Computer Forensics

Definition

The definition of computer forensics is a series of methodical processes and analysis techniques to gather and preserve evidence while maintaining a documented chain of the evidence . It is to discover the chain of events on a computer and who was responsible. It is not limited to computers but various storage devices and/or digital media. Evidence needs to be in a coherent and meaningful format for presentation in a court of law.

Historical Time-line

1970s

- First crimes cases involving computers, mainly financial fraud.

1980's

- Financial investigators and courts realize that in some cases all the records and evidences were only on computers.
- Norton Utilities, "Un-erase" tool created.
- Association of Certified Fraud Examiners began to seek training in what became computer forensics.
- SEARCH High Tech Crimes training created.
- Regular classes began to be taught to Federal agents in California and at FLETC in Georgia.
- HTCIA formed in Southern California.

1984

- FBI Magnetic Media Program created. Later it become (became) Computer Analysis and Response Team (CART).

1987

- Access Data – Cyber Forensic Company formed.

1988

- Creation of IACIS, the International Association of Computer Investigative Specialists.
- First Seized Computer Evidence Recovery Specialists (SCERS) classes held.

1993

- First International Conference on Computer Evidence held.

1995

- International Organization on Computer Evidence (IOCE) formed.

1997

- The G8 countries in Moscow declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes".

1998

- In March G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence.

1998

- INTERPOL Forensic Science Symposium.

1999

- FBI CART case load exceeds 2000 cases, examining 17 terabytes of data.

2000

- First FBI Regional Computer Forensic Laboratory established.

2003

- FBI CART case load exceeds 6500 cases, examining 782 terabytes of data. .

(Kedziora, 2012)

The Importance of Computer Forensics

The importance may be criminal actions such as fraud, phishing, identity theft or many other criminal activities. Many companies may find themselves in a civil suit like sexual harassment, a disgruntled employee that stole information or a discrimination suit. Information from their computer, emails and personal files on the network would need to be recovered. The information will need to be documented and a chain of custody started to make the information admissible in court.

The government has issued several writing and resources available on computer forensics. They are concerns about corporations having the ability to practice and apply sound principles of computer forensics. A corporation has to be confident in the overall integrity and the survivability of their network infrastructure and data. The Computer Emergency Response Team (CERT) takes an approach of "defense in depth". The idea is to have organizations understand forensics from thel egal and technical aspects in order to assist in preserving latent evidence and catch the intruder.

What is Digital Evidence Really?

The National Center for Forensic Science terms digital evidence as information stored or transmitted in a binary form having proven, tending to prove or actually proven in a legal litigation or crime. Digital evidence is not limited to computers but all can include digital audio and video. It can also come in different forms -- hardware from jump drives, network attached storage units, play stations, cell phones and digital cameras with SD cards. It may actually be any type of hardware that can store remnants of data.

Highlights of Forensics Methods

The best and thorough resource is written by J. Philip Craiger,PhD., CISSP. He is assistant Director for Digital Evidence. You will find him listed in references and further reading sections. He is truly worth the read. His association is with the National Center for Forensic Science & Department of Engineering Technology and University of Central Florida National Center, University of Central Florida.
The highlight are high over view of the different procedures and forenscics methods.

- The introduction covers the forensic tools and the forensic server- It is an overview and an introduction to fundamental methods and procedures. It describes the tools needed and how to get them. It also you tells to specification the environment for recovery of the questionable data.
- Sound computer forensic practice- Treat every case as it would be taken to court follow the same procedures and chain of custody. An investigator will never know if or when a current case may go to trial.
- Preparing a crime scene when arriving: the initial response- Two rules of thumbs apply. First rule is to restrict access to the scene. Please keep in mind to make the restricted access bigger than what you need. It is always easier to make it smaller scene than try to make it bigger after evidence has been contaminated. Second rule is to document and photograph. This is crucial in several ways because it will refresh your memory and allows the court to verify the procedures performed.

Best Practices:
a. Immediately determine if a destructive program is running on the computer. If one is running, the investigator should pull the power plug from the back of the computer (not at the outlet).
b. Document the computer and its surroundings. Video tape and photographs are good supplements to handwritten notes.
c. If the computer is running, take a photograph of the screen.
d. Take photographs of the front, side, and back of the computer.
e. Physically open the computer and take photographs of the inside of the computer.
f. Bag-and-tag of all potential evidence.
g. If the computer is to be transported to an off site forensics lab, label each computer part and place in an appropriate container for transport.
h. Search for ‘sticky notes’ or any other written documentation near the computer (including under the keyboard, under the desk, in desk drawers, etc.). Users often write down passwords and leave them in convenient places near the computer.
I. Take any computer manuals in case they are needed for reference back at the forensics lab.
j. If the original evidence is to be confiscated it should be stored in a secure place.

