

Computer forensics

Computer forensics (also known as **computer forensic science**^[1]) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.



Computer forensics analysis is not limited only to computer media

Contents

Overview

Use as evidence

Forensic process

- Techniques

- Volatile data

- Analysis tools

Certifications

See also

References

Further reading

- Related journals

External links

Overview

In the early 1980s personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as cracking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. Since then computer crime and computer related crime has grown, and has jumped 67% between 2002 and 2003.^[2] Today it is used to investigate a wide variety of crime, including child pornography, fraud, espionage, cyberstalking, murder and rape. The discipline also features in civil proceedings as a form of information gathering (for example, Electronic discovery)

Forensic techniques and expert knowledge are used to explain the current state of a *digital artifact*, such as a computer system, storage medium (e.g. hard disk or CD-ROM), or an electronic document (e.g. an email message or JPEG image).^[3] The scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events. In a 2002 book, *Computer Forensics*, authors Kruse and Heiser define computer forensics as involving "the preservation, identification, extraction, documentation and interpretation of computer data".^[4] They go on to describe the discipline as "more of an art than a science", indicating that forensic methodology is backed by flexibility and extensive domain knowledge. However, while several methods can be used to extract evidence from a given computer the strategies used by law enforcement are fairly rigid and lack the flexibility found in the civilian world.^[5]

Use as evidence

In court, computer forensic evidence is subject to the usual requirements for digital evidence. This requires that information be authentic, reliably obtained, and admissible.^[6] Different countries have specific guidelines and practices for evidence recovery. In the United Kingdom, examiners often follow Association of Chief Police Officers guidelines that help ensure the authenticity and integrity of evidence. While voluntary, the guidelines are widely accepted in British courts.

Computer forensics has been used as evidence in criminal law since the mid-1980s, some notable examples include:^[7]

- BTK Killer: Dennis Rader was convicted of a string of serial killings that occurred over a period of sixteen years. Towards the end of this period, Rader sent letters to the police on a floppy disk. Metadata within the documents implicated an author named "Dennis" at "Christ Lutheran Church"; this evidence helped lead to Rader's arrest.
- Joseph E. Duncan III: A spreadsheet recovered from Duncan's computer contained evidence that showed him planning his crimes. Prosecutors used this to show premeditation and secure the death penalty.^[8]
- Sharon Lopatka: Hundreds of emails on Lopatka's computer lead investigators to her killer, Robert Glass.^[7]
- Corcoran Group: This case confirmed parties' duties to preserve digital evidence when litigation has commenced or is reasonably anticipated. Hard drives were analyzed by a computer forensics expert who could not find relevant emails the Defendants should have had. Though the expert found no evidence of deletion on the hard drives, evidence came out that the defendants were found to have intentionally destroyed emails, and misled and failed to disclose material facts to the plaintiffs and the court.
- Dr. Conrad Murray: Dr. Conrad Murray, the doctor of the deceased Michael Jackson, was convicted partially by digital evidence on his computer. This evidence included medical documentation showing lethal amounts of propofol.

Forensic process

Computer forensic investigations usually follow the standard digital forensic process or phases: acquisition, examination, analysis and reporting. Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

Techniques

A number of techniques are used during computer forensics investigations and much has been written on the many techniques used by law enforcement in particular. See, e.g., "Defending Child Pornography Cases". (<http://www.robertperezlaw.com/resources-and-faqs/criminal-defense-resources/publications/defending-child-pornography-cases>)

Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly



A portable Tableau write blocker attached to a Hard Drive

detection.^{[9][10]}

Live analysis

The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data.^[11] Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

Stochastic forensics

A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

Steganography

One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes.^[12]

Volatile data

When seizing evidence, if the machine is still active, any information stored solely in RAM that is not recovered before powering down may be lost.^[8] One application of "live analysis" is to recover RAM data (for example, using Microsoft's COFEE tool, windd, WindowsSCOPE) prior to removing an exhibit. CaptureGUARD Gateway bypasses Windows login for locked computers, allowing for the analysis and acquisition of physical memory on a locked computer.

