December 2003

Forensic Computing

X. Li
University of Wollongong

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Forensic Computing

Abstract

Technology is rapidly changing the speed and manner in which people interact with each other and with the world. As technology helps criminals to operate more easily and quickly across borders, so law enforcement capability must continuously improve to keep one step ahead. Computer forensics has become a specialized and accepted investigative technique with its own tools and legal precedents that validate the discipline. Specially designed forensic software is also widely used during the whole process of computer forensic investigation. This article introduces computer forensic and computer evidence, introduces and compares some forensic software, and summarizes its likely future development.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Li, X and Seberry, J, Forensic Computing, in Proceedings of INDOCRYPT'03, Lecture Notes in Computer Science, 2904, 2003, 18-35. Original Springer-Verlag journal available here.

Forensic Computing

Xiang Li and Jennifer Seberry *

Abstract

Technology is rapidly changing the speed and manner in which people interact with each other and with the world. As technology helps criminals to operate more easily and quickly across borders, so law enforcement capability must continuously improve to keep one step ahead. Computer forensics has become a specialized and accepted investigative technique with its own tools and legal precedents that validate the discipline. Specially designed forensic software is also widely used during the whole process of computer forensic investigation. This article introduces computer forensic and computer evidence, introduces and compares some forensic software, and summarizes its likely future development.

1 Background

1.1 Computer forensics defined

Computer forensics or forensic computing has become a popular topic in computer security circles and in the legal community. So what is computer forensics?

Dorothy A. Lunn's (Dorothy) definition of computer forensics is, "The employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity." Judd Robbins (Judd), a computer forensics investigator, defines computer forensics as "Simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence." James Borck (James), in his article "Leave the cybersleuthing to the experts". Defines Computer forensics as "the equivalent of surveying a crime scene or performing an autopsy on a victim".

From these descriptions, we can see computer forensics can be defined as the application of computer investigation and analysis techniques in the interests of determining potential evidence. It deals with the application of law to a science and it involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing.

1.2 Requirements for computer forensics

Nowadays more and more criminals have been shifting their attention from armed robbery to computer crime. Criminals may use computers in one of two ways in support of their actions. Either as the repository for information relating to their criminal activity, which is called computer related crime, or as a tool in actually committing a crime, this is so called computer crime. For them, a computer is much more powerful than a knife or a gun. More seriously, the probability of being caught on their

*Centre for Computer Security Research, SITACS, University of Wollongong, Wollongong, NSW, 2522, Australia.

actions is very low. For example, a hacker can break into a bank's online transaction system and steal $250,000 without being caught or charged for lack of enough evidence even if he is caught. The fact is that the criminals are no longer stupid and always easily caught as in the show on TV or in the movies. Many modern criminals are trying to use computers and other modern technologies to realize their crimes without being discovered, this is so called high tech crime. Therefore, the needs for professionals capable of performing electronic investigations that can produce the necessary evidence to convict have increased.

Another requirement for computer forensics is because of the vast number of documents now exist in electronic form. Years ago, most evidence collected was on paper. Today, the majority of evidence resides on a computer this makes it fragile by its very nature. No investigation involving the review of documents, either in a criminal or corporate setting, is complete without including properly handled computer evidence. Additionally, computer forensics ensures the preservation and authentication of computer data and greatly facilitates the recovery and analysis of deleted files and many other forms of compelling information normally invisible to the user.

On the other hand, the basic nature of Internet technology offers criminals many ways to hide their tracks and disguise their crimes. Computer crimes are borderless; the crime can be committed over a modem from next door or from ten thousand miles away, with equally effective outcomes. However, at the same time, technology provides many clues as to the nature of the crime, how it was committed, and who was behind it. In computer forensics, things are not always as they seem. The criminals tend to stay a few steps ahead of law enforcement, and often come up with the most inventive means of protecting themselves and destroying evidence. It is the job of the computer forensics expert to work with law enforcement to preserve evidence, reconstruct crimes, and ensure that the evidence collected is usable in court. Only after extensive analysis is there any hope of finding out who is responsible for computer crimes.

1.3 Computer evidence

1.3.1 Introduction

Obviously, evidence plays a significantly important role in a criminal case. The target of computer forensic investigation is to find potential computer evidence that could be used in court. "Computer evidence could be defined as any item that supports the criminal enterprise currently under investigation." (Anderson) It will include hardware, software, messages of transmissions, session logs, and password authorizations or any other item that helps to define or establish that criminal conduct has occurred The first step to any computer related investigation is to recognize and search for the evidence specific to that offence being investigated. In many instances the type of physical evidence will be easily recognizable. E-mail threats, denial of service attacks or password hacking all leaves electronic trails that must be preserved. Other kinds of computer crime, such as Internet child pornography, hacking, and virus attacks, may not be as apparent and may require the forensic examination of hardware components as well.

