

**The Use of Random Forest to Develop an
Intelligent Computer Forensic Tool**

Lakisha S. Dailey

Technical Report #NSUCS-2004-007

**Norfolk State University
Department of Computer Science**

Abstract

Forensics is the use of science and technology to investigate and establish facts in criminal or civil courts of law. Therefore, computer forensics is the science whereby experts dig up data from computer media in such a way that it may be utilized in a court of law. This proof may consist of such things as, theft, malicious destruction of software, deleted files, spreadsheets, computer logs, etc. Computer Forensics occupies the safety, discovery, extraction, credentials, and understanding of computer data. This evidence is possibly used to state that a crime has been committed or emphasize other points of fact in a court, such as, defend the innocent, prosecute the guilty, and be aware of motives and intents of individuals.

The purpose of this paper is to provide information on developing a better technique in using forensic tools. It is not to recommend any tool over another, but to compare my new techniques with other popular tools to establish similar or better findings.

Table of Contents

Introduction	3
What is Computer Forensics?	3
Background Information	4-5
Computer Evidence Steps	5-7
Research	7-9
Future Work	9
Bibliography	10

Introduction

Computers have altered the way the world does business today. They have also changed the world's view of evidence because computers are used more and more as tools in the task of "traditional" crimes. Evidence relative to personnel problems, malicious destruction of software, employee sabotage, blackmail, identity theft, sexual harassment and government espionage is emerging. Criminals are becoming wiser in committing crimes. Personal computers are being encountered in nearly every kind of criminal action. People use computers to clone cellular phones and re-code credit cards. Forgers use computers to construct realistic looking false identification. Information such as credit card numbers and social security numbers has been exposed on personal computers. This new technology twist in crime patterns has brought computer proof to the front position in law enforcement circles.

Computer forensics is quickly becoming a science recognized on parity with other forensic sciences by the legal and law enforcement communities. As this development proceeds, it will become even more important to control and observe computer evidence appropriately.

What is Computer Forensics?

Computer forensics has been defined as "the application of computer investigation and analysis techniques in the interests of determining potential legal evidence", according to Judd Robbins. Another definition is "Forensic computing is the science of capturing, processing and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law [1]." The subject matter includes: the secure collection of computer data, the examination of the suspect's data to determine details, the presentation of computer based information to court of law and the application of the country's laws to computer practice. The main purpose in computer forensics is to recover, analyze and present computer based material where the information that is retrieved is valid, convincing and compelling to the court of law.

Background Information

Computer forensics is the recovery of deleted computer-based information and the science examining and piecing back together the who, what, when, where, and how of computer-related conduct. Computers are being increasingly used to oblige crimes. When working with these kinds of cases, the judicial authorities have to turn to digital processes to come with substantiation and indication. This is where the forensic security tools and assessments become helpful.

The forensic security tool makes it possible to gather and analyze computer data. Around 1984, the FBI Laboratory and other law enforcement agencies began developing programs to scrutinize computer evidence. The FBI established the Computer Analysis and Response team and charged it with the responsibility for computer analysis to accurately address the growing demands of investigators and prosecutors in a planned and programmatic manner. A dilemma that occurred by law enforcement was to identify resources within the organization that could examine computer evidence. These resources were frequently spread throughout the agency. Today, there appears to be a trend toward moving these examinations to a laboratory environment. Since 1985, Kroll Ontrack has helped hundreds of thousands of clients recover, restore, search, and produce electronic information. It is recognized as the worldwide leader in the industry. Law firms, Fortune 500 companies, financial institutions, and government agencies have trusted this company with their most difficult, critical and time-sensitive data. In 1995, a survey conducted by the United States Secret Service indicated that forty eight percent of the agencies had computer forensic laboratories and that sixty eight percent of the computer verification seized was forwarded to the experts in those laboratories. As encouraging as these statistics are for a controlled programmatic response to computer forensic needs, the same survey reported that seventy percent of these same law enforcement agencies were doing the work without a written manual. Computer forensic examinations are conducted in forensic laboratories, data processing departments, and in some cases, the detective's squad room. The assignment of personnel to conduct these examinations is based often on available expertise, as well as department policy. Despite of where the examinations are conducted, a legitimate and dependable

forensic examination is required. This requirement recognized no political, methodological, industrial, or jurisdictional boundaries.

