

INTRODUCTION

The proliferation of computer use in today's networked society is creating some complex side effects in the application of the age-old greed, jealousy, and revenge. Criminals are becoming much more sophisticated in committing crimes. Computers are being encountered in almost every type of criminal activity. Gangs use computers to clone mobile telephones and to re-encode credit cards. Drug dealers use computers to store their transaction ledgers. Child pornography distributors use the Internet to peddle and trade their wares. Fraud schemes have been advertised on the Internet. Counterfeiters and forgers use computers to make passable copies of paper currency or counterfeit cashiers checks, and to create realistic looking false identification. In addition, information stored in computers has become the target of criminal activity. Information such as social security and credit card numbers, intellectual property, proprietary information, contract information, classified documents, etc., have been targeted. Further, the threat of malicious destruction of software, employee sabotage, identity theft, blackmail, sexual harassment, and commercial and government espionage is on the rise. Personnel problems are manifesting themselves in the automated environment with inappropriate or unauthorized use complaints resulting in lawsuits against employers as well as loss of proprietary information costing millions of dollars. All of this has led to an explosion in the number and complexity of computers and computer systems encountered in the course of criminal or internal investigations and the subsequent seizure of computer systems and stored electronic communications.

Computer evidence has become a 'fact of life' for essentially all law enforcement agencies and many are just beginning to explore their options in dealing with this new venue. Almost overnight, personal computers have changed the way the world does business. They have also changed the world's view of evidence because computers are used more and more as tools in the commission of 'traditional' crimes. Evidence relative to embezzlement, theft, extortion and even murder has been discovered on personal computers. This new technology twist in crime patterns has brought computer evidence to the forefront in law enforcement circles.

WHAT IS COMPUTER FORENSICS?

Computer forensics is simply the application of disciplined investigative techniques in the automated environment and the search, discovery, and analysis of potential evidence. It is the method used to investigate and analyze data maintained on or retrieved from electronic data storage media for the purposes of presentation in a court of law, civil or administrative proceeding. Evidence may be sought in a wide range of computer crime or misuse cases.

Computer forensics is rapidly becoming a science recognized on a par with other forensic sciences by the legal and law enforcement communities. As this trend continues, it will become even more important to handle and examine computer evidence properly. Not every department or organization has the resources to have trained computer forensic specialists on staff.

COMPUTER FORENSIC PROCESS

As in any investigation, establishing that an incident has occurred is the first key step. Secondly, the incident needs to be evaluated to determine if computer forensics may be required. Generally, if the computer incident resulted in a loss of time or money, or the destruction or compromise of information, it will require the application of computer forensic investigative techniques. When applied, the preservation of evidence is the first rule in the process. Failure to preserve evidence in its original state could jeopardize the entire investigation. Knowledge of how the crime was initiated and committed may be lost for good. Assignment of responsibility may not be possible if evidence is not meticulously and diligently preserved. The level of training and expertise required to execute a forensics task will largely depend on the level of evidence required in the case. If the result of the investigation were limited to administrative actions against an employee, the requirement would be lower than taking the case to court for civil or criminal litigation.

WHO CAN USE COMPUTER FORENSIC EVIDENCE?

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists:

Criminal Prosecutors use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.

Civil litigations can readily make use of personal and business records found on computer systems that bear on: fraud, divorce, discrimination, and harassment cases.

Insurance Companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.

Corporations often hire computer forensics specialists to ascertain evidence relating to: sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.

Law Enforcement Officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.

Individuals sometimes hire computer forensics specialists in support of possible claims of: wrongful termination, sexual harassment, or age discrimination.

EXAMINATION STANDARDS

Many software applications keep temporary records, temporary documents and other temporary data that the user is not aware of, and therefore, does not delete, password protect or otherwise try to hide. This data can normally be quickly located and accessed by forensic examiners.

Windows keeps a swap file that is used when memory resources are low. This is a dynamic file that grows with use. This swap file can hold complete files or other data that can significantly help a case.

Web browsers keep a number of temporary files, including cache and history files that tell where and when websites were visited and keeps copies of files that were viewed. These temporary files can be accessed, viewed and copied. The data contained in these files can be very valuable to a case or investigation.

The most common method used to hide data is to delete files or format the drive or diskette. Deleting a file or formatting a drive or diskette does not destroy the data. An experienced forensic examiner can recover the deleted data and draw expert conclusions as to when, how or why the data was deleted or removed from the media.

Frequently recovering deleted or formatted data and showing which particular files were deleted or removed is a good indication of culpability or valuable insight into what the person was trying to do at the time of the deletions.