Gathering evidence in a computing environment is not simple as copying files from the suspects' computer and printing them out for presentation, although it is really an important part of the computer forensic investigation. In fact, to access and find such data we need specialized tools and knowledge. The challenging problem is to be aware of what kinds of information exist on a computer and how to go about gathering and preserving the original data and making certificated copies of that evidence. Deliberately disguised information in the form of encrypted, misnamed or steganographically-hidden data will also be explained. In certain cases, we will be able to decrypt data that has been found encrypted and the means to do so will be explained and sources noted. But where can forensic investigators find potential computer evidence? The following are some hints for them.

- List of URLs recently visited (obtained from the temporary Internet files or Web cache and History

folders)

- E-mail messages and list of e-mail addresses stored in the suspect's Address book; the filename depends on the e-mail program in use for example, the .pst file for Outlook (In some cases, this information will be stored on an e-mail server, such as an Exchange server)
- Word-processing documents; the file extension is dependent on the program used to create them common extensions are .doc, .wpd, .wps, .rtf, and .txt
- Spreadsheet documents; the file extension is dependent on the program used to create them examples include .xls. .wgl, and .wkl
- Graphics, in the case of child pornography cases; the file extensions include .jpg, .gif, .bmp,, .tif, and others
- Chat logs; the filename depends on the chat program
- The Windows Registry (where applicable)
- Event viewer logs
- Application logs
- Print spool files

Once the extraction of the computer evidence has been accomplished, protecting the integrity of computer evidence becomes of paramount concern for investigators, prosecutors and those accused. Computer evidence is very fragile and can easily and unintentionally be altered or destroyed. Therefore, it is important that only properly trained computer evidence specialists proves computer evidence.

1.3.2 Rules of computer evidence

In Australia the Commonwealth of Australia's Evidence Act's requirements, a list of five rules of evidence that need to be followed in order for computer evidence to be useful to the court, and make them easy to understand. Other jurisdictions have similar laws.

• Admissiblity

This is the most basic rule: the evidence must be able to be used in court or elsewhere. Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

• Authenticity

If an evidence can't be tied positively to the corresponding incident, it can't be used to prove anything. Forensic investigators must be able to show that the evidence relates to the incident in a relevant way.

• Completeness

It's not enough to collect evidence that just shows one perspective of the incident. Forensic investigators must not only collect evidence that can help prove the attacker's actions but also consider and evaluate all evidence available and retain it. Similarly, it is vital to collect evidence that eliminates alternative suspects. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and demonstrate why you think they didn't do it.

• Reliability

The process of evidence collecting and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

• Believability

The evidence being presented should be clear, easy to understand and believable by a jury. There's no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if the evidence is presented with a formatted version that can be readily understood by a jury, you must be able to show the relationship to the original binary, otherwise there's no way for the jury to know whether you've faked it.

1.3.3 Legal issues about computer evidence

This is important for computer forensics as often an incident occurs which involves more that one jurisdiction, and could also involve overseas jurisdictions. Currently an Australian investigator has to have a working knowledge of all eight Australian Evidence Acts and the corresponding crime legislations. A common 'local' Evidence Act would improve the functionality of investigations where only one set of domestic 'rules' is required

Investigators also need to beware that what is acceptable, legal practice in one jurisdiction may be unacceptable in another, rendering the evidence collected inadmissible in that jurisdiction's law courts.

An example where standard legislation would be beneficial is where an incident occurs in Western Australia in a national company whose head office, and internal investigators reside in NSW. The investigators, in addition to their local NSW Act also need to know the Western Australia Act, and the corresponding crime legislations.

Similarly an incident for an Australian based international company could occur in their Tokyo or London office requiring an Australian investigator to attend the scene and conduct an investigation. This is where knowledge of international evidence handling rules is essential.

1.4 The Computer forensic process

As forensics is the recovery of evidence through a scientific method and methodology is the heart of any forensic science, computer forensics is no exception. A standard procedure for collecting, protecting, and examining computer evidence must be made and adhered to from start to finish, so as to preserve the integrity of the evidence. A standard computer forensic process should include four steps:

1. Identifying
2. Preserving
3. Analysing
4. Presenting

Identifying is the process of identifying such things as what evidence is present, where and how it is stored, and which operating system is being used. From this information the investigator can identify the appropriate recovery methodologies, and the tools to be used.

