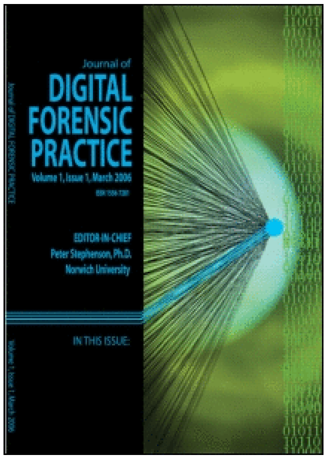


Journal of Digital Forensic Practice

Journal of Digital Forensic Practice, 2:57–61, 2008
Copyright © Taylor & Francis Group, LLC
ISSN: 1556-7281 print / 1556-7346 online
DOI: 10.1080/15567280801958464

Taylor & Francis
Taylor & Francis Group

ARTICLE

Computer Forensics–What Is It Good For?

Ronald E. Kaplan, MS, MBA
System Integration Consultants,
Los Angeles, CA, USA

ABSTRACT Computer forensic examiners need to combine art and science to produce the highest valued electronic data content. The wide variety of document types, tremendous volume of dissimilar media, operating systems, programs, and compaction and encryption algorithms all present daunting tasks for the examiner to efficiently organize, process, and filter. The art involves how to get to the core documents, the smoking gun. Individual disk drives, in and of themselves, are very large reservoirs of information. The investigator's job is to assist counsel in establishing priorities for searching drives, directories, and document types. This is where the experience of the examiner and the art of forensic examinations come in. The science involves the tools that capture, sort, and select the data for review by counsel. Further, there exists a wealth of knowledge about how computers operate and where programs and operating systems store data or encode information about where and when information was placed on a computer's hard drive. Experts who excel at combining the science with the art are the ones who are most helpful in assisting counsel making arguments that win court decisions.

KEYWORDS expert testimony, computer forensics, spoliation, evidence

Almost all operating businesses today utilize computers for record-keeping and correspondence. Many types of computer records can be modified or deleted easily with little or no visible audit trail, making the computer a common vehicle for business fraud and deception. Fortunately, deletion or modification of computer records is very difficult to accomplish without leaving a trail beneath the surface. A knowledgeable forensic computer expert oftentimes can find the trail of data modification or recover deleted data. If this trail is uncovered and carefully documented with proper procedures, the evidence obtained is very difficult to challenge or invalidate. Additionally, while the task of finding this evidence may be technically challenging, once found it is usually easy to understand and interpret.

Over the past few years lawyers have embraced the value of the data stored in electronic format. In the millions of pages of these digital documents that never reach the file cabinet, they have found emails, drafts, missing and deleted documents, accounting system audit trails, Internet searching activity, Internet browsing history, and a host of other data that would otherwise be difficult to find if they had been printed, and simply impossible if never printed. This potential treasure trove cannot be properly accessed without the assistance of a

Address correspondence to
Ronald E. Kaplan, System Integration
Consultants, 10277 West Olympic
Boulevard, Los Angeles, CA 90067.
E-mail: rkaplan@sicons.com

trained expert. The challenge is not just in finding the "smoking gun" but also in the efforts to preserve data in all the locales where it might exist, at a point in time before it is intentionally or unintentionally rendered irrecoverable from the electronic medium where it is stored. The large volume of data stored on even a single hard drive presents challenges to the examiners, who must be thorough in their review and selection of material relevant to the matter.

One of the cases that I worked on illustrates the importance of this point. My examination of the computer records revealed that a second set of books had been created for the company and hidden on the hard drive. All the records produced at the request of counsel before we got involved were from records that had been screened and sanitized and showed only a fraction of the activity in which the enterprise had actually been engaged. My team resurrected the complete records and produced the accurate reports and transaction logs, which enabled counsel to produce a more accurate assessment of the damages.

The courts have recognized the importance of electronic data. A large number of cases have been heard and the opinions from these cases have established case law governing electronic discovery procedures, cost sharing, privilege, and discoverability. An example lies in discovery, where even in adversarial litigation it is nearly impossible to prevent discovery of electronic data. The law is clear that employees do not have any right of privacy with respect to the information stored on company-owned computers they utilize. Further, if a personally owned computer is used to conduct company business, that computer is subject to discovery. The new federal discovery and preservation rules instituted at the end of 2006 present additional obligations to litigants in terms of electronic data.

