)).

Boot
Root
FAT
FAT
Datos

Cuadro A5.10

(Microsoft Windows 2000 server. (2000))

La FAT crece con respecto al tamaño de volumen; así con un volumen muy grande, se tiene una FAT muy grande, lo cual hace que calcular el espacio libre tome mucho tiempo y, en general, el comportamiento del sistema operativo con una FAT grande hace que los tiempos de búsqueda aumenten (Microsoft Windows 2000 server. (2000)).

El cuadro maestro de archivos es una lista de registros de 32 bits, que tiene una relación uno a uno, con los clusters de datos. La única diferencia en el manejo de este cuadro es la adición al cluster de una palabra larga en la entrada de los directorios que accedan el cluster (Microsoft Windows 2000 server. (2000)).

El tamaño máximo de un volumen de FAT32 depende del máximo número de entradas en el cuadro maestro, el número de sectores por cluster, y el conteo de 32 bits en el cuadro de particiones; aquí se asume un sector de 512 (*cuadro A5.11* (Microsoft Windows 2000 server. (2000)).

Tamaño del cluster	Tamaño máximo del volumen
512 bytes	127,9 GB
1 kB	255,9 GB
2 kB	511,9 GB
4 kB	1.023,9 GB
8 kB	2.047 GB
16 kB	2.047 GB
32 kB	2.047 GB

Cuadro A5.11

(Microsoft Windows 2000 server. (2000)).

En el *gráfico A5.2* hay tres archivos en la FAT. File1.txt ocupa tres clusters, File2.txt está fragmentado y también ocupa tres clusters, mientras que File3.txt solamente ocupa un cluster. En el directorio se guarda la información del primer cluster de cada archivo.

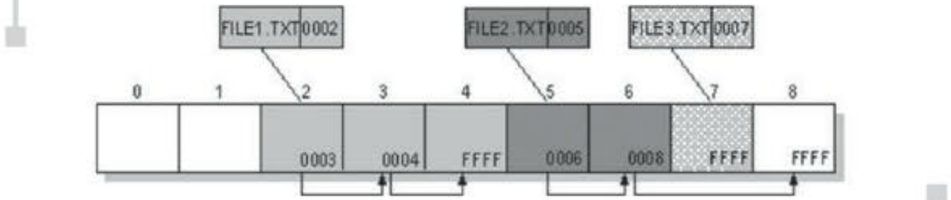


Gráfico A5.2

Ejemplo de la Tabla de Asignación de Archivos

La primera estructura importante en un volumen FAT es la BPB (BIOS Parameter Block), que se aloja en el primer sector del volumen en la región reservada. Este sector a veces se denomina "sector de arranque", o sector reservado o sector 0. Este sector no existía en MS-DOS 1.x, debido que sólo manejaba discos flexibles. En MS-DOS 2.x únicamente se permitía que el volumen tuviera 65.536 sectores, debido a que el número de sectores se almacenaba en 16 bits. En las versiones 3.x se asignó un campo de 32 bits para el número total de sectores. Antes de Windows 95, FAT16 estaba limitada en 2 GB para el tamaño máximo de cluster si el volumen es de sectores de 512 bytes, pero FAT32 resuelve parcialmente este problema al permitir volúmenes mayores de 2 GB pero con una sola partición.

¿Qué permite?

La FAT fue uno de los primeros sistemas de archivos; sus diseñadores no utilizaron el conocimiento que ya existía en ese tiempo sobre diseño de sistemas de archivos. Su organización simple permite un manejo fácil de la fragmentación de archivos, lo que afecta el desempeño en el resto de las operaciones del sistema de archivos. FAT no fue diseñada para manejar la redundancia de la información, en caso de que el sistema colapse.

2. BORRADO

2.1 Borrar *vs.* Eliminar

Cada cluster contiene algo, ya sea archivo o un archivo que se elimino, lo cual implica tres formas de borrar un archivo o carpeta, la primera es simplemente poner en la FAT el cluster como libre, lo cual deja el archivo en el disco, pero no se puede hallar; en este caso es el "delete" de Windows; luego se da que se registra por un apuntador especial que es papelera de reciclaje de Windows, y por último se tiene borrado seguro.

Cuando se coloca el cluster como libre, el archivo todavía está en disco, pero no hay una forma de llegar a él sin usar software especializado (que se cubre más adelante). Cuando se marca con el apuntador especial de la papelera de reciclaje (Managing Deleted Files. (Abril 13 de 2004)), lo único que hace es ubicar el archivo en una carpeta especial del sistema, en la cual, luego de un tiempo determinado, o por elección del usuario, son eliminados todos los archivos. Por último, se tiene el borrado seguro, que es eliminar el archivo totalmente; esto se hace sobrescribiendo el lugar físico que ocupa el archivo.

Se puede recalcar que los sistemas de archivos son estructuras que manejan apuntadores para poder encontrar archivos, y que todo lo que el usuario ve es una ilusión (Disk Geometry. (s.f.)).

2.2 Metodologías para eliminar

El Departamento de Defensa de los Estados Unidos ha definido una serie de métodos de eliminado de información no clasificada de sus computadores, antes que éstos sean redistribuidos. El método escogido depende del tipo de disco (NetworkWorldFusion. (Abril 12 de 2004)):

- *Degaussing:* En este proceso el medio retorna a su estado inicial de fabricación. La coercitividad es la medida de la cantidad de campo magnético necesario para reducir la inducción magnética de un medio a 0, y se mide en Oersteds. Según el Gobierno de los Estados Unidos, los degaussers se clasifican en distintas clases: Clase 1 para coercitividad de 0 a 350 Oe, Clase 2 para coercitividad de 350 a 750 Oe. Clase 3 para coercitividad de más de 720 Oe. En la actualidad los degaussers existentes son solamente de clases 1 y 2 (Apendix E. (s.f.)).
- *Sobrescritura múltiple:* Se trata de ejecutar sobre el medio varias técnicas de sobrescritura, como sobrescribir los campos magnéticos del medio de forma alternada para exponerlo a un campo magnético oscilante, sobrescribir el medio con basura, etc. Usa la menor frecuencia posible para la sobrescritura (Apendix E. (s.f.)).
- *Técnica de sobrescritura de Guttman:* Esta técnica especifica 35 diferentes formas de sobrescritura, y tiene como propósito vencer todas las técnicas de recuperación, lo cual lo logra con éxito (Apendix E. (s.f.)).
- *Destrucción física:* Desde la utilización de sierras, mazos, o la incineración. Sin embargo, es sorprendente lo resistentes que son los medios magnéticos; por ejemplo, los discos duros.

3. RECUPERACIÓN DE INFORMACIÓN EN FAT

Durante las primeras versiones de Windows, se incluía en DOS un software de recuperación, después de Windows 95, con la aparición de la papelera de reciclaje, un archivo eliminado de esta era "irrecuperable", pero eso no es cierto. ((6Get Practical! (Octubre 31 de 2001);) (10PC IN. (Marzo 21de 2004))). Actualmente existe bastante software que permite recuperar archivos borrados de la FAT.

3.1 Borrado en FAT

Las tablas del FAT se encuentran organizadas como arreglos lineales de entradas. Estas entradas son valores de cierto número de bits (según la versión de la FAT; por ejemplo, 12, 16 o 32). En el *gráfico A5.3* se encuentra una representación de la organización de la FAT (Leithead, Travis; Richards Mark. (Agosto 20 de 2002)).

Cuando un archivo es borrado no se hace nada a los clusters que contienen la información, lo que se hace es desvincular de la tabla de la FAT la dirección al archivo, y añadir un carácter especial (0xe5) al directorio, indicando que está libre para escribir sobre él (Leithead, Travis; Richards Mark. (Agosto 20 de 2002)).

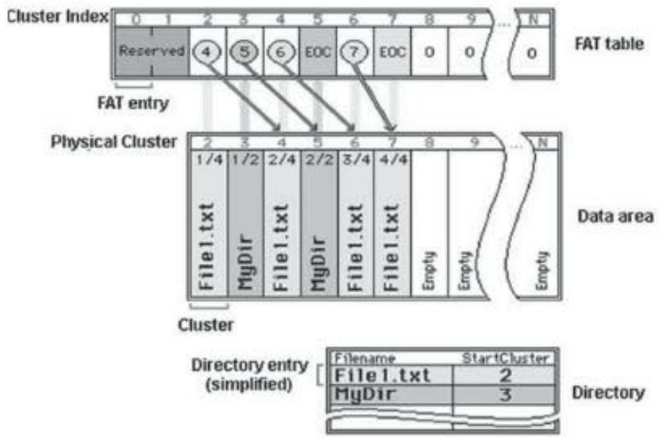


Gráfico A5.3

Organización de la FAT

La acción de desindexar un archivo de la FAT equivale a decirle al sistema operativo que estas direcciones están ahora libres, pero hasta que un nuevo archivo sea escrito sobre este espacio, el archivo borrado estará aun en el disco duro. De este modo, con la ayuda de software especializado (algunos de bajo costo o gratuitos) se puede recuperar esta información (NASA (National Aeronautics and Space Administration). (2004, Marzo 21)).

Es importante tener en cuenta que 'eliminar' algo de la papelera de reciclaje no es realmente eliminar, sino es borrar.

3.2 Eliminar en FAT

Para eliminar un archivo del FAT se necesita borrarlo y después escribir sobre el mismo. Este proceso puede darse a voluntad de una persona o como consecuencia de borrar un archivo. Después de borrar un archivo, el sistema operativo considera el espacio que éste utiliza como libre, de modo que cuando necesite guardar algo es posible que sobrescriba el archivo (Jeita. (Marzo 21de 2004)).

En el mercado existen varias herramientas que se encargan de eliminar archivos del disco duro. Estas herramientas escriben un patrón dado al área de memoria de la que se desea eliminar la información. Este método es independiente del sistema operativo; por lo tanto, puede eliminar archivos aun si están corruptos o dañados y no pueden ser accedidos (Jeita. (Marzo 21de 2004)).

Para que se pueda asegurar que se ha eliminado completamente el archivo se necesitan más de una pasada de escritura sobre el espacio, métodos de borrado seguro como el de Peter Gutmann que aconsejan 27 pasadas. Otros métodos más veloces pueden no ser tan seguros. En informática forense se considera borrado seguro aquel que haya sido generado con 35 o más pasadas (Coconubo, Juan Carlos. (Febrero 4 de 2004)).

Para eliminar toda la información del disco duro se puede usar un degausser que desmagnetiza el disco, eliminando la información guardada en él (ya que éste es un medio magnético (Degauss. Computer Hope. (Marzo 21de 2004)).

El proceso de degaussing consiste en exponer el medio a un campo magnético, de modo que se anulen las direcciones magnéticas guardadas en éste.

El cambio de una sola partícula magnética de una dirección a otra requiere que se sobrepase una barrera de energía, con un campo magnético externo que ayude a disminuir esta barrera. El cambio depende no solamente de la magnitud del campo externo, también de la cantidad de tiempo en que es aplicado. Para borrar un medio efectivamente se requiere una fuerza magnética de alrededor de cinco veces la coercitividad del medio. A continuación se presenta el *cuadro A5.12* con la coercitividad media típica:

Medio	Coercitividad
5.25" 360K floppy disk	300 Oe
5.25" 1.2M floppy disk	675 Oe
3.5" 720K floppy disk	300 Oe
3.5" 1.44M floppy disk	700 Oe
3.5" 2.88M floppy disk	750 Oe
3.5" 21M floptical disk	750 Oe
(1980's) disco duro	900-1.400 Oe
(1990's) disco duro	1.400-2.200 Oe
1/2" cinta magnética	300 Oe
1/4" QIC metálica	550 Oe
8 mm cinta metálica	1.500 Oe
DAT cinta metálica	1.500 Oe

Cuadro A5.12

Coercitividad media típica

3.3 Evidencias de borrado para recuperación

Al realizar un análisis forense, se puede encontrar cuando un archivo ha sido eliminado, evidencia de archivos temporales, e incluso algunas herramientas de recuperación de archivos generan logs sobre la tarea realizada (NASA (National Aeronautics and Space Administration). (2004, Marzo 21)).

Revisando el disco se puede buscar el valor 0x5e (que significa que el archivo fue borrado); de esta manera se puede encontrar que áreas de memoria han sido borradas.

Del mismo modo, usando una visor hexadecimal del disco, se pueden encontrar inconsistencias sobre el tamaño o dirección del primer cluster de un archivo, de modo que se puede ver si un archivo ha sido eliminado de la FAT con intención.

3.4 Recuperar borrado en FAT

Recuperar información en FAT no es tan difícil como parece; todo depende de las circunstancias, y del estado actual del sistema de archivos. Las circunstancias de las que se habla dependen principalmente del estado de fragmentación del disco, y de la utilización del mismo. Si el disco está muy fragmentado, y la utilización del disco es alta; hay una gran probabilidad de que un nuevo archivo ocupe uno de los clusters que pertenece al archivo que se quiere recuperar. Si en este caso es muy poco probable que se pueda recuperar la información. Si ocurre el caso contrario, es mucho más fácil, ya que como la FAT hace una asignación secuencial y cíclica del espacio disponible, es poco probable que se pierda un cluster (Kjoernes, Thomas. (Abril 3 de 2004); Kozierok, Charles M. (Abril 3 de 2004)).

Técnicamente hablando, el proceso de recuperación de un archivo eliminado es el siguiente: Primero hay que buscar en el Root Directory, o en la sección de datos, según sea el caso, el registro (Directory Entry), que contenga el archivo eliminado. Un archivo eliminado se puede identificar fácilmente, porque en su registro, en el nombre de éste, el primer carácter ha sido reemplazado por E5h. Lo que hay que hacer es cambiar este carácter por su carácter original. Después de hacer esto, hay que buscar el registro del cluster lógico, dentro de la FAT, que corresponde al valor que está almacenado, en el campo Cluster Number, del registro anteriormente nombrado, y cambiar el valor de éste con uno de los dos siguientes criterios: Si el tamaño del archivo, el cual también se encuentra en el registro, es menor que el tamaño del cluster, hay que colocar en el cluster lógico, en la FAT, el valor de fin de archivo, que para el caso de FAT12 puede ser FF7-FFF, o para FAT16 es FFF7-FFFF, y con la misma teoría funciona FAT32 (Kjoernes, Thomas. (Abril 3 de 2004); Kozierok, Charles M. (Abril 3 de 2004)).

Si el tamaño del archivo es mayor que el del cluster, hay que calcular el número de cluster que ocupa. Si hay suerte, el siguiente cluster lógico disponible debe también ser parte del archivo. Al cluster lógico se le coloca el valor del siguiente cluster disponible, y así, hasta que se complete el número de cluster requerido, y para el último se hace lo mismo que en el caso anterior. Lo anterior es válido si el disco no está muy fragmentado, porque si lo está, es muy posible que se encadene mal el archivo y se corrompa (Kjoernes, Thomas. (Abril 3 de 2004) y Kozierok, Charles M. (Abril 3 de 2004)).

4. RECUPERACIÓN DE INFORMACIÓN EN NTFS

Es muy importante notar que NTFS es un sistema de archivos basado en transacciones, por lo cual ciertas operaciones se pueden deshacer solamente usando las funciones del sistema de archivos. NTFS tiene la capacidad de recuperar información después de un error crítico en el sistema de archivos. La s operaciones a medio terminar no están permitidas en NTFS. Pero inclusive una vez se termina una operación o transacción, ésta se puede deshacer (Kozierok, Charles M. (Abril 3 de 2004)).

4.1 Recuperación Automática de NTFS

NTFS realiza lo que es conocido como recuperación de 3 pasadas después de una falla crítica del sistema; ésta solamente se hace cuando en el log de persistencia se tiene que una transacción del sistema de archivos no fue completada y pueden encontrarse errores en el sistema de archivos.

Así es como se realizan las tres pasadas:

- Paso de análisis: Se analiza el log de persistencia para determinar cuáles sectores necesitan ser examinados o corregidos (Kozierok, Charles M. (Abril 3 de 2004)).
- El sistema rehace todas las transacciones desde el último punto control conocido (Kozierok, Charles M. (Abril 3 de 2004)).
- Paso de deshacer, el sistema deshace todas las transacciones conocidas (Kozierok, Charles M. (Abril 3 de 2004)).

