Global Information Assurance Certification Paper

Computer Forensics – An Overview
Dorothy A. Lunn
February 20, 2001

Introduction:

The purpose of this paper is to generate an interest in and awareness of computer forensics by providing some basic information.. I will define computer forensics and briefly discuss computer forensics history and computer related crime. Then, I will continue with preparing the organization for incident handling, employing computer forensics, computer forensics training, and computer forensics software.

What is Computer Forensics?

My simple definition of computer forensics is, "The employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity."

Judd Robbins, a computer forensics investigator, defines computer forensics as "Simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence."[1]

New Technologies Inc. expands on Robbins' definition.

> "Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information (data)."[2]

History of Computer Forensics:

Evidence derived from computers has appeared in court for almost 30 years. Initially, judges accepted the evidence as no different from forms of evidence they were already seeing. As computer technology advanced, it became apparent that similarity to traditional evidential material was becoming ambiguous. The US Federal Rules of Evidence of 1976 addressed some of the issues. Other laws relating to computer crime include:

- The Economic Espionage Act of 1996 which deals with trade secret theft and includes the following:
  - 18 USC Sec. 1831
  - 18 USC Sec. 1832
- The Electronic Communications Privacy Act of 1986 which deals with interception of electronic communications and includes the following:
  - 18 USC Sec. 2511
  - 18 USC Sec. 2701
  - The Computer Security Act of 1987 (Public Law 100-235) deals with the security of government computer systems.

Since the USC is all legal language, I've used several other, and much more interesting, references for research for this paper. However, for those legal wizards who might be interested, you may research details of the United States code at

http://www4.law.cornell.edu/uscode/

Computer Related Crimes:

When thinking about cybercrime, most people think of hackers cracking web sites as a prank or criminals looking to gain information such as bank account numbers, credit card numbers or trade secrets for financial gain and espionage data like top secret information from the military. In addition to business and everyday practical use, technology also offers the criminal the same practical uses. The underworld keeps accounting and client information on their businesses whether it is drug distribution, a prostitution ring or illegal gambling using computer software.

Criminals may use computers in one of two ways in support of their actions. Either as the repository for information relating to their criminal activity or as a tool in actually committing a crime. The Federal Guidelines for Searching and Seizing Computers states that, "Any home PC can be connected to a network simply by adding a modem. Thus, in any case where a modem is present, agents should consider the possibility that the computer user has stored valuable information at some remote location."[3] Criminal activity can be executed from anywhere in the world. This not only makes the crime more difficult to investigate, it also makes committing a cybercrime attractive for people who wouldn't think of committing a crime in person. Loek Weerd is quoted by Illena Armstrong as saying, "Since data appears on the screens of their own computers in their own trusted environments, ethical limitations like what's yours and what's mine seem to disappear for a lot of people."[4]

Judd Robbins lists the following types of criminal and civil proceedings that can make use of evidence revealed by computer forensics:[1]

- **Criminal Prosecutors** use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
- **Civil litigations** can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.
- **Insurance Companies** may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
- **Corporations** often hire computer forensics specialists to ascertain evidence relating to: sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.
- **Law Enforcement Officials** frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
- **Individuals** sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination.

Preparing the Organization to Handle Incidents:

Not only are many organizations careless about implementing appropriate security to protect their networks and data, but they are ill prepared to handle a significant intrusion from outside or an incident perpetrated by an insider. Organizations should implement an Incident Response and Reporting Plan, create a Computer Incident Response Team (CIRT) and have extended resources available to them for this purpose in the event of a significant intrusion.

