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 DataRecovery

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 over burden 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. We must be ready for consequences.

- **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.**

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.

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 tocopies.**

***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 bedocumented.**

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

***Donotexceedyourknowledge:*Ifyoueverfindyourself—outofyourdepth, ||eithergo 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 somedifficulties.**

***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 originaldata.**

***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 sameresults.**

***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 systemsare 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 lookingfor.**

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. **Cache**
4. **Process table**
5. **Kernel statistics andmodules**
6. **Main memory**
7. **Temporary filesystems**
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.**

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.

Honey potting

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 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.**