Examination of Computer-Resident Evidence

Cosgrove Computer Systems Inc.
7411 Earldom Avenue
Playa del Rey, California 90293-8058
(310) 823-9448, JCosgrove@computer.org

7/7/01

Summary of Methods Used to Access Computer-Resident Data

- Preserve two or more copies of the disk contents using methods which faithfully reproduce the original version of the entire contents of the storage media -- whether used or not. This requires specially configured examination computers to avoid using the original computer system to provide access to the evidentiary media. Alternately, specialized evidence capturing software such as EnCase can be used to capture a single copy. This copy cannot be modified during examination when the EnCase examination tools are used in the analysis of the contents.
- Maintain records (chain-of-control) and backup copies of the original to allow recreation of all steps used in preparation of the evidence.
- Provide clear contextual and explanatory material in non-technical terms for all computer-based evidence. Often this requires the use of simple analogies for understanding followed by more detailed technical supporting data which supplies the necessary foundation.
- Issues involving computers are usually complex, but the underlying issues important to the court are normally simple. Translating the complex into the understandable is a major role of the computer expert.

Preserving the Evidence

Proper handling of the contents of a computer disk drive requires a disciplined process in order to preserve the full integrity of the evidence. Key to this is a special type of copying the entire disk which is called "cloning". This process preserves the record in a manner that then allows a thorough analysis of obscure information resident in the disk while also preserving the original data. In most cases, this is only possible with special software and/or hardware access under computer laboratory conditions. Particular care must be used in the "cloning" process as some common software products create files on the original disk in the process of cloning. This compromises the integrity of the evidence.

- Prior to any analysis or viewing of the contents, at least two fully-cloned copies of the disk must be made (see exception noted above) with the option enabled to copy all contents, not just the currently active files (the default is normally to copy only active file contents). Usually this requires temporary removal of the internal disk drive in order to perform the clone with another specially configured computer.
- Some data retrieval methods copy the contents onto CDROM disks. Making copies of drive contents to CDROM seldom preserves all of the contents – both active and deleted files – because of the storage volume available on a CDROM. Additionally, the critical properties of the files which contain the time history are usually not preserved when copied onto another type of media.
- Care must be made to not view the contents of the evidence drive using the software system resident on the drive being examined, as this alters the contents in several important ways. In other words, you cannot use the evidence to examine the evidence. Using a special laboratory setup is typically the only practical way to do this. Performing this in the field is possible but difficult and time consuming.
- Analysis of the contents of deleted files and the use characteristics of each file frequently reveal the most important elements of computer-resident evidence.

Deleted: 08/03/01

- During analysis, one of the copies may need to be altered in a minor way to completely retrieve deleted file data. For this reason, the other copy is necessary in order to preserve the original state. When using the specialty software products, this can be treated in a different manner. If an executable version of the original contents is necessary, an executable image can be created while still retaining the integrity of the original. Because it is always possible to restore the original contents, the analyst is free to experiment on the executable image in any manner useful to the investigation.
- Viewing the directory contents improperly changes the "last-viewed" (last accessed property) time history which is often a critical part of the record. Even some clone programs can alter the "last-viewed" time record and thus corrupt important evidence.

Examination of Computer-Resident Evidence

Steps Used in Preserving Evidence

These are described as typical steps that implement the above methods.

1. Remove the internal disk drive and clone (copy entire contents, both used and unused) with another computer system before the original system is started-up or any other operations are performed.
2. Clone two copies at the earliest possible time to guarantee availability of an original version for the future.
3. Perform all analysis of the cloned drive contents using a system different from the one being examined.
4. As a first step in analysis, create full directory records of the three critical time-based properties of each file – creation, last modification and last access (use). This must be done with software which does not update the last access property (note, most Windows software changes this property).
5. Perform analysis of the contents using various software utilities. It is important to include access to deleted files, some of which may be fragmentary.

Likely Investigative Process

A typical analysis includes the following courses of action. In any given case some of these steps may not be required, depending on circumstances. These steps are always subject to change as the discovery proceeds.

1. Identify the files critical to the investigation and record their properties, particularly the time-based ones.
2. Using the names of these critical files, look for all occurrences of these names so that a history of the source and any use of these files might be determined. Examples of this would be the name being used to designate an attachment in an email. These often appear in deleted temporary files typically created during Internet operations.
3. When file names are not available, searches can be made for relevant text strings likely to be unique to the issues such as proper names, technical titles, etc. In this manner, obscure files and deleted, incomplete fragments can be found and used very successfully.
4. Search for any records of activity in the computer during and after the critical period at issue.
5. Perform an overall survey of the contents of the computer, which may provide any contextual information, which could be relevant to the process. For instance, improper manipulation of the system date & time often leaves footprints in obscure system files.
6. Prepare the evidence showing the results of the analysis in a manner which allows full traceability back to the original contents of the disk drive. It should be possible to physically demonstrate each of these steps which led to the results presented. This is the only certain means of defending the accuracy of your results.

Deleted: 08/03/01