Determining dates and times of deletion or formatting frequently coincides with actions taken by employers and law enforcement, i.e. the employee formats his Hard Disk Drive one hour after being accused of selling or using company sensitive data.

Data that is password protected is usually data that the user does not want others to see or access. Password protected data frequently contains relevant information to the investigation or inquiry at hand. An experienced forensic examiner has the knowledge and equipment to unlock passwords and access the data.

It is relatively simple to alter an operating system or its internal commands (i.e., DIR, COPY, TYPE, etc.) to do something other than Boot or display the Directory listing, Copy files or Type files.

Alterations to the operating system or internal commands are usually made by persons who want to conceal or destroy data that they do not want others to see. This is usually the kind of data that will be important to an investigation or inquiry.

Simply booting a target or suspect's machine will cause the alteration of certain operating system files. Although this normally will not cause the alteration of user created files. This will, arguably, cause the alteration of the original media.

Simply booting a target or suspect's machine may cause the loss or destruction of data or destructive processes set up by the suspect to occur. Typing an internal command such as, DIR to see what's on the machine, could activate destructive processes. Any or all of the data on the machine could be completely destroyed and the operating system could be made inoperative.

Valid lawsuits could follow if an untrained person looking at the system crashed the machine or destroyed critical data. An experienced forensic examiner will not fall into this sort of trap.

It is also relatively simple to hide files that normal DOS/WINDOWS commands, such as, DIR and other commands cannot find. The hidden file simply will not be displayed, and its contents will not be found or examined. An untrained person may not know if a file that appears to contain no data is corrupted or encrypted or actually contains no data. An untrained person may not know that a file that appears normal, actually contains hidden data.

Data can be hidden or located in many places on a computer Hard Disk Drive or other media. Untrained persons probably will probably not find the data.

The use of an untrained person could cause the inadvertent destruction of data, overlook deleted, hidden or encrypted data and could cause inadvertent writes back to and alter the original media.

Even if the untrained person found relevant data, the data will probably not be legally admissible or unusable. This is because of the untrained person's lack of forensic training and credentials, that the methods used were not forensically sound, and their lack of understanding of the technical issues involved.

Law enforcement agencies have been trained in and have used forensic computer examinations for a number of years. Law enforcement agencies have the only court proven expertise in computer forensics. You, your company, your firm or your agency can now benefit from our law enforcement training, our considerable experience and expertise.

DISK IMAGING

Introduction

In solving computer crime cases, computer forensics is used to gather evidence, which will be analyzed and presented to a court of law to prove the illegal activity. It is important that when doing computer forensics no alteration, virus introduction, damages or data corruption occurs. In order to do a good analysis the first step is to do secure collection of computer evidence. Secure collection of evidence is important to guarantee the evidential integrity and security of information. The best approach for this matter is to use disk imaging tool. Choosing and using the right tool is very important in computer forensics investigation.

Disk Imaging Definition

A few forensics professionals and companies have illustrated disk imaging in various terms and definition. These are as quoted below:

Disk imaging as defined by Jim Bates, Technical Director of Computer Forensics Ltd, refers to:

“An image of the whole disk was copied. This was regardless of any software on the disk and the important point was that the complete content of the disk was copied including the location of the data. Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image.”

Tech Assist, Inc. has defined disk imaging as following:

“Term given to creating physical sector copy of a disk and compressing this image in the form of a file. This image file can then be stored on dissimilar media for archiving or later restoration.”

In simple words, disk imaging can be defined as to make a secure forensically sound copy to media that can retain the data for extended period. Disk imaging is also one of the approaches for backup except that backup only copies the active file. In backup, ambient data will not be copied. This is an area where the most important source for the evidence could be found. Ambient data is a data stored in Windows swap file, unallocated space and file slack.

The result of the analysis also can be duplicated to another media using disk imaging tool. A good imaging tool will not alter the original evidence. It can copy all the information from the drive and make the contents available for forensic analysis. Even ambient data that is inaccessible to the residential of operating system will be copied. From the definition of the disk imaging, many diskimaging tools have been invented. The first imaging tool was sold on 1991 by Computer Forensics Ltd where now sold under the trademark DIBS.

Current Issues

Users scare that if they use disk imaging tools, it might altered the layout of the copy and omits free and deleted space. In computer forensics, priority and emphasis are on accuracy and evidential integrity and security. Doing analysis directly on original evidence might changes or alters the evidence. Due to that, it is essential to have a forensically sound of copy from original evidence.

Another issue is regarding internal verification. When done with imaging process, it is important to have one procedure or mechanism to determine that the evidence has not been altered or damaged. Internal verification is the only way to check the validity of the copy from the original drive.

In computer forensics, for cases that take years to be resolved, the evidence that has been imaged need to be stored into appropriate media. Appropriate media must be chosen to avoid any alteration or contamination of the evidence.