Los puntos de control se realizan cada 8 segundos, el sistema marca el log de persistencia; así únicamente lo tiene que revisar son unos cuantos registros en el log de persistencia (Kozierok, Charles M. (Abril 3 de 2004)).

Es importante anotar que este sistema automático no garantiza que la información no se pierda; si una transacción no se completa y el sistema falla, esta transacción se pierde, y dada la naturaleza de esta autorrecuperación, el usuario no sabrá que la transacción no se completó.

4.2 Borrado en NTFS

El proceso de borrado en NTFS es similar al de FAT. Cuando el usuario decide que ya no necesita un archivo, selecciona el archivo y da la opción de enviar a la papelera de reciclaje (dependiendo de la configuración del sistema, el archivo a veces puede ser borrado directamente), la cual es solamente una carpeta especial. Al seleccionar "Eliminar", el sistema de archivos va a la MTF y busca el registro del archivo y elimina el apuntador a éste; de esta forma, no es posible direccionar el archivo y el cluster donde se encuentra queda disponible, y además queda un registro en el log de persistencia (Kozierok, Charles M. (Abril 3 de 2004)).

4.3 Eliminar en NTFS

El proceso de eliminación, en NTFS, es más complicado que en FAT, ya que la seguridad y el registro (log) de NTFS son muy superiores. Pero en general lo mejor para eliminar la información es sobrescribir sobre los clusters que almacenan los datos. Ya que, de lo contrario, es muy probable que se logre recuperar la información.

4.4 Evidencias de borrado para recuperación

Además de rastrear archivos desindexados en el disco, los sistemas operativos que funcionan con NTFS proveen sistemas de auditoría y detección de intrusos, donde se registran sucesos como el borrado de archivos. En NT, el evento de borrar un archivo queda registrado en el security.log. En Windows 2000 hay herramientas de auditoría de instalación opcional que registran varios tipos de eventos, incluido el borrado de archivos. Los archivos residentes en MFT al ser borrados, dependiendo de dónde estaban residiendo, puede ser que no sean borrados, y a los archivos grandes solamente se les borra la referencia (49 Kozierok, Charles M. (Abril 3 de 2004)).

4.5 Recuperar borrado en NTFS

Dado que NTFS también funciona por referencia, la recuperación de archivos es posible, pero un poco más compleja que en FAT. Ya que en NTFS los directorios contienen información de sí mismos, no de los archivos que contienen; es decir, únicamente contienen los clusters virtuales que están dentro del directorio. Por esto la recuperación de archivos en NTFS es más complicada. Y también debido a que un archivo es una colección de atributos, al borrar un registro de la MFT se está borrando el archivo en sí, pero solamente marca el atributo en uso como falso, lo cual es borrado para NTFS (NTFS (2002)).

Al recuperar, una de las opciones es buscar en el log de persistencia el momento en el cual fue borrado un registro de la MFT, y así recuperar el archivo; esto se debe al USN el cual se explicó con anterioridad. Con ese número y la información en el log de persistencia, el sistema de archivos recupera el archivo borrado.

Pero pasado un tiempo, el diario de operaciones o log de persistencia para esa transacción desaparece, y ahí es cuando es necesario usar software especializado. Este software primero busca en la MFT por registros de borrado, y los recupera (NTFS.com. (2002); después busca el bloque de datos donde está el archivo; este bloque se puede encontrar ya que se encuentra entre los clusters que están disponibles; busca en ellos y recupera el archivo (NTFS.com. (2002)). Estos clusters virtuales disponibles son agrupados a medida que se liberan, y se van usando conforme aumenta la cantidad de información en el disco. Entonces al buscar en los clusters disponibles, se encuentran los archivos que fueron eliminados (Russinovich, Mark. (Noviembre 19 de 2000)).

La búsqueda de archivos borrados en NTFS es posible, ya que se buscan atributos comunes, que mantienen los archivos inclusive después del borrado, nombre, tamaño, fechas, etc. (NTFS (2002)). A diferencia de la FAT, los archivos o directorios borrados en NTFS, tienen un campo en el encabezado del archivo o directorio que indica que fue borrado; este campo son 2 bytes. Estos 2 bytes definen el estado del archivo; para nuestro caso, solamente nos importa el primer byte que define si está en uso o borrado (NTFS (2002)).

Ahora cuando se encontró el registro borrado, debemos encadenar los clusters hasta recuperar completamente el archivo. Esto se hace buscando cluster por cluster hasta alcanzar el tamaño del archivo que indica su atributo (NTFS (2002)). Encadenar los clusters es un poco más complicado, ya que NTFS tiene un atributo de archivo llamado DATA, el cual está encriptado y posee la información de los clusters donde se deben buscar los datos del archivo. Solamente resta encadenar los datos para reconstruir el archivo; así que esta tarea es fácil (NTFS (2002)).

4.6 Recuperar el sector de arranque

En NTFS se puede recuperar un sector de arranque (boot sector), porque el sistema de archivos guarda una copia de éste (Microsoft Corporation. (Abril 12 de 2004)). En FAT, el sistema no guarda una copia del sector de arranque.

5. DEMOSTRACIÓN

Se han recogido diferentes herramientas de uso gratuito o que le permiten al usuario bajar un programa de evaluación, de modo que éstas serán analizadas y expuestas como parte de este paper. El demo consiste en estas herramientas, su revisión y su uso.

FileRecovery ➔ (*gráfico A5.4*) es un programa de recuperación de datos que soporta los sistemas de archivos FAT12/16/32 y NTFS. Este programa encuentra particiones automáticamente, aun si el sector de boot ha sido borrado o dañado (esto solamente en FAT, no en NTFS); recupera archivos con sus marcas de fecha y hora originales; los archivos salvados pueden ser guardados en unidades en la red; recupera archivos aun si su encabezado no está disponible (ésta es una característica que cumplen muy pocos productos), en este caso soporta arj, exe, mov, zip, avi, gif, mp3, bmp, hlp, pdf, cdr, html, png, doc, htm, rtf, dxf, jpg, tar, dbf, lzh, tif, xsl, mid y wav.

Gráfico A5.4

Este programa se presenta como freeware. No sirve si se tienen problemas mecánicos con el drive; por ejemplo, si el disco duro no es reconocido por el BIOS o hace ruidos inusuales (PC Inspector File Recovery. (Abril 8 de 2004)).

Las siguientes imágenes de la pantalla son tomadas para explicar la funcionalidad del software.

La pantalla de bienvenida permite recuperar archivos eliminados, encontrar datos perdidos o encontrar unidades perdidas (*gráfico A5.5*).

Gráfico A5.5

Pantalla de bienvenida

La siguiente pantalla (*gráfico A5.6*) permite seleccionar la unidad lógica o física según sea el caso.

Gráfico A5.6

Selección de la unidad lógica

Una vez escogida la unidad, el programa se demora unos segundos encontrando los archivos y carpetas que estaban perdidos o borrados. En esta imagen se presenta el caso de recuperación de archivos eliminados. Estos archivos pueden ser guardados en un directorio específico, pueden ser renombrados, y ser recuperados como texto o en hexadecimal (*gráfico A5.7*).

Gráfico A5.7

Recuperación de archivos

Este programa no repara unidades dañadas ni recupera datos de los CD o DVD. Además, este software no puede ser corrido desde un disquete, debe estar en un disco duro con una versión instalada de Windows 95/98/ME/ NT/2000/ XP. Bajo Windows XP, es necesario tener derechos de administrador para ver todas las unidades lógicas (PC Inspector File Recovery. (Abril 8 de 2004)).

Se realizaron pruebas con este programa, y se encontró que puede recuperar bastante información, incluso si la FAT y el directorio están corruptos o dañados. Busca los archivos con un diccionario de 'headers' o encabezados, y con ellos revisa los clusters hasta encontrar el final de los archivos; igualmente encuentra archivos ocultos, o cuya extensión es desconocida. Recupera información eliminada con precisión, pero tiene problemas al hacer borrado seguro. La búsqueda de archivos suele resultar en archivos que contienen más información de la que originalmente fue pensada, ya que escoge un end of file, que puede no ser el correcto.

File Scavenger➔ (gráfico A5.9), un programa diseñado para NTFS en Windows XP, 2000 o NT, permite recuperar archivos borrados accidentalmente, incluyendo archivos borrados de la papelera de reciclaje. File Scavenger soporta discos básicos y dinámicos, compresión NTFS, secuencias de datos alternas, nombres de archivo Unicode, etc.

Se recuperan el archivo y la dirección en la que éste se encontraba, con excepción de casos extremos.

Se pueden recuperar archivos de volúmenes reformateados o corruptos; esto es posible incluso si el volumen ha sido borrado y su posición original y su tamaño son desconocidos. Este programa maneja discos con sectores dañados y con particiones corruptas de manera transparente al usuario (Quetek. (Abril 7 de 2004)).

Este software puede ser instalado y corrido desde un disquete.

Se puede conseguir una versión gratuita que está restringida a 64 kilobytes de datos recuperables. La licencia personal más económica tiene un costo de 39,95 dólares (Quetek. (Abril 7 de 2004)).

Las siguientes ventanas son imágenes tomadas de la versión gratuita del programa.

El *gráfico A5.8* muestra la ventana de las licencias que es posible adquirir:

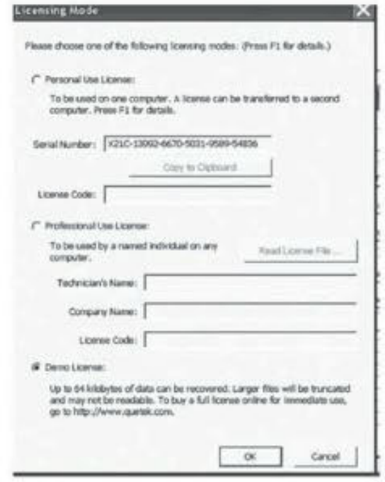


Gráfico A5.8

Ventana de licencias

La ventana principal del programa permite escoger el modo de búsqueda, y explica las posibilidades:

- *Normal,* que es una búsqueda rápida por los archivos recientemente borrados, incluidos los que fueron borrados en la papelera de reciclaje.
- *Exhaustiva,* que verifica cada sector del disco. Es útil cuando el disco ha sido formateado o cuando no se dan resultados con la búsqueda normal.
- *Búsqueda en volúmenes 'muertos'*, que es una búsqueda igual a la búsqueda exhaustiva, pero para volúmenes dañados o borrados, o para reconstruir volúmenes tipo RAID 0 o RAID 5, o sets de volúmenes.

Se puede elegir el tipo de archivo que se está buscando, el asterisco significa que se están buscando todos los archivos.

Una vez realizada la búsqueda, los archivos encontrados pueden ser ordenados por cualquiera de las características que se exponen en la parte inferior de la pantalla; además pueden ser vistos en directorios o como archivos individuales. Igualmente se puede escoger la carpeta a la cual serán recuperados los archivos.

Gráfico A5.9

File scavenger

Después de realizar pruebas, se concluye que es una herramienta buena, pero no es precisa al recuperar archivos perdidos; aunque tiene un buen diccionario de encabezados, no es seguro que al utilizarla se estén encontrando todos los archivos perdidos. Pese a que dice que está diseñada solamente para NTFS, funciona en disquetes (FAT12).

Un ejemplo de proceso

La primera parte del proceso es ejercer el método de Guttman en el espacio libre, así el espacio libre que tiene el disco duro queda estéril, de tal manera que la recuperación del archivo es única y confiable. Se sigue el procedimiento siguiente:

- Se esteriliza el disco duro.
- Se mira que no tenga archivos sin referencia en el disco duro (verificó la esterilización).
- Se copia el archivo a recuperar.
- Se elimina el archivo.
- Se recupera el archivo.
- Se repite el proceso pero con borrado seguro US DoD 5220.

El documento tiene la siguiente configuración, será eliminado por el método estándar de Windows.

- doc_prueba.doc
- Cluster: 1382271
- Tamaño: 298496

Stellar Phoenix FAT & NTFS

Cuando se realiza la recuperación para verificar la esterilización, pero no se encontró ningún archivo recuperable.

PC Inspector File Recovery

Cuando se realizó la verificación de esterilización, se encontraron 4.275 archivos perdidos, de los cuales, algunos son mp3, y otros son unos archivos de texto. En los archivos mp3, después de reconstruir los encabezados, es posible oír pedazos de las canciones, en promedio, 1 segundo de música por cada 10 segundos de grabación; para los archivos de texto, son imposibles de leer.

El documento tiene la siguiente configuración, será eliminado por el método estándar de Windows.

- doc_prueba.doc
- Cluster: 1382271
- Tamaño: 298496

Luego será recuperado por ambos programas con los siguientes resultados.

Stellar Phoenix FAT & NTFS

Encontró y pudo recuperar el archivo sin mayores problemas, el formato de Word quedó intacto.

PC Inspector File Recovery

Encontró pero dice que su condición es pobre, al recuperarlo se puede extraer el texto, pero algunos datos se pierden.

US DoD 5220 (8-306. /E) (3 pasadas)

PC Inspector File Recovery

Encuentra un archivo de Word, pero no recupera el nombre. Y el contenido es basura aparentemente.

Stellar Phoenix FAT & NTFS

No recupera nada, una vez se elimina el archivo, que ese borrado del todo (*gráfico A5.10*).

Gráfico A5.10

Stellar Phoenix FAT & NTFS

Winhex

Winhex-> es una herramienta para editar archivos en hexadecimal, y muy potente que permite manipular en sistema de archivos en una gran variedad de formas.

En el *gráfico A5.11*, el editor de imágenes permite explorar cada volumen, directorio y archivo del disco en forma hexadecimal, tal como están grabados físicamente. En la primera sección vemos los volúmenes lógicos, en este caso Removable Medium, Windows, Applications, Fun, Setup, Test1, Test2, CD-ROM Drive, RAMDrive.

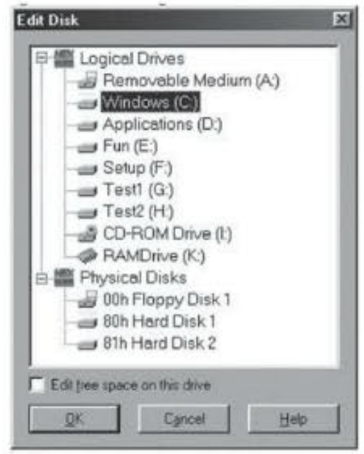


Gráfico A5.11

Editor de imágenes

En la segunda sección vemos que todos esos volúmenes son en realidad dos discos físicos, 80h Hard Disk 1 y 81h Hard Disk 2. De esta forma, si exploramos los discos y carpetas en la primera sección encontramos los datos de los archivos, tal como aparecen en cada directorio, mientras que en la segunda sección estamos viendo realmente el "raw data"; es decir, se despliega la información, tal cual está escrita físicamente en cada volumen físico.

Winhex posee una herramienta de recuperación de archivos. Seleccionando en el Menú de Herramientas (Tools Menu)->Disk Tools, ofrece una búsqueda de archivos que pueden ser reconocidos por su encabezado. Existe la opción de Búsqueda por Tipo de Archivo, así como Búsqueda por nombre de Archivo. La opción por tipo de archivo depende solamente del formato del tipo del archivo; por ejemplo, el encabezado y, por lo tanto, es independiente del sistema de archivos del sistema operacional. Esta opción es viable solamente si los archivos no están fragmentados. El usuario selecciona el lugar en donde quiere que Winhex guarde los archivos encontrados, los cuales tienen usualmente un formato de nombres "file~~~~" , donde los ~ significan números que se incrementan.

