LEGAL METHODS OF USING COMPUTER FORENSICS TECHNIQUES
FOR COMPUTER CRIME ANALYSIS AND INVESTIGATION

Daphyne Saunders Thomas, James Madison University, Harrisonburg, Virginia
Thomasds@jmu.edu
Karen A. Forcht, Utah State University, Logan, Utah

ABSTRACT

Computer forensics is the scientific collection, recovery preservation, legal analysis and presentation of data held or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. Forensics specialists must consider the legal and ethical parameters of evidence collection so that critical elements are not corrupted.

Keywords: Computer forensics, digital computer forensic science, electronic investigation, forensics techniques, imaging, investigation, law enforcement techniques, legal use of forensics

INTRODUCTION

Computer forensics and investigation has been considered a professional field for many years. Most of the experts in the field have been self-taught due to the lack of formal education and training in the computer forensics field. Although training within the private sector has recently become increasingly popular and important, forensics has been prevalent in the law enforcement fields and government agencies since the mid-1980s.

Definition of Computer Forensics

Computer forensics is defined as “the application of computer investigation and analysis techniques in the interests of determining potential legal evidence”. Reasons that legal evidence might be sought constitute a wide range of computer crimes or misuses, including theft of trade secrets, theft of or destruction of intellectual property, and fraud. Computer specialists have many ways of discovering data that reside in a computer system, or of recovering deleted, encrypted, or damaged file information. The data discovered is important in litigation and in solving various computer crimes. The benefits of being able to use computer forensics are numerous when compared to paper evidence. Data on a computer has the potential to exist in many formats, such as on the hard drive or a disk.

Forensics Specialists

A computer forensics specialist has many duties and responsibilities relating to computer systems analysis, such as:

- Protecting the computer system from any tampering, data corruption, damage, or viruses
- Ensuring that the computer system is not destroyed or damaged in any way
- Discovering all hidden, deleted, encrypted, or password protected files
- Recovering as much as possible about the deleted files and accessing the protected or encrypted files
• Analyzing the data found and providing printout of the overall analysis
• Providing testimony and expert consultation about the corrupted computer system

Individuals who implement computer forensics analysis techniques include: criminal prosecutors, insurance companies, corporations, and law enforcement officials (8) In each case, the computer specialist has specific knowledge of the hardware and software. The expert has knowledge of the different formats in which the evidence can be discovered and tries to find a form that the criminal forgot. These experienced experts look at and search backups that are available.

Before the investigation starts, it is vital that the computer is handled with care so that no evidence is destroyed or damaged, no computer virus may infect the system, and no evidence is destroyed by mechanical or electromagnetical influences. It is also crucial that the evidence is always kept in custody and that none of the confidential information on the suspect’s system is misused. After the expert discovers all hidden files, recovers all deleted files and access all encrypted files, they create an overall analysis in which an overview of the computer system is given and every conspicuous pattern is displayed. The electronic investigations also show which files have been deleted or protected. The computer forensic expert will then assist in the investigation or litigation as a consultant.

When computer investigators arrive at a crime scene, they first unplug the computer in case it is running a file-erasure program that could potentially destroy evidence. An image backup (a byte-by-byte copy of a computer’s hard drive) is made and used for all examination of the data so that there is no chance of damage to the original drive. The backup will include all active and deleted files, fragments of data not completely overwritten; swap files, embedded data and metadata, and much more. Because of the volatile nature of electronic evidence, simple tasks such as booting up a computer or saving a document can alter data or other files.

A computer forensics expert is able to make an image backup without damaging or tampering with potential evidence, which is critical in the legal system. Next, the mirror image is taken to the lab for retrieval and analysis. Some criminals use encryption programs to make their files unreadable, but experts are able to recover encrypted or password protected documents during the retrieval process. A forensics expert can also recover deleted computer files and email, identify what websites have been visited and what files have been downloaded, and find any attempts to conceal or destroy evidence.