Most computer users cannot even recall everything they created and viewed on their computer last week, much less last month or last year. If a document or email was deleted, users feel secure that it will never resurface. The fact that virtually all computer activity is date and time stamped and retained in a computer's hard drive memory makes computers an invaluable resource for pinpointing details that are often lost or forgotten. The deleted information, which still resides on the hard drive, cannot be easily found and produced by a user who needs it or wiped by a user trying to cover their tracks.

WHAT IS WORTH SEARCHING?

Cost is always a factor when conducting computer investigations. All the potential hardware suspects need to be identified, evaluated, and prioritized. Depending on what is at issue, consideration should be given to searching file servers, email servers, hard drives of local machines, BlackBerry, or other PDA (personal digital assistant) devices. Third-party service providers like AOL, Yahoo!, Gmail and host of others can be very expensive, if possible at all, to gain access to and success in locating relevant data much less likely than from hard drives under the client's control.

Determining what to search can be very difficult, especially if you don't know the precise object of your searches.

The computers where the document could have been produced were identified and searched for some words within the document that were believed to be unique to this particular document. It is not uncommon for a document search to find multiple copies of the document on a single hard drive.

If the search is of a more nebulous nature, like activity documenting intellectual property theft, conducting the search is much more difficult to structure and execute. These types of searches are often done as an iterative process where the list of search terms grows as results from initial searches are reviewed. The local hard drives of any individuals who might have created or received any relevant document or email are the best places to start. The associated hard drives from these PCs should be preserved at the earliest possible time. Other network devices like firewall machines, DHCP servers, file servers, etc., may also be very important to preserve, depending on the goals of a forensic examination.

I recall a matter where we fought hard to get the plaintiff to produce the hard drive from his laptop computer. While we were unable to get the plaintiff to produce the hard drive to us we were able to have the drive examined and data recovered by a third-party expert. The third-party expert produced a report listing all recoverable files on the drive. The report was several thousand pages of file names with associated file dates and times. Our analysis of the report led us to conclude that the plaintiff had lied in his deposition about when the laptop was last used and about his efforts to spoliate data contained on the hard drive.

Shortly after we presented our evidence to the judge, the plaintiff changed his demands and agreed to a settlement.

WHAT ARE THE COSTS INVOLVED?

Costs can be broken down in to three categories: preservation, examination, and reporting. The first category, preservation, is where computers are forensically imaged. The entire disk, including the areas of the disk that may never have been used, is digitally copied. In other words, the entire 100 GB of a 100 GB source drive are placed onto a destination drive. It is very important that all potentially valuable drives are imaged as soon as possible to avoid data loss. The cost of preservation depends upon the number of drives, the size of each drive, the drive interface technology (e.g., SCSI interface, RAID, IDE), and the reliability of the data on the drive. These factors will establish the difficulty and time required to create a valid image. A good rule of thumb is 2 to 4 hours per drive.

