Computer Forensics:
an approach to evidence in cyberspace

Abstract

This paper defines the term computer forensics, discusses how digital media relates to the legal requirements for admissibility of paper-based evidence and suggests a methodology for dealing with potential evidence. The conclusion is that digitally based evidence must be both scientifically sound and legally acceptable.

Keywords: law, law enforcement, evidence, forensics, criminal, testimony, court

Introduction

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 behavior 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.

The Document Paradigm

In the paper-based world, the law assumes a process which is mutually understood and observed by all the parties. Almost without thinking, a four-part process takes place. When we try to apply this process to digital evidence, we see that we have a new set of problems.

First, a document is acquired. How it is acquired (via consent, search warrant, a public record, business record) is subject to a set of rules 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. It's 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.

Evaluation of the document follows. This is the time when the reader determines if the information contained in the document is relevant and determines who could testify concerning this document. When our digital data is in human readable form, we can also make these determinations. However, the electronic context of a file is arguably still significant. This will impact on how the evidence is introduced and by whom.

Ultimately, the document may be offered for evidence. This must be done by a warm, breathing, human being who has legal standing to explain it's origin, it's meaning, or both. In the case of paper evidence, the judge and jury may physically inspect the paper and will hear someone who is personally aware of the document describe it and it's significance. It is not necessary to explain the three prior steps to the court, as these

are generally accepted by all participants. At this stage of legal history, such is not the case for digital evidence. As a result, it is often necessary to have the testimony of someone who can explain the process of acquisition, identification, and evaluation.

This process can be summarized as follows:

Acquisition
⇓
Identification
⇓
evaluation
⇓
Admission as evidence

The Digital Paradigm

In the case of paper evidence, this process is very clear and is intuitively obvious. Digital evidence, by it's very nature is invisible to the eye. Therefore the evidence must be developed using tools other than the human eye. It is only logical that the process used in the case of digital evidence mimic the process that is used for paper evidence. Because each step requires the use of tools or knowledge, the process must be documented, reliable and repeatable. The process itself must be understandable to the members of the court.

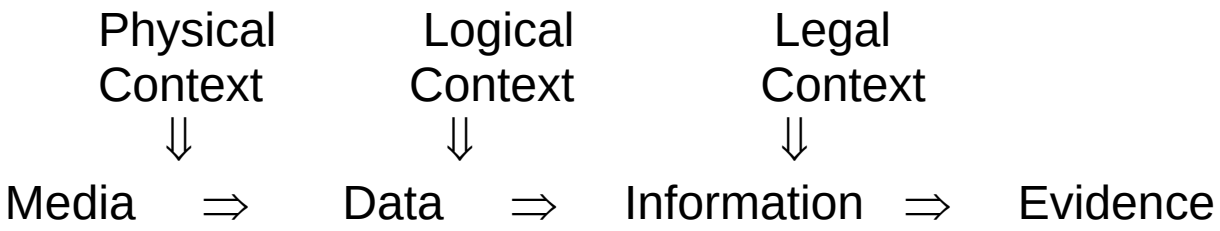
Acquisition of evidence is both a legal and technical problem. In fact, these two aspects are irrevocably related. The law specifies what can be seized, under what conditions, from whom, and from where it may be seized. The determination of what a particular piece of digital evidence is, requires its 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 it's meaning. This may require looking at the evidence as machine language, for example, ASCII or EBCDIC, or by means of an application (program).

Each of these steps requires technical skills and may subsequently require testimony at trial. At this point, we have translated the media into data.

Evaluation of the data involves both technical and legal judgements. Data that is placed in its proper context is called information. From a technical standpoint, it may be possible to make conclusions as to: how the data was produced, when and by whom. The legal issues are the relevance of the information, its reliability, and who can testify to it.

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



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 it's 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:

Catherine H. Conly *Organizing for Computer Crime Investigation and Prosecution* (Washington, DC: National Institute of Justice, 1989).

Donn B. Parker *Computer Crime: Criminal Justice Resource Manual* (Washington, DC: National Institute of Justice, 1989).

United States Department of Justice *Guidelines for Searching and Seizing Computers* (Washington, DC.: U.S. Government Printing Office, 1994)

United States Department of Justice *Basic Considerations in Investigating and Proving Computer-Related Federal Crimes* (Washington, DC.: U.S. Government Printing Office, 1988)