The biggest challenge in computer investigations is not the encryption (because the majority of suspects do not bother with it). The biggest challenge in computer investigations is the size of today’s computer hard drives. The bigger the hard drive, the longer the investigation takes. Once the files have been obtained from the computer, the rest of the process is a matter of old-fashioned research as investigators scrutinize the information. Seldom does a computer search provide evidence that positively proves a suspect’s guilt. The evidence found often only contributes pieces to the investigation.
LEGAL CONSIDERATIONS OF FORENSICS

Computer forensics involves essentially taking an autopsy of the computer using specialized software and techniques to analyze exactly what actions the computer has taken and what data is stored. It does not, however, prove causality. The evidence obtained may then be explained and presented to those who will make the ultimate decision about how to proceed in the criminal investigation.

Computer forensics requires more than merely copying files from a computer. The investigator must also consider issues such as: where the data is stored, how the operating system deals with files (specifically reading and writing to disk), how to deal with encrypted data, and many other computer specific details. In addition to technical issues, investigators must be very careful with how they gather this evidence so that it can be proven that no tampering has occurred. The teaching of the investigatory techniques and usage of these specialized tools has recently become more widespread to help catch computer criminals and obtain proof of their actions.

The field of computer forensics has become more widespread and so too has its validity in a court of law. Computer crimes are now being assigned more specific and severe punishments as these acts become more common; and as this continues, computer forensics will become more important to help curb the occurrences of these crimes.

According to New Technologies Inc, the term “Computer Forensics” was coined back in 1991 in the first training session held by the International Association of Computer Specialists (IACIS). ‘Computer forensics’ refers to the application of law in the field of computing. It deals with the preservation, identification, extraction and documentation of computer evidence. Computer evidence can be anything from entire copies of hard drives to individual files on a desktop. (22)

The field of computer forensics has grown rapidly in the past decade as the amount of computer-related crime has risen. Corporations are using the techniques not only to investigate computer crimes within a company, but also as a preventative measure to deter future crimes. In addition, law enforcement agencies are learning to use computer forensics to gain evidence in crimes not computer related. Thomas Rude of CISSP writes “The Science of Computer Forensics is fast becoming a very necessary skillset for law enforcement departments, government entities, and corporations worldwide. As society becomes more digitized, the need for skilled personnel in this arena becomes more and more pressing.” (27)

Rude also outlined a few key elements of a computer forensics investigation:

1) A forensic examiner is impartial. Our job is to analyze the media and report our findings with no presumption of guilt or innocence.
2) The media used in forensic examinations must be sterilized before each use.
3) A true image (bit stream) of the original media must be made and used for the analysis.
4) The integrity of the original media must be maintained throughout the entire investigation. (27)
Examples of Forensics Application

The United States Secret Service website offers a list of recommendations in the event that there is a possible crime and a computer needs to be seized for examination. They suggest first determining what role the computer played in the alleged crime. For instance, is the computer hardware or software stolen, or was the computer used as a tool in committing the crime? Once the role is determined, it is then necessary to determine whether there is sufficient probable cause to seize the hardware, software, or data. The site also emphasizes the importance of keeping the data from being corrupted or contaminated in any way. If the data becomes corrupted or contaminated, it could cause the loss of important information. In the event that the information is needed as proof in court, it is important to have forensically sound evidence. (37)

There are many groups of people who benefit from the usage of computer forensic methods. For example, individuals who are the victims of fraud will benefit from the evidence that forensic professionals can retrieve from the computers of the accused criminal. Corporations can also benefit from computer forensics in case they are the victims of stolen trade secrets. Corporations can even obtain evidence of embezzling and other illegal activities within the company. Ultimately, with the rise of computer crimes, it is important for people to recognize that a new digital crime scene has taken shape. There is a wealth of potential evidence to be found through computer forensics, and the effectiveness and benefits of this form of forensics is only now beginning to be realized.