Preserving is the process of preserving the integrity of the digital evidence, ensuring the chain of custody is not broken. The data needs to be preserved on stable media such as CD-ROM, using reproducible methodologies. All steps taken to capture the data must be documented. Any changes to the evidence must also be documented, including what the change was and the reason for the change. You may need to prove the integrity of the data in a court of law

Analysing is the process of reviewing and examining the data. The advantage of copying this data onto CD-ROMs is the fact that it can be viewed without risk of accidental changes, therefore maintaining the integrity whilst examining the evidence.

Presenting is the process of presenting the evidence in a legally acceptable and understandable manner. If the matter is presented in court the jury, who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original; otherwise all your efforts could be futile.

As the first step of computer forensic examination, Identifying plays an important role and it should be followed as a standard processing. The following is a general evidence processing guidelines from New Technologies Inc. (NTICEPS):

1. Shut down the computer; this should be done as quickly as possibleconsideration should be given to possible destructive processes that may be operating in the background.

2. Document the hardware configuration of the computer system being investigated and pay attention to how the computer is set up before it is dismantled it will need to be restored to its original condition at a secure location. A proper chain of custody can be maintained and evidence processing can begin. A chain of custody is a roadmap that shows how evidence was collected, analysed, and preserved in order to be presented as evidence in court. Establishing a clear chain of custody is crucial because electronic evidence can be easily altered.

3. Transport the computer system to a secure location and don't leave the computer unattended unless it is locked up in a secure location.

4. Make a bit stream copy of hard disks and floppy disks: The compputer should not be operated and computer evidence should not be processed until bit stream backups have been made of all hard disk drives and floppy disks. All evidence processing, should be done on a restored copy of the bit stream backup, not on the original computer. During this step, special designed forensic software is strongly recommended to use.

   Preservation of computer evidence is vitally important because computer evidence is always fragile and can easily be altered or destroyed. Such alteration or destruction of data is beyond recovery. Bit stream backups are much like an insurance policy and they are essential for any serious computer evidence processing.

5. Mathematically authenticate data on all storage devices: To be able to prove that the evidences haven't been changed, all files and disks must be authenticated. Such proof will help you rebut challenge that you changed or altered the original evidence. Due to the improvement of today's speed of computers and the vast amount of storage capacity on computer hard disk drives, the level of accuracy for A 32 bit CRC is no longer accurate enough. Therefore, currently most forensic examination tools using a 128 bit level of accuracy to mathematically authenticate data.

6. Document the system date and time: The dates and times associated with computer files can be extremely important from an evidence standpoint. Document the system data and time settings at the time the computer is taken into evidence.

7. Make a list of key search words: There are forensic tools available to search for relevant evidence. Gathering information from individuals familiar with the case to help compile a list of relevant key words is important these can be used to search the disk drives.

8. Evaluate the Windows swap file: The Windows swap file is a potentially valuable source of evidence and leads. The evaluation of the swap file can be automated with forensic tools. Unix system uses either a swap file on one existing file system or an individual swap partition to store information temporarily. So the swap file or the swap partition must be checked for potential evidence.

9. Evaluate file slack: File slack is a data storage area of which most computer users are unaware. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or view of the user. Forensic tools are required to view and evaluate file slack and it can provide a wealth of information and investigative leads.

10. Evaluate unallocated space (erased files): The DOS and Windows 'delete' function does not completely erase file names or file content. Unallocated space may contain erased files and file slack associated with the erased files. The DOS Undelete program can be used to restore the previously erased files. However, Unix system doesn't provide any tool to directly recover the "deleted" files. The solution is to find the raw data's location and modify it.

11. Search files, file slack and unallocated space for key words: The list of relevant key words identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes.

12. Document file names, dates and times: From an evidence standpoint, file names, creation dates, last modified dates and times can be relevant. Therefore, it is important to catalog all allocated and 'erased' files.

13. Identify encrypted or compressed files and graphic files that store data in binary format: As a result, data stored in these file formats cannot be identified by a text search program. Manual evaluation of these files is required and in the case of encrypted files, much work may be involved. Reviewing the partitioning on seized hard disk drives is also important.

14. Evaluate program functionality: Depending on the application software involved, running programs to learn their purpose may be necessary.

15. Document the findings: It is important to document the finding as issues are identified and as evidence is found. It is also important to document the software that was used in the forensic evaluation of the evidence including the version numbers of the programs.

16. Retain copies of software used: As part of the documentation process, it is recommended that a copy of the software used to included with the output of the forensic tool involved. Often it is necessary to duplicate forensic processing results during or before trial. Duplication of results can be difficult or impossible to achieve if the software has been upgraded and the original version used was not retained.

