Jesse D. Kornblum

Email: research@jessekornblum.com
Web: http://jessekornblum.com/
Twitter: @jessekornblum

Education

M. Eng., Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1999

B.S., Computer Science, Massachusetts Institute of Technology, 1999

Employment

Facebook	2013-Present
Network Security Engineer	Menlo Park, CA
SANS Institute	2011-2013
Instructor, Forensics Track	Bethesda, MD
Kyrus Technology Corporation	2010-2012
Computer Forensics Research Guru	Sterling, VA
ManTech International Corporation	2005-2010
Senior Computer Forensic Scientist	Falls Church, VA
United States Department of Justice, Computer Crime and Intellectual Property Section	2004-2005
Lead Information Technology Specialist	Washington D.C.
United States Naval Academy	2003-2004
Instructor, Computer Science Department	Annapolis, MD
Air Force Office of Special Investigations, Computer Investigations and Operations Division	2003
Chief	Andrews AFB, MD
Air Force Office of Special Investigations, Computer Investigations and Operations Division	2001-2003
Chief of Research and Development	Andrews AFB, MD
Air Force Office of Special Investigations	1999-2001
Computer Crime Investigator	Andrews AFB, MD

Service

Program Committee Member for Malware Memory Forensics Workshop, 2014

Administrator for *Forensics Wiki* project, 2008-Present

Member of the Editorial Board for the journal *Digital Investigation*, 2008-Present

Technical Program Committee Member for Digital Forensic Research Workshop 2005-Present

Technical Editor for *Windows Forensic Analysis* by Harlan Carvey, 2007

Member of the DFRWS Common Digital Evidence Storage Format Working Group, 2005-2007

Awards and Honors

USNA Computer Science Department "Top Geek", Fall 2003

HQ AFOSI Company Grade Officer of the Quarter, 2nd Quarter 2002

Refereed Papers

J. Kornblum, *Implementing BitLocker Drive Encryption for Forensic Analysis*, Digital Investigation, 5(3): 75-84, March 2009.

J. Kornblum, *Auditing Hash Sets: Lessons Learned from* Jurassic Park, Digital Forensic Practice, 2(3):108-112, July 2008.

E. Libster and J. Kornblum, *A Proposal for an Integrated Memory Acquisition Mechanism*, Operating Systems Review, 42(3):14-20, April 2008.

J. Kornblum, *Using Every Part of the Buffalo in Windows Memory Analysis*, Digital Investigation, 4(1):24-29, March 2007.

J. Kornblum, *Exploiting the Rootkit Paradox with Windows Memory Analysis*, International Journal of Digital Evidence, 5(1), Fall 2006.

B. Carrier, E. Casey, S. Garfinkel, J. Kornblum, C. Hosmer, M. Rogers, and P. Turner, *Standardizing Digital Evidence Storage*, Communications of the ACM, February, 2006.

J. Kornblum, *The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors*, International Journal of Digital Evidence, Volume 3(2), Fall 2004.

Conference Papers

J. Kornblum, *Using JPEG Quantization Tables to Identify Imagery Processed by Software*, Digital Investigation, 5(S):21-25, Proceedings of the Digital Forensic Workshop, August 2008.

J. Kornblum, *Identifying Almost Identical Files Using Context Triggered Piecewise Hashing*, Digital Investigation, 3(S):91-97, Proceedings of the Digital Forensic Workshop, August 2006.

J. Kornblum, *Preservation of Fragile Digital Evidence by First Responders*, Digital Forensic Research Workshop, Syracuse, NY, August 2002.

Other Publications

J. Kornblum, *A Call to Action*, 4:mag, 1(1):6-8, March 2013.

J. Kornblum, *When I'm Sixty Four (Bits)*, ManTech Tech Note 2009-01, August 2009.

Courses Authored

Windows Memory Forensics In-Depth, SANS Institute, 2012.

Forensic Tools

J. Kornblum, `Samecat`, Identifies similar looking pictures.

J. Kornblum, `encase2txt`, Converts EnCase hash files to plain text.

J. Kornblum, `findaes`, Finds AES key schedules.

J. Kornblum, `hashdeep`, Audits a set of known hashes against a given directory.

J. Kornblum, `Miss Identify`, Identifies PE executables that do not have an executable extension. Optionally identifies all executables in a set of input files.

J. Kornblum, `dc3dd`, a version of GNU dd patched for computer forensics.

J. Kornblum, `ssdeep`, Computes and matches context triggered piecewise hashes, also called fuzzy hashing. Matches similar but not identical files.

J. Kornblum, `md5deep`, A set of recursive programs for computing MD5, SHA-1, SHA-256, Tiger, and Whirlpool hashes. Capable of both positive and negative matching.

J. Kornblum, `Investigator Controlled Evidence Extraction Engine (ICE`^{3}`)`. Boot CD for automated disk imaging.

J. Kornblum, `First Responder's Evidence Disk (FRED)`. Automated Windows incident response tool.

K. Kendall, J. Kornblum, N. Mikus, `foremost`. A linux based file carving program. Recovers files from disk images based on their headers and footers.