For those organizations that are hesitant, don't have the resources or just can't afford to invest in setting up their own plan and CIRT, there are many businesses providing security and expert computer forensic services. A resourceful organization will investigate the experts available and identify one or two as potential resource that can be called upon if a significant intrusion occurs. Peter Sommer of Virtual City Associates lists the following key features to look for when considering a forensic technician.[5]

1. Careful methodology of approach, including record keeping
2. A sound knowledge of computing, particularly in any specialist areas claimed
3. A sound knowledge of the law of evidence
4. A sound knowledge of legal procedures
5. Access to and skill in the use of, appropriate utilities

The Incident Reporting and Response Plan sets out how to identify a significant event, the steps necessary deal with the incident and when and to whom to report it. A skilled CIRT will insure that the appropriate staff is identified and trained to direct incident response and handling. Thomas Welch in The Information Security Management Handbook, Vol. 1[6] pg. 601, states that "We, as computer security practitioners, must be aware of the myriad of technological and legal issues that affect our systems and their users, including issues dealing with investigations and enforcement." The Information Security Management Handbook, Vol. 2[7] pg. 559 lists the following examples of incidents that a CIRT team might identify.

1. Viruses
2. Unauthorized access, regardless of source
3. Information theft or loss of confidentiality
4. Attacks against systems
5. Denial of service
6. Information corruption

The National Institute of Standards and Technology (NIST) provides a publication as guidance in setting up a CIRT. It is SP800-3, "Establishing a Computer Security Incident Response Capability." and the document can be downloaded in PDF format at the following site.

http://csrc.nist.gov/csrc/advisories.html

This is an excellent source for information that would be useful in defining the functions and charter for a CIRT. NIST is currently revising the document to include policy and procedures for setting up an incident handling capability.

Employing A Computer Forensics Expert:

An organization's Incident Response and Reporting Plan should provide guidance on assessing an incident and its seriousness. Once the seriousness has been determined, a plan of action is developed. Most organizations can handle a virus infection but the other five incidents listed above may require special handling. James O. Holly, National Computer Forensics Lab Director for Ernst & Young , states that, "You'll want to keep the door open for administrative, civil or criminal proceedings in response to computer crime." and "….. your investigator needs to handle an incident , from the very beginning as if it is, in fact going to court."[8] Because of this, special steps need to be taken to protect the evidence. Very few organizations have the in-house expertise or tools needed to deal with a serious incident. Security professionals are very seldom trained in computer forensics and can very easily lose, or through lack of proper procedures, make evidence inadmissible in court.

The International Association of Computer Investigative Specialists (IACIS) lists the following three essential requirements of a competent forensic examination:[9]

1. Forensically sterile examination media *must be* used.
2. The examination must maintain the integrity of the original media.
3. Printouts, copies of data and exhibits resulting from the examination must be properly marked, controlled and transmitted.[7]

In addition there are several cardinal rules that the forensic services I researched agree on:

1. Ensure that no forensics evidence is damaged, destroyed, or otherwise compromised by the procedures used during the investigation,
2. Never work on the original evidence,
3. Establish and maintain a continuing chain of custody, and
4. Document everything, people with physical access, software/tools used and what they do, research results and every procedure followed.

If you are still in doubt as to the advisability of using a computer forensics expert, consider this list of activities a forensics investigation must address (Judd Robbins):[10]

1. Protecting the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
2. Discovering all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
3. Recovering all (or as much as possible) of discovered deleted files.
4. Revealing (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
5. Accessing (if possible and if legally appropriate) the contents of protected or encrypted files.
6. Analyzing all possibly relevant data found in special (and typically inaccessible) areas of a disk. This includes but is not limited to what is called 'unallocated' space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as 'slack' space in a file (the remnant area at the end of a file, in the last assigned disk

cluster, that is unused by current file data, but once again may be a possible site for previously created and relevant evidence).

7. Printing out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data. Further, provides an opinion of the system layout, the file structures discovered, any discovered data and authorship information, any attempts to hide, delete, protect, encrypt information, and anything else that has been discovered and appears to be relevant to the overall computer system examination.
8. Providing expert consultation and/or testimony, as required.

In some cases an organization may become involved in an investigation being carried out by a local, state or federal law enforcement agency. An organization may have been used by a suspect to launch an attack on a computer located at another site or data is suspected of being stored on a PC or server by an employee suspected of committing a crime. Anyone with a modem and access to an organizations resources can use those resources to store data associated with their criminal activity. If an organization is asked to cooperate in an on going investigation, the law enforcement agency will most likely bring in their own experts to conduct the forensic process.

