



DIGITAL FORENSICS WITH OPEN SOURCE TOOLS⁽¹⁾, XBOX 360 FORENSICS⁽²⁾, ANDROID FORENSICS⁽³⁾, e IPHONE AND iOS FORENSICS⁽⁴⁾

Autores: Cory Altheide y Harlan Carvey⁽¹⁾; Steven Bolt⁽²⁾; Andrew Hoog⁽³⁾; y Andrew Hoog y Katie Strzempka⁽⁴⁾
Editorial: Syngress
Año: 2011
ISBN: 978-1-59749-586-8⁽¹⁾, 978-1-59749-623-0⁽²⁾, 978-1-59749-651-3⁽³⁾ y 978-1-59749-659-9⁽⁴⁾
www.syngress.com

esencia, se explican también las diferencias con respecto a un PC a la hora de descifrar la información en estas plataformas, y se describe la utilización de herramientas convencionales y no convencionales en su investigación forense.

Respecto a las entregas tercera y cuarta, *Android Forensics* e *iPhone and iOS Forensics*, ambas están dedicadas, en sus respectivos campos, a brindar una visión completa de las plataformas analizadas, incluyendo el análisis de los componentes hardware y software, y de las estructuras de datos y sistemas de archivos, así como diversas consideraciones de seguridad de la información, una detallada visión de las técnicas forenses y una relación de estrategias para el requerido análisis subsiguiente. Ambos libros están articulados en siete capítulos.

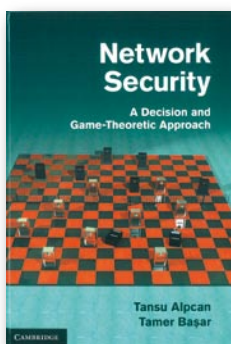
La editorial Syngress ha publicado, dentro de una serie dedicada al análisis forense, estos cuatro libros que abordan el tema desde la perspectiva de cuatro escenarios distintos: la práctica digital con herramientas de código abierto; la consola Xbox 360; el sistema operativo Android; y los dispositivos iPhone y los basados en el sistema operativo iOS.

El primero del cuarteto, *Digital Forensics with Open Source Tools*

(9 capítulos y 1 apéndice) se adentra en el análisis e investigación de sistemas informáticos con herramientas de código abierto. Se presenta como una guía de procedimientos técnicos y explica el uso de estas herramientas en sistemas Linux, Windows y Mac, haciendo especial hincapié en las herramientas gráficas de código abierto y de líneas de comando.

En cuanto al libro dedicado al análisis forense para máquinas

Xbox 360, *Xbox 360 Forensics* (11 capítulos y 4 apéndices), se parte de la idea de que estos dispositivos ya no se pueden considerar solo consolas de videojuegos, al poder conectarse también a Internet, visualizar películas o transferir archivos. Por ello, en este volumen se provee de un mapa de actuación forense a seguir y se constatan todos los avances en este sentido surgidos desde el primer estudio de investigación sobre Xbox. En



NETWORK SECURITY A Decision and Game- Theoretic Approach

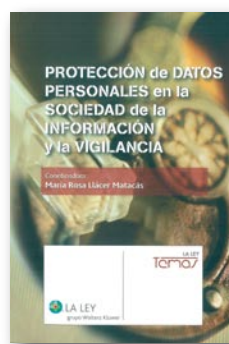
Autores: Tansu Alpcan y Tamer Başar
Editorial: Cambridge University Press
Año: 2011 – 314 páginas
ISBN: 978-0-521-11932-0
www.cambridge.org

La protección de los sistemas de red es de importancia indiscutible desde el comienzo de la era de la información, pero ciertamente no se ha de tratar solamente como un problema de ingeniería a resolver mediante el diseño de mejores protocolos, lenguajes o algoritmos, sino que requiere de la formación de los usuarios y las organizaciones, un cambio de perspectivas y la dotación con mejores herramientas para evaluar y abordar los problemas de seguridad de las redes.

El presente libro tiene como objetivo presentar unas bases teóricas para la toma de decisiones de asignación de recursos que equilibren las capacidades disponibles y los riesgos percibidos de seguridad de una forma responsable. Para ello, se centra en modelos analíticos basados en las teorías de juegos, información, comunicación, optimización,

decisión y control que se aplican a diversos ámbitos de la seguridad. Asimismo, se exponen las relaciones entre los modelos teóricos y los problemas de seguridad del mundo real.

En su estructura, conformada por cuatro grandes apartados, se detiene en una primera introducción básica sobre los conceptos más relevantes en seguridad de las redes; presenta los juegos de seguridad, e ilustra en el uso de varios modelos de la teoría de juegos como forma de cuantificar la interacción entre los ataques maliciosos y las defensas en los sistemas de red; realiza una aproximación en la toma de decisiones de seguridad, y proporciona ejemplos de aplicaciones de modelos cuantitativos de teorías de control y optimización a varios problemas de seguridad; además de estudiar los esquemas distribuidos para la detección de ataques y *malware* descentralizados.



PROTECCIÓN DE DATOS PERSONALES EN LA SOCIEDAD DE LA INFORMACIÓN Y LA VIGILANCIA

Coordinadora: María Rosa Llácer Matacás
Editorial: La Ley
Año: 2011 – 377 páginas
ISBN: 978-84-8126-820-1
www.laley.es

El volumen que aquí se presenta es el resultado del interés compartido por la salvaguarda de los datos personales de los miembros del denominado Gredint (Grup de Recerca en Dret Privat, Consum i Noves Tecnologies), que reúne a profesores de la Universidad de Barcelona, del Instituto de Derecho Comparado de la Universidad Complutense, y de varias universidades belgas e italianas. El debate en torno a la protección de la información personal merece, según los autores del libro, un doble enfoque: un debate jurídico y la difusión social de sus resultados. El objetivo es conseguir una cultura de la privacidad que aúne la conciencia de por qué y cómo proteger los datos personales.

En este contexto, el volumen se articula en dos partes. La primera, rubricada como “La autodeterminación informativa en la sociedad de la información y la vigilancia”, aborda en sus seis capítulos la idiosincrasia de la sociedad de la información; el consentimiento y autodeterminación

informativa según la experiencia italiana; la autodeterminación informativa en la sociedad de la vigilancia; el amparo de la información referida a los menores; los códigos de conducta y buenas prácticas en la gestión de datos personales; y lo referido al respecto en el derecho interno y la jurisprudencia del Tribunal Europeo de los Derechos Humanos y de las Libertades Fundamentales. Por otro lado, la segunda parte del libro, “Aproximación sectorial a la protección de datos personales”, recoge, en otros siete capítulos más, el tratamiento de la información genética en la Ley de investigación biomédica; la protección de los datos personales en Internet y las comunicaciones electrónicas; su aplicación en la sociedad de la información y el marketing; las particularidades del tema con respecto a Facebook y la Directiva 95/46; la obtención, consentimiento y utilización de perfiles económicos; los datos relativos a la salud e historia clínica; y, finalmente, el asesoramiento jurídico al responsable del tratamiento.