There are constant efforts to extend examination standards and to give structure to computer forensic examinations. As early as 1991, a group of six international law enforcements agencies met with several United State federal law enforcement agencies in Charleston, South Carolina, to converse computer forensic science and the need for a standardized approach to examinations. In 1993, the FBI hosted an International Law Enforcement Conference on Computer Evidence that was attended by seventy representatives for a range of U.S. federal, state, and local law enforcement agencies and international law enforcement agencies. They all decided that standards for computer forensic science were lacking and needed. This conference again convened in Baltimore, Maryland, in 1995, Australia in 1996, and the Netherlands in 1997, and ultimately resulted in the formation of the International Organization on Computer Evidence. In addition, a Scientific Working Group on Digital Evidence, also known as SWGDE was created to address these same problems along with federal law enforcement agencies.

There are methods to investigate and analyze data that is obtained from electronic storage. Computer forensic is a science that is now linked to other forensic science that is utilized in the legal and law enforcement field. In computer forensics a process is used for investigations. The first step is to establish an occurred incident by collecting the data. Secondly, examine the evidence and determine whether or not computer forensic is needed. Next, one must present the data, meaning a technical report that includes charts and graphs.

Computer Evidence Steps

There are no strict rules that must be followed concerning the processing of computer data, but there are general rules one can take. Every case is different and depending on the case certain actions should be taken first. As long as good technical knowledge and common sense is used it makes the distinction between success and failure.

Usually the first step taken is shutting down the computer. Time is very valuable and this step should be done as soon as possible. The second step is to document the hardware configuration of the system. Before moving the computer to a secure location it is imperative that pictures are taken of the device from all angles and views to document the system hardware components. Next, is to ship the computer system to a protected location. It is vital that the subject computer is treated as proof and it should be stored out of reach of unauthorized users. After placing the computer in the proper location experts should make bit stream backups of hard disks and floppy disks. The computer should not be tampered with until this is done. The original evidence should be left untouched and undamaged. Afterwards one may mathematically authenticate data on all storage devices.

Once the computer is in your hands, you want to confirm that you did not modify any of the evidence. Whether if there was a robbery, murder, or computer crime committed, documenting the date and time of the incident is extremely crucial. The exact date and time can justify many situations. Along with documenting the date and time make a list of key search words. It is almost impracticable for an expert to physically view and evaluate every file on a hard disk drive because the drive is extremely enormous. As a result, high-tech forensic text search tools are highly recommended to help uncover valuable information. Next it is necessary to evaluate the windows swap file, file slack and unallocated space. The swap file is usually an important cause of evidence and it definitely provides a great deal of lead way. File slack potentially contains randomly selected bytes of data from computer memory. This happens because DOS/Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, DOS/Windows makes up the difference by padding the remaining space with data from the memory buffers of the operating system. File slack is created at the time a file is saved to a disk. When a file is deleted under DOS, Windows, Windows 95, Windows 98 and Windows NT/2000/XP, the data associated with RAM slack and drive slack remains in the cluster that was formerly assigned to the end of the 'deleted' file. It is important to understand the significance of file slack in computer-related investigations. File slack potentially contains data dumped

randomly from the computer's memory, and it is possible to identify network logon names, passwords and other sensitive information associated with computer usage. File slack can also be analyzed to identify prior uses of the subject computer and such data can help the computer forensics investigator [7]. Specialized forensic tools are mandatory to view and evaluate file slack and it may prove to provide tons of information and once again lead way. Many computer users do not know that the DOS and Windows delete function does not completely erase files. Users are unacquainted with the fact that the storage space associated with such files simply becomes unallocated and available to be overwritten with new files.

Last but not least document the findings and retain copies of the software used. Copies are generally done on an archive zip disk, jazz disk or other external storage devices. Like stated before, it is vital to organize and keep a record of your findings [8].

