The Proper Acquisition, Preservation, & Analysis of Computer Evidence: Guidelines & Best-Practices

Introduction

As organizations rely more heavily on technology-based methods of communication, many corporations and legal professionals are increasingly looking to computer forensics for the recovery of electronic information. Computer forensics can be utilized as a means to combat corporate fraud, investigate theft of trade secrets, monitor employee misconduct or malfeasance, and support a broad range of criminal and civil litigations.

Courts are recognizing and accepting the high level of discoverability associated with technology-based communication and documents, and lawyers are hiring computer forensic consultants and experts to recover electronic documents that users have attempted to dispose of or destroy. Therefore, computer forensics and electronic discovery have become critical components to augment and support attorneys in the identification of electronic evidence, development of case strategy, and response to discovery requests for electronic data.

Computer Forensics

Computer forensics is the process of preserving, identifying, analyzing, and documenting computer evidence stored in the form of magnetically encoded information (data) with the objective of uncovering evidence.

A thorough forensic analysis performed by a skilled examiner can result in the reconstruction of the activities of a computer user, recovery of deleted files, and exploration of sensitive data, while providing insight into an investigation.

The performance of computer forensics often uncovers information that can be classified as a "smoking gun", as in the case of Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass. Super. June 16, 1999). Through the forensic recovery of incriminating email messages, the parties involved were forced to settle rather than proceed through a trial after it was found that the makers of the drug Phen-Fen understood about the harmful side effects it caused.

However, paramount to computer forensic activities is the proper acquisition, preservation, and verification of collected data, which is predicated on the strict adherence to industry accepted best-practices, United States Department of Justice methodologies, and strict legal guidelines.

Electronic Evidence Processing Guidelines

Many hazards and risks exist regarding the handling and processing of computer evidence, as, by its very nature, it is extremely fragile and can potentially be easily destroyed, even by the computer's simple operation. Therefore, specific evidence processing guidelines should be followed to ensure that no sensitive information is destroyed, especially that which may be hidden in unallocated space, File Slack Space, or in the Windows swap file.

The following evidence processing guidelines were developed to best uncover electronic evidence in a forensically sound manner and are based and expand upon the United States Department of Justice search and seizure manual, Searching and Seizing Computers and Obtaining Electronic Evidence.

Step 1: Shut Down the Computer

Shutting down the computer system generally involves simply removing the computer's plug from the electrical outlet or utilizing applicable commands to shut down a network computer. At the time the computer is shut down, the forensic investigator may choose to take pictures of the screen image at his/her discretion. It is important for the forensic investigator to consider that the computer may have potentially damaging operations running in the background in areas such as the memory or a remaining modem connection. In addition, depending on the operating system utilized, it is possible for a password protected screen saver to appear, possibly making it more difficult to shutdown the computer. Time is an important factor during the shutdown process and forensic investigators must be careful to follow this step as quickly and efficiently as possible.

Step 2: Execute Chain of Custody

A proper chain of custody should be followed, which involves creating evidence tags and beginning a detailed list of individuals who have had control of the evidence at any point, from its collection to its conclusion. Once the chain of custody has been executed, the computer system should be relocated to a secure location, at which time the actual evidence processing can begin. Pictures of the computer from numerous angles should be taken to formally document the system hardware components and their connections before the computer is actually dismantled. In addition, each wire should be properly labeled so that it may be easily reconnected after the system configuration has been reinstated.

Step 3: Make Bit Stream Backups

Safeguarding any and all computer evidence is critical to the overall investigation, therefore, the computer should not be run and evidence should not be processed until bit stream backups have been made of all hard disk drives and floppy disks. Bit stream backups are utilized in a manner similar to an insurance policy and are necessary to process any computer evidence. All evidence should be processed on a restored copy of the bit stream backup instead of the original computer system, and the primary evidence should remain untouched unless undeniable conditions exist.

Step 4: Mathematically Authenticate Data

In order to show that none of the evidence was altered after the computer has come under the possession of the forensic investigator and that a true bit stream backup was created, a mathematical validation process based on the utilization of an MD5 sum is employed for authentication purposes.