Following a standard evidence investigating process will help investigators find the right information and keep the potential evidence reliable and believable by the court. However, during the investigating process, good knowledge of computer systems and legal issues can't guarantee the success of the investigation; specially designed forensic software is another esseential weapon for forensic examiners.

2 Forensic software

2.1 Introduction

The science of forensics is a highly technical and detailed discipline. The methodology of a computer forensics expert is that he has a wide range of computer hardware and software expertise. He can identify the intrusion by knowing where to look, what to look for, and what other evidence may be needed. Hw should gather enough information to decide if law enforcement should be involved. Most important, a

computer forensics expert has to possess a wide variety off skills, own or develop a suite of software forensics tools, and maintain the integrity of the chain off evidence according to accepted legal practices. To ensure that computer evidence is admissible in court, it is best practice and use of forensic software which can help computer forensic investigators. From the point of forensic investigation, forensic software can be used through out the whole process from identifying to analysing evidence.

Generally, there are some specific criteria for forensic investigators to choose the right forensic software:

- It must not alter the data as a side effect of the collection process.
- It must collect all of the data wanted, and only the data wanted.
- The user must be able to ensure whether the software works properly.
- It must be generally accepted by the computer forensic investigative community.
- The results produced must be repeatable.

2.2 Classification of forensic software

Depending on their functions and targets, forensic software can be divided into several groups.

2.2.1 Hashing functions

To mathematically create a unique signature for the content of a computer hard disk drive is very important to keep evidence reliable. Special hashing algorithms must be used to create the unique identity for files and disks.

Most law enforcement computer forensic specialists rely upon mathematical validation to verify that the restored mirror image of a computer disk drive and relevant files exactly match the contents of the original computer. Such comparisons help resolve questions that might be raised during litigation about the accuracy of the restored mirror image. They also act as a means of protection for the computer forensic specialists concerning allegations that files were altered or planted by law enforcement officials during the processing of the computer evidence.

In the past 32 bit algorithms were used for this purpose and programs such as CRCHECK and CRC32 became popular. More recently it has become necessary to use more accurate mathematical calculations for this purpose, i.e. 128 bit hashes. The reasons are tied to the potential for brute force attacks using today's powerful desktop computers and also the volume of files that exist on contemporary computer hard disk drives. It is not uncommon to find over 100,000 files to be stored on computer hard disk drives today and the storage capacity increases each in few months due to advances in technology.

The following is a comparison of methods to create the unique identity for computer files and data.

Checksums

A method of checking for errors in digital data. Typically a 16- or 32-bit polynomial is applied to each byte of digital data that you are trying to protect. The result is a small integer value that is 16 or 32 bits in length and represents the concatenation of the data. This integer value must be saved and secured. At any point in the future the same polynomial can be applied to the data and then compared with the original result. If the results match some level of integrity exists.

Common types:

CRC 16

CRC 32

Advantages:

1. Easy to compute

2. Fast Small data storage
3. Useful for detecting random errors
Disadvantages:
1. Low assurance against malicious attack
2. Simple to create new data with matching checksum
3. Must maintain secure storage of checksum values

One-way hash algorithm
A method for protecting digital data against unauthorized change. The method produces a fixed length large integer value (ranging from 80 to 240 bits) representing the digital data. The method is said to have one-wayness because it has two unique characteristics. First given the hash value it is difficult to construct new data resulting in the same hash. Second given the original data it is difficult to find other data matching the same hash value.
Common types:
SHA-1
MD5
MD4
MD2
Advantages:
1. Easy to compute
2. Can detect both random errors and malicious alterations
Disadvantages:
1. Must maintain secure storage of hash values
2. Does not bind identity with the data
3. Does not bind time with the data

Digital Signatures
A secure method of binding the identity of the signer with digital data integrity methods such as one-way hash values. These methods use a public key cryptosystem where the signer uses a secret key to generate a digital signature. Anyone can then validate the signature generated by using the published public key certificate of the signer. The signature produces a large integer number (512- 4096 bits)
Common types:
RSA
DSA
PGP
Advantages:
1. Binds identity to the integrity operation
2. Prevents unauthorized regeneration of signature unless private key is compromised
Disadvantages:
1. Slow
2. Must protect the private key
3. Does not bind time with the data
4. If the keys are compromised or certificate expires digital signature can cause difficullties

3 Bit-stream function

Computer evidence is, by its nature, fragile. Some data is volatile that is, it is transient in nature and, unlike data stored on disk, will be lost when the computer is shut down. Data on a computer disk can be easily damaged, destroyed, or changed either deliberately or accidentally. The first step in handling such digital evidence is to protect it from any sort of manipulation or accident. The best way to do this is to immediately make a complete bit stream image of the media on which the evidence is stored. A bit stream image is a copy in which every bit is copied sector by sector from the original disk to the duplicate. It significantly differs to the disk backup we normally used. Special forensics software must be used to undertake bit stream imaging for forensic examination.