Research

Given the opportunity to utilize computer forensic tools within my academia gave me the advantage to incorporate my knowledge into my research. There are many tools that will help detect computer crimes. Computer crimes are criminal acts in which a computer is essential to the perpetration of the crime [2]. Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization or committing theft commits a computer crime [10]. Utilizing the tool Encase allowed me to track down malicious computer crimes. EnCase is a very interesting piece of software. It's a software suite manufactured by Guidance Software out of Pasadena that allows an investigator, forensic investigator to obtain or acquire an exact bit to bit, byte to byte duplicate image of suspected media; that can be a hard drive, a floppy disk, a CD-ROM, or a zip disk. EnCase is a forensic data acquisition and analysis program for Window 95/98 and NT that is based on the specification and requirements of the law enforcement community. Its' purpose is to

aid in computer-related investigations. EnCase is a software used by many law enforcement agencies to scan the hard drive of computers that have been detained so evidence may be extracted for the case against the person or company the computer was detained from [5]. It provides a much simpler way to conduct a search of a computer system, document the findings, and make evidentiary and discovery copies. Since EnCase is completely non-invasive, the original computer evidence is never changed or modified. In addition, a hard drive of any size can be compressed and stored on removable media, allowing one to take the evidence with them. Even files that have been deleted, hidden or renamed can be located quickly and easily with this unique software. EnCase also authenticates and verifies all copies of original evidence. This ensures that the integrity of the evidence is protected and that it can meet foundation and authentication challenges [6].

I utilized EnCase on a scenario where on December 8, 2003 I noticed that one of the documents that were to be presented at a Computer Security Conference had been tampered with. Also, many files had been deleted. The information contained in the document was confidential, as it contained individual's social security numbers. My task was to investigate the date and time this breach occurred in order to narrow the suspect down to one individual.

EnCase allowed me to search for times and dates that the document had been modified which narrowed the suspect down to one person who had the availability and motive to commit such an act. This tool made it possible to run search strings on the data. Additionally, I was able to sort and look at the dates that files were accessed, created, and modified to determine when the computer was last used.

In a Windows environment every time a file is opened, EnCase would show that that file had been accessed on that particular date and time. I was able to look at valuable information without changing a modified or accessed date because of the write block that it puts on the data. As a result, viewing the document did not, in any way change the data that was present. When an individual runs searches in EnCase, it searches the entire hard drive including what is in an allocated space, which is an area in the hard drive that operating systems typically write data to. Thus, EnCase searches all areas, including folders and areas where data is to reside.

I definitely realized that EnCase is a very effective tool. This software is unquestionably helpful when tracking malicious computer crimes. Every piece of media is shown in a Windows Explorer-type format, and the examiner can view all files including deleted folders, file fragments and unallocated clusters with altering the evidence of changing file date stamps. EnCase has been successfully admitted into evidence in thousands of trials and hearings throughout the world and is now the standard by which computer investigations are conducted.

Future Work

Computer crimes will continue to grow and it will be necessary to further develop tools that will facilitate the investigative process. My future work includes examining several forensic tools, extracting their best features and ultimately developing my own. Subsequently, I will utilize this tool to guide an examiner through a scenario where information will be examined and compare the results with existing tools. The results will determine what tools resulted in the best findings or if all the tools figured out the same findings.

VIII. Bibliography

- [1]. Computer Forensics
URL: <http://members.ozemail.com.au/~cyberspace/overview1.htm>
(March 1, 2004)
- [2]. Computer Crime Investigation Using Computer Forensics
URL: <http://members.ozemail.com.au/~cyberspace/overview3.htm>
(March 1, 2004)
- [3]. Technology Pathways LLC. “The Art of Key Word Searching”
URL: www.TechPathways.com
(March 11, 2004)
- [4]. Adv. Rohas Nagpal. “Recovery of Digital Evidence.”
URL: http://www.asianlaws.org/cyberlaw/library/cc/dig_evi.htm
(January 2004)
- [5]. WorldNet News. “Encase”
URL: <http://www.worldneet-new.com/encase.htm>
(May 27, 2004)
- [6]. Keightley, R. “Forensic Duplication and Analysis Using EnCase”
URL: <http://faculty.ncwc.edu/toconnor/426/426lect07.htm>
(May 27, 2004)
- [7]. ISP Glossary: Slack Space
URL: http://isp.webopedia.com/TERM/S/slack_space.html
(May 21, 2004)
- [8]. New Technologies Armor, Inc. “Computer Evidence Processing Steps”
URL: <http://www.forensics-intl.com/evidguid.html>
(January 18, 2004)
- [9]. “Tools and Methods”
URL: <http://members.ozemail.com.au/~cyberspace/tools.htm>
(January 2004)
- [10]. “Computer Crimes”
URL: http://home.mesastate.edu/~jerry/systeminfo/computer_crime/html
(April 22, 2004)