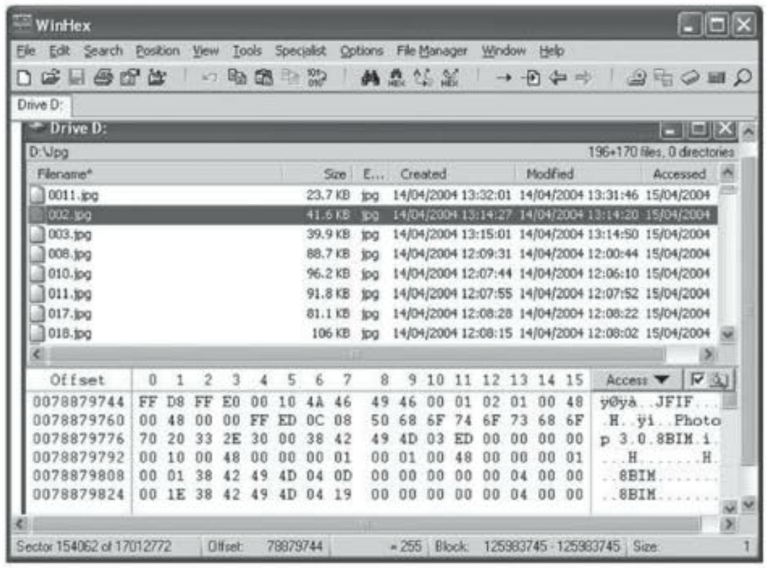
Opcionalmente, el programa puede buscar archivos a partir de determinado desplazamiento dentro de los clusters, es decir, no necesariamente en el principio de cada cluster. Esto es indispensable al recuperar archivos de cintas de soporte donde no se usan clusters. También permite la recuperación de archivos que deliberadamente estaban almacenados en lugares ocultos.

Por ejemplo, para extraer todos los archivos .jpg, Winhex buscan los valores FFD8FF (cuya interpretación ascii es el característico yøyá). Normalmente el encabezado se encontrará en un desplazamiento cero dentro del cluster (offset 0). En el *Anexo A5.1* vemos un ejemplo de cómo Winhex presenta parte del archivo 002.jpg en hexadecimal.

Winhex es una herramienta de borrado seguro de forma manual usando técnicas de sobrescritura porque permite editar directamente los valores en el disco. Para efectuar el borrado seguro sobre un archivo que haya sido borrado por el sistema, el usuario puede ubicar en el raw data del disco la posición del archivo, ya sea identificando una cadena dentro del archivo, o verificando el tamaño; y luego procediendo a sobrescribir los valores de formatoe que sea difícil volver a reconstruir el archivo.

Anexo 5.1

Ejemplo de exploración en Winhex



Exploración en Winhex

Conclusiones

Al recuperar archivos en FAT hay que tener en cuenta que fue uno de los primeros sistemas de archivos diseñados (Microsoft Corporation. (Abril 12 de 2004)), y que presenta varias limitaciones, especialmente en las primeras versiones. La FAT no soporta redundancia ni guarda una copia del sector de arranque.

Existen muchas herramientas que permiten recuperar información en NTFS y FAT. La forma como estos sistemas de archivos funcionan da muchas posibilidades al usuario de recuperar información o partes de ésta.

No se puede confiar 100% en los métodos de borrado seguros, lo cual hace dudar de la privacidad de la información. El objetivo del borrado seguro es lograr que la recuperación de la información sea lo más ineficiente y costosa posible.

NTFS definitivamente permite recuperar archivos con mayor precisión; esto se debe a que las características del sistema del archivos fue diseñado pensado en redundancia y seguridad, los cuales son factores importantes en la recuperación de archivos.

✓ ***Resumen:*** Este documento recopila información sobre los sistemas de archivos NTFS y FAT. Con esta información se hace un resumen de las posibilidades forenses de recuperar información en estos sistemas de archivos, y se diferencia entre borrado y eliminado, y se explica la seguridad que permiten estos sistemas en cuanto al borrado y recuperación de información confidencial.

✓ ***Términos clave:*** archivos, clusters.

Enlaces en el Web

http://sourceforge.net/projects/hcovert/?abmode=1 –Hcovert– Herramienta para crear canales encubiertos sobre http.
http://www.aic.gov.au/topics/cybercrime/ –Página del Instituto Australiano de Criminología– Tema: Cibercrimen.
http://www.aic.gov.au/topics/cybercrime/cyberterror.html –Página del Instituto Australiano de Criminología – Tema: Ciberterrorismo.
http://www.antsight.com/zsl/rainbowcrack/ –Proyecto RainbowCrack, para descubrimiento de contraseñas en texto plano.
http://www.cybercrime.gov –Sitio norteamericano donde se encuentran documentados algunos casos sobre delitos informáticos.
http://www.firstmonday.org/issues/issue2_5/rowland/ –Canales encubiertos sobre TCP/IP.
http://www.forensicmag.com/ – Forensic Magazine.
http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf –FAQ Esteganografía.
http://www.metasploit.com/research/projects/antiforensics/ –Proyecto Antiforense de Metasploit.
http://www.rand.org/pubs/monograph_reports/MR1382/ –Libro digital– Networks and Netwars: The Future of Terror, Crime, and Militancy.
http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf –Google desktop as a source of digital evidence.

Referencias*

Active @ Data Recovery Software. (Abril 3 de 2004). Partition Boot Sector is Damaged. Disponible en: http://www.uneraser.com/boot-sector-damaged.htm. Adams, Blake C. (s.f.). Microsoft NTFS 5.0. Milwaukee School of egineering. Design of Operating Systems . CS - 384 . Documento en formato PFD, Blake Adams - NTFS 5.0.pdf

Apendix E. (s.f.). AR 380-19 Information Systems Security, Disponible en: http://www.fas.org/irp/doddir/army/ar380-19/appendix_e.htm

Coconubo, Juan Carlos. (Febrero 4 de 2004). Borrado Seguro. No es público.

Degauss. Computer Hope. (Marzo 21 de 2004). Disponible en: http://www.computerhope.com/jargon/d/degauss.htm

Disk Geometry. (s.f.).

Get Practical! (Octubre 31 de 2001). Managing deleted Files. Disponible en: http://www.glencoe.com/norton/online/ezine/display_article.phtml?id=161

Introducción a VCR. (Marzo 20 de 2004). Disponible en: http://www.monografias.com/trabajos5/vcr/vcr.shtml#magne

Jeita. (Marzo 21 de 2004). Technical Analysis of Data Erasure Issues. Disponible en: http://it.jeita.or.jp/perinfo-e/memorycard-e/refer.html

Kjoernes, Thomas. (Abril 3 de 2004). File Allocation Table. Disponible en: http://home.no.net/tkos/info/fat.html.

Kozierok, Charles M. (Abril 3 de 2004). Compression. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/other_Compr.htm.

* Referencias de la sección Para profundizar. (N. del E.).

Kozierok, Charles M. (Abril 3 de 2004). File Chaining and FAT Cluster Allocation. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/clust_Chaining.htm.

Kozierok, Charles M. (Abril 3 de 2004). File Deletion and Undeletion. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/clustDeletion-c.html.

Kozierok, Charles M. (Abril 3 de 2004). High Performance File System (HPFS). The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/file_HPFS.htm.

Kozierok, Charles M. (Abril 3 de 2004). NTFS 1.1/4.0. The PC Guide Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/verNTFS11-c.html

Kozierok, Charles M. (Abril 3 de 2004). NTFS 5.0. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/ver_NTFS50.htm.

Kozierok, Charles M. (Abril 3 de 2004). NTFS Architecture Overview. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/archArch-c.html.

Kozierok, Charles M. (Abril 3 de 2004). NTFS Clusters and Clusters Sizes. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/arch_Cluster.htm.

Kozierok, Charles M. (Abril 3 de 2004). NTFS Master File Table (MFT). The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/arch_MFT.htm.

Kozierok, Charles M. (Abril 3 de 2004). NTFS Partitioning Strategies The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/impl_Part.htm.

Kozierok, Charles M. (Abril 3 de 2004). NTFS Transaction Recovery. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/ver_NTFS50.htm.

Kozierok, Charles M. (Abril 3 de 2004). NTFS Version Compatibility. The PC Guide. http://www.pcguide.com/ref/hdd/file/ntfs/verCompat-c.html.

Kozierok, Charles M. (Abril 3 de 2004). NTFS VersionsThe PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/ver.htm.

Kozierok, Charles M. (Abril 3 de 2004). NTFS Volume Boot Sector. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/archSector-c.html.

Kozierok, Charles M. (Abril 3 de 2004). OS/2. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/os_OS2.htm.

Kozierok, Charles M. (Abril de 3 2004). Overview and History of NTFS. The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/over.htm

Kozierok, Charles M.. (Abril 3 de 2004). Master File Table (MFT). The PC Guide. Disponible en: http://www.pcguide.com/ref/hdd/file/ntfs/archMFT-c.html.

Leithead, Travis; Richards Mark. (Agosto 20 de 2002). MS-DOS® FAT File System Labs 1 & 2: Help Index. Disponible en: http://students.cs.byu.edu/~cs345ta/labs/winter04_specs/lab_fat_help.htm#How%20DOS%20deletes%20files/directories

Lynch, Michael. (Abril 3 de 2004). The Windows NTFS File System. Disponible en: http://www.qvctc.commnet.edu/classes/csc277/ntfs.html.

Managing Deleted Files. (Abril 13 de 2004). Disponible en: http://www.glencoe.com/norton/onli-ne/ezine/display_article.phtml?id=161

Microsoft Corporation. (Abril 12 de 2004). "Overview of FAT, HPFS, and NTFS file systems". Disponible en L http://support.microsoft.com/default.aspx?scid=kb;en-us;100108 No está citada

Microsoft Corporation. (Abril 12 de 2004). "Recovering NTFS Boot Sector on NTFS Partitions". Disponible en : http://support.microsoft.com/default.aspx?scid=kb;EN-US;q153973

Microsoft Windows 2000 server. (2000). MCSE training kit: Redmond, WA: Microsoft Press, c2000.
Mikhailov, Dmitrey. (Abril 3 de 2004). NTFS File Systrem. Digit-Life.com. Disponible en: http://www.digit-life.com/articles/ntfs/?14227.
NASA (National Aeronautics and Space Administration). (2004, Marzo 21). Clearing Information from your Computer's Hard Drive. Disponible en: www.hq.nasa.gov/office/oig/hq/harddrive.pdf
National Archives of Australia. (Junio 1 de 2002). Protecting and handling magnetic media. Disponible en: http://www.naa.gov.au/récordkeeping/rkpubs/advices/advice5.html
NetworkWorldFusion. (Abril 12 de 2004). "Wipe out" Disponible en: http://www.nwfusion.com/newsletters/techexec/2003/0414techexec1.html No está citada
NTFS (2002). Defining clusters chain for the deleted ntry. Disponibl en: http://www.ntfs.com/assemble-clusters.htm
NTFS (2002). Disk Scan for deleted entries. Disponible en: http://www.ntfs.com/disk-scan.htm
NTFS (2002). NTFS File Types, Disponible en: http://www.ntfs.com/ntfs-files-types.htm
NTFS Basics. NTFS.com. (Abril 3 de 2004). Disponible en: http://www.ntfs.com/ntfs_basics.htm.
NTFS.com. (2002). File Recovery Concepts. Disponible en: http://www.ntfs.com/file-recovery-concepts.htm
NTFS.com. (Abril 3 de 2004). Partition Boot Sector. Disponible en: http://www.ntfs.com/ntfs-partition-boot-sector.htm.
NTFS.com. (Abril 3 de 2004).NTFS Master File Table (MFT). Disponible en: http://www.ntfs.com/ntfs-mft.htm.
NTFS.com. (Marzo 21 de 2004). NTFS vs. FAT. Disponible en: http://www.ntfs.com/ntfs_vs_fat.htm
PC IN. (Marzo 21 de 2004). What does it mean to 'Delete' something?. Disponible en: http://www.pcin.net/help/articles/undelete.php
PC Inspector File Recovery. (Abril 8 de 2004). Disponible en: http://www.pcinspector.de/file_recovery/UK/welcome.htm
Quetek. (Abril 7 de 2004). File Scavenger. Disponible en: http://www.quetek.com/prod02.htm#notice
Richter, Jeffrey. (Abril 3 de 2004). Keeping an Eye on Your NTFS Drives: The Windows 2000 Change Journal Explained. Jeffrey Cooperstein, Microsoft Disponible en :http://www.microsoft.com/msj/0999/journal/journal.aspx.
Roosa, Mark. (s.f.). Magnetic Media Preservation: Selected Bibliography. National Preservation Program Office. Library of Congress. Disponible en: http://palimpsest.stanford.edu/byauth/roosa/roosamag.html
Russinovich, Mark. (Noviembre 19 de 2000). Inside Win2K NTFS. Windows &.net Magazine. Disponible en: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=157
Russon, Richard. (Abril 3 de 2004). Flatcap. File - $Boot (7). Disponible en: http://www.uneraser.com/boot-sector-damaged.htm.
Sedory, Daniel B. (Abril 3 de 2004). A Disk Editor View of the NTFS Boot Récord and Bootstrap Code. Disponible en: http://www.geocities.com/thestarman3/asm/mbr/NTFSbrHexEd.htm .
Sedory, Daniel B. (Abril 3 de 2004). An Examination of the NTFS Boot Récord.

http://www.geocities.com/thestarman3/asm/mbr/NTFSBR.htm.
Sedory, Daniel B. (Abril 3 de 2004). The Bootstrap Code from an NTFS Partition. Disponible en: http://www.geocities.com/thestarman3/asm/mbr/NTLDR.htm.
Sitani, Aditya. (Febrero 3 de 2003). NTFS and FAT32. Disponible en: http://people.msoe.edu/~taylor/cs384/sitania.pdf No está citada
Siyan, Karanjit S. (1996). Windows NT server 4: Professional reference. (1996). New Riders, c1996.
Smith, Jan. (Agosto 27 de 2003). Jan's Ilustrated computer Literacy. Disponible en: http://www.jegsworks.com/Lessons/lesson6/lesson6-2.htm

Bibliografía

Adams, C. (2007). Legal Issues Pertaining to the Development of Digital Forensic Tools. *En Third International Workshop on Systematic Approaches to Digital Forensic Engineering.*
Andrew, M. (2007). Defining a Process Model for Forensic Analysis of Digital Devices and storage media. En *Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (Sadfe'07).*
Branigan, S. (2005). *High-tech crimes revealed*. Addison Wesley.
Cano, J. (2007). Administrando la confidencialidad de la información: algunas consideraciones sobre el saneamiento de medios de almacenamiento. Disponible en: http://www.criptored.upm.es Sección Docencia.
Carrier, B. (2003). Open source digital forensic tools. The legal argument. Disponible en: http://www.digital-evidence.org/papers/opensrc_legal.pdf (Consultado: 18-08-2008).
Carrier, B. (2006). Risks of live digital forensic analysis. *Commun. ACM*. Vol. 49, No. 2. February, pp. 56-61.
Carrier, B. y Grand, J. (2004). A Hardware-Based Memory Acquisition Procedure for Digital Investigations. Digital Investigation Journal. February. Disponible en: http://www.digital-evidence.org/papers/tribble-preprint.pdf (Consultado: 22-12-2008).
Casey, E. (2000). *Digital Evidence and Computer Crime*. Academic Press.
Casey, E. (2001). *Handbook of Computer Crime Investigation*. Academic Press.
Casey, E. y Stellatos, G. (2008). The impact of full disk encryption on digital forensics. *Sigops Oper. Syst. Rev*. Vol. 42, No. 3. April, pp 93-98.
Collins, D. y McGuire, T. (2008). Using the dc3 forensic challenge as a basis for a special topics digital forensics upper level undergraduate course. En *Proceedings of Consortium for Computing Sciences in Colleges.*
Council of Europe (2007). *Cyberterrorism. The use of internet for terrorist purposes.*
Counter-terrorism Task Force. Council of Europe Publishing.
Craiger, P., Ponte, L., Whitcomb, C., Pollitt, M. y Eaglin, R. (2007). Master's degree in Digital Forensics. En *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (Hicss'07).*
Denning, D. (2000). Cyberterrorism. Disponible en: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Consultado: 16-03-2008).
Dixon, L. y Gill, B. (2001). Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases Since the Daubert Decision. Monografía. *RAND Corporation*. Disponible en el Web: http://www.rand.org/pubs/monograph_reports/2005/MR1439.pdf. (Consultado: 19-08-2008).

Garfinkel, S. (2007). Anti-Forensics: Techniques, Detection and Countermeasures. *Proceeding of The 2nd International Conference on i-Warfare and Security (ICIW)*, Naval Postgraduate School, Monterey, CA, March 8-9. Disponible en: http://www.simson.net/clips/academic/2007.ICIOW.AntiForensics.pdf (Consultado: 24-03-2007).