National Institute of Standards and Technology (NIST) defines Disk imaging tool top-level requirement as following:

- The tool shall make a bit-stream duplicate or an image of an original disk or partition.
- The tool shall not alter the original disk.
- The tool shall be able to verify the integrity of a disk image file.
- The tool shall log I/O errors.
- The tool's documentation shall be correct.

Basically, a bit-stream imaging tool should not alter the original disk, must log every issue during the imaging process and notify the user if error happens. In addition, for security considerations, internal verification should be made. It is used to verify the imaging procedures and to check if there are any changes during imaging process. Checksums is one of the ways to check the validity of the copy from the original drive. It will apply an advanced mathematics algorithm to the information stored on a drive or file. The output of this mathematics will give a unique output. This means that we can compare the original with the copy using the checksum. The same checksums between original and copy shows an exact copy has been produced. It is almost impossible and extremely difficult ot change the information on the drive without changing the checksums. On the other hand, some of the disk-imaging tools use cyclical redundancy checksums (CRC) or MD5 checksums to ensure the integrity of the evidence.

3.0.2 Data process function

Normally computer evidence can be easily found in spreadsheet, database or word processing files. On the other hand, potential evidence can also be found in Windows swap file, page files, file slack or unallocated file space by using special forensic tools.

In such circumstances, data stored in non-traditional computer storage areas and formats is called ambient data. Special tools are needed to find these ambient data for potential evidence.

For example, many Windows applications create temporary files to facilitate sorting functions, the creation of indexes, and scrolling. Such files can contain fragments of the work session that generated the creation and use of the temporary files. Most temporary files created by Windows applications, e.g., databases and word processing programs, are automatically deleted when the file and/or application is closed. As with other files erased under Windows, the data remains behind on the computer storage device. Windows also creates temporary files as a normal process during the operation of the computer. Most temporary files created by Windows are not deleted by the operating system.

The Unix operating system is completely different from the Windows platform. Swap space is a complimentary composition of Unix file system. You can use either a swap file on one existing file system or an individual swap partition to store information temporarily. Basically, there's no individual

temporary files created for applications. So in most circumstance, the Unix swap partition is an extremely important source for seeking potential evidence.

3.0.3 Windows system temporary files

Operating System: Windows 3x
Filename: 386SPART.PAR
Default Location: WindowsSystem subdirectory or root directory of the drive designated in the virtual memory dialog box

Operating System: Windows 9x
Filename: WIN386.SWP
Default Location: Root directory of the drive designated in the virtual memory dialog box

Operating System: Windows NT2000XP
Filename: PAGEFILE.SYS
Default Location: Root directory of the drive on which the system root directory (WINNT by default) is installed

3.1 Other data recover functions

In some circumstances, computer files are not really completely removed from computer system. The "delete" identity appears to have been used but the data is still kept. These files or data can be recovered by special tools and identified as potential evidence.

3.1.1 Content searching function

Sometimes, we need a quickly search on hard disks, zip disks or floppy disks for keywords or specific patterns of text. Different forensic case has different keyword. For example, in a child pornography investigating scene, we can use "lolita" as keyword to search potential evidence, however, it is absolutely not the right keyword for a financial fraud case

3.1.2 Password recovery function

Files or data in personal computers sometimes may be encrypted for personal purposes. Sometimes, access to these files and data is required for evidence collection. Cryptography technology will be used for cracking the password or decrypt the encrypted computer system. However, investigators should consider personal privacy issues before using this function.

3.1.3 Audio and video enhancement function

Audio or video data got from surveillance maybe hard to be examined dur to clarity problems. Special tools can be used to enhance the signals of audio or video data such that investigators can obtain more information from it. For example, speech enhancement technology can be used for analysing forensic recording on tapes.

4 Forensic software products

Currently there are several professional forensic software products on the market. Besides the main hashing, bit-stream imaging, and test searching functions, they also provide some other features.

4.1 Storage Media Archival Recovery Toolkit (SMART)

is a forensic software product provided by ASR Data Acquisition Analysis, LLC. It is designed and optimised to facilitate data forensic practitioners and Law Enforcement personnel.