Create a forensic image to the exact physical evidence. Never ever use the original image. Once the orginal is lost you can never get it back. Verify the image integrity by doing a check sum of md5sum. It will calculate a MD% cryptographic hash known as the message digest or the hash. You will know if the image is good or not. If the removing a hard drive is not an option. You can do a network acquisition. If both computers have ethernet cards you can retrieve the image of the drive by a bootable Knoppix CD or USB and a crossover cable.

- Analysis of a forensic image has been broken down into logical analysis and physical analysis. A logical analysis views the perspective files in the file system. The investigator can use many different forms of graphical tools and file management tools to analyze the file structure. The physical analysis views the forensic image from a physical view points without the file structure. Tools you will be using are hex editor or similar tools to read disk space: allocated,unallocated and slack. The work will be very detailed oriented and it will make you think about the physical design. There is so much more information that could be detailed in both types of analysis. It would be out of the scope of this wikipedia posting but the site is listed in references and further reading.

- Collecting volatile evidence is important. It is evidence that purges from a running system in a short period of time. There are commands to collect that evidence and the commands included in brief includes:

  a. Running processes (ps or the /proc file system)
  b. Active network connections (netstat)
  c.ARP cache (arp)
  d. List of open files (lsof)
  e. Virtual and physical memory (/dev/mem, /dev/kmem)

  There are details on the proper procedure and collection of violate evidence in Craiger, J. Philip. Computer Forensics Procedures and Methods. It is absoluetly the how to in an computer forensics. Unfortunately , more details is out of the scope of this wikipedia posting.

Training

There are many schools, private companies and universities teaching computer forensics. You really need to look at cost, commitment and credentials of these institutions. Excellent sites to visit are EC-Council, Computer Forensics World, National Center for Forensic Science and the Computer Emergency Response Team (CERT). The EC-Council and Encase offers several certifications that are self-study and you can take the tests at a nearby prometric center.

Conclusion

In the last several decades information technology has grown to a phenomenal size in corporations and personal use. It effects every age, sex and origin. There is not one person that you can talk to that does not use some form technology. Technology can be used for good or bad. It is tool like a phone, chain saw or an egg beater. Not all people have alternative motives but some people do. We need people with a moral concision that can follow the computer evidence and understand the bigger picture in society. You may not like the evidence you discover but you need present it without prejudice. I believe there are people that belong to society that can make a difference. This is growing field in the technology industry and as science it is here to stay.

References

Craiger, J. Philip. Computer Forensics Procedures and Methods._Retrieved from http://www.ncfs.ucf.edu/craiger.forensics.methods.procedures.final.pdf

Digital forensic computing news syndication. (2007). Computer forensics world. Retrieved from http://www.computerforensicsworld.com/index.php

EC-Council. (2012). Ec-council. Retrieved from http://www.eccouncil.org/

Guidance Software, Inc. (2012). Guidance software-encase. Retrieved from http://www.guidance software.com\

Kedziora, M. (2012). Computer forensics history. Retrieved from http://www.forensics-research.com/index.php/computer-forensics/computer-forensics-history/

National Center for Forensic Science. Retrieved from http://www.ncfs.ucf.edu/digital_evd.html

Rouse, M. (2007, February). Computer forensics (cyberforensics) . Retrieved from http://searchsecurity.techtarget.com/definition/computer-forensics

US-CERT. (2008). Computer forensics. Retrieved from http://www.uscert.gov/reading _room /forensics.pdf

Further Reading

Altheide, C., Carvey, H., & , R. (2011). *Digital forensics with open source tools.* Waltham,Massachusetts : Syngress. Retrieved from http://www.syngress.com/

Carvey, H. (2009). *Windows forensic analysis dvd toolkit 2e*. Burlington,Massachusetts: Syngress Publishing Company. Retrieved from http://www.syngress.com/

Digital forensic computing news syndication. (2007). Computer forensics world. Retrieved from http://www.computerforensicsworld.com/index.php

EC-Council. (2012). *Ec-council*. Retrieved from http://www.eccouncil.org/

Guidance Software, Inc. (2012). Guidence software-encase. Retrieved from http://www.guidances oftware.com/

Mandia, K., Prosise, C., & Pepe, M. (2003). *Incident response &computer forensics*. Emeryville, California: McGraw-Hill/Osborne. Retrieved from http://www.mcgraw-hill.com/

Volonino, L., Anzaldua, R., & Godwin, J. (2007). *Security computer forensics principles and practices*. Upper Saddle River, New Jersey: Pearson Prentice Hall. Retrieved from http://prenticehall.com/