Garfinkel, T. y Rosenblum, M. (2005). When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. Department of Computer Science. Stanford University. Disponible en: http://www.stanford.edu/~talg/papers/HOTOS05/virtual-harder-hotos05.pdf (Consultado: 19-08-2008).

Gordon, S. y Ford, R. (2003). Cyberterrorism. Symantec. White Paper. http://www.symantec.com/avcenter/reference/cyberterrorism.pdf (Consultado: 16-03-2008).

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digital Investigation. Pp 44-49. Disponible: http://www.dfrws.org/2006/proceedings/6-Harris.pdf (Consultado: 24-03-2007).

Hewardt, M. y Pravat, D. (2008). *Advanced Windows Debugging*. Addison Wesley.

Hoglund, G y Butler, J. (2006). *Subverting the windows kernel*. Rootkits. Addison Wesley.

Howard, J. (1997). An Analysis of Security Incidents On The Internet 1989 –1995. Tesis doctoral. Carnigie Mellon University. Disponible en: http://www.cert.org/research/JHThesis/Start.html (Consultado: 16-03-2008).

Leong, R. y Leung, H. (2007). Deriving case-specific live forensics investigation procedures from Forza. En *Proceedings of the 2007 ACM Symposium on Applied Computing (Seúl, Corea, March 11-15, 2007)*. SAC '07, pp. 175-180.

Knetzger, M. y Muraski, J. (2008). *Investigating high-tech crime*. Pearson Prentice Hall.

Kovacich, G. (2000). *High-Technology Crime. Investigator's Handbook.* Butterworth Heinemann.

McDonald, J. T., Kim, Y. C. y Yasinsac, A. (2008). Software issues in digital forensics. *Sigops Oper. Syst. Rev*. Vol. 42, No. 3. April, pp 29-40.

Myers J. L. (2000). *High Technology Crimen Investigation: A Curricular Needs Assesment of The Largest Criminal Justice and Criminology Programs in The United States.* Texas A&M University. Tesis doctoral. Diciembre.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M. y Gagnon, G. (1999). Cyberterror. Prospect and Implications. United States Navy. Naval Postgraduate School. Disponible en: http://handle.dtic.mil/100.2/ADA393147 (Consultado: 16-03-2008).

Parker, D. B. (1976). *Crime by Computer.* Charles Scribner's Sons.

Parker, D. B. (2007). Risks of risk-based security. Commun. ACM. Vol. 50, No. 3. March, p. 120.

Parker, D. B. (2007b). The Dark Side of Computing: SRI International and the Study of Computer Crime. *IEEE Annals of the History of Computing. January-March,* pp, 3-15.

Parker, D. B. y Nycum, S. (1984). Computer Crime. Commun. ACM. Vol. 27, No. 4. April, pp. 313-315.

Peikari, C y Chuvakin, A. (2004).Security warrior. O'Reilly.

Raymond Choo, K. K, Smith, R. y McCusker, R. (2007). Future directions in technology-enabled crime: 2007-09. Research and Public Policy Series. No. 78. Disponible en: http://www.aic.gov.au/publications/rpp/78/rpp78.pdf (Consultado: 16-03-2008).

Riofrío, J. (2004).La prueba electrónica. Temis.

Rollins, J. y Wilson, C. (2007). Terrorist capabilities for cyberattack: Overview and policy issues. CRS Report for Congress. Code: RL33123.

Sammes, T. y Jenkinson, B. (2007). Forensic computing. A practitioner's guide. Second Edition. Springer-Verlag.

Schneier, B. (2003). Beyond fear. Thinking sensible about security in an uncertain world. Copernicus Books.

Shmalleger, F. y Pittaro, M. (2009). Crimes of the Internet. Pearson-Prentice Hall.

Taylor, C., Endicott-Popovsky, B. y Phillips, A. (2007). Forensics Education: Assessment and Measures of Excellence. En Proceedings of Second International Workshop.

Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E. y Liederbach, J. (2006). Digital Crime and digital terrorism. Pearson Prentice Hall.

Unión Internacional de Telecomunicaciones –UIT. (2008). Agenda sobre ciberseguridad global. Disponible. en: http://www.itu.int/cybersecurity/ (Consultado: 16-03-2008).

Walden, I. (2007). Computer crimes and digital investigations. Oxford Press.

Yasinac, A., Erbacher, R., Marks, D., Pollitt, M. y Sommer, P. (2003). Computer forensics Education. IEEE Security & Privacy. July-August.

6

ANEXOS COMPLEMENTARIOS

Objetivos

✓ Complementar los conceptos revisados a lo largo de cada uno de los capítulos, con guías o procedimientos prácticos que puedan ser adaptados por cada uno de los lectores.

INTRODUCCIÓN

En este capítulo se presenta una serie de guías y conceptos prácticos, para los lectores que buscan profundizar en los elementos académicos revisados a lo largo del libro. Cada una de las guías registradas a continuación ha sido analizada y confrontada en la realidad internacional sobre el desarrollo de la informática forense, buscando que los lectores de habla hispana continúen su perfeccionamiento y ajuste, en cada una de las realidades de sus países.

En seguida se hace un breve resumen de cada una de ellas.

Buenas prácticas en la administración de la evidencia digital

Este documento es un compendio de prácticas internacionales en el tema de la evidencia digital, disponibles a la fecha, que busca ofrecer un conjunto de elementos teóricos y prácticos para apoyar procesos donde esta clase de evidencia es fundamental para avanzar en la solución de un caso. Este documento es resultado de las investigaciones adelantadas por el autor de este libro en el Grupo de Estudios en

Comercio Electrónico, Telecomunicaciones e Informática –Gecti– de la Facultad de Derecho de la Universidad de Los Andes.

Nota: Las aplicaciones o los detalles que se relacionan en este documento son recomendaciones o sugerencias académicas, las cuales no pretenden ser un conjunto formal de prácticas que obliguen para demostrar la pertinencia o admisibilidad de una evidencia digital.

Fuentes potenciales de evidencia digital

Es un listado parcial de fuentes potenciales de evidencia digital desarrollado en el contexto de la investigación adelantada por el Dr. Peter Sommer, plasmado en el documento: *Directors and Corporate Advisor's Guide to Digital Investigations and Evidence*, creado para el Information Assurance Advisory Council en el Reino Unido.

Evidencia digital en la práctica

Es un listado de conceptos en el lenguaje técnico que puede ser catalogado como elementos materiales probatorios, y que luego de las diferentes instancias de un proceso, puede ser catalogado como evidencia digital del mismo. Al igual que el listado comentado en el numeral 2, también pertenece a la publicación del Information Assurance Advisory Council.

Características para seleccionar un informático forense

Son un listado de preguntas y conceptos desarrollado por la firma Key Computer Services, Inc., para determinar la idoneidad del informático forense que se contrate para adelantar los análisis que se requieran. Es importante anotar que si bien es una lista detallada de características requeridas, no pretende ser un referente de obligatorio cumplimiento, solamente una excusa académica para valorar las condiciones del servicio de informática forense que se requiere. La lista en inglés está disponible en el Web en: http://www.keycomputer.net/equest.htm

Consejos y sugerencias para los abogados litigantes frente a las pruebas informáticas

Este compendio de consejos y sugerencias ha sido extraído de diferentes fuentes académicas y de la práctica misma de las audiencias donde se han manejado pruebas informáticas. Nuevamente es un conjunto de recomendaciones, que esperamos sean útiles, para los abogados en el

momento de presentar, analizar y controvertir evidencia en formato informático o digital.

Consejos prácticos para sustentar un reporte técnico en una audiencia

Esta lista de recomendaciones y sugerencias se ha extraído de la buena práctica internacional en el tema y de fuentes bibliográficas especializadas, con el único fin de establecer una base de ejercicios y posturas prácticas que lleven a buen término la sustentación de un informe técnico por parte de un testigo experto o un perito informático.

Anexo 6.1

Buenas prácticas en la administración de evidencia digital

Las prácticas relacionadas a continuación se agrupan alrededor de lo establecido en el *HB171:2003 Handbook Guidelines for the management of IT evidence, desarrollado en Australia.*

De acuerdo con lo previsto en el documento referenciado en el párrafo anterior, se detallan el ciclo de administración de evidencia digital y sus respectivos elementos, los cuales se complementan con prácticas (cinco prácticas básicas) y procedimientos que permitan a los responsables establecer directrices claras sobre la administración de esta clase de evidencia.

El ciclo de vida para la administración de evidencia digital consta de seis pasos (*gráfico 6.1*), a saber:

1. Diseño de la evidencia
2. Producción de la evidencia
3. Recolección de la evidencia
4. Análisis de la evidencia
5. Reporte y presentación
6. Determinación de la relevancia de la evidencia

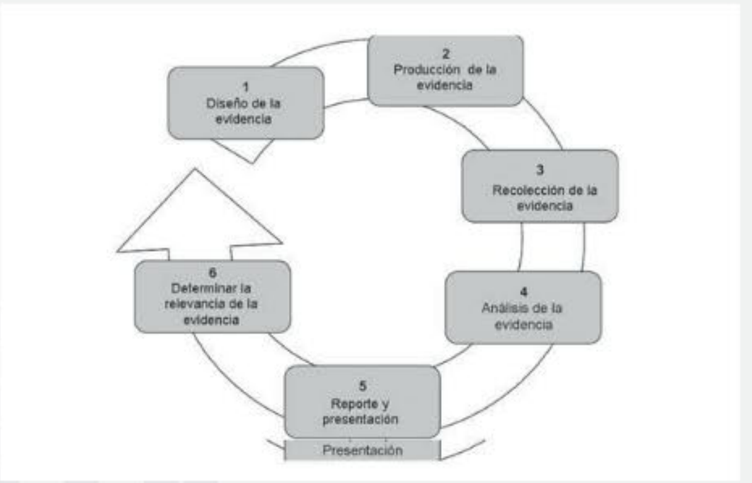


Gráfico 6.1
Ciclo de vida de la administración de la evidencia digital. (Tomado de: HB171:2003 Handbook Guidelines for the management of IT evidence)

Diseño de la evidencia

Concepto

Con el fin de fortalecer la admisibilidad y la relevancia de la evidencia producida por las tecnologías de información, a continuación se detallan cinco objetivos (Standards Australia International 2003, p. 13), que se deben considerar para el diseño de la evidencia digital:

1. Asegúrese de que se ha determinado la relevancia de los registros electrónicos, que éstos se han identificado, están disponibles y son utilizables.
2. Los registros electrónicos tienen un autor claramente identificado.
3. Los registros electrónicos cuentan con una fecha y una hora de creación o de alteración.
4. Los registros electrónicos cuentan con elementos que permiten validar su autenticidad.
5. Se debe verificar la confiabilidad de la producción o la generación de los registros electrónicos por parte del sistema de información.

Prácticas

Para procurar lo establecido por esta primera fase, algunas de las prácticas asociadas son:

1. Clasificar la información de la organización, de tal forma que se pueda establecer cuál es la evidencia más relevante y formal que se tiene. Para ello, las oficinas de archivo o documentación en conjunto con el área de tecnología deben adelantar un estudio de las características de la información que soporta las decisiones administrativas y sus medidas tecnologías de protección, almacenamiento y recuperación posterior.
2. Determinar los tiempos de retención de documentos electrónicos, la transformación de éstos (cambios de formato) y la disposición final de los mismos.
3. Diseñar los registros de auditoría de las aplicaciones, como parte fundamental de la fase de diseño de la aplicación. Este diseño debe considerar la completitud y el nivel de detalle (granularidad) de los registros.

4. Utilización de medidas tecnológicas de seguridad informática para validar la autenticidad y la integridad de los registros electrónicos. Las tecnologías como certificados digitales, *token* criptográficos, entre otras, podrían ser candidatas en esta práctica.
5. La infraestructura tecnológica debe asegurar la sincronización de las máquinas o de los dispositivos que generen la información, de tal manera que se puedan identificar con claridad la fecha y la hora de los registros electrónicos.

Producción de la evidencia

Concepto

En esta fase, de acuerdo con el estándar, se requiere el cumplimiento de los objetivos siguientes (ídem, p. 20):

1. Que el sistema o la tecnología de información produzca los registros electrónicos.
2. Identificar el autor de los registros electrónicos almacenados.
3. Identificar la fecha y hora de creación.
4. Verificar que la aplicación está operando correctamente en el momento de la generación de los registros, bien sea en su creación o modificación.
5. Verificar la completitud de los registros generados.

Prácticas

1. Desarrollar y documentar un plan de pruebas formal para validar la correcta generación de los registros de la aplicación.
2. Diseñar mecanismos de seguridad basados en certificados digitales para las aplicaciones, de tal forma que se pueda validar que es la aplicación la que genera los registros electrónicos.
3. En la medida de lo posible, establecer un servidor de tiempo contra el cual se pueda verificar la fecha y la hora de creación de los archivos.
4. Contar con pruebas y auditorías frecuentes alrededor de la confiabilidad de los registros y su completitud, frente al diseño previo de los registros electrónicos.
5. Diseñar y mantener un control de integridad de los registros electrónicos, que permita identificar los cambios que se hayan presentado en ellos.

Recolección de la evidencia

Concepto

En el ciclo de vida de administración de la evidencia digital, el objetivo de esta fase es localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales (aquellos disponibles y asegurados en las máquinas o los dispositivos) no han sido alterados. Para ello el estándar establece algunos elementos a considerar, como:

1. Establecer buenas prácticas y estándares para recolección de evidencia digital.
2. Preparar las evidencias para ser utilizadas en la actualidad y en tiempo futuro.
3. Mantener y verificar la cadena de custodia.
4. Respetar y validar las regulaciones y normativas alrededor de la recolección de la evidencia digital.
5. Desarrollar criterios para establecer la relevancia o no de la evidencia recolectada.

Prácticas

1. Establecer un criterio de recolección de evidencia digital según su volatibilidad: de la más volátil a la menos volátil (Brezinski, D. y Killalea, T. 2002):
    a. Registros de memoria, memoria caché.
    b. Tablas de enrutamiento, cache de arp, estadísticas del funcionamiento del sistema operacional.
    c. Archivos temporales
    d. Almacenamiento en disquetes, memorias USB, CD, DVD.
    e. Registro remoto de las actividades de la aplicación y monitoreo del tráfico de los datos.
    f. Configuración física de dispositivos y topología de red.
    g. Manuales y registros disponibles de los dispositivos y software bajo estudio.
2. Documentar todas las actividades que el profesional a cargo de la recolección ha efectuado durante el proceso, de tal manera que se pueda auditar el proceso en sí mismo y se cuente con la evidencia de este proceso.

3. Asegurar el área en donde ocurrió el siniestro, con el fin de custodiar el área o la escena del delito, y así fortalecer la cadena de custodia y recolección de la evidencia.
4. Registrar en medio fotográfico o video la escena del posible ilícito, detallando los elementos informáticos allí involucrados.
5. Levantar un mapa o un diagrama de conexiones de los elementos informáticos involucrados, los cuales deberán ser parte del reporte del levantamiento de información en la escena del posible ilícito.

Análisis de la evidencia

Concepto

Una vez se ha recolectado la evidencia, tomado las imágenes de los datos requeridos y su debida cadena de custodia, es el tiempo para iniciar el ensamble, el análisis y la articulación de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación bajo análisis, o establecer si hacen falta evidencias para completar o aclarar los hechos.

Prácticas

a. Hacer copias autenticadas de los registros electrónicos originales sobre medios forenses estériles para adelantar el análisis de los datos disponibles (Information Security and Forensics 2004, p. 23).
b. Capacitar y formar en aspectos técnicos y legales a los profesionales que adelantarán las labores de análisis de datos. Para un posible plan de formación en estos temas, ver: "Estado del arte del peritaje informático en Latinoamérica". http://www.alfa-redi.org/ar-dnt-documento.shtml?x=728
c. Validar y verificar la confiabilidad y limitaciones de las herramientas de hardware y software utilizadas para adelantar los análisis de los datos.
d. Establecer el rango de tiempo de análisis y correlacionar los eventos en el contexto de los registros electrónicos recolectados y validados previamente (US Department of Justice 2004, p. 16).
e. Mantener la perspectiva de los análisis efectuados sin descartar lo obvio, desentrañar lo escondido y validando las limitaciones de las tecnologías o las aplicaciones que generaron los registros electrónicos.