SMART can acquire digital evidence from a wide variety of devices by creating a true and accurate bit-image copy of the original, authenticate the data it acquires using any or all of the CRC32, MD5 and SHA-1 hashing algorithms. It supports BeFS, VFAT, FAT32, HFS, HFS+,, NTFS, EXT2,EXT3, ReiserFS and many more files systems. SMART automatically logs an investigator's actions, providing a self-documenting chain of custody should it be required in court. Furthermore, SMART can generate a comprehensive report detaining the hardware, software, configuration and contents of a device or an entire system, quickly and easily.

The core requirement of professional forensic software is to seek potential evidence without changing anything on the evidence storage media. To ensure the reliability of the evidence by the law enforcement, SMART creates a true image of the seized evidence disk bit by bit and authenticates the coherence of the image file against the original media by checking the hashing value to prove the evidence was found in a unmodified environment.

Currently SMART only support BeOS and Linux operating system. The support to other platforms such as Windows or Mac OS will be available next.

4.1.1 Core features of SMART

- Data Acquisition (disk imaging, wiping and restoring)
- Data Authentication (hashing)
- Data Analysis (media Searching)
- Log and Report

4.2 EnCase

4.2.1 Core features of EnCase

- Multiple Sorting Fields, Including Time Stamps
- Automated Search and Analysis of Zip Files and E-Mail Attachments
- File Signature and Hash Library Support
- Escript Macro Language
- Unicode Support

4.3 Maresware

is Mares and Company's forensics software product. "It provides an essential set of tools for investigating computer records and securing private information."

4.4 Law Enforcement Software (LESS)

is the NTI's (New Technologies Inc.) forensic software product. It includes several forensic tools running under Windows or DOS platform, which have special forensic functionalities.

5 Forensic special purpose software

5.1 Forensic software for steganography

Steganography is the art of hiding information within information so as to not arouse suspicion and the process of injecting information into covert channels so ass to conceal the information. It is an effective tool for protecting personal information, and organizations are spending a lot of energy and time ain analysing steganography techniques to protect their integrity. However, steganography can also be detrimental. It is hindering law enforcement authorities in gathering evidence to stop illegal activities, because these techniques of hiding information are becoming more sophisticated.

Steganography hides the existence of a message by transmitting information through various carriers. Its goal is to prevent the detection of a secret message. The most common use of steganography is hiding information from one file within the information of another file. For example, cover carriers, such as images, audio, video, text, or code represented digitally, hold the hidden information. The hidden information may be plaintext, cipher text, images, or information hidden in a bit stream.

As criminals become more aware of the capabilities of forensic examiners to recover computer evidence they are making more use of encryption technology such as to conceal incriminating data. Online child pornographers use steganography technology to create private communications and hide the files they exchanged into normal computer files.

On the contrary, the police can use the steganography technologies to obtain more evidence. For example, one application off steganography is data structure enhancement. The police could use this technology to enhance the surveillant video pictures in order to find more details about the crime scene and suspects. They also can use attack methods on steganography to find the hidden crime evidence.

The normal solution to detect hidden information is to build a library of hash sets and compare them with hash values of files being investigated. The hash sets will identify steganography file matches. Investigators must use safe hash sets to filter harmless files from their investigation. System files that have not been modified since installation are included in a safe hash set. National Institute of Standards and Technology (NIST)'s Information Technology Laboratory one ongoing computer forensics research project called National Software Reference Library (NSRL), which try to compute a unique identifier for each file in the normal operating systems based on the file's contents. These identifiers are created by SHA-1 hash algorithm. So if a perpetrator tries to hide a pornographic image by renaming it as a nondescript operating system file, .EXE, renaming a .JPG image as an .EXE file, The hash value derived from the image will not match that from the known operating system file and will thus be uncovered.

5.1.1 Forensic software for PDAs

Currently, most computer forensic software products are designed for desktop or laptop. However, Personal Digital Assistant (PDA) is now being widely used for business communication and personal mobile computing, which may also be involved in many criminal scenes. Thus, special forensic software designed to examine and identify computer evidence on PDA is needed.

Joseph Grand (Joseph), in his article "pdd: Memory Imaging and Forensic Analysis of Palm OS Devices" introduces a Windows-based tool for memory imaging and forensic acquisition of data from the

Palm operating system (OS) family off .pdd can preserve the crime scene by obtaining a bit-for-bit image or "snapshot" of the Palm device's memory contents.

The data retrieved by pdd includes all user applications and databases (along with stray databases that old applications left behind). This provides a significant amount of information for forensic analysis.

For example, records that have been marked for deletion by applications using the Palm APID-mDeleteRecord function (e.g., from the Address Book, Memo Pad, To Do Lisst, Ccallendar, etc.(are not actually removed and will remain on the device until a successful HotSync operation to a desktop machine. So the data can still be recovered before the HotSync has taken place but after records have been 'deleted'.