The FBI uses computer forensics to retrieve information from a computer’s storage media (hard drive), chips, boards, central processing units, monitors, and printers. After research, the FBI developed techniques to restore even deleted information. When a file is deleted from one’s computer, the information still remains on the hard drive because the operating system only considers the file open to being overwritten. Information on one’s computer is only truly deleted when the sector on the hard drive is overwritten. Therefore, the FBI scans the hard drive for all the information stored on servers or networks on a user’s computer in order to create timelines of crimes or whereabouts. (24)

Validating electronic forensics

Like any new evidentiary procedure, electronic forensics has had to be validated. In the late 19th century, fingerprints had to be proven as valid evidence. Fingerprints have become one of the most valuable trace evidence types in use today. In the 20th century, the uniqueness of striations found on fired bullets became a valid method of tying a gun to a specific crime.

The polygraph has a long and colourful history of being used to distinguish between truth and falsehood but has no basis in science and is therefore, not valid in any court of law. There has never been a scientifically controlled study that proves conclusively any linkage between physiologic change and truth or falsehood. It has been investigated in 1965, 1976, and again in 1983 by the Office of Technology Assessment (formerly an office of Congress) which concluded: “There is very little research or scientific evidence to establish polygraph validity.” Justice Clarence Thomas in *US vs. Scheffer* (No. 96-133-March 31, 1998) stated in his opinion:
“scientific field studies suggest the accuracy rate of the control question technique’ polygraph is ‘little better then could be obtained by the toss of a coin, ‘that is, 50 percent’.

Not all evidentiary techniques put forward are or have been accepted. In the US, for example, there was a precedent setting case in 1993; Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993). That case lays out a set of five elements that must be achieved in order for evidence gathered by an unproven technique to be accepted:

1. Whether the theory or technique can be and has been tested.
2. Whether it has been subjected to peer review and publication.
3. The known or potential error.
4. The general acceptance of the theory in the scientific community.
5. Whether the proffered testimony is based upon the expert’s special skill.

Other countries have their own precedents that validate electronic forensics evidence gathering methods. The tools, techniques and methodologies of electronic investigation, gathering and analysis have been tried and proven and are accepted in many countries.(34

**Forensic evidence in computing**

The gathering of evidence in a computing environment is not merely copying files from the suspect’s computer and printing them out for presentation in a proceeding. While that indeed may be an important part of it, there is data that may be pertinent to such proceedings that is not readily or apparently available through ordinary means. Moreover, accessing and finding such data requires an awareness of what kinds of information exist on a PC and how to go about gathering and preserving the original data and making certified copies of that evidence.

When working with a potential case, all exculpatory evidence (evidence tending to exonerate or diminish the liability of a defendant) must be disclosed. Lack of disclosure to the court and judge could result in an accusation of evidence tampering or withholding. Depositions are often conducted prior to a trial. Two types of depositions are discovery- and testimony preservation. Both are used to verify facts and to substantiate the background information provided by the expert. (21)

**SUMMARY**

Computer forensics has been around for a while and is rapidly becoming a specialized and accepted investigative technique (in a court of law) with its own tools and legal precedents that validate the discipline. It is basically a computing profession dedicated to “finding the truth”. (34) The domain of computer forensics is not to assign guilt or innocence but rather to find facts in the form of electronic evidence that can be presented in a coherent way so that others may weigh the evidence and then assign guilt or innocence where appropriate.

The field of computer forensics will, no doubt, grow rapidly at an exponential rate over the next decade as the development of new and better technologies relating to computer use bring vulnerability of information and the potential of risk and abuse.
REFERENCES

3. Center for computer forensics (computer-forensics.net)
6. Computer conversions, Inc. (computer-conversions.com)
22. New Technologies, Inc. (Forensics-intl.com)
32. The International Association of Computer Investigative Specialists (IACIS.com)
36. www.csoonline.com
37. www.forensics.com