Reporte y presentación

Concepto

El profesional a cargo de la investigación es responsable de la precisión y la completitud del reporte, sus hallazgos y resultados luego del análisis de la evidencia digital o los registros electrónicos. En este sentido, toda la documentación debe ser completa, precisa, comprensiva y auditable.

En este sentido, las prácticas internacionales aconsejan:

a. Documentar los procedimientos efectuados por el profesional a cargo.
b. Mantener una bitácora de uso y aplicación de los procedimientos técnicos utilizados.
c. Cumplir con exhaustivo cuidado con los procedimientos previstos para el mantenimiento de la cadena de custodia.

Prácticas

1. Mantener una copia de la cadena de custodia y de la notificación oficial para adelantar el análisis de los registros electrónicos.
2. Incluir las irregularidades encontradas o cualquier acción que pudiese ser irregular durante el análisis de la evidencia.
3. Preparar una presentación del caso, de manera pedagógica, que permita a las partes observar claramente el contexto del caso y las evidencias identificadas.
4. Detallar las conclusiones de los análisis realizados sustentados en los hechos identificados. Evitar los juicios de valor o las afirmaciones no verificables.
5. Contar con un formato de presentación de informe de análisis de evidencia digital que detalle, entre otros aspectos (US Department of Justice 2004, p. 20), los siguientes:

    a. Identificación de la agencia o la empresa que adelantó el análisis.
    b. Identificador del caso.
    c. Investigador o profesional que ha adelantado el caso.
    d. Identificación de las entidades que han provisto las evidencias.
    e. Fechas de recepción y reporte.
    Lista detallada de elementos recibidos para análisis en

    f. donde se detallen aspectos como serial, marca y modelo.
    g. Breve descripción de los pasos metodológicos seguidos.
    h. Resultados de los análisis en donde se detallen con claridad los hallazgos.
    i. Conclusiones.

Determinar la relevancia de la evidencia

Concepto

En esta fase, el estándar establece valorar las evidencias, de tal manera que se identifiquen las mejores pruebas que permitan presentar, de manera clara y eficaz, los elementos que se desean aportar en el proceso y en el juicio que se lleve. El objetivo es que el ente que valore las pruebas aportadas observe en sus análisis y aportes los objetos de prueba más relevantes, para el esclarecimiento de los hechos en discusión.

En este sentido, el estándar sugiere dos criterios para tener en cuenta (Standards Australia International 2003, p. 26), a saber:

a. *Valor probatorio:* que establece aquel registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación y confiabilidad del sistema.
b. *Reglas de la evidencia:* que establece que se han seguido los procedimientos y reglas establecidas para la adecuada recolección y el manejo de la evidencia.

Prácticas

a. Demostrar con hechos y documentación que los procedimientos aplicados para recolectar y analizar los registros electrónicos son razonables y fuertes.
b. Verificar y validar con pruebas que los resultados obtenidos, luego de efectuar el análisis de los datos, son repetibles y verificables por un tercero especializado.
c. Auditar periódicamente los procedimientos de recolección y análisis de registros electrónicos, de tal manera que se procuren cada vez mayor formalidad y detalles en los análisis efectuados.
d. Fortalecer las políticas, los procesos y procedimientos de seguridad de la información asociados con el manejo de la evidencia digital.

f. Procurar certificaciones profesionales y corporativas en temas relacionados con computación forense, no como signos distintivos de la experiencia de la organización en el área, sino como una manera de validar la constante revisión y la actualización del tema y sus mejores prácticas.

RECOMENDACIONES ADICIONALES

Como profesional a cargo de una investigación, Recuerde que usted:

1. Debe proveer un concepto de los hechos identificados en sus análisis. Usted es un científico, y como tal debe ser concreto y claro en sus afirmaciones.
2. Los reportes que como profesional encargado de una investigación adelante deben ser concretos, libres de la jerga propia de su disciplina, pedagógicos y sobremanera consistentes con los hechos y resultados obtenidos.
3. Si al preparar un reporte de un análisis de datos, considera que puede estar incompleto o no cuenta con las calificaciones y condiciones requeridas para efectuarlo, debe documentarlo en el informe o manifestar esta condición a la parte que ha solicitado sus servicios.
4. Los profesionales que apoyan las labores en el ciclo de administración de la evidencia digital no deben contar con altos niveles de ética, sino con los más altos estándares y niveles de ética, pues en ellos recaen los conceptos sobre los cuales el juez toma sus decisiones.
5. Documéntese muy bien sobre la normatividad y las regulaciones vigentes alrededor del tema de evidencias digitales en su nación, de tal forma que los procedimientos se ajusten a tales disposiciones y las buenas prácticas internacionales.

Anexo 6.2

Fuentes potenciales de evidencia digital

Fuente potencial	Comentarios
Registros de transacciones	Éstos incluyen todas las compras, ventas y otros arreglos contractuales, que son parte del corazón del negocio.
Registros de negocios	Éstos incluyen todos los mencionados en el segmento anterior, y adicionalmente todos los documentos y datos que puedan ser necesarios para el cumplimiento legal y regulatorio.
Tráfico de correo electrónico	Los correos electrónicos pueden proveer potencialmente evidencia de contactos formales o informales.
Computadores personales específicos	Si existe un individuo bajo sospecha, la organización deberá tener la posibilidad de tener acceso a recoger la información de dicho equipo y proceder a efectuar una imagen idéntica del mismo, lo que produce una foto precisa del mismo, para luego, una vez cursadas las autorizaciones del caso, se analice detalladamente dicha imagen.
Medios de almacenamiento externo	Muchos de los computadores tienen características para almacenamiento de información en dispositivos externos, dentro de los cuales se tienen: CD ROMS, DVD, disquetes 3½, cintas, discos externos, memorias USB. En este sentido, es necesario que se identifiquen y aseguren todos éstos para su examen posterior.
Registros de control de acceso	Por lo general, los computadores corporativos y aun los personales tienen mecanismos de autenticación para permitir el acceso o no a los mismos. Usualmente estos mecanismos de control de acceso tienen registros configurados para acciones, como cambio de contraseña, intentos fallidos, otorgamiento de permisos a usuarios, entre otros. En este sentido, estos registros adecuadamente manejados y preservados, son evidencia fundamental para rastrear la actividad en un computador.
Configuración, eventos, errores, otros archivos y registros internos	Todos los computadores tienen archivos que ayudan a conocer cómo opera el sistema operacional y varios programas individuales instalados. En los sistemas Windows, dichas características se encuentran en el registro. Desde esta fuente de información, los especialistas en informática forense pueden descubrir datos relacionados con la actividad reciente en la máquina, como son, entre otros, archivos abiertos y accedidos, contraseñas, cambios en el registro. Es importante anotar que muchos sistemas operacionales también generan errores y otros registros internos de sus fallas.

(Continúa Anexo 6.2)

Registros de actividad en Internet	El computador personal mantiene registros de la navegación en la Web, en la forma de archivos históricos y memoria temporal almacenada en el disco duro, como parte de la configuración de los navegadores. Adicionalmente, las organizaciones cuentan con servicios de red asociadas con dispositivos, como los proxies, los cuales reciben las conexiones internas hacia la Web y las canaliza por un solo punto hacia el exterior. Ambas son algunas de las formas como las organizaciones mantienen la calidad del servicio, y verifican que no se materialicen abusos contra la infraestructura de la organización.
Registros de los antivirus	Estos registros de actividad de control de código malicioso es realizado por el software antivirus previsto para esta labor. En ellos se registran la búsqueda, la detección y los tratamientos de posibles códigos maliciosos. Si bien esta tecnología no es infalible, como ninguna de las mencionadas anteriormente, se recomienda que cualquier actividad o comportamiento sospechoso en la máquina se reporte al área respectiva que atienda estos eventos.
Registros de los sistemas de detección y prevención de intrusos	Como parte de las medidas de seguridad de la información, las organizaciones tienen sistemas de detección y prevención de intrusos. Mientras el primero detecta y registra actividad maliciosa en la red de una organización, el segundo actúa frente a la presencia de dicha actividad, siempre y cuando se le haya configurado para tal fin. Los registros que producen ambos sistemas son útiles para la identificación y la caracterización del intruso, así como el insumo para fortalecer las medidas de seguridad y control de la organización.
Sistemas de respaldos de información	Los registros de backup y sistemas dedicados a efectuar los respaldos de la información son parte fundamental de una infraestructura de tecnologías de de información. Estos archivos son fuentes de evidencia importantes, como puede ser información de sistema en caliente o en vivo, así como lugares para identificar la información que ha sido borrada del sistema en producción en un momento en el tiempo. Al igual que los registros de control de acceso, deben ser bien administrados y protegidos para que sean fuente valiosa de evidencia digital formal.
Registros telefónicos	Los Private Branch Exchanges –o mejor conocidos PBX– cuentan con características extendidas para el registros de sus actividades. Considerando los temas de interceptación de llamadas o de escucha pasiva de las comunicaciones, se presentan dificultades para la presentación de la evidencia extraída de estos dispositivos.
Registros del control de acceso físico	Muchas edificaciones cuentan con sistemas de control de acceso por uso de tarjetas de aproximación o token de acceso. Dichos sistemas se extienden desde las zonas de ingreso hasta las zonas de máxima seguridad de la organización. Los registros que se generan de esta actividad nos permiten complementar las actividades detectadas en los sistemas informáticos, y correlacionar los movimientos de los individuos dentro de la organización.

(Continúa Anexo 6.2)

(Continuación Anexo 6.2)

Registros de mecanismos de seguridad en redes	Los sistemas antispam, los cortafuegos, los sensores de detección de actividad maliciosa, entre otros, generan registros de la actividad de la red y de los individuos en las organizaciones. La correlación de todos ellos, en un escenario de una falla o un incidente de seguridad, es fuente valiosa para comprender lo que ha ocurrido y como estrategia para entender el perfil del atacante. Al igual que los sistemas de respaldo y autenticación, deben ser bien manejados y protegidos para que tengan la eficacia probatoria requerida.

Anexo 6.3

Evidencia digital en la práctica

La evidencia informática que se puede encontrar en un sistema computacional está conformada, entre otros, por los elementos siguientes:

Elemento	Comentario
Contenido	De un archivo, típicamente las palabras y figuras en el documento o reporte, imágenes diseñadas con aplicaciones especiales, una base de datos, o selección de correos electrónicos, páginas Web, archivos descargados entre otros.
Metadatos	Disponible en ciertos archivos. Estos meta-datos son información sobre los datos, que no es visible a simple vista, pero indica entre otros aspectos quién creo el documento, cuántas veces ha sido editado, cuándo se envió a la impresora. Por lo general los productos de Microsoft y Adobe tienen información de metadatos detalladas en sus archivos.
Datos del directorio	Siguiendo con lo anterior, podríamos decir que son los meta-datos del directorio, la información relacionada con lo archivos allí residentes, detalles sobre su nombre, asociaciones de fecha y estampillas de tiempo, así como sobre su tamaño. Dependiendo del sistema de archivos se puede tener mayor o menor información.
Datos de configuración	Esta información sobre la forma como opera una aplicación, donde ubica sus directorios de trabajo, sus archivos principales y las variables de ejecución de su entorno, generalmente se ubica en los sistemas Windows en el registro. En sistemas Linux o Unix, se materializa en archivos en directorios específicos para cada aplicación.
Datos de auditoría (logging data)	Es la información creada por los sistemas informáticos sobre las actividades realizadas por sus usuarios sobre sus módulos o estructuras, siempre y cuando éstas hayan sido configuradas, bien sea por defecto o por el administrador de la misma. Estos registros nos permiten reconstruir la historia, sesiones o archivos que se hayan utilizado recientemente.
Información de los backups	Es la información almacenada por la organización que considera relevante para la operación de la empresa, bien sea, desde el punto de vista de negocio o tecnológico.
Datos recuperados de forma forense	Datos recuperados de los medios de almacenamiento de datos que aparentemente no se encuentra en él, como pueden ser archivos borrados, archivos en el slack space, archivos de intercambio, memorias temporales, fragmentos de archivos, entre otros.
Monitoreo de datos	Material documental obtenido por el monitoreo de conexiones telefónicas o de redes, la cual puede ser datos técnicos del tráfico o el contenido mismo de la información capturada.
Interpretaciones de expertos	Conceptos ofrecidos por especialistas sobre cualquiera de los elementos mencionados previamente.

Anexo 6.4

Características para seleccionar un informático forense

1. ¿Cuáles son las calificaciones del investigador forense contratado?
   ¿El investigador puede testificar en la corte si es necesario?
   - — ¿Ha testificado previamente en una audiencia?
   - — ¿Cuántas pericias forenses ha realizado en el pasado?
   - — ¿Posee alguna certificación en temas de informática forense o similares?
   - — ¿Qué institución ofreció ese entrenamiento?
   - — ¿Cuánto tiempo el investigador ha desarrollado investigaciones? (No solamente cuánto tiempo ha esta la compañía en el negocio).
2. ¿El investigador comprende todas las técnicas y/o los elementos descritos abajo para adelantar una revisión forense informática, o cuenta con el software, el hardware y las instalaciones para adelantar dicha revisión?
   - — El investigador debe estar calificado para ser un testigo experto (perito informático), no el software.
3. ¿El investigador forense está familiarizado con el sistema operativo que va a examinar?
4. ¿El investigador tiene conocimiento sobre la adquisición de datos en medios magnéticos, ópticos o similares, y puede notificarle y apoyarlo para adelantar la recolección de datos en el medio original?
   - — ¿La recolección de los datos es voluntaria o involuntaria?
   - — ¿Qué procedimientos recomienda el investigador forense para preservar los datos originales durante la adquisición de los mismos?
   - — ¿El investigador recomienda procedimientos para reducir la probabilidad de que alguien trate de destruir la evidencia, mientras ésta es recolectada?

5. ¿Qué sugerencias efectúa el investigador forense para preservar el medio original de escrituras o alteraciones accidentales, virus o interrupciones maliciosas?
   - — ¿Estas sugerencias o procedimientos pueden prevenir la introducción de virus o la destrucción accidental de los datos?
   - — ¿El investigador trabaja con una copia idéntica bit a bit?
   - — Si es correcto lo anterior, ¿qué software utiliza para ello?

6. ¿El investigador tiene el conocimiento, la habilidad y el software para recuperar archivos borrados?
   - — ¿Puede dar una explicación sencilla de cómo los archivos son almacenados, borrados y recuperados en un sistema de archivos?
   - — ¿Puede explicar cómo los archivos de nombre largo en Windows son almacenados y recuperados? ¿Pueden ser recuperados?

7. ¿El investigador tiene el conocimiento, la habilidad y el software para darle formato a un disco duro o disquete?
   - — ¿Puede dar una explicación sencilla de qué pasa cuando a un disco duro o a un disquete se le da formato, y cómo los datos pueden ser recuperados, luego de este procedimiento?

8. ¿El investigador tiene el conocimiento, la habilidad y el software para encontrar y recuperar archivos escondidos?
   - — ¿Puede dar una explicación sencilla sobre los métodos utilizados para esconder la información en medios informáticos?

9. ¿El investigador tiene el conocimiento, la habilidad y el software para recuperar archivos protegidos con contraseña?
   - — ¿Puede dar una explicación sencilla sobre los métodos utilizados para proteger los archivos con contraseña?
   - — ¿Puede comentar el tipo de software que utiliza para ello?
   - — ¿Qué estrategias tiene para enfrentar archivos cifrados con RSA, PGP, 3DES u otros cifrarios, así como para quebrar otros esquemas de protección con contraseñas?

10. ¿El investigador tiene el conocimiento, la habilidad y el software para buscar, acceder y traducir el contenido de archivos, como son, entre otros, el de swap, los temporales y el cache?

11. ¿El investigador tiene el conocimiento para ofrecer opiniones claras y precisas sobre la creación, el acceso y el borrado de fechas y temas relacionados?
    - — ¿Qué fechas y tiempos son almacenados en las entradas de los archivos en Windows y Linux?