RAM can be analyzed for prior content after power loss, because the electrical charge stored in the memory cells takes time to dissipate, an effect exploited by the cold boot attack. The length of time that data is recoverable is increased by low temperatures and higher cell voltages. Holding unpowered RAM below -60 °C helps preserve residual data by an order of magnitude, improving the chances of successful recovery. However, it can be impractical to do this during a field examination.^[13]

Some of the tools needed to extract volatile data, however, require that a computer be in a forensic lab, both to maintain a legitimate chain of evidence, and to facilitate work on the machine. If necessary, law enforcement applies techniques to move a live, running desktop computer. These include a mouse jiggler, which moves the mouse rapidly in small movements and prevents the computer from going to sleep accidentally. Usually, an uninterruptible power supply (UPS) provides power during transit.

However, one of the easiest ways to capture data is by actually saving the RAM data to disk. Various file systems that have journaling features such as NTFS and ReiserFS keep a large portion of the RAM data on the main storage media during operation, and these page files can be reassembled to reconstruct what was in RAM at that time.^[14]

Analysis tools

A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review.^[7]

Certifications

There are several computer forensics certifications available, such as the ISFCE Certified Computer Examiner, Digital Forensics Investigation Professional (DFIP) and IACRB Certified Computer Forensics Examiner.

The top *vendor independent* certification (especially within EU) is considered the [**CCFP** - Certified Cyber Forensics Professional ^[1] (<https://www.isc2.org/ccfp/default.aspx>)].^[15]

Others, worth to mention for USA or APAC are the: IACIS (the International Association of Computer Investigative Specialists) offers the Certified Computer Forensic Examiner (CFCE) program.


Asian School of Cyber Laws offers international level certifications in Digital Evidence Analysis and in Digital Forensic Investigation. These Courses are available in online and class room mode.

Many commercial based forensic software companies are now also offering proprietary certifications on their products. For example, Guidance Software offering the (EnCE) certification on their tool EnCase, AccessData offering (ACE) certification on their tool FTK, PassMark Software offering (OCE) certification on their tool OSForensics, and X-Ways Software Technology offering (X-PERT) certification for their software, X-Ways Forensics.^[16]

See also

- Certified Computer Examiner
- Certified Forensic Computer Examiner
- Counter forensics
- Cryptanalysis
- Data remanence
- Disk encryption
- Encryption
- Hidden file and hidden directory
- Information technology audit
- MAC times
- Steganalysis
- United States v. Arnold

References

1. Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence" (<https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm>). Retrieved 26 July 2010.
2. Leigland, R (September 2004). "A Formalization of Digital Forensics" (<http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8472C-D1D2-8F98-8F7597844CF74DF8.pdf>) (PDF).
3. A Yasinsac; RF Erbacher; DG Marks; MM Pollitt (2003). "Computer forensics education". IEEE Security & Privacy. CiteSeerX 10.1.1.1.9510 (<https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.9510>).

4. Warren G. Kruse; Jay G. Heiser (2002). *Computer forensics: incident response essentials* (<https://books.google.com/books?id=nNpQAAAAAAAJ>). Addison-Wesley. p. 392. ISBN 0-201-70719-5. Retrieved 6 December 2010.
5. Gunsch, G (August 2002). "An Examination of Digital Forensic Models" (<http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf>) (PDF).
6. Adams, R. (2012). "The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice" (<http://trove.nla.gov.au/work/178427331?versionId=194240020>).
7. Casey, Eoghan (2004). *Digital Evidence and Computer Crime, Second Edition* (https://books.google.com/books?id=Xo8GMt_AbQsC). Elsevier. ISBN 0-12-163104-4.
8. Various (2009). Eoghan Casey, ed. *Handbook of Digital Forensics and Investigation* (<https://books.google.com/books?id=xNjsDprqtUYC>). Academic Press. p. 567. ISBN 0-12-374267-6. Retrieved 27 August 2010.
9. Garfinkel, S. (August 2006). "Forensic Feature Extraction and Cross-Drive Analysis" (<http://www.simson.net/clips/academic/2006.DFRWS.pdf>) (PDF).
10. "EXP-SA: Prediction and Detection of Network Membership through Automated Hard Drive Analysis" (<http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0730389>).
11. Aaron Phillip; David Cowen; Chris Davis (2009). *Hacking Exposed: Computer Forensics* (<https://books.google.com/books?id=yMdNrgSBUq0C>). McGraw Hill Professional. p. 544. ISBN 0-07-162677-8. Retrieved 27 August 2010.
12. Dunbar, B (January 2001). "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment" (http://www.sans.org/reading_room/whitepapers/covert/detailed-steganographic-techniques-open-systems-environment_677).
13. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten (2008-02-21). "Lest We Remember: Cold Boot Attacks on Encryption Keys" (<http://citp.princeton.edu/research/memory/>). Princeton University. Retrieved 2009-11-20.
14. Geiger, M (March 2005). "Evaluating Commercial Counter-Forensic Tools" (http://www.dfrws.org/2005/proceedings/geiger_couterforensics.pdf) (PDF).
15. "CCFP Salaries surveys" (<https://www.itjobswatch.co.uk/jobs/uk/ccfp.do>). ITJobsWatch. Retrieved 2017-06-15.
16. "X-PERT Certification Program" (<http://www.x-pert.eu/>). X-pert.eu. Retrieved 2015-11-26.