“During the last part of 1998, most computers on the market had hard drives of 6-8 gigabytes (GB). Very soon 13-27 GB hard drives will become the norm. By the end of 2000, we will be seeing 60-80 GB hard drives.”

Criteria considered before buying or using disk imaging tool

Accurate and dependable disk imaging tools are required in computer forensic investigation.

Recommended solutions:

Based on my analysis and observation, below are the recommended solutions regarding disk imaging tools issues.

Never work on the original evidence

Although it is easier to do analysis directly on original evidence it is not best practice in computer forensics. Evidence would be exposed to the risk of contamination. One of the cardinal rules in computer forensics is never work on the original evidence. Because evidence is very fragile. Evidence must be handled properly and very easily destroyed. With only one strike on keyboard evidence could be accidentally destroyed or modified.]

During computer forensic process, the risk of alterations, damage and virus introduction on evidence must be eliminated or minimized. In this situation, disk imaging tool can be used to make a bit-stream duplicate or forensically sound copy of an original disk. The best way to do analysis is on copy evidence. If something went wrong, everything can be done all over again.

Every information that has been imaged must has no relationship or dependency on any hardware or software.

Evidential integrity and security

1. Internal Verification

For security consideration, internal verification should be made. It is used to verify the imaging procedures and to check if there are any changes during imaging process.

Disk imaging tool would generate log file. In log file it has all records of parameter of the process from disk geometry, interface health and packet checksums to case details such as date, time and analyst's name.

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 between the original with the copy using the checksum. Same checksums between original and copy shows an exact copy has been produced. It is impossible and difficult to change the information on the drive without changing the checksums. At present, some of the disk imaging tool use cyclical redundancy checksums (CRC) or MD5 checksums to ensure the integrity of the evidence.

2. Evidence preservation

Electronic evidences might be altered or tampered without trace. Original copy should be placed in secure storage. Consider a situation when the victim claimed that if his computer is being taken, his business will suffer. As Jim Bates suggested (taken from Fundamentals of Computer Forensics) two forensically sound copies would help to solve this problem. Forensic investigation is done on one copy and another copy can be sealed in secure storage. When in doubt about evidence there is always another copy as reference.

The evidence that has been imaged needs to be stored into appropriate media or reliable mass storage. Optical media can be use as the mass storage. It is reliable, fast, longer life span and reusable compared to CD-ROM or tape device that is slow and unreliable for accurate storage of evidential data. It also has limited life span. In five to ten years time this media may no be longer available for sale, degrade over time and evidence could at some point become no longer recoverable. In computer forensics some of the cases mat takes more than two or three year to be solved. A secure storage space to store the original evidence is very important to avoid any contamination or alteration of data.

Presentation of evidence

It can be difficult to explain the findings of computer evidence in a court especially to non-technical person. The value of the evidence will ultimately depend on the way it is presented in a court. In court cases, even slightest doubt about the computer evidence makes the evidence invalid proof of any crime.

Result or report produce by the disk imaging tool must be easily understood either by non technical person or person from non computer literate background such as judges, jury and lawyers. Technical evidence should be presented in simple and precise way so that everyone in the court can understand the technical evidence presented.

Rapidly increasing storage capacity

The speed of imaging process varies based on number of factors such as physical state of the media and processor. In the past, to copy one computer to another, DISKCOPY command is used and it is very helpful due to small capacity storage. However presently where 60 GB is normal, disk imaging tools that could do fast imaging process is very important.

Right job with the right tools

Nowadays many companies claim that they sell the best product for disk imaging purpose. A few suggestions or guidance in choosing the right tool are:

a. Disk imaging tool top level requirement (provided by National Institute of Standards and Technology) are:

- **The tool shall make a bit-stream duplicate or an image of an original disk or partition on fixed or removable media.**
- **The tool shall not alter the original disk**
- **The tool shall be able to access both IDE and SCSI disks.**
- **The tool shall be able to verify the integrity of a disk image file**
- **The tool shall log I/O errors**
- **Provides good documentation**

b. If necessary use the combination of different tools that has been developed independently which can help guarantee accuracy of the evidence.

c. Simple to use and quick to learn.

-This helps even non technical person to do imaging process without destroying the evidence especially in emergency case. User interactive that is well designed and interactive makes the imaging process easier.

d. Provides fast imaging process.

-Technology such as SmartSector imaging helps to make imaging process faster. This is additional requirement. When time is limited especially on-site and the need to conduct an initial analysis of drive contents, technology such as SmartSector is highly recommended.

e. Provides compression method, which helps to reduce the amount of space to store all the evidence files.