12. ¿El investigador tiene el conocimiento, la habilidad y el software para recuperar datos en espacios no asignados, que no están enlazados con entradas de directorios conocidos en el disco?
    - — ¿Cómo el investigador hace esto?
    - — ¿Qué software utiliza?

13. ¿Cómo el investigador presentará sus resultados?
    - — ¿Informes impresos?
    - — ¿CD Roms, DVD, USB?
    - — ¿Puede el investigador convertir el formato de los datos originales a un formato que pueda ser útil para usted? (p.e., una hoja de cálculo Microsoft Excel o programa semejante).

14. ¿Qué controles tendrá el investigador en sitio para asegurar la cadena de custodia de cualquier inadecuado manejo de la evidencia recuperada?
    - — El investigador comprende clara y ampliamente las reglas del manejo de la evidencia y lo relacionado con la cadena de custodia, sabiendo con claridad que, de no seguirse los protocolos respectivos, el caso puede comprometerse y perderse.

15. ¿Cuánto tiempo tomará el investigador en entregar el resultado de la pericia?

16. ¿El investigador pertenece a una gran compañía y lo ve como uno de sus clientes, o tendrá atención personalizada para su caso?

17. ¿El informe es claro y explica sin términos técnicos que son entendibles por cualquiera de las partes involucradas?

Anexo 6.5

Consejos y sugerencias para los abogados litigantes frente a las pruebas informáticas

La siguientes son algunas de las preguntas que un abogado litigante debe considerar cuando se adelante la audiencia y se revisen las pruebas informáticas recolectadas, bien por la fiscalía o por un perito de parte contratado.

1. **¿La evidencia extraída del dispositivo informático y utilizada para acusar a mi cliente, ha sido alterada, dañada, se ha corrompido o ha sido modificada en alguna forma mientras ésta estaba siendo obtenida y manejada?**

   Nota: Con esta pregunta La idea es validar los procesos de recolección de evidencia digital en sitio y los momentos de pérdida de evidencia volátil, situación que es viable, cuando el sistema analizado está activo y en funcionamiento.

2. **¿Son auditables todos los procedimientos de investigación forense, en el sentido de que un experto calificado puede seguir y verificar los mismos?**

   Nota: Esta pregunta busca establecer la formalidad y la calidad del perito informático y sus procedimientos aplicados, de tal forma que una inspección independiente pueda validar las actividades adelantadas por el investigador forense que ha realizado la pericia.

3. **¿Existe alguna información que pueda haberse obtenido por la fiscalía durante el examen forense del dispositivo tecnológico que esté cubierto por la protección de la confidencialidad entre el abogado defensor y su cliente?**

   Nota: Esta pregunta busca proteger los temas de intimidad y privacidad propias de la relación cliente-defendido. En este caso, siempre es importante que el investigador forense que contrate la defensa, actúe siempre bajo la supervisión del abogado de la defensa, y así evitar la filtración de la información propia del manejo del caso.

4. **¿Puede la fiscalía demostrar que la cadena de custodia de los datos presentados limita cualquier posibilidad de que tales puedan ser contaminados en cualquier forma?**

   Nota: Esta pregunta va dirigida a evidenciar la fortaleza de la cadena de custodia, el buen uso de los formatos de registro y control, el debido almacenamiento (utilización de medios de almacenamiento estériles) y el transporte de los datos que se han obtenido y permanecen bajo custodia del ente acusador.

5. **¿Es posible considerar que un virus, troyano, o gusano o código malicioso pueda ser activado o se active después de que los datos fueron copiados, causando así una alteración de los mismos?**

   Nota: Este interrogante busca validar las revisiones previas y posteriores que deben adelantar los investigadores forenses en informática con la evidencia, para evitar su contaminación con código malicioso que pueda comprometer la prueba.

6. **¿Puede la fiscalía comprobar que el acusado era el único usuario del computador en cuestión?**

   Nota: Al efectuar esta pregunta se busca desarrollar una duda metódica para evidenciar que su cliente no era la única persona con acceso al dispositivo de tecnología. Es importante anotar que en un ambiente corporativo las cosas pueden ser diferentes, porque los dispositivos tecnológicos, como puede ser el computador personal, se entregan para uso personal del empleado y el cumplimiento de sus deberes.

7. **¿Es posible que los datos utilizados como evidencia, hallados en el computador de mi cliente, hayan sido ubicados allí sin el conocimiento y la aceptación del mismo?**

   Nota: Este cuestionamiento busca revisar la posibilidad de registro o descarga de información, desde lugares remotos vía Internet, de manera automática, por la interacción entre el navegador o cualquier otro programa y el sitio remoto. Si esta posibilidad existe, habrá un escenario de debate y duda que puede favorecer su caso.

8. **¿Usted puede indicarle a esta audiencia qué tipo de medidas de seguridad y control tienen los logs o registros de auditoría que la fiscalía presenta como prueba de los hechos?**

Nota: Esta pregunta busca recabar sobre los mecanismos de protección y aseguramiento de estos registros, los cuales por lo general contienen los rastros de las actividades efectuadas por los usuarios del sistema.

9. **¿Usted, como investigador forense en informática o experto en informática forense, puede ilustrarle a la corte sus credenciales académicas como profesional calificado y los registro legales pertinentes para el ejercicio de su profesión, como lo es su licencia o su tarjeta de ejercicio profesional?**

Nota: Esta pregunta busca determinar el nivel de experiencia y la formalidad que tiene el testigo experto presentado por la fiscalía o la defensa, y así determinar la validez del trabajo realizado, desde la perspectiva legal y profesional.

10. **¿Usted puede probar que la evidencia recolectada y presentada en este juicio cumple con lo establecido en las normas del manejo de pruebas electrónicas vigentes, o sus equivalentes, en la buena práctica internacional?**

Nota: Esta pregunta se puede adaptar o reformular, especificando las normas vigentes para cada uno de los ordenamientos jurídicos de los países de los lectores.

Anexo 6.6

Consejos prácticos para sustentar un reporte técnico en una audiencia

Cuando un investigador forense o experto en informática forense debe sustentar un reporte técnico en una audiencia, deberá observar comportamientos formales y específicos que aumenten su credibilidad, capacidad de persuasión y profesionalismo en la audiencia. Para ello, a continuación se detallan algunas recomendaciones mínimas al respecto.

1. Llegue con anticipación a la hora prevista (se recomiendan al menos 30 minutos antes) de la audiencia, para revisar el escenario, el público y los medios audiovisuales o las ayudas tecnológicas que vaya a requerir para efectuar su presentación.
2. No actuar con miedo o bajo presión de terceros. Cuando el miedo asome en su presentación, enfréntelo, haga una pausa moderada en su discurso y continúe su revisión del informe.
3. Su informe no es infalible, pero ha hecho lo que su buen criterio y lo que la buena práctica le indican, por lo que el resultado de sus análisis puede ser sometido a una revisión de terceros expertos.
4. Sea elocuente y haga uso apropiado del lenguaje, sin caer en la jerga particular de su disciplina. Esto combinado con una adecuada expresión oral y manejo del escenario le dará una presentación clara y contundente.
5. La presentación de sus resultados corresponden a la formalidad ética y profesional. Existe un registro de auditoría detallado de sus actividades realizadas en el desarrollo de la pericia informática adelantada.
6. Su presentación debe ser asertiva, seguro de sí mismo y abierto a los comentarios de terceros. Las preguntas que traten de atacar su dictamen deben ser capitalizadas como refuerzo de la buena práctica aplicada en su pericia, y no como una forma de perder el control de su presentación.
7. Sus apreciaciones en el dictamen deben estar libres (en la medida que sea posible) de juicios de valor sin fundamento. Si se tiene un

juicio de valor, éste debe ser bien fundado, basado en evidencia real y concreta. Evitar a toda costa las suposiciones o las posiciones ambiguas.

8. Preséntese a la audiencia bien vestido y arreglado, de tal forma que proyecte seguridad, confianza y seriedad en el escenario. Algunas veces se recomienda vestir tonos suaves, como una forma de disminuir comportamientos agresivos de la contraparte sugeridos por los tonos fuertes.
9. El perito informático debe estar perfectamente documentado sobre los aspectos legales que revisten su actuación y los alcances de sus declaraciones y procedimientos presentados.
10. Aclarar desde el inicio de la presentación del informe, si sus servicios fueron o no sufragados por una de las partes en litigio, para tener claridad de este asunto. Seguidamente detalle los principios y buenas prácticas utilizadas para el ejercicio pericial realizado, que muestre la formalidad de sus actividades y análisis realizados.
11. Evite ser desviado de la presentación de sus resultados por comentarios imprevistos o mal intencionados del abogado de la contraparte. Atienda y analice el comentario; dé una respuesta consistente y sin ambigüedades, y continúe con la presentación de sus hallazgos.
12. Evite mencionar fuentes bibliográficas específicas como fuente autorizadas en temas que requiera explicar. Busque armonizar las mismas como conjuntos de fuentes consultadas, dentro de los múltiples autores que han revisado y documentado el tema.
13. Recuerde que las pruebas informáticas son pruebas científicas que requieren formalidad en su presentación y validaciones tanto del software como de los procedimientos aplicados para obtener las mismas.
14. Sus palabras deben estar dirigidas a presentar hechos relevantes sobre el objeto de su estudio, evitando énfasis o direccionamiento de sus resultados sobre un tema particular, más allá de lo que sus hallazgos le indiquen.
15. Para terminar su presentación del informe, tómese un momento para resumir su proceso y las conclusiones a las que ha llegado, reiterando el proceso metodológico seguido para llegar a sus resultados.

Apéndice

Para profundizar

Correlación y visualización de bitácoras para el análisis forense

Roberto Gómez Cárdenas, Ph.D

Las bitácoras de eventos (Allen, S. 2001) son un medio para llevar un registro o historial de acontecimientos. El propósito de éstas es registrar toda la información relacionada con un evento para responder a las preguntas quién, qué, cuándo, dónde y por qué. Funcionan como una herramienta para el administrador, proporcionándole información para monitorear las actividades de cierta aplicación, y así poder asegurar las operaciones normales y esperadas.

Aparte del evento reportado (baja de un servidor, autenticación de un usuario, envío de un correo, etc.), una bitácora contiene información sobre la fecha y la hora en que ocurrió el evento, dirección IP de la máquina en que se produjo y, en algunas ocasiones, el número del proceso que lo generó.

La importancia de llevar este registro se hace evidente después de un incidente de cualquier tipo, desde una pérdida accidental de información hasta un ataque dirigido a la organización. En caso de que un ataque suceda, las bitácoras son una valiosa fuente de información para recuperar el activo más importante de las organizaciones, la información, además de apoyar en las tareas de cómputo forense.

A pesar de su gran utilidad, la escritura de bitácoras presenta dos grandes problemas: la falta de estándares con respecto al formato de los mismos y la enorme cantidad de eventos registrados que hace difícil la búsqueda de información.

El primer punto, la falta de un formato estándar, se debe a que los desarrolladores de las aplicaciones determinan el formato y el contenido de la salida. Ya que las bitácoras no están pensadas para ser leídas por el usuario común, no se pone especial cuidado en hacerlas de fácil lectura.

Por otro lado, no hay organismos que regulen el formato de las bitácoras, por lo que la mayoría de las aplicaciones registran los eventos en un formato propietario. Esto significa grandes problemas para los administradores, ya que es necesario aprender el formato particular de cada aplicación. Esto toma especial énfasis si tomamos en cuenta el elevado número de aplicaciones y dispositivos que corren en un sistema y que generan bitácoras. Por supuesto, la industria en algunos casos ha formado

comités para estandarizar los formatos; sin embargo, hay mucho trabajo por hacer.

Actualmente se está trabajando en una propuesta por parte de la CEE (Common Event Expresión) de la mitre, el mismo organismo encargado de la base de datos para la descripción de vulnerabilidades. No obstante, no hay nada definido, tan sólo la invitación a formar parte del grupo de trabajo.

Si a este problema le sumamos que cada una de las bitácoras registra una enorme cantidad de eventos, la lectura regular de las mismas se convierte en una tarea poco factible de realizar. En caso de buscar un evento específico, esto se vuelve aún más difícil.

Se han hecho esfuerzos para proporcionarle al investigador forense técnicas y herramientas para la búsqueda de información en las bitácoras. La tendencia ha sido crear programas conocidos como analizadores de bitácoras. Sin embargo, la palabra analizador es muy ambiciosa para estos programas, ya que su función primordial es tan sólo obtener estadísticas de los eventos.

Las bitácoras pueden ser clasificadas de acuerdo con su procedencia, en bitácoras del sistema, bitácoras de dispositivos de seguridad, bitácoras de dispositivos de red y bitácoras de aplicaciones.

Las bitácoras producidas por el sistema reflejan el estado y las actividades del sistema operativo, así como de algunas aplicaciones que hacen llamadas o utilizan librerías del mismo.

Las bitácoras de aplicación son generadas por programas destinados a cumplir con las necesidades directas de los usuarios; es decir, aquellos servicios que no son propios del sistema operativo.

Las aplicaciones de seguridad más comunes y que ahora forman parte de un mínimo indispensable para estar relativamente protegidos son los *firewalls* y los sistemas de detección de intrusos[1]. Los firewalls son sistemas de filtrado de paquetes típicamente basados en reglas, mientras que los detectores de intrusos complementan la seguridad ya que éstos buscan cualquier tipo de anomalía, llamémosle intrusión, mientras ésta está sucediendo (en el mejor de los casos).

Las bitácoras producidas por dispositivos de red, tales como *ruteadores* y *switches*, proporcionan información sobre los paquetes que entran y salen a una red. Esta información puede ir desde un simple conteo, hasta una clasificación de la proveniencia y el destino de los paquetes con base en direcciones IP.

---

[1]. En adelante, nos referimos a los detectores de intrusos también como IDS por sus siglas en inglés.

1. BITÁCORAS Y CÓMPUTO FORENSE

La principal fuente de datos con la que cuenta el investigador forense son las bitácoras producidas, ya sea por el sistema o las distintas aplicaciones, en donde, en el mejor de los casos, se encuentra registrado cada uno de los eventos y de las acciones llevadas a cabo por los usuarios autorizados o no autorizados.

Uno de los grandes problemas de estas bitácoras, y que dificultan las tareas del analista forense, es la tremenda cantidad de información que se almacena. La mayoría de esta información no es relevante, ya que no está relacionada directamente con la violación del sistema, por lo que la búsqueda de estos eventos se puede comparar con la búsqueda de "una aguja en un pajar".

La reconstrucción de los acontecimientos puede ser vista como una correlación de eventos. Esta correlación se refiere a la asignación de relaciones entre múltiples eventos relacionados directa o indirectamente con un determinado incidente. Estos eventos se encuentran en las bitácoras de distintas aplicaciones y/o dispositivos; por esta razón también pueden encontrarse en distintos formatos y plataformas, incluso pueden reportar síntomas totalmente diferentes.

Antes de que la correlación tenga lugar, los datos deben ser normalizados y filtrados para no perder tiempo con eventos inútiles, o que se lleven a cabo operaciones que pueden ser realizadas en otros componentes. Muchos de los dispositivos de red generan cientos de tipos de eventos para reportar varios síntomas o problemas, por lo que el procesamiento para su correlación puede llegar a ser muy pesado. También es necesario tomar en cuenta la existencia de distintas versiones de las aplicaciones y productos, lo que dificulta en gran medida la caracterización de los eventos, debido a la falta de consistencia entre bitácoras. No debemos olvidar que este problema persiste aun cuando se trate de eventos relacionados con el mismo síntoma.

La normalización de los eventos permite estandarizar la información de las bitácoras, es decir, ajustar la información proveniente de cada bitácora a campos de datos específicos, dependiendo del tipo de evento; de esta manera se pretende que el procesamiento de estos eventos sea más rápido y eficiente que el procesamiento de eventos no normalizados. Para lograr eso, se debe llevar a cabo una traducción mediante una capa de normalización de los datos. Esta capa debe conocer las especificaciones de las bitácoras de cada dispositivo, así como las especificaciones de los datos esperados por un motor de correlación.

Una vez que los eventos son normalizados, se lleva a cabo un proceso de filtrado. El objetivo de este proceso es reducir el número de eventos; esto se hace quitando los eventos que no estén relacionados con el problema, y conservando los eventos relevantes para su análisis posterior. Para alcanzar

este objetivo, cuatro tareas son útiles: compresión, conteo, supresión y generalización (Tiffany, M. 2004).

