BIBLIOGRAFÍA

Análisis forense en sistemas Windows

Raúl Siles, Consultor de seguridad, HP
David Pérez Conde, Consultor independiente de seguridad

PARTE I: "Análisis forense de sistemas de ficheros de Windows"

En la Web

"Forensic Computing & Analysis". Dan Farmer, Wietse Venema.

- *http://www.fish.com/security/forensics.html*
- *http://www.porcupine.org/forensics/*

"TCT: The Coroner's Toolkit". *Dan Farmer,* Wietse Venema.

- *http://www.fish.com/tct/*

"The Sleuth Kit & Autopsy". Brian Carrier.

- *http://www.sleuthkit.org/*

"Forensic Focus: Computer forensics news, information & community".

- *http://www.forensicfocus.com/*

"KYE: Known Your Enemy papers". The Honeynet Project.

- *http://www.honeynet.org/papers/index.html*

"Default Cluster Size for FAT (16) and NTFS". Microsoft KB. ID: 140365. 31 January, 2005.

- *http://support.microsoft.com/default.aspx?scid=kb;en;140365*

"The Default Cluster Size for the NTFS and FAT File Systems". Microsoft KB. ID: 314878. 31 January, 2002.

- *http://support.microsoft.com/default.aspx?scid=kb;en;314878*

"Detailed Explanation of FAT Boot Sector". Microsoft KB. ID: 140418. 6 December, 2003.

- *http://support.microsoft.com/default.aspx?scid=kb;en;140418*

"Description of the FAT32 File System in Windows XP". Microsoft KB. ID: 310525. 14 January, 2004.

- *http://support.microsoft.com/default.aspx?scid=kb;en;310525*

"Limitations of FAT32 File System". Microsoft KB. ID: 184006. 16 December, 2004.

- *http://support.microsoft.com/default.aspx?scid=kb;en;184006*

"Computer Forensic Investigation: Analyze an Unknown Image". GCFA. Raúl Siles. 21 December, 2004.

- http://www.giac.org/certified_professionals/practicals/gcfa/146.php
- http://www.raulsiles.com/downloads/practicals/Raul_Siles_GCFA.pdf

[ESPAÑOL]

"Forensic-es.org: Portal dedicado a la ciencia informática forense".

- http://www.forensic-es.org

"Principio de Intercambio de (Edmund) Locard". Román Ramírez. Mayo 2004.

- http://www.chasethesun.es/docs/locard.pdf

"Principio de indeterminación de Heisenberg". Wikipedia.

- http://es.wikipedia.org/wiki/Principio_de_indeterminaci%C3%B3n_de_Heisenberg

"II Foro de seguridad RedIRIS: Módulo de análisis forense". Rafael Calzada. UCIII Madrid. (17/2/2004).

- http://www.rediris.es/cert/doc/reuniones/fs2004/
- http://www.rediris.es/cert/doc/reuniones/fs2004/archivo/USC-Forense.pdf

" Lista ANAFON: Análisis forense de ordenadores". RedIRIS.

- http://www.rediris.es/list/info/anafon.es.html

"Ausejo.net. Análisis Forense". Rafael Ausejo.

- http://www.ausejo.net/seguridad/forense.htm

"Portal de delitos informáticos".

- http://www.delitosinformaticos.com

"Infoperitos.com". AI2.

- http://www.infoperitos.com

"Delítos informáticos en el Código Penal Español". CNP-BIT.

- http://www.mir.es/policia/bit/legisla.htm

"Convenio sobre la ciberdelincuencia". Consejo de Europa. Budapest. 23 Noviembre 2001.

- http://www.guardiacivil.org/telematicos/formatos/ciberdelincuencia.pdf

"Grupo de delítos telemáticos". Guardia Civil.

- http://www.guardiacivil.org/telematicos/index.htm

"Brigada de Investigación Tecnológica (BIT)". Cuerpo Nacional de Policía.

- http://www.mir.es/policia/bit/index.htm

Libros

- *"Forensic Discovery"*. Dan Farmer, Wietse Venema. Addison-Wesley International. March 2005. ISBN: 0-2016-3497-X

- *"File System Forensic Analysis*". Brian Carrier. Addison-Wesley. March 2005. ISBN: 0321268172
- "*Hacking Exposed Computer Forensics (Hacking Exposed)*". Chris Davis, Aaron Philipp, David Cowen. McGraw-Hill Osborne Media. November 2004. ISBN: 0072256753
- "*Windows Forensics and Incident Recovery*". Harlan Carvey. Addison-Wesley Professional. July 2004. ISBN: 0321200985

Concursos/Desafíos

"The Forensic Challenge". The Honeynet Project. 2001.

- *http://project.honeynet.org/challenge/index.html*

"The Reverse Challenge". The Honeynet Project. 2002.

- *http://project.honeynet.org/reverse/index.html*

"SotM: Scan of the Month challenges". The Honeynet Project. 2000-2005.

- *http://project.honeynet.org/scans/index.html*

"Reto de Análisis Forense". RedIRIS. Diciembre 2004.

- *http://www.rediris.es/cert/ped/reto/*

"Reto Forense v2.0". DSC/UNAM-CERT, RedIRIS IRIS-CERT. Marzo 2005.

- *http://www.seguridad.unam.mx/eventos/reto/*

PARTE II: "Análisis forense de binarios desconocidos de Windows"

En la Web

"Reverse-Engineering Malware". Lenny Zeltser.

- http://www.zeltser.com/reverse-malware-paper/

"Availability and description of the File Checksum Integrity Verifier utility". Microsoft Corporation.

- http://support.microsoft.com/?kbid=841290

"PE Executable Info Viewer & [Utility]". Frederic Rouyre.

- http://www.inter-land.net/~rfr/pexe/

"SotM: Scan of the Month challenge #32". The Honeynet Project. 2000-2005.

- http://www.honeynet.org/scans/scan32/

"The IDA Pro disassembler and Debugger." DataRescue Inc.

- http://www.datarescue.com/idabase/

"Setiri: Advances in Trojan Technology." Temmingh, R. & Meer, H.

- http://www.sensepost.com/misc/bh2002lv.pdf

"OllyDbg". Yuschuk, O.

- http://home.t-online.de/home/Ollydbg/

"Filemon for Windows." Russinovich, M. and Cogswell, B.

- http://www.sysinternals.com/ntw2k/source/filemon.shtml

"Regmon for Windows NT/9x." Russinovich, M. and Cogswell, B

- http://www.sysinternals.com/ntw2k/source/regmon.shtml

"TDIMon." Russinovich, M.

- http://www.sysinternals.com/ntw2k/freeware/tdimon.shtml

"Regshot". TiANWEi.

- http://the7thlab.mybesthost.com/

"BinText."

- http://www.foundstone.com/resources/termsofuse.htm?file=bintext.zip

"The Ultimate Packer for eXecutables". Oberhumer, M. & Molnar, L.

- http://upx.sourceforge.net

"VMware Workstation". VMware, Inc.

- http://www.vmware.com/products/desktop/ws_features.html

"Safe at Home?". David Pérez.

- http://www.giac.org/practical/GCFA/David_Perez_GCFA.pdf

Libros

- *"Malware: Fighting Malicious Code"*. Ed Skoudis, Lenny Zeltser. Prentice Hall PTR. November 9, 2003. ISBN: 0131014056.