Examples of disk imaging tool

Below is a summary of disk imaging tool taken from a report on forensic tools evaluation from SC InfoSecurity Magazine, Pick of 2000, Computer Forensics and from my lab.

<u>Products</u>	Image file/internal verification	-	Imaging SCSI / IDE drive	Copying sector - by sector / file-by-file
Features		Imaged to appropriate media		
1.Safe Back Version 2.0	▪ CRC checksum	Hard drive, tape, removable media	IDE drive	Sector- by-sector
- 2.SnapBack DatArrest Version 4.12	▪ MD5 checksum	Hard drive, tape, removable media	SCSI drive	Sector- by-sector
Linux "dd" Version 7.0	MD5 checksum	Hard drive, tape, removable media	SCSI drive and IDE drive	Sector- by-sector and file-by-file
1.DIBS PERU (Portable Evidence Recovery Unit) 2. DIBS RAID (Rapid Action Imaging)	▪ DIVA	Optical media	SCSI drive and IDE drive	Sector- by-sector

TOOLS EMPLOYED IN COMPUTER FORENSICS EXAMINATIONS

Below are the examples of some of the tools employed in forensics procedures:

GetFree - Forensic Data Capture Tool



When files are 'deleted' in DOS, Windows, Windows 95 and Windows 98, the data associated with the file is not actually eliminated. It is simply reassigned to unallocated storage space where it may eventually be overwritten by the creation of new files over time. Such data can provide the computer forensics investigator with valuable leads and evidence. However, the same data can create a significant security risk when sensitive data has been erased using DOS, Windows, Windows 95 and Windows 98 file deletion procedures and commands.

GetFree software is used to capture all of the unallocated file space on DOS, Windows, Windows 95 and Windows 98 based computer systems. The program can be used to identify leads and evidence. It is also effectively used to validate the secure scrubbing of unallocated storage space with programs like NTI's M-Sweep ambient data deletion software.

When GetFree software is used as an investigative tool, it eliminates the need to restore potentially hundreds or thousands of files on computer hard disk drives and floppy diskettes. The software was primarily developed as a computer forensic tool for use in computer related investigations and internal audits. However, GetFree has also proven to be an ideal tool for use in computer security risk assessments because the software automatically captures the data associated with unallocated file space. Such data can be reviewed and analyzed using other NTI forensic tools, e.g., Filter_I, Net Threat Analyzer and Graphics Image File Extractor.

GetFree Software - Primary Uses:

- **Calculates the amount of unallocated storage space on a computer storage device.**
- **Automatically captures all logical unallocated storage space on one or more computer hard disk drives and floppy diskettes.**
- **Captures the contents of a dynamic Windows swap file for analysis with other tools.**
- **Used in internal audits, security reviews and computer-related investigations.**
- **Validates the effectiveness of computer security data scrubbers.**
- **Identifies classified data spills in unallocated data storage areas.**
- **Identifies violations of company policy through the identification of sensitive data leakage into unallocated storage space.**
- **Used very effectively with NTI's Image File Extractor in investigations involving computer generated graphic file images, e.g., child pornography investigations.**

GetFree - Program Features and Benefits:

- **DOS-based for speed and ease of use.**
- **Compact program size easily fits on one floppy diskette with other forensic software tools.**

- **Non-printable characters (ASCII values 0-31 and non ASCII values 127-255) are replaced by a space character, at the option of the user.**
- **Does not alter any data on the target computer and can therefore be operated covertly.**
- **Captures unallocated clusters marked as bad (by a user or the operating system) in the event that sensitive data is stored in sectors associated with such clusters.**
- **Compatible with DOS, Windows 3.x, Windows 95 and Windows 98.**
- **Estimates the output storage space needed for the data capture prior to use.**
- **Processes more than one logical drive in one work session.**
- **Automatically increments the output file names and prompts the user for additional removable media in the event additional storage space is needed in achieving the data capture.**
- **Supports 12 bit, 16 bit and 32 bit FAT types (32-bit FATs).**
- **If 32 bit FAT (FAT32) file systems are involved, GetFree should be run with a FAT 32 aware version of DOS, e.g., DOS 7x.**
- **Automatically creates output files which are less than 2 gigabytes in capacity. This aids in the analysis of the output files and avoids the 2 gigabyte DOS file limitations.**

GetSlack - Forensic Data Capture Utility



This software is used to capture all of the file slack contained on a logical hard disk drive or floppy diskette on a DOS, Windows, Windows 95 and/or Windows 98 computer system. The resulting output from GetSlack can be analyzed with standard computer utilities or with special NTI tools, e.g., Filter_I and Net Threat Analyzer software. GetSlack software is an ideal computer forensics tool for use in investigations, internal audits and in computer security reviews. NTI places special importance on the use of this tool in computer security risk assessments because memory dumps in file slack are the cause for security related concerns. Typically, network logons and passwords are found in file slack. It is also possible for passwords used in file encryption to be stored as memory dumps in file slack.