6 Conclusion and Future Directions

Computer forensics is used to identify evidence when personal computers are used in the commission of crimes or in the abuse of company policies. Evidence is the foundation of every criminal case, including those involving computer crimes. The collection and preservation of computer evidence differs in many ways from the methods law enforcement officers are used to using for traditional types of evidence.

The technology in computer forensic filed is changing at an unprecedented rate and we can only anticipate that the task of the computer forensic experts is going to become ever more challenging. A good grasp of the theoretical and practical principles of computer and legal knowledge is an essential prerequisite for the professional forensic analyst.

Computer forensic specialists guarantee accuracy of evidence processing results through the use of time-tested evidence processing procedures and through the use of multiple forensic software. The use of different forensic software tools that have been developed independently to validate results is important to avoid inaccuracies introduced by potential software design flaws and software bugs.

Historically computer forensics was focused on the imaging, analysis, and reporting of a stand- alone personal computer hard drive perhaps 1 GB in size using DOS-based tools. However, due to a number of changes and advances in technology an evolution has begun in the field of computer forensics.

The first type of change consists of larger hard drives. It is now common for hard drives on personal computers to be 40-60GB in size. And, in the corporate environment, it is not uncommon to have enterprise-class servers containing multiple 80GB hard drives in each. There has also been a significant increase in the number off PCs, and a noteworthy rise in the use of PCs to commit crimes or aid in criminal activities. The second type of change includes the popularity of non-PC devices such as handhelds, mobile cellular telephones, digital cameras, servers, etc. The third type of change is the increase in the number of non-Windows operating systems, including both UNIX and Linus variants, MacOS, BeOS, etc.

Increasingly, forensic examiners are faced with analyzing 'non-traditional' PCs, corporate security professionals are doubling as in-house forensic examiners and incident first responders, and critical data is residing in volatile system memory.

Thomas Rude (Thomas), in his article "Next Generation Data Forensics and Linux" defines 'Next Generation Data Forensics' as "The process of imaging and analysing data stored in any electronic format, for the purpose of reporting findings in a neutral manner, with no predisposition ass to guilt or innocence."

So, what's next? New automated software into the computer forensics investigative process will be introduced, stable foundation built on scientific rigor to support the introduction of evidence and expert testimony in court will be provided. In general, the new generation computer forensic software will support significantly larger hard drivers, non-PC devices such as servers, handhelds, digital cameras, etc. and more non-Windows operating systems such as MacOS, AIX, and Solaris etc

"Improve law enforcement capacity to fully engage with the scientific community. Appoint a high level Science and Technology policy group, underpinned by a science and technology clearing house. Identify

mechanisms to encourage Australian industry and research agencies to participate in the development and production of new, affordable technologies for law enforcement".

These are three recommendations from Prime Minister's Science, Engineering and Innovation Council (PMSEIC) for stakeholders of crime prevention and law enforcement. Look ahead, computer forensic scientists and forensic software developers still have a long way to go.

References

[1] Albert J Marcella and Robert Greenfield, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, CRC Press, Boca Raton, Florida, 2002

[2] Michael R Anderson, "Computer evidence processing, the third step: preserve the electronic crime scene." http://www.forensics-intl.com/art7.html Last visited 12 March 2003

[3] ASR Data http://www.asrdata.com/ Last visited 25 May 2003

[4] Matthew Braid, "Collecting electronic evidence after a system compromise", http://www.auscert.org.au/render.html?it=2247&ciddd=1920 Last visited 15 April 2003

[5] Bruce Middleton, *Cyber crime investigator's field guide*, CRC Press, Boca Raton, Florida, 2002

[6] Damian Tsoutsouris, "Computer forensic legal standards and equipment", http://rr.sans.org/incccident/legal_standards.php Last visited 5 March 2003

[7] Dan Farmer and Wietse Venema, "Forensic computer analysis: an introduction" http://xxx.ddj.com/documents/s=881/ddj0009f/0009f.htm Last visited 5 December 2002

[8] David Icove, Karl Seger, and William VonStorch, *Computer Crime-A crimefighter's Handbook*, O'Reilly & Associates, Sebastopol, California, 1995

[9] "Disk Imaging Tool Specification." Version 3.1.6.NIST (National Institute of Standards and Technology). October 12, 2001. http://www.cftt.nist.gov/testdocs.html Last visited 17 April 2003

[10] Dorothy A Lunn, "Computer Forensics: An Overview", http://www.sans.org/rr/incident/forensiccs.php Last visited 8 March 2003

