DIGITAL EVIDENCE: THE FUTURE OF COMPUTING IN LAW ENFORCEMENT

Cory Knobler
Villanova University
800 Lancaster Ave, Villanova, Pa 19085
cory.knobler@villanova.edu

ABSTRACT

Digital Evidence is a topic that has been a part of the criminal investigation culture ever since the invention of the personal computer. In recent years there has been a surge of interest in the field due to a number of high profile criminal cases involving technology. Within the past thirty years, computerized systems and networks have become more and more prevalent in society. This widespread reliance on the computing infrastructure has inevitably led to an increase in computer technology being involved in the crime. Thus, it is of vital importance that law enforcement entitles, and the computer scientists who support them understand the nature and role of digital evidence in the modern legal system.

KEY WORDS
digital evidence, data recovery, forensic

1. INTRODUCTION

As stated by Lee[1], the content and the nature of a crime that involves computers and other electronic technology is the determining factor in what classifies evidence as being digital. While this definition appears overly broad with the continual and widespread increase in and reliance on technology, it would be incorrect to assume that digital evidence is limited to computers. Rather, the field of digital evidence and its handling is multi-disciplinary and is likely to continue to expand.

The beginning of digital crime dates back to the late 1970’s beginning with the enactment of the Florida Computer Crimes Act[2] in 1978. The act was initiated in response to an incident at the Flagler Dog Track in Miami, FL. In the FCCA it states under Fla. Stat. 815.05 Offenses against Computer Equipment or Supplies Section 1.a “Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.”[2] This set a precedent for a series of laws in the field of digital evidence.

In the 1980’s there was a massive boom in the production and consumption of the personal computer[3]. Although the internet was not as widespread as it is today, there were some who used some variant of the internet at the time. This opened the door for an entire new type of crime that could be committed, cybercrime[4]. As the internet became more common, there was increase of computer crimes. Of course, because of new technologies such as digital cameras, digital video recorders, and cell phones the field of study is almost limitless.

An important aspect to note in digital evidence is that evidence commonly comes in the form of computer data. As a result, that data is then collected and analyzed by investigators. This process, which is commonly practiced, is known as data recovery.

2. DATA RECOVERY

In a vast majority of crimes that occur involving digital evidence, the primary source of the evidence is generally in some form of data. Accessibility to the data can often present a problem for investigators. In many cases the data can be corrupted or lost and needs to be recovered. However, with advances in technology, law enforcement officials now have the ability to recover data and convert it into a form that is coherent, and therefore, admissible as evidence in a court room. This paper will explore various methods of how to recover data correctly and effectively.

Data recovery is a very complex process that can sometimes require years to complete. There are a plethora of variables that can determine what methods should be used to recover the data. Whether or not the data is recoverable and approximately how long it will take to recover the data are just two of the important questions the investigator must evaluate. This can only be determined after a detailed analysis of the data is performed by the investigator.
3.1 Type of Data

The type of data stored on a computer hard drive can have tremendous variability. Possibilities include, but are not limited to, text files, audio files, and video files. These are all forms of multimedia that can be stored on a computer hard drive. Text files are the easiest of the three types of data to perform recovery because they lack the complexity of an audio file or a video file.

3.2 Condition of Data

The condition that data comes in is very important. Sometimes accessing the data can be difficult because it is hidden behind an encryption. For instance, if data is protected through a weak form of encryption, officials can view the file via a hexadecimal viewer[5]. This will give the examiners an idea of how to decrypt the data and reveal what was hidden.

However, in some cases, criminals have used stronger encryption methods. If a criminal were to use a Data Encryption Standard (DES) algorithm, it is possible to decrypt the data by using a brute force technique. The brute force technique involves a program that will attempt every possible solution for what the passphrase might be until it finds the correct one[5]. There are also programs like AccessData™ DNA Manager that have the ability to decrypt Microsoft Word files or Adobe Acrobat files which are encrypted up to 40-bits[5].

3.3 Type of Operating System

The type of operating system that the computer is running on definitely plays a significant role in how an investigator must go about recovering data. The four major operating systems that exist are the Windows NT platform, the Mac OS platform, the UNIX platform, and the Linux platform. The difference in each operating system is how the hard drive(s) are formatted. Although formatting in both NTFS and FAT is possible on the platforms, it is more common to see NTFS on a Windows machine and FAT on a Mac OS machine. One major difference between UNIX and the other systems is that UNIX does not have any slack space[3]. Slack space is a location on the hard drive were data is sent when it is deleted but the location is formatted[3]. Unallocated space which is the alternate to slack space, is the location where data is sent when it is deleted and the location is not formatted[3]. Therefore, there is a limit in programs for recovering data from UNIX systems, as opposed to Mac and Windows platforms.

3.4 Methods for Recovering Data

There are a multitude of programs that exist on the market that will recover data on hard drives that have either been corrupted or have been overwritten. One of the more common ones is EnCase Forensic™.

3.4.1 EnCase Forensic™

This software is viewed as one of the top analytical and processing programs that exist on the market today. It comes with multiple features including a decryption suite, cell phone analysis, and drive imaging. It allows the user to break down the data into separate components without damaging the original source[6]. This is crucial because it preserves the integrity of the data to still be considered admissible as evidence.

4. LEGAL SYSTEM

With digital evidence only in its infancy, there has been much debate in courtrooms all across the world, particularly in the United States, regarding the admissibility of digital evidence. However, a wider acceptance of digital evidence is gradually building.

4.1 Collecting Digital Evidence

Gathering digital evidence from a crime scene can sometimes be a very daunting task. The most important component of the process is that protocol is always enforced. Most importantly, the search and seizure laws expressed in the U.S. Constitution’s 4th Amendment strictly inhibit law enforcement from collecting potential evidence without going through the proper procedures.

4.2 Use in the Courtrooms

If the evidence is treated properly and is unfettered, than it has the possibility of appearing in court as admissible evidence for the case. The rules of evidence vary from state to state, however, there do exist federal rules that will always overrule any state or local laws.

5. CONCLUSION

With the field continuing to grow, it is important for law enforcement agencies to continue to develop counter measures against these crimes. Although some computer crimes can be just a matter of a financial settlement for illegal music downloads, other crimes exist that are much more malicious and dangerous.

A huge concern of Americans is the security of the infrastructure of the nation from cyber attacks from other nations. With practically every system in our country controlled by computers, the nation has become very susceptible to terrorist attacks through hacking into our networks.
Other crimes that are more prevalent today involving computers are the proliferation of child pornography and identity theft. With the development of social networking sites such as MySpace™ and facebook™, criminals have easier access to contacting children and committing heinous crimes. Identity theft has now increased dramatically due to extensive use of shopping websites as well as online banking.

It is important to continue to research methods of how these hacks are accomplished as a preventative measure for the future.

REFERENCES