La compresión se refiere a reducir múltiples ocurrencias del mismo evento a uno sólo, semejante a un contador de eventos. El conteo es muy parecido a la compresión de eventos; sin embargo, éste se refiere a la sustitución de un número específico de eventos similares en un evento único; la diferencia radica en que los eventos no deben ser necesariamente iguales. La supresión asocia una prioridad a los eventos, por lo que si ésta es muy baja, los eventos pueden ser descartados. Por último, la generalización clasifica los eventos dentro de una clase, la cual es reportada en lugar del evento específico.

En resumen, en la capa de filtrado y normalizado, los eventos son reducidos y traducidos de su formato original a un formato normalizado y, posteriormente, enviados a un motor de correlación.

2. CORRELACIÓN DE BITÁCORAS

La correlación de bitácoras hace exactamente lo que su nombre indica, asociar una serie de eventos de forma que nos proporcionen la información que buscamos. De manera más específica, la correlación de eventos puede ser vista como una mejor forma para identificar las acciones de un atacante, analizando los eventos en conjunto, los cuales se encuentran ligados por algún parámetro común.

De acuerdo con Viinikka y otros (2006), los tres principales objetivos de un método de correlación de alertas consisten en reducir el volumen de alertas, mejorar el contenido de las alertas y rastrear ataques que involucran varios pasos. Este último objetivo es de especial interés para la computación forense.

Xu, D. y Ning, P. (2005) mencionan que existen diferentes métodos de correlación de eventos, los cuales se pueden clasificar en las cuatro categorías siguientes:

1. *Basados en similitudes.* Realizan análisis de agrupamiento mediante el cálculo de las similitudes entre los atributos de las alertas.
2. *Basados en escenarios de ataque predefinidos.* Construyen escenarios de ataque mediante la correspondencia de alertas con plantillas predefinidas.
3. *Basados en prerrequisitos y consecuencias.* Crean escenarios de ataque mediante la correspondencia entre la consecuencia de un ataque con el prerrequisito de otro.
4. *Basados en múltiples fuentes de información.* Correlacionan las alertas que provienen de múltiples sistemas de seguridad como firewalls e IDS.

2.1 Basados en probabilidades

En este tipo de métodos, las alertas se correlacionan entre sí, basándose en las similitudes entre sus atributos.

Aunque estas técnicas de correlación basadas en probabilidades son útiles para correlacionar algunas alertas (p. e., se pueden formar grupos de alertas que tienen una misma dirección IP o descripción de alerta), en realidad no permiten descubrir de manera completa las relaciones que existen entre éstas.

Un ejemplo de este enfoque se presenta en Sheppard J.W. y W.R. Simpson (1996), donde se usa la teoría de Dempster-Shafer en la que se combinan las perspectivas de varios espacios de observación. Uno de los beneficios de este método es la capacidad para producir probabilidades para cada problema, por lo que ellos pueden ser fácilmente evaluados y jerarquizados de acuerdo con su nivel de relevancia.

2.2 Basados en escenarios de ataques predefinidos

Los escenarios de ataque predefinidos son patrones de secuencias conocidas que se componen de ataques individuales. Estos métodos encuentran una correspondencia entre las alertas generadas por sistemas de detección de intrusos a pasos de ataques en los escenarios de ataques. Algunos de los enfoques en esta categoría especifican escenarios de ataque a través de lenguajes de ataques, como Statl y Chronicles (Ning, P. 2004).

2.2.1 *Sec*

La SEC es una herramienta de correlación de eventos *open-source* que utiliza un enfoque basado en reglas para el procesamiento de eventos (Vaarandi, R. 2002). Sus principales objetivos de diseño fueron la independencia de la plataforma, de configuración simple, aplicable a una variedad de tareas de correlación de eventos, y de bajo consumo de recursos del sistema.

La SEC está escrita en el lenguaje Perl. La SEC lee los eventos de un archivo y produce eventos de salida mediante comandos especificados por el usuario en la línea de comandos. La SEC utiliza expresiones regulares para el reconocimiento de los archivos de entrada. La configuración de SEC está almacenada en archivos de texto que pueden ser creados y modificados en cualquier editor de textos. Cada archivo de configuración contiene una o más reglas, y se pueden aplicar en paralelo los conjuntos de reglas de diferentes archivos.

Además de encontrar el mapeo entre las reglas definidas y los eventos de entrada, la mayoría de las definiciones de reglas también especifican acciones y opcionalmente una expresión binaria de contextos. Los contextos de la SEC representan el conocimiento que la SEC ha aprendido durante el proceso de correlación de eventos, en el que cada contexto tiene un

cierto tiempo de vida. Los contextos pueden ser utilizados para activar o desactivar reglas dinámicamente en tiempo de ejecución.

La correlación basada en escenarios de ataques predefinidos puede reducir las falsas alarmas, pero tiene como principal desventaja requerir que los escenarios sean especificados previamente por las personas, o que sean aprendidos mediante conjuntos de datos de entrenamiento (Serrano, A. 2003). Asimismo, estos métodos de correlación están limitados a detectar ataques conocidos, por lo cual, a pesar de que el IDS sea capaz de detectar una serie de eventos que componen un ataque complejo, si estos eventos no están predefinidos en un escenario de ataque, entonces es posible que no se detecte el ataque complejo.

Los métodos de correlación basados en escenarios de ataque predefinidos son útiles para identificar una secuencia de pasos que componen un ataque complejo en particular; sin embargo, la principal desventaja que presentan estos métodos es estar restringidos a escenarios de ataques conocidos, por lo cual, si no se tiene especificada una secuencia en particular, entonces es posible que no se detecte el ataque complejo, aun cuando se cuente con los eventos individuales reportados.

Otro de los métodos de correlación que caen dentro de esta categoría son los que utilizan técnicas de aprendizaje supervisado para obtener conocimiento, a partir de conjuntos de datos de entrenamiento (De Souza, I. y otros. 2006). Una vez que el sistema es entrenado, el motor de correlación puede determinar la probabilidad de que dos eventos estén relacionados entre sí. Una de las principales desventajas de utilizar aprendizaje supervisado en un proceso de correlación de eventos es necesitar una fase de entrenamiento con datos previos, lo que es un proceso que consume tiempo. Asimismo, es necesario que se dedique una cantidad de tiempo para la recolección y el etiquetado de los datos de entrenamiento, lo que normalmente tiene que realizar un experto.

A diferencia de un método de correlación en donde no es necesario tener conocimiento de redes neuronales, el usuario de estos métodos de correlación debe tener cierto conocimiento sobre las técnicas utilizadas, lo que puede no ser utilizado por cualquier usuario que no cuente con esta clase de conocimiento de las técnicas utilizadas.

2.3 Basados en prerrequisitos y consecuencias

Los métodos de correlación de eventos basados en prerrequisitos y consecuencias consisten en definir cuáles son las condiciones que deben existir, para que un ataque en particular se pueda realizar, así como cuáles son los resultados que se tienen una vez que ese ataque en particular tiene éxito. De esta manera, las precondiciones de un ataque se comparan con las consecuencias de otro para crear las relaciones entre éstos.

Templeton propuso un método de correlación en el que se describen los ataques como la composición de conceptos abstractos (Templeton, S. y Levitt, K. 2001). Cada concepto debe proveer capacidades específicas a otros conceptos. Para cada concepto se definen las relaciones requeridas entre los valores de atributos de las capacidades, que incluyen detalles, como el tipo de sistema operativo, el número de dispositivo o puerto, etc.

Por otro lado, la capacidad es la información requerida o la situación que debe existir para que un aspecto en particular del ataque pueda ocurrir. Por ejemplo, una conexión telnet exitosa requiere una clave de usuario y contraseña válidas, así como la condición de que el servicio telnet esté disponible en un puerto particular.

Para cada concepto se definen los requerimientos que deben ser satisfechos. Si los requerimientos se satisfacen, entonces el concepto especifica un mapeo desde los requerimientos hasta las nuevas capacidades. Estas capacidades están disponibles para soportar otros conceptos.

Este modelo de correlación se implementó mediante el lenguaje Jigsaw, que provee una herramienta para describir los componentes de los ataques en términos de capacidades y conceptos. El Jigsaw tiene características que dificultan la correlación de eventos; éstas son las siguientes:

1. Requiere que todas las precondiciones de un ataque sean satisfechas de manera que se puedan considerar sus consecuencias. En la práctica, esto es difícil, ya que si el sistema que reporta los eventos no detecta alguno de los ataques de las precondiciones, entonces es posible que el Jigsaw no correlacione la información.
2. Los eventos se tratan de manera independiente y no se correlaciona un evento si no es la precondición de un evento posterior.

Los métodos de correlación basados en prerrequisitos y consecuencias tienen varias ventajas, como las siguientes:

1. Se tiene una representación de alto nivel de los eventos correlacionados que revela las relaciones entre éstos.
2. Se puede reducir el impacto de falsas alarmas al proveer una manera para diferenciar los eventos. Debido a que los eventos maliciosos tienen más probabilidades de ser correlacionados con otros eventos, entonces los eventos que no corresponden con ataques verdaderos, tienen menos probabilidades de ser correlacionados entre sí.
3. No se tiene dependencia con escenarios de ataque predefinidos para descubrir secuencias de ataques relacionados.
4. Se tiene una representación intuitiva de los eventos correlacionados, que revela la estrategia de alto nivel de los ataques reportados.

Como se mencionó anteriormente, los métodos de correlación basados en prerrequisitos y consecuencias son útiles para descubrir las relaciones entre los eventos reportados, al asociar las condiciones que deben existir para que un ataque se pueda llevar a cabo con las consecuencias de otro que ya ocurrió. Sin embargo, Ning (Ning, P. y otros 2004) menciona que este tipo de método de correlación presenta las desventajas siguientes:

1. Este método de correlación depende del sistema que genera los eventos (p. e., un IDS). Si el IDS no detecta un ataque crítico que enlace dos pasos en una serie de ataques, entonces es posible que se formen dos conjuntos de eventos que no estén relacionados entre sí.
2. En el caso extremo de que el sistema que reporte los eventos no detecte ningún ataque, entonces el mecanismo de correlación no hace nada.
3. Esta clase de mecanismos no es completamente efectiva para eventos entre los que no existe una relación de *prepares-for,* incluso si las alertas están relacionadas.
4. El rendimiento de este mecanismo depende de la calidad de los modelos; esto es, de la definición de los prerrequisitos y las consecuencias de los ataques. Es difícil realizar correlación cuando el modelo de ataques es débil o inconsistente.

Además, se tiene que considerar que el atacante no necesariamente realiza ataques previos para preparar un ataque posterior, aun cuando el ataque posterior tiene ciertos prerrequisitos. Por ejemplo, un atacante puede realizar un ataque individual contra un servicio aleatorio, sin siquiera saber si el servicio existe.

2.4 Basados en múltiples fuentes de información

Los sistemas de correlación de alertas de seguridad basados en múltiples fuentes de información analizan los eventos que se generan en distintas fuentes, como pueden ser IDS, firewalls, antivirus, etc. La utilización de estos sistemas de correlación provee información muy valiosa, ya que se tienen datos que provienen de distintos dispositivos, en donde cada uno se especializa en proteger un componente particular del sistema, por lo que se puede entender de mejor manera la forma como se realizan los ataques. Aunque esta clase de correlación es muy útil, para realizarla correctamente, se requiere considerar que cada dispositivo de seguridad puede utilizar una manera distinta para generar eventos de seguridad (Ning, P. 2004).

La función de correlación está basada en el principio de que el intruso busca alcanzar un objetivo, pero éste generalmente no puede ser alcanzado en un solo paso, sino que debe llevar a cabo una serie de pasos para llegar al mismo. El objetivo de la función de correlación es obtener un conjunto de planes candidatos que corresponden a una posible intrusión.

Este tipo de métodos utiliza alguna técnica de inteligencia artificial o una combinación de ellas para llevar a cabo la correlación. Los sistemas basados en inteligencia artificial tienen la ventaja de aprender; esto elimina la necesidad de conocimiento del experto de los métodos anteriores.

De entre las técnicas usadas podemos mencionar las redes bayesianas, a través de las cuales es posible representar relaciones causales de eventos, que es precisamente la relación que tienen los problemas con los síntomas. Una red bayesiana es una gráfica dirigida no cíclica en la que los nodos son variables aleatorias, y las flechas indican que la fuente ejerce influencia directa sobre el destino. Estas redes han sido usadas para detectar ataques DDOS[2], por poner un ejemplo (C. Howson y P. Urbach 1989).

Las redes neuronales son uno de los exponentes principales de la inteligencia artificial. En un estudio (H. Wietgrefe, K.D. Tuchs, K. Jobmann, G. Carls, P. Froelich, W. Nejdl y S. Steinfeld 1997) se propone una red neuronal conocida como Cascade Correlation para correlacionar alarmas con una técnica denominada aprendizaje inverso. Con el uso de esta técnica, los autores alegan que todos los diagnósticos generados por el sistema son correctos; sin embargo, no siempre se llega a un diagnóstico.

Como podemos ver, hay muchas técnicas de inteligencia artificial que pueden ser usadas para descubrir la forma como un ataque fue llevado a cabo. Éstas presentan algunas ventajas sobre los métodos deterministas; la principal es que no se depende continuamente del conocimiento de un experto para la creación de firmas o escenarios, según sea el caso.

No obstante, la inteligencia artificial siempre introduce cierto grado de incertidumbre en el sistema, ya que es casi imposible predecir la forma como se llegó a una solución. Esto toma importancia en el momento de presentar los resultados en una corte, ya que para que el analista forense tenga credibilidad, debe ser capaz de repetir el proceso con el cual llegó a la conclusión de la forma como fue llevada a cabo la intrusión.

3. VISUALIZACIÓN DE EVENTOS

Los administradores de sistemas necesitan monitorear constantemente sus redes para garantizar la seguridad y la estabilidad de las mismas. Esta tarea de monitoreo se puede realizar mediante el despliegue de cierta información acerca del tráfico de una red en manera de texto, y leyendo esta información. Por infortunio, la cantidad de datos capturados en la red que generalmente se necesita analizar tiende a ser muy grande, y el análisis textual de esta información puede no ser adecuado en ciertos casos.

La idea de aplicar técnicas de visualización en el campo de seguridad informática es reciente. Las herramientas visuales tienen como objetivo el aprovechar las capacidades de procesamiento visual y de reconocimiento de patrones que poseen los seres humanos.

[2] Distributed Denial of Service: Tipo de ataque en el que los servicios de la red o de ciertos servidores quedan indispuestos mediante el envío masivo de tráfico inútil desde diversas fuentes.

Se han desarrollado varias técnicas para desplegar datos de eventos y así realizar análisis de seguridad, de manera que ciertas acciones maliciosas u otro tipo de amenazas se puedan detectar y ser mitigadas. Asimismo, el análisis de alertas de seguridad ha cambiado de la detección de simples ataques a la detección de ataques complejos que involucran varias acciones. La mayoría de las técnicas de visualización de eventos de seguridad se enfocan en la representación de datos de red, bitácoras almacenadas en archivos de texto, etc.

La visualización es útil para guiar un proceso de análisis de datos complejo, ya que la visualización es particularmente buena para mostrar una vista general de los datos que pueden dirigir la atención del analista a los aspectos de la información que requieren más investigación. La habilidad para mostrar los detalles en un contexto determinado es muy poderosa, y esto se puede lograr mediante técnicas de visualización.

Cualquier red expuesta a Internet comúnmente es escaneada o atacada tanto manual como automáticamente. Los intrusos frecuentemente escanean rangos enteros de puertos que puedan ser atacados para tener acceso a un sistema. Los gusanos y los virus normalmente atacan puertos específicos. Todos estos ataques son registrados en bitácoras de seguridad, pero el análisis manual de éstas es una tarea que consume tiempo; por eso se han realizado varios intentos para facilitar la detección de información interesante contenida en estas bitácoras.