[11] Eoghan Casey, "Practical Approaches to Recovering Encrypted Digital Evidence", *International Journal of Digital Evidence*, Fall 2002, Volume 1, Issue 3 http://www/ijde.org/docs/02_fall_art4.pdf Last visited 20 March 2003

[12] Franklin Witter, "Legal Aspects of Collecting and Preserving Computer Forensic Evidence", http://www.sans.org/rr/incident/evidence.php Last visited 5 March 2003

[13] Gary E Fisher, "Computer Forensics Guidance", http://www,nist.gov/itl/lab/bulletns/bltnnov01.htm Last visited 15 March 2003

[14] Guidance Software http://www/guidancesoftware.com/ Last visited 14 May 2003

[15] Jaames Holley, "Computer Forensics." *SCInfo Security Magazine*, September 2000. http://www/scmagazine.com/scmagazine/2000_09/survey/survey.html Last visited 11 April 2003

[16] James O Holley, "Computer Forensics in the new Millennium." http://www.scmagazine.com/scmagazine/1999_09/survey/survey.html Last visited 5 June 2003

[17] High Technology Crime Investigation Association (HTCIA) http://htcia.org Last visited 21 March 2003

[18] James Borck, "Leave the cybersleuthing to the experts", http://www2.idg.com.au/infoage1.nsf/all/957738BOF8F831 Last visited 15 December 2002

[19] Jason Upchurch, "Combating Computer Crime", http://www.aatstake.com/research/tools/index.htm1#pdd Last visited 29 April 2003

[20] Judd Robbins, "An Explanation of Computer Forensics" http://www.knock-knock.com/forens01.htm Last visited 20 November 2002

[21] Karen Ryder, "Computer Forensics - We've had an Incident, Who Do We Get to Investigate?" http://www.sans.org/rr/incident/investigate.php Last visited 5 March 2003

[22] Madihah Mohd Saudi, "An Overview of Disk Imaging Tool in Computer Forensics" http://www.sanss.org/rr/incident/disk_imaging.php Last visited 16 March 2003

[23] Mares and Company http://www.dmares.com/maresware/forensics.htm Last visited 25 May 2003

[24] Matt Welsh, Matthiass Kalle Dalheimer and Lar Kaufman, *Running Linux*, third version, Sebastopol, CA : O'Reilly, 1999

[25] Rodney McKemmish, "What is Forensic Computing?" June 1999 Australian Institute of Criminology trends and issues No. 118: http://www.aic.gov.au/publications/tandi/ti118.pdf Last visited 15 December 2002

[26] Michael R Anderson, "Computer Evidence Processing-Potential Law Enforcement Liabilities" http://www.forensics-intl.com/art3.html Last visited 3 March 2003

[27] Norman Haase, "Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000", http://www.sans.org/rr/incident/comp_forensics3.php Last visited 5 March 2003

[28] (NSWCA) NSW Crimes Amendment (Computer Offences) Bill 2001 http://www.oznetlaw.net/pdffiles/CrimesAmendmentBill_2001.pdf Last visited 28 May 2003

[29] (NSWEA) NSW Evidence Act 1995 http://www.austlii.edu.au/au/legis/nsw/consol_act/ea199580/ Last visited 25 May 2003

[30] (NTI) New Technologies Inc (NTI.) http://www.forensics-intl.com/ Last visited 3 June 2003

[31] (NTICEPS) New Technologies Inc., "Computer Evidence Processing Steps" http://www.forensics-intl.com/evidguid.html Last visited 15 December 2002

[32] Gary L Palmer, "Forensic Analysis in the Digital World" http://www.ijde.org/docs/forensic_analysis.pdf Last visited 16 May 2003

[33] Peter Stephenson, *Investigating Computer-Related Crime*, CRC Press, Boca Raton, Florida, 2000

[34] PMSEIC Working Group on Science, Crime Preevention & Law Enforcement, "Science, Crime Prevention and Law Enforcement, 2 June 2000" http://www.dest.gov.au/science/pmseic/documents/Crime.pdf Last visited 10 December 2002

[35] Scott Grace, "Computer Incident Response and Computer Forensics Overview", http://www.sans.org/rr/incident/IRCF.php Last visited 6 March 2003

[36] Stefan Kaatzenbeisser and Fabien A.P.Petitcolas, *Information Hiding Technique for Steganography and Digital Watermarking*, Artech House, Boston, London, 2000

[37] Thomas Rude, "Next Generation Data Forensics & Linux", http://www.crazytrain.com/monkeyboy/Next_Generation_Forensics_Linux.pdf Last visited 25 April 2002

[38] Tony Sammes and Brian Jenkinson, *Forensic Computing - A Practitioner's Guide*, Springer, London, 2000