Computer Forensics Training:

A computer forensics expert is specially trained and will have software and utilities the organization doesn't own or know about. Computer forensics training is available from many sources. Below are several training vendors I found on the Internet. The lists of training topics give a good overview of the knowledge with which a computer forensics expert should be well-acquainted. Key Computer Services, Inc. offers online classes.

Guidance Software
http://www.guidancesoftware.com/training/frame_fst.html

New Technologies, Inc.
http://www.forensics-intl.com/training.html

AccessData
http://www.accessdata.com/index.html

Key Computer Services, Inc.
http://www.keycomputer.net/

Computer Forensics Software:

Several companies have developed computer forensic software that they market and for which they provide training. I've listed a couple of them because these vendors provide a comprehensive training package that covers all aspects of computer forensics and not just their software.

EnCase, by Guidance Software uses a graphical interface to manage and view all evidence. Additionally, the software has a feature that documents who worked with the data and when.

http://www.guidancesoftware.com/encase/frame_encase.html

SafeBack by New Technologies, Inc is a sophisticated evidence preservation tool that was developed specifically for use by federal law enforcement agencies in the United States in the processing of computer evidence.

http://www.forensics-intl.com/safeback.html

In addition to proprietary software there are many utilities/tools available to aid in performing an investigation. I have listed a few of them as examples:

1. Various password cracker programs
2. WIPEDRV – Used to completely erase all information on a logical or physical drive by overwriting each and every byte with a character which is user selectable.
3. LISTDRV – Used to list all drive on a device.
4. DISKIMAG – Used make a copy or copies of suspect floppy disks onto a hard drive for analysis.
5. CHKSUM – Used to calculate a 64 bit checksum for a physical or logical drive.
6. FREESECS – Used to search a specific logical drive for the unallocated or free space and saves the information contained in unallocated space to one or more files.

Summary:

Most organizations haven't implemented adequate security hardware or software to protected their networks, web sites and data. Neither have they planned for the incidents and intrusions that are bound to occur. Creation of an Incident Response and Reporting Plan and implementation of a Computer Incident Response Team (CIRT) provide the policy and procedures necessary to handle incidents and intrusions. A source of computer forensics expertise should be researched and identified as a resource when a serious incident or intrusion requires expert help.

Is your organization prepared? If the decision is made to prepare to handle incidents and intrusions internally, several vendors provide proprietary computer forensics software and training, at least one course is available online.

---

[1] Robbins, Judd. "An Explanation of Computer Forensics." URL: http://www.computerforensics.net/forensics.htm

[2] "3 Day Computer Forensics Training Course – Oregon.", New Technologies, Inc. 15 February 2001. URL www.forensics-intl.com/forensic.html

[3] "Federal Guidelines for Searching and Seizing Computers." URL http://www.usdoj.gov/criminal/cybercrime/search_docs/sect4.htm

[4] Armstrong, Illena. "Computer Forensics." SC Magazine April 2000. URL:

http://www.scmagazine.com/scmagazine/2000_04/cover/cover.html

[5] Sommer, Peter. "Computer Forensics: An Introduction." 1997. URL
http://www.virtualcity.co.uk/vcaforens.htm#history

[6] Tipton, Harold F. and Krause, Micki Editors; Auerbach "Information Security Management Handbook", 4th Edition, Volume 1 1999

[7] Tipton, Harold F. and Krause, Micki Editors; Auerbach "Information Security Management Handbook", 4th Edition, Volume 2 2000

[8] Holley, James O. "Computer Forensics in the new Millennium." September 1999. URL
http://www.scmagazine.com/scmagazine/1999_09/survey/survey.html

[9] The International Association of Computer Investigative Specialists. "Forensic Procedures." 22 July 2000.:URL
http://cops.org/forensic_examination_procedures.htm

[10] Robbins, Judd. "The Devils Advocate: Computer Forensics Can Support Both Sides of Computer Litigation." URL
http://www.expertnetwork.com/computer_expert.htm