From an investigative standpoint, file slack is a target rich environment to find leads and evidence. File slack can contain leads and evidence in the form of fragments of word processing communications, Internet E-mail communications, Internet chat room communications, Internet news group communications and Internet browsing activity. As a result, this program is a good tool for use in computer related investigations. It also acts as a good validation tool for use with computer security

programs which are designed to eliminate file slack, e.g., NTI's M-Sweep ambient data scrubbing software.

GetSlack Software - Primary Uses:

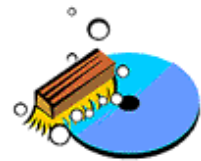
- **Quickly calculates the amount of storage space which is allocated to file slack on a logical DOS/Windows partition.**
- **Captures all file slack on a logical DOS/Windows drive and converts it into one or more files automatically.**
- **Used in covert and overt internal audits, computer security reviews and computer investigations.**
- **Validates the results of computer security scrubbers used to eliminate sensitive or classified data from file slack on computer storage devices.**

GetSlack Software - Program Features and Benefits:

- **DOS based for speed.**
- **Compact program size easily fits on a single floppy diskette with other forensic software tools.**
- **At the option of the user, non-printable characters (ASCII values 0-31 and 127-255) can be replaced with space characters.**
- **Does not alter or modify the data stored on the target computer.**
- **Does not leave any trace of operation. Therefore, it can be used coverly when laws permit such use.**

- **Does not alter evidence on the target drive. Therefore, this tool is ideal for the processing of computer evidence.**
- **Compatible with DOS, Windows 3.x, Windows 95 and Windows 98.**
- **Estimates the output file space needed prior to use.**
- **Multiple logical storage devices can be specified in one operating session.**
- **Configures the output files to fit on one or more removable storage devices depending on the volume of the computed output.**
- **Supports 12 bit, 16 bit and 32 bit FAT types (32-bit FATs are currently found on Windows 95B/98/OSR2/NT).**

DiskScrub - Hard Drive Data Elimination Software



It is becoming standard practice in corporations, government agencies, law firms and accounting firms to reassign computers and to donate older computers to charity. Millions of personal computers have been put to use since 1981 when the IBM Personal Computer came into existence. Many of the older personal computers have been reassigned or donated to charity and many more will fall into this category in the future. However, data security is often ignored when computers change hands.

You must be aware that personal computers were never designed with security in mind. Potentially anything that transpired on a used computer still exists. Multiply that by the number of computers your organization will reassign or surplus this year, and you get the point. Computers should be reassigned and donated to charity but the contents of the hard disk drives should not be ignored.

With computer technology changing almost daily, corporations and government agencies have to stay current while still making the best uses of aging computer resources. Advancements in hard disk drive storage capacities, operating systems and software applications cause corporations to buy or lease new computers every year.

But what is done with the old computers? What is done about the sensitive data still existing, essentially "stored" on these computers when they are sold, transferred or donated? That is a serious problem, and NTI's Disk Scrub software was specifically designed to deal with these risks, for corporations, government agencies, hospitals, financial institutions, law firms and accounting firms.

Forensic Graphics File Extractor



NTI's Forensic Graphics Image File Extractor is a computer forensics software tool which was designed to automatically extract exact copies of graphics file images from ambient data sources and from SafeBack bit stream image backup files. The latter process has the potential of quickly identifying all graphics file images stored on a computers hard disk drive. The resulting output image files can be quickly evaluated using a graphics file viewer, e.g., Firehand Ember Millennium by Firehand Technologies which NTI recommends. Firehand Ember Millennium fits limited law enforcement budgets, e.g., priced at under \$50 and it is an ideal product for investigations involving computer graphic images.

NTI's Image File Extractor software was developed with our law enforcement friends in mind and it has been priced accordingly. Law enforcement computer crime specialists spend much of their valuable time in the investigation of computer crimes involving the possession and distribution of graphic image files which involve child pornography. This computer forensics tool saves time and it was specifically created to accurately and quickly reconstruct evidence grade copies of "deleted" image files. The software can also be used effectively to identify and reconstruct residual graphics file images which passed through Windows Swap and Windows Page files during Internet web browsing sessions. An "after the fact" analysis of such files can quickly determine how a computer may have been used. Such information is invaluable to corporate investigators and law enforcement computer crime specialists alike. NTI's

Graphics Image File Extractor also provides benefits in internal audits involving the misuse of corporate computers by employees and corporate due diligence reviews of computers.