Las gráficas de ataque (S. Mathew y otros 2006) se proponen como un método para analizar debilidades en las redes y ayudar en el entendimiento y la detección de ataques complejos. La generación de las gráficas de ataque frecuentemente requiere modelos que representen los recursos de una red y sus servicios, lo que puede ser una tarea que lleve mucho tiempo para realizarse. En este tipo de gráficas se requiere una enumeración exhaustiva de todos los posibles ataques para diferentes plataformas, y se requieren todas las posibles combinaciones de los ataques representados en la gráfica. Los ataques pueden ser combinados en diferentes formas novedosas, por lo que la enumeración de todas estas posibles combinaciones no es posible.

La mayoría de las técnicas de visualización de datos de seguridad se enfocan en la representación de datos de red, archivos de bitácoras en forma de texto, eventos y alertas de intrusiones así como de datos de flujo de red.

3.1 Herramientas de visualización

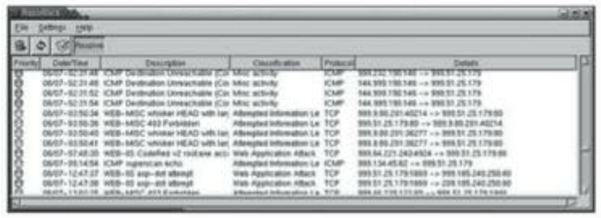
Existen diferentes herramientas de visualización de información de seguridad que permiten analizar no sólo los eventos reportados, sino también otros aspectos de la red, como la cantidad de tráfico o datos transmitidos o el estatus de un sistema. Sin embargo, la mayoría de éstas se encargan de mostrar estadísticas de los eventos reportados o relaciones entre las máquinas involucradas, sin indicar de manera resumida los ataques que se realizaron.

Estas herramientas aprovechan las capacidades visuales de las personas para analizar la información más rápidamente y con menor esfuerzo que si se tuviera que analizar de manera textual. A continuación, presentamos un breve resumen de las herramientas más utilizadas.

3.1.1 *RazorBack*

Ésta es una herramienta que lee información generada por Snort y la despliega en una ventana gráfica (InterSect Alliance. s.f.). Snort es un sistema de detección de intrusos basado en red que se instala en un sistema en una red. Snort realiza tareas de *sniffing* y de creación de bitácoras. El funcionamiento de Snort está controlado por un conjunto de reglas desarrolladas por los usuarios. Snort puede generar alertas en tiempo real. Por lo general, tan pronto como se detecta un nuevo ataque en Internet, se crea una nueva regla que permita identificar este ataque. Estas nuevas reglas se publican en Internet para que los usuarios de Snort las descarguen y las instalen en sus sistemas.

RazorBack provee una *GUI* que permite seleccionar el archivo generado por Snort y representar la prioridad de cada alerta y/o evento por un círculo de color (*ver gráfico A6.1*). Aunque esta herramienta provee una *GUI* que permite trabajar con la información, en realidad solamente despliega la información en texto y no existe alguna diferencia con utilizar los comandos less o more de *UNIX* .



a. RazorBack. b. SnortSnarf y ACID

Gráfico A6.1

Las herramientas RazorBack y SnortSnarf y ACID

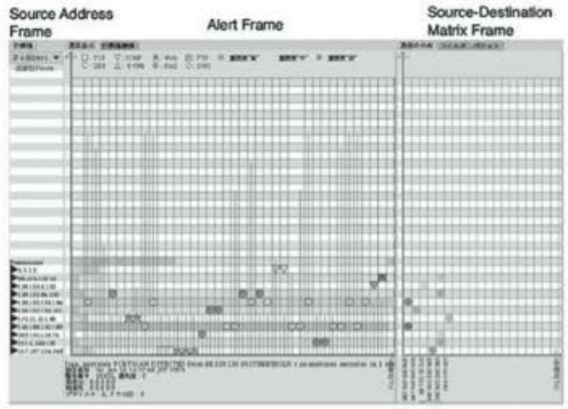
3.1.2 *SnortSnarf y ACID*

SnortSnarf y ACID (Rafeeq Rehman, 2003) son herramientas que permiten analizar las bitácoras producidas por Snort y generar información estadística en código *HTML* (*ver* 6A.1b). SnortSnarf realiza un análisis estadístico de todos los eventos al mismo tiempo, por lo que el análisis en tiempo real de esta información es difícil. Aunque *ACID* realiza análisis en tiempo real, los administradores aún tienen que leer y entender los resultados que están representados en forma de texto.

3.1.3 *SnortView*

SnortView es una herramienta para el monitoreo de ataques en tiempo real y el reconocimiento de falsas alarmas (Koike, H., Ohno, K. 2004). Este sistema está compuesto por dos módulos: análisis de bitácoras y visualización. El módulo de análisis de bitácoras lee la salida producida por syslog y Snort. La utilería syslog se emplea en varias aplicaciones para registrar información del sistema, de manera que sirva como evidencia acerca de actividades maliciosas que fueron realizadas.

SnortView integra las bitácoras tanto de *syslog* como de *Snort* en un solo formato, en el que cada evento es ordenado de acuerdo con el tiempo en el que ocurrió, y para esto se utiliza un diagrama de tiempo en el que cada ataque se representa como un icono cuya forma y color indican el tipo y la prioridad del ataque (*ver gráfico A6.2*).



a. Snort View
b. Spinning cube of potential doom

Gráfico A6.2

Las herramientas SnortView y Spinning cube of potential doom

Esta herramienta le permite al usuario identificar un evento que de otro modo hubiera podido pasar inadvertido; por ejemplo, en el caso de que se tuviera que analizar el archivo de bitácoras línea por línea. Entre las principales ventajas de *SnortView* está la de tener capacidad de monitoreo en tiempo real y ayudar a reducir el tiempo que se tiene que invertir para analizar la información, ya que no es necesario leer miles de líneas en un archivo de texto de manera manual. Una limitante de *SnortView* es que la cantidad de información que puede presentar en la pantalla es limitada.

3.1.4 *Spinning cube of potential doom*

Ésta es una herramienta de visualización tridimensional (Stephen Lau, 2004) que despliega la información en un cubo de acuerdo con las conexiones *TCP* establecidas y a los intentos de conexión (gráfico A6.2b). El eje x del cubo representa las direcciones IP de una red local, el eje z representa las direcciones IP de la red externa, y el eje y representa los números de puertos *TCP*.

Cada conexión TCP es desplegada como un punto cuyo color es blanco si corresponde a una conexión establecida, o tiene un color diferente de acuerdo con el número de puerto del intento de conexión. De esta manera, se enfatizan los intentos de conexión y se detectan fácilmente los intentos de escaneos de puertos, ya que se muestran en el gráfico como zonas de colores.

3.1.5 *Starmine*

STARMINE es una herramienta de visualización de información de seguridad que combina las siguientes tres vistas: geográfica, lógica y temporal (Hideshima, Y. y Koike, H. (2006). En el monitoreo de amenazas cibernéticas, la visualización geográfica es una de las más populares, ya que se puede utilizar un mapa del mundo para mostrar estadísticas de ataques por país, región o continente. Mediante este mapa, se puede determinar qué ataques están activos en el mundo, o cuántos se observan por región. Incluso en el mapa se pueden trazar las direcciones fuente y destino involucradas en el ataque. Sin embargo, algunos de los gusanos de Internet utilizan un algoritmo de propagación llamado *local scan*, que utiliza dirección IP para seleccionar el siguiente objetivo. Por eso en estos casos es más conveniente conocer las relaciones lógicas que la información geográfica.

La visualización lógica se enfoca en la representación de las relaciones lógicas entre las direcciones *IP* involucradas (*ver gráfico A6.3*). La visualización temporal, particularmente el diagrama de tiempo, también es útil para la representación de amenazas cibernéticas. En un diagrama de tiempo, el eje x puede indicar el tiempo y el eje y puede indicar el número de ataques realizados; de esta manera se pueden entender los cambios de los ataques con el tiempo; sin embargo, esta representación no permite visualizar el origen o el destino de los ataques.

3.1.6 *Visual*

VISUAL es una herramienta de visualización de información en dos dimensiones. Esta herramienta se enfoca en el desplegado de las comunicaciones entre la red local que el administrador quiere monitorear y el exterior (Le Malécot, E. y otros 2006). La red monitoreada es representada por una malla cuyos cuadriláteros representan dispositivos. Los dispositivos externos están representados por marcadores alrededor de la malla. Las conexiones

entre los dispositivos internos y externos están representadas por segmentos que enlazan los marcadores con los cuadriláteros asociados. El color de un segmento indica si la comunicación es bidireccional o unidireccional. El ancho de banda de la comunicación está representado por el tamaño de los marcadores.

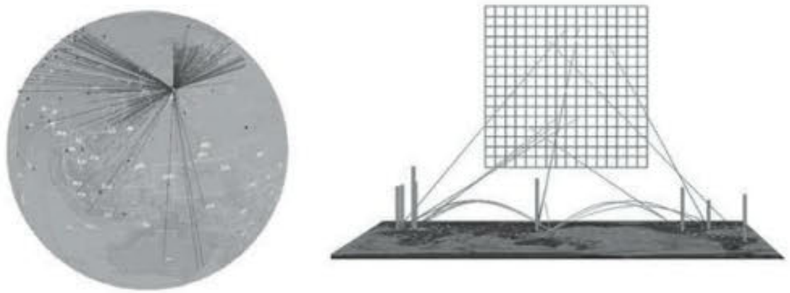


Gráfico A6.3
Starmine

Esta herramienta provee una vista de las interacciones entre una red monitoreada y una red externa; sin embargo, el número de dispositivos externos que puede ser representado es limitado. Además, no se despliega la actividad interna de la red monitoreada, a pesar de que un gran número de ataques se origina en el interior de ésta (*gráfico A6.4*).

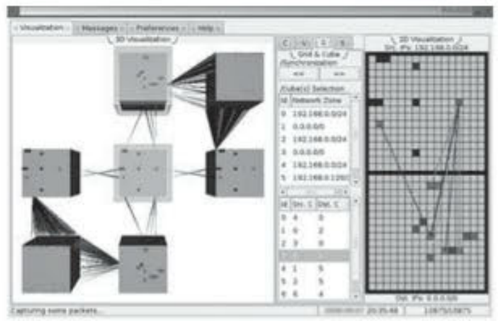


Gráfico A6.4
Visual

Conclusiones

Las bitácoras son la fuente de información que los investigadores forenses utilizan más, por lo que es importante contar con las herramientas necesarias para aprovechar la información contenida dentro de éstas.

La correlación de eventos le permite al investigador forense conocer la información relacionada con el incidente que se está investigando, mientras que la visualización del contenido de las bitácoras le proporciona al investigador una visión global del sistema.

Existen diferentes herramientas y técnicas para la visualización y la correlación de eventos, pero no hay que olvidar que estas herramientas no reemplazan el sentido común y la experiencia de un analista forense; tan sólo le ayudan en su tarea.

Tampoco hay que olvidar que es importante garantizar la seguridad de las bitácoras en sí. Existen diferentes esquemas que permiten el cifrado para garantizar la confidencialidad y la integridad de éstas.

✓ ***Resumen:*** Las bitácoras de eventos sirven para llevar el registro o historial de acontecimientos. Según su procedimiento pueden ser bitácoras del sistema, bitácoras de dispositivos de red y bitácoras de aplicaciones.

✓ ***Términos clave:*** Correlación de bitácoras, escenarios de ataques, eventos normalizados, fuentes de información, ruteadores, switches.

Referencias*

Allen, S. (2001). "Importance of Understanding Logs from an Information Security Standpoint," Tech. rep., SANS Institute.

De Souza, I. y otros. (2006). "Detection of Complex Cyber Attacks". *En Proceedings of the SPIE 2006.* EUA.

Hideshima, Y. y Koike, H. (2006) "Starmine: A Visualization System for Cyber Attacks". En *Proceedings of the Asia Pacific symposium on Information visualization.* Vol. 60. Australian Computer Society Inc. Australia.

Howson, C. y P. Urbach, (1989). Scientific Reasoning: the Bayesian Approach. La Salle, CO: Open Court Publishing Company.

InterSect Alliance. (s.f.). Razorback –snort network intrusion detection front-end. URL: http://www.intersectalliance.com/projects/RazorBack/.

Koike, H., Ohno, K. (2004). "SnortView: Visualization System of Snort Logs" en Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security VizSEC/DmSEC'04. ACM Press. EUA.

Le Malécot, E. y otros. (2006) "Interactively Combining 2D and 3D Visualization for Network Traffic Monitoring". En VizSEC'06. EUA.

Mathew, S., y otros. (2006). "Understanding Multistage Attacks by Attack-Track Based Visualization of Heterogeneous Event Streams". En VizSEC'06. EUA.

Ning, P. (2004). "Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems". *En ACM Transactions on Information and System Security (Tissec).* Vol. 7. EUA.

Ning, P. (2004). "Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems". *En ACM Transactions on Information and System Security (Tissec).* Vol. 7. EUA.

Ning, P. y otros. (2004). "Techniques and Tools for Analyzing Intrusion Alerts" en ACM Transactions on Information and System Security (Tissec). Vol. 7. Issue 2. Pp. 274-318. ACM Press, EUA.

Rafeeq Rehman, (2003). Intrusion Detection with SNORT: Advanced IDS Techniques Using Snort, Apache, ySQL, PHP, and ACID, Chapter 6, Ed. Prentice Hall.

Serrano, A. (2003). Integrating Alerts From Multiple Homogeneous Intrusion Detection Systems. Tesis de maestría. North Carolina State University. EUA.

Sheppard J.W. y W.R. Simpson, (1996). "Improving the Accuracy of Diagnostics Provided by Fault Dictionaries". En Proceedings of the 14th IEEE VLSI Test Symposium.

Stephen Lau (2004). "The Spinning Cube of Potential Doom", Communications of the ACM. Vol. 47, Issue 6, June 2004

Templeton, S. y Levitt, K. (2001). "A Requires/Provides Model for Computer Attacks". En Proceedings of the 2000 workshop on New security paradigms. Pp. 31- 38. ACM Press. EUA.

Tiffany, M. (2004). Computer World, "A survey of Event Correlation Techniques and Related Topics". October 2004, http://www.cc.gatech.edu/fac/Russell. Clark/papers/tiffany-netman.html.

Vaarandi, R. (2002). "SEC –A lightweight Event Correlation Tool". En IEEE Workshop on IP Operations and Management IPOM. Pp. 111-115 IEEE.

* Referencias de la sección Para profundizar. (N. del E.).

Viinikka, J. y otros. (2006). "Time Series Modeling for IDS Alert Management". En Proceedings of the 2006 ACM Symposium on Information, computer and communications security. Pp. 102-113. ACM Press. EUA.

Wietgrefe, H., K.D. Tuchs, K. Jobmann, G. Carls, P. Froelich, W. Nejdl y S. Steinfeld. (1997). "Using Neural Networks for Alarm Correlation in Cellular Phone Networks". En International Workshop on Applications of Neural Networks to Telecommunications (Iwannt).

Xu, D., Ning, P. (2005). "Privacy-Preserving Alert Correlation: A Concept Hierarchy Based Approach". En 21st Computer Security Applications Conference.

Bibliografía

Asociation of Chief Police Officers (1999). Good practice guide for computer based evidence. http://www.digital-detective.co.uk/documents/acpo.pdf. (Consultado: 22-04-2006).

Brezinski, D. y Killalea, T. (2002). RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. http://www.rfc editor.org/rfc/rfc3227.txt

Cano, J. (2003). Admisibilidad de la evidencia digital: Algunos elementos de revisión y análisis. *Revista Electrónica de Derecho Informático*. No. 61. Agosto. http://www.alfa-redi.org/rdi-artículo.shtml?x=1304. (Consultado: 22-04-2006).

Information Security and Forensics. (2004). Computer forensics. Part 2. Best practices. http://www.isfs.org.hk/publications/ComputerForensics/ComputerForensics_part2.pdf. (Consultado: 22-04-2006).

International Organization of Computer Evidence –Ioce. (2002).. Guidelines for the best practices in the forensic examination of digital technology. http://www. ioce.org/2002/ioce_bp_exam_digit_tech.html. (Consultado: 22-04-2006).

Standards Australia International. (2003). HB171: 2003 *Handbook Guidelines for the management of IT evidence.*

US Department of Justice. (2004). Forensic examination of digital evidence. A guide for law enforcement. Special Report.