A STUDY OF THE APPLICATIONS OF COMPUTER INVESTIGATION TO GATHER EVIDENCE SUITABLE FOR PRESENTATION IN THE LEGAL CONSTITUTION FOR FORENSIC DEPARTMENT

D. S. Jadhav
Assistant Professor,
Sinhgad Institute of Computer Sciences (MCA),
India

S. K. Patil
Associate Professor and Head,
Department of Accountancy,
B. P. Sulakhe College of Commerce, India

ABSTRACT

This paper takes a look at the applications of computer investigation and analysis techniques together evidence suitable for presentation in the court laws. According to the paper, computer forensics, i.e. the applications of computer investigation and analysis techniques to gather evidence suitable for presentation in the court laws, is one of the new professions that resulted from the ubiquitous use of computers and the Internet. The paper reports that computer forensics professionals are the modern-day centurions or praetorian guards that ensure the continued use of new and emerging information technologies. “The discipline of computer forensics can be called both an art and a science. An art because like programmers and hardware developers, they can add elegance and form to how they go about doing their jobs and by putting "their personal touch" to it they leave an important legacy for others to follow. It is a science because computer forensics expert go to the same scientific methodology in determining the outcome of their work. The process is well defined and controlled so as not to leave any doubt as to the integrity of the work. “The scope of computer forensics covers a wide field, which continues to grow as computer technology proliferates its way into every aspect of modern life. The base of computer forensics is recovering data from floppy disks, hard drives, and removable drive cartridges. Recovering data can be just finding it among the active files. Often, it will also include searching the media for files that have been deleted and been listed as unallocated space. When dealing with someone, who is actively attempting to hide information, scouring media space the operating system has registered as free or corrupted.”

Keywords: Centurions, Structured investigation.

Introduction:

The spread of crime using computers was inevitable; the question is how much damage computer crime has caused and still may. The domain of computers, for the purposes of this paper, is confined to media that is intended for a computer to read or be used as a peripheral. For example, a digital telephone answering machine is not within the scope, but the use of a compact disc containing data or written by a computer would qualify. For this paper, computer forensics is defined as “the use of an expert to preserve, analyze, and produce data” from volatile and non-volatile media storage. Computer forensics is in the early stages of development and as a result, problems are emerging that bring into question the validity of computer forensics usage in the United States (U.S.) federal and state court systems. For practical purposes, the legal issues relevant to computer forensics are:

- standards and certifications,
- analysis and preservation

Historically, a significant portion of court cases has been settled before the trial. In other instances, computer forensics evidence was never contested. Conversely, when computer forensics evidence has been contested, it has provided the foundation for evaluating what, why, and how those issues should be considered when creating computer forensic standards and certifications for the U.S. federal and state court systems.

The inevitable fact that technology is becoming more intertwined in the daily life of the individual will lead to an increase in court cases where computer evidence is a vital component. Because the judicial system is having difficulties in mandating and interpreting standardization for computer forensics, it becomes the responsibility of the scientific community to assist in this endeavour.
Computer Forensics Deployed In:

- Hacking
- Fraud
- Paedophiliac Rings
- Defamation
- Immigration Fraud
- Narcotics Trafficking
- Credit Card Cloning
- Software Piracy
- Electoral Law
- Obscene Publication
- Perjury
- Forgery
- Murder
- Sexual Harassment
- Data Theft – Industrial Espionage
- Divorce

But this has been mostly about DISK forensics, specifically disks in PCs. What about:

- Evidence from large systems?
- Evidence from remote sites?
- Evidence from networks?
- Evidence from data eavesdropped in transmission?

Are the very high standards now existing for disk forensics creating unrealistic expectations for all other forms of computer-derived evidence?

A. Threats to the Enterprise:

1) Internal:
- Hacking tools and discovery tools
- Unauthorized applications
- Unauthorized communications
- Counterfeiting/ fraud
- Rogue servers and services
- Wrongful Termination

2) External:
- Unauthorized users/ intruders

Goal of Forensic Investigations:

- Conduct structured investigation
- Preserve and secure electronic data using methods that withstood judicial scrutiny
- Obtain all data potentially relevant to a matter
- Minimize cost and business disruption
- Obtain relevant information
- Document
- Integrate into litigation function

Comprehensive Security Model

An Approach To Evidence In Cyberspace:

A government official is caught embezzling hundreds of thousands of dollars from his agency. A Federal Search Warrant is executed at his residence for evidence of his crime and to locate the money. The money is not found, but on his computer is a letter discussing the disposition of the illegally obtained funds. A pedophile is caught attempting to molest children. His residence is
searched for evidence which will prove that this incident is part of a long-standing pattern of behaviour and which will identify additional victims.