Forensic Graphics File Extractor - Primary Uses:

- **Used to find evidence in corporate, civil and criminal investigations which involve computer graphics files, e.g., investigations which potentially involve child pornography and/or inappropriate Internet web browsing in a corporate or government setting.**
- **Used with other computer forensic software to quickly reconstruct previously deleted BMP, GIF and JPEG graphics files stored on computer storage media.**
- **Used to quickly identify and preview BMP, GIF and JPEG image files stored on a computer hard disk drive when used with SafeBack and Firehand Embers.**
- **Used effectively in computer investigations involving the distribution of child pornography.**
- **Used "after the fact" to determine what files may have been viewed over or downloaded from the Internet.**
- **Used very effectively with NTI's GetFree software this can be purchased separately.**

Forensic Graphics File Extractor - Program Features and Benefits:

- **Operates under DOS/WIN9x/WINNT/WIN2000/WINXP for ease of operation and speed.**
- **Compact program size which easily fits on one floppy diskette with other forensic software utilities for portability.**

- **Searches a targeted Windows Swap File or a file created from erased file space for patterns of BMP, GIF and JPG file images and it reconstructs partial or complete image files in one highly accurate operation. The accuracy of this process is dependant upon the degree of fragmentation involved, etc.**
- **When complete image files are identified and reconstructed by the program the output of restored graphics images files is exact. Our tests indicate that a majority of reconstructed files will pass a CRCMD5 hash test when restored image files are compared with the original files prior to deletion. This feature makes the software ideal for evidence reconstruction in criminal cases. It also allows for the exact reconstruction of graphics image files which may contain hidden files or other messages through the use of steganography.**
- **Partial image file patterns (caused due to fragmentation and/or file corruption) can be automatically reconstructed and viewed.**
- **The highly accurate graphics file identification search engine ensures that every byte is checked for integrity.**
- **The software operates in batch file mode for automatic processing when combined with other NTI software processes.**
- **It automatically creates a complete log of the processing steps taken by the program to aid in expert witness testimony.**
- **Priced to easily fit limited law enforcement budgets.**
- **Operation of the software is easy and is not hampered by hardware anti-theft software protection.**
- **Free Upgrades for one year from the date of purchase.**
- **Quantity discounts are available.**

NETWORK FORENSICS

As technology has advanced, computers have become incredibly powerful. Unfortunately, as computers get more sophisticated, so do the crimes committed with them. Distributed Denial of Service Attacks, ILOVEYOU and other viruses, Domain Name Hijacking, Trojan Horses, and Websites shut down are just a few of the hundreds of documented attack types generated by computers against other computers usually using an electronic network.

The need for security measures to prevent malicious attacks is well recognized and is a fertile research area as well as a promising practitioner's marketplace. Though there is an immense effort ongoing to secure computer systems and prevent attacks, it is clear that computer and network attacks will continue to be successful. When attacks are successful, forensics techniques are needed to catch and punish the perpetrators, as well as to allow recovery of property and/or revenue lost in the attack.

Computer and Network Forensics (CNF) techniques are used to discover evidence in a variety of crimes ranging from theft of trade secrets, to protection of intellectual property, to general misuse of computers. The ultimate goal of computer and network forensics is to provide sufficient evidence to allow the criminal perpetrator to be successfully prosecuted. As such, CNF efforts are mainly centered in law enforcement agencies. Any enterprise that depends on, or utilizes, computers and networks should have a balanced concern for security and forensic capabilities. Unfortunately, there is little academic or industrial research literature available on CNF. Forensic techniques are developed by the try and fix method, and few organizations have plans for conducting forensics in response to successful attacks. We propose several categories of policies that will help enterprises deter computer crime and will position them to respond effectively to successful attacks by improving their ability to conduct

computer and network forensics. These policies correlate to taxonomy of approaches common to computer attacks. We present policies in the following categories: Retaining Information, Planning the Response, Training, Accelerating the Investigation, Preventing Anonymous Activities and Protecting the Evidence.

COMPUTER AND NETWORK FORENSICS

The evidence found during a forensic investigation may depend on the type of crime committed. For example, in a criminal case, incriminating evidence may be found such as documents related to homicides, financial fraud, drug or embezzlement record keeping, or child pornography. In a civil case, evidence of personal and business records related to fraud, divorce, discrimination, or harassment could be found.