Step 5: Document the System Date & Time

The accurate dates and times associated with computer files are often vital to an investigation. It is essential to document the system date and time when the system is taken into evidence so that file time stamps will reflect the same time as the system clock.

Step 6: Make a List of Key Search Words

It is almost impossible for a forensic investigator to manually view and determine the relevance of every file on a computer hard disk, since most computer hard disk drives are extremely large. As a result of this, forensic investigators utilize automated text search tools to uncover relevant evidence based on information collected from individuals involved in the case that should help to compile a list of relevant key words. These keywords are used to search the entire computer hard disk and any floppy disks.

Step 7: Evaluate the Windows Swap File

The Windows Swap File often contains a wealth of valuable evidence and potential leads and its evaluation is often automated through the use of specific forensic tools. However, when Windows 95 or 98 is operating on the computer system in question, the swap file may, by default, be set to be dynamically created as the computer is operated, and when the computer is turned off, the swap file is erased.

Step 8: Evaluate File Slack Space

Most computer users are unaware of File Slack Space, a data storage area that often contains significant amounts of information, including raw memory dumps that take place as files are closed throughout work sessions. Any data dumped from the computer's memory is stored at the end of allocated files, which is usually unknown to the computer user. Often, specific forensic tools are necessary to examine and analyze File Slack Space, as it can provide a wealth of information and additional investigative leads.

It is necessary for File Slack Space to be evaluated, as it may possess relevant key words to supplement the previously identified keywords.

Step 9: Evaluate Unallocated Space (Erased Files)

Generally, when a computer user deletes a file, he/she assumes that it has been thoroughly erased. However, the DOS and Windows "delete" function does not thoroughly erase either file

names or file content and instead the storage space associated with such files simply becomes unallocated and available to be overwritten with new files. Such unallocated space is often a significant source of information that potentially includes erased files and File Slack Space associated with files that have been "deleted".

In addition, it is often possible to utilize the DOS Undelete program to restore the previously erased files, providing additional relevant keywords and leads.

Step 10: Search Files, File Slack Space, & Unallocated Space

Keywords previously identified should be utilized to investigate all suspect computer hard disk drives and floppy disks. When relevant evidence is identified as a result of keyword searching, it should be documented and the identified data should be completely evaluated to uncover whether it contains any additional keywords. In addition, when new keywords are identified as a result of the investigation, they should be added to the complete keyword list and a new search should be conducted.

Step 11: Document File Names, Dates, & Times

File names, creation dates, and last modified dates and times are extremely relevant to forensic investigations, and they should be documented for all allocated and uncovered "deleted" files.

Step 12: Identify File, Program, & Storage Anomalies

Encrypted, compressed, and graphic files store data in a binary format and, as a result, a text search program cannot identify text data stored in these file formats; therefore, these files must be manually evaluated instead. Many forensic tools are able to detect the most common compressed and graphic file formats, which can be used to identify files that necessitate additional comprehensive manual evaluation.

The partitioning on seized hard disk drives should also be evaluated as it is possible that hidden partitions and/or partitions that have been formatted with an operating system other than a DOS compatible operating system. When hidden partitions are uncovered, they should be analyzed for evidence and their existence should be documented.

In addition, the files contained in the Recycle Bin should also be evaluated. The Recycle Bin is a repository of files that the computer user has selected to be deleted, which may be significant from an evidentiary standpoint. If relevant files are found, they should be thoroughly documented.

Step 13: Evaluate Program Functionality

Depending on the application software involved, it may be necessary to run certain programs to learn their purpose. As a result of this, detrimental processes may be exposed that are connected to relevant evidence, which can often prove willfulness. These detrimental processes can be correlated to the execution of common operating commands that are connected to the operating

system or applications in use by the computer system.

Step 14: Document Your Findings

All findings should be documented, as should all of the software and its version numbers utilized throughout the course of the forensic investigation.