Further reading

- A Practice Guide to Computer Forensics, First Edition (Paperback) by David Benton (Author), Frank Grindstaff (Author)
- Casey, Eoghan; Stellatos, Gerasimos J. (2008). "The impact of full disk encryption on digital forensics". *Operating Systems Review*. **42** (3): 93–98. doi:10.1145/1368506.1368519 (<https://doi.org/10.1145/1368506.1368519>).
- YiZhen Huang; YangJing Long (2008). "Demosaicking recognition with applications in digital photo authentication based on a quadratic pixel correlation model" (http://pages.cs.wisc.edu/~huangyz/cvpr08_Huang.pdf) (PDF). *Proc. IEEE Conference on Computer Vision and Pattern Recognition*: 1–8.
- Incident Response and Computer Forensics, Second Edition (Paperback) by Chris Prosise (Author), Kevin Mandia (Author), Matt Pepe (Author) "Truth is stranger than fiction..." (more)
- Ross, S.; Gow, A. (1999). *Digital archaeology? Rescuing Neglected or Damaged Data Resources* (<http://www.ukoln.ac.uk/services/elib/papers/supporting/pdf/p2.pdf>) (PDF). Bristol & London: British Library and Joint Information Systems Committee. ISBN 1-900508-51-6.
- George M. Mohay (2003). *Computer and intrusion forensics* (<https://books.google.com/books?id=z4GLgpwsYrkC>). Artech House. p. 395. ISBN 1-58053-369-8.
- Chuck Easttom (2013). *System Forensics, Investigation, and Response* (<http://www.jblearning.com/catalog/9780763791346/>). Jones & Bartlett. p. 318. ISBN 1284031055.

Related journals

- *IEEE Transactions on Information Forensics and Security* (<http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206>)
- *Journal of Digital Forensics, Security and Law* (<http://www.jdfsl.org>)

- *International Journal of Digital Crime and Forensics* (<http://www.igi-global.com/journal/international-journal-digital-crime-forensics/1112>)
- *Journal of Digital Investigation* (http://www.elsevier.com/wps/find/journaldescription.cws_home/702130/description#description)
- *International Journal of Digital Evidence* (<https://web.archive.org/web/20100905202407/http://www.utica.edu/academic/institutes/ecii/ijde/>)
- *International Journal of Forensic Computer Science* (<http://www.ijofcs.org/>)
- *Journal of Digital Forensic Practice* (<https://web.archive.org/web/20100527045358/http://www.tandf.co.uk/journals/titles/15567281.asp>)
- *Cryptologia* (<http://www.tandf.co.uk/journals/titles/01611194.asp>)
- *Small Scale Digital Device Forensic Journal* (<http://www.ssddfj.org>)

External links

- US NIST Digital Data Acquisition Tool Specification (<http://www.cfft.nist.gov/Pub-Draft-1-DDA-Require.pdf>) (PDF)
 - Computer Forensics World Forum (<http://www.computerforensicsworld.com>)
 - Original Computer Forensics Wiki (<http://computer-forensics.safemode.org/>)
 - Forensic Focus (<http://www.forensicfocus.com>)
 - Digital Forensic Research Workshop (DFRWS) (<http://www.dfrws.org>)
 - Computer Forensic Whitepapers (SANS) (<http://computer-forensics.sans.org/community/whitepapers>)
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Computer_forensics&oldid=827452113"

This page was last edited on 24 February 2018, at 20:24.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.