CNF experts are not only hired by lawyers. CNF techniques are sometimes needed by insurance companies to discover evidence to decrease the amount paid in an insurance claim. Individuals may also hire CNF experts to support a claim of wrongful termination, sexual harassment, or discrimination. Gathering evidence is at the heart of CNF. In computer-related crimes, evidence is accumulated from information collected by different components of the system. The information does not become evidence until a crime is committed and this data is used to find clues. For this reason, we call the data collected by the system potential evidence. There are many sources of potential evidence in computers and network components. Files are an obvious source of potential evidence. Application output word processors, spread sheets, etc. are almost always valuable potential evidence, as are hidden application files that may contain history information, caches, backups, or activity logs. Occasionally, sophisticated criminals may encrypt incriminating files or attempt to hide them with system-oriented or otherwise unlikely looking names. There are numerous sources of potential evidence, which we discuss more exhaustively in the section dedicated to establishing recommended policies. Because gathering potential

evidence may not be as easy as finding application files on a computer, it requires someone with special skills. CNF experts are specially trained with the skills necessary to successfully carry out a forensic investigation. A forensics expert must have the investigative skills of a detective, the legal skills of a lawyer, and the computing skills of the criminal. Even with these skills, CNF is not an exact science, so there is no guarantee that an expert will find sufficient evidence. However, experienced forensics specialists can find more potential evidence than even the best hackers will expect.

POLICIES TO ENHANCE COMPUTER AND NETWORK FORENSICS

A. Retaining Information

1) Copy and Retain Application and Local User Files

The first step that an enterprise interested in being able to catch and prosecute cyber criminals on their networks should take is to institute a policy that systematically stores and retains the contents of application and user files as potential evidence. The value of retaining central backups of local files is well known as a reliability protection technique, and the costs and complexity of storing such backups are declining.

2) Copy and Retain Computer and Network Activity Logs

While application files have a clear connection to computer users, system and network information may be equally as telling of user activities. Logged network

activity can reveal the actions of a criminal in the clearest detail of any source. Thus, system logs are a vital source of potential evidence.

B. Planning the Response

1) Establish a Forensics Team.

Dealing with CNF requires the commitment of a forensic team. According to Robert Graham, a response team should include members from upper management, Human Resources, the technical staff, and outside members. The upper management member can ensure that the decisions made by the forensic team are balanced with the overall goals and best interests of the enterprise and that the decisions of the team have appropriate weight. Because of the personnel issues involved, there should be a member from human resources department. There should also be a member of the Information Technology (IT) staff on the forensics team. Security issues are often handled separately from normal IT activity.

2) Establish an Intrusion Response Procedure

The enterprise should establish a step-by-step guide that employees can follow if an attack is suspected. A mistaken response by an employee that detects an attack can damage any subsequent CNF effort. The procedure should include who to contact, how to contact them, and what information to report.

3) Formalize the Investigative Procedure

The procedure to follow during a preliminary investigation is similar to that followed by a computer forensics expert during a forensic investigation. However,

since the preliminary investigation is not as rigorous as the investigation carried out by a computer forensics expert, the procedure for it is also less rigorous. The goal here is not to restrict the investigators from freely utilizing their forensics skills. Rather, it is to provide a baseline of activity that must be accomplished when intrusions are detected.

C. Training

1) Training the Response Team.

Once a response team is assembled, the members of the team need to be prepared for the kinds of decisions they will have to make. For example, if the company under attack is an online trading service, pulling the plug might be the best answer. Going off-line on such a service will certainly disrupt business, but may be better than having hackers trading away the stock of valued clients.

2) Training The Investigative Team.

The investigative procedure that follows an attack needs to be carried out with precaution and the investigative team must have computer forensics skills. We have to make sure the investigative team members have the abilities necessary to follow the investigative procedure. During a preliminary investigation, the investigative team will use these skills to determine whether an attack actually occurred, and if possible to identify the crime by determining how it was committed and who did it, and find the evidence left behind. In order to do this, the investigative team needs to understand the steps followed by the attacker so that they can be retraced.

3) Training for All Personnel That Use Computers

It is necessary to train all personnel in company security policies. The general personnel should be familiarized with the response procedure. The last step of the response procedure is to alert the response team, so it is necessary for employees to also be familiar with the structure of the response team. No matter how much planning we do, we cannot ensure the success of the response unless we test the procedure under real circumstances. It is not advisable to wait until an attack occurs to try the response procedure. It is instead advisable to simulate an attack, and put the response to the test. This way the employees, as well as the response team, will have some experience when a real attack occurs.

D. Accelerating the Investigation

1) Prohibit Personal File Encryption

Encrypted files should be prohibited in a company system unless specifically authorized. When a forensic investigation is in progress, one of the first steps is to recover application files. Personal encryption technology may be used when an attacker does not want anyone to have access to the content of a file. Cryptanalysis of encrypted files is a very difficult and time consuming process. If the encryption system was sufficiently strong, it may not be possible to ever recover the original contents. During an investigation, we cannot count on the owner to give us the key to decrypt the file, so it is wise to avoid this situation.

2) Prohibit Disk Scrubbing Tools and File Shredding Software

Deleted files are also a source of potential evidence. The process of recovering deleted files is usually not difficult or time consuming. However, it can be made very difficult and time consuming by using scrubbing tools and shredding software, which

are programs designed to destroy information. They wipe clean the targeted space by writing over clusters several times.

3) Utilize Data Indexes

The first step of an investigation is to check all the potential evidence collected. This is easier said than done, especially since extensive logging produces a great volume of data. The amount of time to search through each entry in a log file is analogous to the amount of time necessary to go through all the books on a shelf one by one. Examples of the type of information we may want to include in the summaries are the date, source/origin, destination, service port, and duration of TCP connection occurring on the network, the URL from every web request, the origin and destination of SMTP sessions, and the user identification from all Telnet, FTP, and relogin sessions .

4) Utilize Information Fusion

An invaluable source of potential evidence is the output of Intrusion Detection Systems (IDS). IDSs monitor the activities in an environment and then determine if the activities represent an attack, or are a legitimate use of the environment. An IDS produces Indications and Warnings (IW) values that are analyzed to determine if an attack has occurred.

E. Preventing Anonymous Activities

1) Onion Routing

"The Onion Routing research project is building an Internet based system that strongly resists traffic analysis, eavesdropping, and other attacks both by outsiders (e.g. Internet routers) and insiders (Onion Routers themselves). It prevents the transport medium from knowing who is communicating with whom; the network knows only that communication is taking place .

2) Require Date, Time, User Stamps in File

During an investigation, time, date, and suspect are three key elements. When an investigation is in progress, the investigator needs to know what date a file was created, or modified, or deleted, and who did it. This is a key point to be able to determine what happened exactly. Establishing and enforcing a policy of enabling this automatic administration capability of most application packages can prove invaluable to the investigative team.

3) Use Strong User Authentication

No unauthorized access to the system should be allowed. Whenever a user tries to connect to the system, the enterprise must make sure that it is a valid user. Passwords are the most widely used method of authentication today. However, passwords are vulnerable to attack. Strong authentication based on encryption is key to enabling effective CNF.

4) Use Strong Access Control Mechanisms.

Authorization identifies entities, but does not control who sees or does what on the system. Access control is a mechanism for limiting use of resources to authorized users. This process establishes a relationship between users and files or other resources.

F. Protect the Evidence

1) Exercise Rigid Control Over Administrative Access for Systems Housing Potential Evidence

A cornerstone of effective CNF is to have strong authentication and integrity services that control administrative access to network devices. While all computer criminals are not sophisticated, many will be, and weak control of administrative access is a blueprint for disaster in protecting potential evidence.

2) Encrypt Evidence Files and Connections

The evidence gathered should be protected at least with a password. However, password protection alone may not be enough to guarantee the security and integrity of the data. Passwords can be broken using password cracker software, so they are not very reliable.

3) Apply Strong Integrity Checking Technology.

Just protecting the data is not enough. To use the potential evidence in court, we must be able to show that the evidence has not been corrupted. To accomplish this, periodic integrity checks should be conducted on the data collected.

Conclusion

Practical investigations tend to rely on multiple streams of evidence which corroborate each other - each stream may have its weaknesses, but taken together may point to a single conclusion.

Disk forensics may remain for some time the single most important form of digital evidence .Increasing number of computer crime means increasing demand for computer forensics services. In doing computer forensics investigation, choosing the right disk imaging tool is very important. There is no standard conformity of computer forensic imaging methodology or tool. This paper only provides guidance and suggestions regarding imaging tool. It should not be constructed as mandatory requirement.

Today, everyone is exposed to potential attacks and has a responsibility to its network neighbors to minimize their own vulnerabilities in an effort to provide a more secure and stable network. As the enormity of the problem unfolds, we will better comprehend how vital it is to work towards dramatic changes in research, prevention, detection and reporting, and computer crime investigation. Security can no longer be thought of as an impediment to accomplishing the mission, but rather a basic requirement that is properly resourced.

Our focus has been to implement the newest and most advanced technology, but little has prepared us for the gaping security holes we've neglected to mend along the way. From the ranks of management to every employee that works behind each terminal, the policies that protect and mitigate risks must be current, understood, and aggressively enforced. Reporting must be standard operating procedure so that everyone can realize the total impact and define what is required for a secure cyber environment. The responsibility belongs to everyone and it is with that effort we will be able to harness the security of this new technological age. An enormous challenge lies before us and we must attack it with the same enthusiasm and determination that brought us to this new frontier.