On his computer numerous images are stored which depict the subject, his residence and several neighborhood children committing sex acts. A terrorist bombing suspect’s home is searched for evidence of the conspiracy and the motive for the crime. Fragments of documents and drawings are found on the computer of the suspect which link him to the bombing and provide insight as to the motive for the crime. A con man is tried in Federal Court for running a scam in which the prizes will never be given away.

A computer forensic specialist testifies that the computer program which is used to determine the winning numbers is programmed in such a way that the prizes are outside the range of the program’s variables. In each of these cases the critical evidence was developed from the perpetrator’s own computer and subsequently used in legal proceedings.

Law enforcement and the legal establishment are facing a new challenge. Criminal acts are being committed and the evidence of these activities are recorded in electronic form. Additionally, crimes are being committed in cyberspace. Evidence in these crimes is almost always recorded in digital fashion. It is important that computer security professionals be aware of some of the requirements of the legal system and understand the developing field of computer forensics.

Hundreds of years of tradition and countless court decisions have developed the complex set of rules that apply to evidence which can be used in legal proceedings. The reality of the Information Age is having a significant impact on the legal establishment. One major area in which this is being felt is that of the acquisition, authentication, evaluation, and legal admissibility of information stored on magnetic and other media.

This information can be referred to as digital evidence. Computer forensics is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law. At one extreme is the pure science of ones and zeros. At this level, the laws of physics and mathematics rule. At the other extreme, is the courtroom.

To get something admitted into court requires two things. First, the information must be factual. Secondly, it must be introduced by a witness who can explain the facts and answer questions. While the first may be pure science, the latter requires training, experience, and an ability to communicate the science.

Paradigm:

A. The Document Paradigm:

First, a document is acquired. How it is acquired (via consent, search warrant, a public record, business record) is subject to a set of rule that have a long and well-documented history. Even so, there are often cases where there will be room for disagreement which will then result in litigation. Rarely is determining that the document physically exists or where it came from, a problem. With digital evidence, this is often a problem. What does this binary string represent? Where did it come from? While these questions, to the computer literate, may seem obvious at first glance, they are neither obvious nor understandable to the layman. These problems then require a substantial foundation being laid prior to their admission into evidence at trial.

Next, a document will undergo an identification process. If the document is in English, then anyone who can read English can probably determine what the document says. Its format and content define its purpose. A binary file requires conversion, in the form of a program, which will transform the data into a form which is humanly readable. Only then, can a human determine what the document is. This process can be summarized as follows:

1. **Acquisition**
2. **Identification**
3. **Evaluation**
4. **Admission as evidence**

B. The Digital Paradigm:

Acquisition of evidence is both a legal and technical problem. In fact, these two aspects are irrevocably related. The law specifies what can be seized, under what conditions, from whom, and from where it may be seized. The determination of what a particular piece of digital evidence is, requires its examination. Is a particular file a word processing document or an executable program? It may require examination to determine where a particular piece of evidence is physically located. Is the file on a local hard drive or is it on a server located in another legal jurisdiction? In short, it may be necessary to show a technical basis for obtaining the legal authority to search. Likewise, it may require technical skills in order to actually accomplish the search. The product of this phase is usually raw media, devoid of meaning or usefulness. Actually identifying a piece of digital evidence represents a three-step process. It must be definable in its physical form. That is, that it resides on a specific piece of media. Next, it must be identifiable as to its logical position. Where does it reside relative to the file system? Lastly, we must place the evidence in the correct context in order to read its meaning. This may require looking at the evidence as machine language, for example, ASCII or EBCDIC, or by means of an application (program).

The path that digital evidence takes can be depicted as follows:

- **Physical Context**
- **Logical Context**
- **Legal Context**

 Media ⇒ Data ⇒ Information ⇒ Evidence
Conclusion:
In law, if information is not admitted into evidence, then, for legal purposes, it does not exist. Testimony by both the forensic specialist who developed the evidence and someone who can explain its significance to the case is often required. Only then does the information become evidence. It should be clear from the above that technical skills and legal expertise must be combined in order to discover, develop and utilize digital evidence. The process used must conform to both the law and science. Failure in either arena renders the product legally worthless. The preceding has been based on the use of computer forensics to exploit stored digital information. Certainly, this need will grow dramatically in the future, as more and more of society's information are stored electronically. However, a potentially even larger use may be to document activities and processes that take place electronically. In other words, to examine data that is not only at rest, but also that which is in motion. And while the law will slowly evolve and accept more and more technical issues, computer forensic specialists will continue the process of education for all parties in the legal process.

References: