COMPUTER FORENSICS EVIDENCE and CAPTURE

Data Recovery

Computers systems may crash. Files may be accidentally deleted. Disks may accidentally be reformatted. Computer viruses may corrupt files. Files may be accidentally overwritten. Disgruntled employees may try to destroy your files. All of these can lead to the loss of your critical data. You may think it's lost for- ever, but you should employ the latest tools and techniques to recover your data. In many instances, the data cannot be found using the limited software tools available to most users. The advanced tools that you utilize should allow us to find your files and restore them for your use. In those instances where the files have been irreparably damaged, your computer forensics expertise should allow you to recover even the smallest remaining fragments.

Data Recovery Definition: Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact (complete) format.

Many people, even computer experts, fail to recognize data recovery as an option during a data crisis. But it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.

Data Back-up and Recovery

Back up Obstacles

The following are obstacles to backing up applications:

- **Backup window**
- **Network bandwidth**
- **System throughput**
- **Lack of resource**

Back-up Window:

The back-up window is the period of time when back-ups can be run. The back-up window is generally timed to occur during nonproduction periods when network bandwidth and CPU utilization are low.

Network bandwidth: Many companies now have more data to protect than can be transported across existing local area networks (LANs) and wide area networks (WANs). If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, the organization's centralized backup strategy is not feasible.

System throughput: Three I/O bottlenecks are commonly found in traditional backup schemes. These are

1. The ability of the system being backed up to push data to the backup server

2. The ability of the backup server to accept data from multiple systems simultaneously

3. The available throughput of the tape device onto which the data is moved

Lack-of Resources: Many companies fail to make appropriate investments in data protection until it is too late. Often, information technology (IT) managers choose not to allocate funding for centralized data protection because of competing demands resulting

from emerging issues such as e-commerce , Internet and intranet applications, and other new technologies.

The Role of Back-up in Data Recovery

There are many factors that affect back-up. For example:

Storage costs are decreasing: The cost per megabyte of primary (online) storage has fallen dramatically over the past several years and continues to do so as disk drive technologies advance. This has a huge impact on back-up.

Systems have to be on-line continuously: Seven/twenty-four (7 x 24) operations have become the norm in many of today's businesses. The amount of data that has to be kept on-line and available (operationally ready data), is very large and constantly increasing.

The role of Back-up has changed: Operationally, ready or mirrored data does not guard against data corruption and user error. The role of backup now includes the responsibility for recovering user errors and ensuring that good data has been saved and can quickly be restored.

Conventional tape back-up in today's market

Tape backup is the practice of periodically copying data from a primary storage device to a tape cartridge so the data can be recovered if there is a hard disk crash or failure. Tape backups can be done manually or be programmed to happen automatically with appropriate software.

A typical tape management system consists of a dedicated workstation with the front-end interfaced to the network and the back-end controlling a repository of tape devices. The media server is running tape management software. It can administer backup devices across an enterprise and can run continuous parallel backups and restores.

Issues with today's back-up

NETWORK BACKUP creates network performance problems. Using the production network to carry backup data, as well as for normal user data access, can severely overburden today's busy network resources.

OFFLINE BACKUP affects data accessibility. The time that the host is offline for data backup must be minimized. This requires extremely high- speed, continuous parallel backup of the raw image of the data.

LIVE BACKUPS allow data access during the backup process but affect performance. Many database vendors offer live back-up features. The downside to the live backup is that it puts a tremendous burden on the host.

MIRRORING doesn't protect against user error and replication of bad data. Also, duplicating data after a user has deleted a critical file or making a mirrored copy of a file that has been corrupted by a host process doesn't help. Mirroring has its place in back-up/recovery, but cannot solve the problem by itself.

New architectures and techniques are required

Backup at extremely high speed is required. Recovery must be available at the file level. Backup of critical data is still required to ensure against data errors and user errors.

The Data Recovery Solution

Now the world has changed! It's now common to offer extended service hours in which a customer can call for help with a bill, inquiry or complaint. Even if a live agent is not available to help, many enterprise applications are Web-enabled so that customers can access their accounts in the middle of the night while sitting at home.

Shrinking expertise, growing complexity

Most of the bright youngsters who are graduating from college this term haven't had much exposure to mainframe concepts in their course work, much less any meaningful grasp of the day-to-day requirements for keeping mainframe systems running.

The complex systems that have evolved over the past 30 years must be monitored, managed, controlled, and optimized. Backups often take place while an application is running. Application changes take place on the fly, under the watchful eye of the change-control police.

FAILURES:

Disk storage is more reliable than ever, but hardware failures are still possible. A simple mistake can be made by an application programmer, system programmer, or operations person. Logic errors in programs or application of the wrong update at the wrong time can result in a system crash or, worse. Disasters do really occur! Floods,

tornadoes, earthquakes, tsunamis, and even terrorism can do strike. We must be ready.

BUDGETS AND DOWNTIME

We have fewer resources (people, processing power, time, and money) to do more work than ever before, and we must keep your expenses under control. Shrinking expertise and growing complexity cry out for tools to make systems management more manageable, but the tools that can save resources also cost you resources to obtain, implement, and operate.

Systems must remain available to make money and serve customers. Downtime is too much expensive to be tolerated. You must balance your data management budget against the cost of downtime.

RECOVERY: THINK BEFORE YOU BACK-UP

One of the most critical data-management tasks involves recovering data in the event of a problem. You must evaluate your preparations, make sure that all resources are available in usable condition, automate processes as much as possible, and make sure you have the right kind of resources.

Evaluate your preparation

If all of the resources (image copies and logs) are available at recovery time, these preparations certainly allow for a standard recovery. Finding out at recovery time that some critical resource is missing can be disastrous!

Don’t let your resources fall through the cracks

In a complex environment, how do you check to make sure that every database is being backed-up? How do you find out whether you are taking image copies as frequently as you planned? What if media errors occur? Identifying these types of conditions is critical to ensuring a successful recovery.

Automated Recovery

With proper planning and automation, recovery is made possible, reliance on specific personnel is reduced, and the human-error factor is nearly eliminated.

Data integrity and your business relay on building recovery job control language (JCL). In the event of a disaster, the Information Management System (IMS) recovery control (RECON) data sets must be modified in preparation for the recovery.

Make Recoveries Efficient

Multithreading tasks shorten the recovery process. Recovering multiple databases with one pass through your log data certainly will save time. Taking image copies, rebuilding indexes, and validating pointers concurrently with the recovery process further reduce downtime.

Take Back-ups

The first step to a successful recovery is the backup of your data. Your goal in backing up data is to do so quickly, efficiently, and usually with minimal impact to your customers. You might need only very brief outages to take instant copies of your data, or you might have intelligent storage devices that allow you to take a snapshot of your

data. Both methods call for tools to assist in the management of resources.

EVIDENCE COLLECTION AND DATA SEIZURE

Evidence is difficult to collect at the best of times, but when that evidence is electronic an investigator faces some extra complexities. Electronic evidence has none of the permanence that conventional evidence has, and it is ever more difficult to form into a coherent (clear) argument. The purpose of this chapter is to point out these difficulties and what must be done to overcome them.

Why Collect Evidence?

Electronic evidence can be very expensive to collect the processes are strict and exhaustive, the systems affected may be unavailable for regular use for a long period of time, and analysis of the data collected must be performed. There are two simple reasons-future prevention and responsibility.

The simple reasons for collecting evidence are:

→ Future Prevention: Without knowing what happened, you have no hope of ever being able to stop someone else from doing it again.

→ Responsibility: The attacker is responsible for the damage done, and the only way to bring him to justice is with adequate evidence to prove their actions. The victim has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks.

Collection Options

Once a compromise has been detected, you have two options:

→ **Pull the system off the network and begin collecting evidence: If you disconnect the system from the network, you may find that you have insufficient evidence or, worse, that the attacker left a *dead man switch* that destroys any evidence once the system detects that it is offline.**

→ **Leave it online and attempt to monitor the intruder: you may accidentally alert the intruder while monitoring and cause them to wipe their tracks any way necessary, destroying evidence as they go.**

Obstacles

Computer transactions are fast, they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible

Any paper trail of computer records they may leave can be easily modified or destroyed, or may be only temporary.

→Auditing programs may automatically destroy the records left when computer transactions are finished with them.

→Investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously.

→The best we can do is to follow the rules of evidence collection and be as attentive as possible.

Types of Evidence

Real Evidence: Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function— provided that the log can be shown to be free from contamination.

Testimonial Evidence: Testimonial evidence is any evidence supplied by a witness. As long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence.

Hearsay: Hearsay is any evidence presented by a person who was not a direct witness. Hearsay is generally inadmissible in court and should be avoided.

The Rules of Evidence

Admissible: Admissible is the most basic rule. The evidence must be able to be used in court.

Authentic: You must be able to show that the evidence relates to the incident in a relevant way.

Complete: It's not enough to collect evidence that just shows one perspective of the incident.

Reliable: Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

Believable: The evidence you present should be clearly understandable and believable to a jury.

Using the preceding five rules, we can derive some basic dos and don'ts:

Minimize handling and corruption of original data: Once you've created a master copy of the original data, don't touch it or the original. Any changes made to the originals will affect the outcomes of any analysis later done to copies.

Account for any changes and keep detailed logs of your actions: Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented.

Comply with the five rules of evidence: Following these rules is essential to guaranteeing successful evidence collection.

Do not exceed your knowledge: If you ever find yourself ‑out of your depth,‖ either go and learn more before continuing (if time is available) or find someone who knows the territory.

Follow your local security policy: If you fail to comply with your company's security policy, you may find yourself with some difficulties.

Capture as accurate an image of the system as possible: Capturing an accurate image of the system is related to minimizing the handling or corruption of original data.

Be prepared to testify: If you're not willing to testify to the evidence you have collected, you might as well stop before you start. No one is going to believe you if they can't replicate your actions and reach the same results.

Work fast: The faster you work, the less likely the data is going to change. Volatile evidence may vanish entirely if you don't collect it in time. If multiple systems are involved, work parallel.

Proceed from volatile to persistent evidence: Always try to collect the most volatile evidence first.

Don't shutdown before collecting evidence: You should never, ever shutdown a system before you collect the evidence. Not only do you lose any volatile evidence, but also the attacker may have trojaned the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out.

Don't run any programs on the affected system: The attacker may have left trojaned programs and libraries on the system; you may inadvertently trigger something that could change or destroy the evidence you're looking for.

Volatile Evidence

Always try to collect the most volatile evidence first.
An example an order of volatility would be:

1. **Registers and cache**
2. **Routing tables**
3. **Arp cache**
4. **Process table**
5. **Kernel statistics and modules**
6. **Main memory**
7. **Temporary file systems**
8. **Secondary memory**
9. **Router configuration**
10. **Network topology**

General Procedure

When collecting and analyzing evidence, there is a general four-step procedure you should follow.

Identification of Evidence: You must be able to distinguish between evidence and junk data

Preservation of Evidence: The evidence you find must be preserved as close as possible to its original state.

Analysis of Evidence: Analysis requires in-depth knowledge of what you are looking for and how to get it.

Presentation of Evidence: The manner of presentation is important, and it must be understandable by a layman to be effective.

Collecting and Archiving

Once you've developed a plan of attack and identified the evidence that needs to be collected, it's time to start the actual process of capturing the data. Storage of that data is also important, as it can affect how the data is perceived.

Logs and Logging: You should run some kind of system logging function. It is important to keep these logs secure and to back them up periodically. Messages and logs from programs can be used to show what damage an attacker did.

Monitoring: By monitoring we can gather statistics, watch out for irregular, and trace where an attacker is coming from and what he is doing. Unusual activity or the sudden appearance of unknown users should be considered definite cause for closer inspection. You should display a disclaimer stating what monitoring is done when users log on.

Methods of Collection

There are two basic forms of collection: freezing the scene and honey potting.

Freezing the Scene

It involves taking a snapshot of the system in its compromised state. You should then start to collect whatever data is important onto removable nonvolatile media in a standard format.

All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification

Honeypotting

It is the process of creating a replica (imitation) system and luring(attracting) the attacker into it for further monitoring.

The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.

Artifacts (Objects)

There is almost always something left behind by the attacker be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as artifacts.

Never attempt to analyze an artifact on the compromised system.

Artifacts are capable of anything, and we want to make sure their effects are controlled.

Artifacts may be difficult to find; trojaned programs may be identical in all obvious ways to the originals (file size, medium access control

[MAC] times, etc.). If you are performing regular file integrity assessments, this shouldn't be a problem.

Analysis of artifacts can be useful in finding other systems the attacker (or his tools) has broken into.

Evidence Collection Steps

You now have enough information to build a step-by-step guide for the collection of the evidence. Once again, this is only a guide. You should customize it to your specific situation. You should perform the following collection steps:

Find the Evidence: Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.

Find the Relevant Data: Once you've found the evidence, you must figure out what part of it is relevant to the case.

Create an Order of Volatility: The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.

Remove external avenues of change: It is essential that you avoid alterations to the original data.

Collect the Evidence: Collect the evidence using the appropriate tools for the job.

Document everything: Collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important.

Preserving the Digital Crime Scene

Evidence is easily found in typical storage areas (spreadsheet, database, and word processing files). Unfortunately potential evidence can also reside in file slack, erased files, and the Windows swap file. Such evidence is usually in the form of data fragments and can be easily overwritten by something as simple as the booting of the computer or the running of Microsoft Windows. When Windows starts, it potentially creates new files and opens existing ones as a normal process. This situation can cause erased files to be overwritten, and data previously stored in the Windows swap file can be altered or destroyed. Furthermore, all of the Windows operating systems (Windows 2000, XP and especially 2003) have a habit of updating directory entries for files as a normal operating process. As you can imagine, file dates are important from an evidence standpoint.

Another concern of the computer investigator is the running of any programs on the subject computer. Criminals can easily modify the operating system to destroy evidence when standard operating systems commands are executed. Perpetrators could modify the operating system such that the execution of the DIR command destroys simulated evidence. Standard program names and familiar Windows program icons can also be altered and tied to destructive processes by a crafty high-tech criminal. Even trusted word processing programs such as Microsoft Word and WordPerfectTM can become the enemy of the cyber cop. It works this way: When word processing

files are opened and viewed, the word processing program creates temporary files. These files overwrite the temporary files that existed previously, and potential evidence stored in those files can be lost forever.

After securing the computer, we should make a complete bit stream backup of all computer data before it is reviewed or processed.

- **Bit stream backups are much more thorough than standard backups.**
- **They involve copying of every bit of data on a storage device, and it is recommended that two such copies be made of the original when hard disk drives are involved.**
- **Any processing should be performed on one of the backup copies.**
- **IMDUMP was the first software for taking bit stream back-ups developed by Michael White.**

SafeBack

- **SafeBack has become a law enforcement standard and is used by numerous government intelligence agencies, military agencies, and law enforcement agencies worldwide.**
- **SafeBack program copies and preserves all data contained on the hard disk.**
- **Even it goes so far as to circumvent attempts made to hide data in bad clusters and even sectors with invalid CRCs.**

SnapBack

- **Another bit stream back-up program, called SnapBack, is also available and is used by some law enforcement agencies primarily because of its ease of use.**

- **Its prices several hundreds of dollars higher than SafeBack.**
- **It has error-checking built into every phase of the evidence back-up and restoration process.**
- **The hard disk drive should be imaged using specialized bit stream back-up software.**
- **The floppy diskettes can be imaged using the standard DOS DISKCOPY program.**

Computer Evidence Processing Steps

Computer evidence is fragile (delicate) by its nature, and the problem is compounded by the potential of destructive programs and hidden data. Even the normal operation of the computer can destroy computer evidence that might be loitering in unallocated space, file slack, or in the Windows swap file. There really are no strict rules that must be followed regarding the processing of computer evidence. Every case is different, and flexibility on the part of the computer investigator is important. With that in mind, the following general computer evidence processing steps have been provided. Remember that these do not represent the only true way of processing computer evidence.

The following are general computer evidence processing steps:

Shut down the computer.

Depending on the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved. Generally, time is of the essence, and the computer system should be shut down as quickly as possible.

Document the hardware configuration of the system.

Be-fore dismantling the computer, it is important that pictures are taken of the computer from all angles to document the system hardware components and how they are connected. Labeling each wire is also important, so that it can easily be reconnected when the system configuration is restored to its original condition at a secure location.

Transport the computer system to a secure location.

A seized computer left unattended can easily be compromised. Don't leave the computer unattended unless it is locked up in a secure location.

Make bit stream backups of hard disks and floppy disks.

All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. Bit stream backups are much like an insurance policy and are essential for any serious computer evidence processing.

Mathematically authenticate data on all storage devices.

You want to be able to prove that you did not alter any of the evidence after the computer came into your possession. Since 1989, law enforcement and military agencies have used a 32- bit mathematical process to do the authentication process.

Document the system date and time.

If the system clock is one hour slow because of daylight-savings time, then file timestamps will also reflect the wrong time. To adjust for

these inaccuracies, documenting the system date and time settings at the time the computer is taken into evidence is essential.

Make a list of search key words.

It is all but impossible for a computer specialist to manually view and evaluate every file on a computer hard disk drive. Gathering information from individuals familiar with the case to help compile a list of relevant keywords is important. Such keywords can be used in the search of all computer hard disk drives and floppy diskettes using automated soft-ware.

Evaluate the Windows swap file.

The Windows swap file is a potentially valuable source of evidence and leads. When the computer is turned off, the swap file is erased. But the content of the swap file can easily be captured and evaluated.

Evaluate file slack.

It is a source of significant security leakage and consists of raw memory dumps that occur during the work session as files are closed. File slack should be evaluated for relevant keywords to supplement the keywords identified in the previous steps. File slack is typically a good source of Internet leads. Tests suggest that file slack provides approximately 80 times more Internet leads than the Windows swap file.

Evaluate unallocated space (erased files).

Unallocated space should be evaluated for relevant keywords to supplement the keywords identified in the previous steps.

Search files, file slack, and unallocated space for keywords.

The list of relevant keywords identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes. It is important to review the output of the text search utility and equally important to document relevant findings.

Document file names, dates, and times.

From an evidence standpoint, file names, creation dates, and last modified dates and times can be relevant. The output should be in the form of a word-processing-compatible file that can be used to help document computer evidence issues tied to specific files.

Identify file, program, and storage anomalies.

Encrypted, compressed, and graphic files store data in binary format. As a result, text data stored in these file formats cannot be identified by a text search program. Manual evaluation of these files is required. Depending on the type of file involved, the contents should be viewed and evaluated for its potential as evidence.

Evaluate program functionality.

Depending on the application software involved, running programs to learn their purpose may be necessary. When destructive processes that are tied to relevant evidence are discovered, this can be used to prove willfulness.

Document your findings.

It is important to document your findings as is-sues are identified and as evidence is found. Documenting all of the software used in your

forensic evaluation of the evidence, including the version numbers of the programs used, is also important. Be sure you are legally licensed to USE the forensic software. Screen prints of the operating software also help document the version of the software and how it was used to find or process the evidence.

Retain copies of software used.

As part of your documentation process, it is recommended that a copy of the software used be included with the output of the forensic tool involved. Duplication of results can be difficult or impossible to achieve if the soft-ware has been upgraded and the original version used was not retained.

LEGAL ASPECTS OF COLLECTING AND PRESERVING COMPUTER FORENSIC EVIDENCE

Definition

In simple terms, a chain of custody is a roadmap that shows how evidence was collected, analyzed, 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.

Preserving a chain of custody for electronic evidence, at a minimum, requires proving that:

- **No information has been added or changed.**
- **A complete copy was made.**
- **A reliable copying process was used.**
- **All media was secured**

Legal Requirements

When evidence is collected, certain legal requirements must be met. These legal requirements are vast, complex, and vary from country to country.

CERT Advisory CA-1992-19 suggests the following text be tailored to a

corporation's specific needs under the guidance of legal counsel:

- **This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.**
- **In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.**
- **Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.**

Evidence Collection Procedure

When the time arrives to begin collecting evidence, the first rule that must be followed is do not rush. Tensions will probably be high and people will want to find answers as quickly as possible.

The investigation team will need to bring certain tools with them to the incident site. They will need a copy of their incident-handling procedure, an evidence collection notebook, and evidence identification tags.

At a minimum, items to be recorded in the notebook include

- **Who initially reported the suspected incident along with time, date, and circumstances surrounding the suspected incident?**
- **Details of the initial assessment leading to the formal investigation.**
- **Names of all persons conducting the investigation.**
- **The case number of the incident.**
- **Reasons for the investigation.**
- **A list of all computer systems included in the investigation, along with complete system specifications. Also include identification tag numbers assigned to the systems or individual parts of the system.**
- **Network diagrams.**
- **Applications running on the computer systems previously listed.**

- **A copy of the policy or policies that relate to accessing and using the systems previously listed.**
- **A list of administrators responsible for the routine maintenance of the system.**
- **A detailed list of steps used in collecting and analyzing evidence. Specifically, this list needs to identify the date and time each task was performed, a description of the task, who performed the task, where the task was performed, and the results of the analysis. An access control list of who had access to the collected evidence at what date and time.**

Once all evidence is collected and logged, it can be securely transported to the forensics lab. A detailed description of how data was transported and who was responsible for the transport, along with date, time, and route, should be included in the log. It is required that the evidence be transported under dual control.