Preservation of Digital Evidence

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-upsoftware.**
- **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:

Before 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 software.

Evaluate the Windows swapfile:

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 fileslack:

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 issues 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.