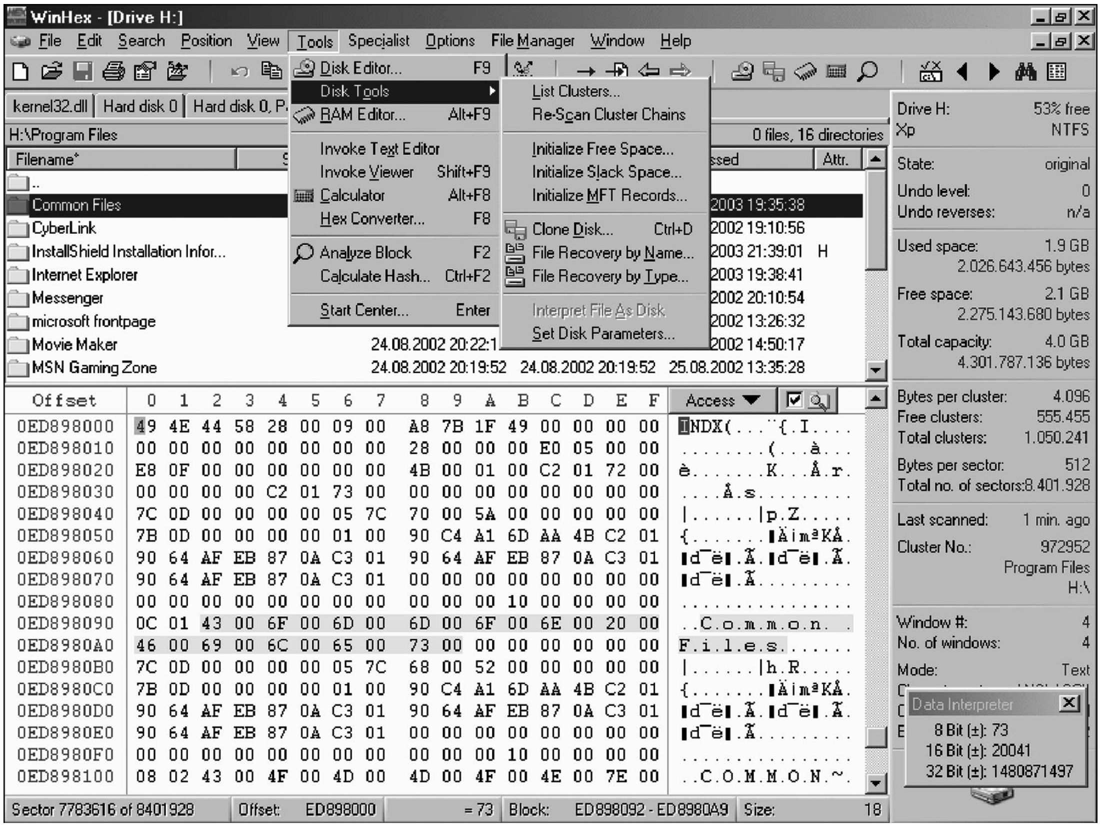
Drive examination costs are even more difficult to anticipate. This is due to the variety of applications and data formats that may be present of each drive. This examination involves the following steps:

- Loading the preserved image into the appropriate search software
- Defining and loading the loading terms
- Launching the search
- Reviewing the results (see Figure 1)

Review of the results may involve manual filtering of the search "hits."

The final category of cost is reporting. In establishing the costs involved in reporting, the purpose of the report must be considered. If, as is often the case, the report is to go to opposing counsel for privilege/privacy review, a report that enables the recipient to review and mark privilege/privacy items must be created. It must be done in a format consistent with the software available and must be simple to use. The amount of data selected for the report, the purpose of the report, and the format(s) of the data reported all contribute to the costs.

Depending on the testifying experience, technical expertise, and geographic location of the computer



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0ED898000  49 4E 44 58 28 00 09 00  A8 7B 1F 49 00 00 00 00  INDX(...¨{.I....
0ED898010  00 00 00 00 00 00 00 00  28 00 00 00 E0 05 00 00  ........(...à...
0ED898020  E8 0F 00 00 00 00 00 00  4B 00 01 00 C2 01 72 00  è.......K...Å.r.
0ED898030  00 00 00 00 C2 01 73 00  00 00 00 00 00 00 00 00  ....Å.s.........
0ED898040  7C 0D 00 00 00 00 05 7C  70 00 5A 00 00 00 00 00  |......|p.Z.....
0ED898050  7B 0D 00 00 00 00 01 00  90 C4 A1 6D AA 4B C2 01  {.......▮Äimª KÅ.
0ED898060  90 64 AF EB 87 0A C3 01  90 64 AF EB 87 0A C3 01  ▮d¯ë▮.Ã.▮d¯ë▮.Ã.
0ED898070  90 64 AF EB 87 0A C3 01  00 00 00 00 00 00 00 00  ▮d¯ë▮.Ã.........
0ED898080  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00  ................
0ED898090  0C 01 43 00 6F 00 6D 00  6D 00 6F 00 6E 00 20 00  ..C.o.m.m.o.n. .
0ED8980A0  46 00 69 00 6C 00 65 00  73 00 00 00 00 00 00 00  F.i.l.e.s.......
0ED8980B0  7C 0D 00 00 00 00 05 7C  68 00 52 00 00 00 00 00  |......|h.R.....
0ED8980C0  7B 0D 00 00 00 00 01 00  90 C4 A1 6D AA 4B C2 01  {.......▮Äimª KÅ.
0ED8980D0  90 64 AF EB 87 0A C3 01  90 64 AF EB 87 0A C3 01  ▮d¯ë▮.Ã.▮d¯ë▮.Ã.
0ED8980E0  90 64 AF EB 87 0A C3 01  00 00 00 00 00 00 00 00  ▮d¯ë▮.Ã.........
0ED8980F0  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00  ................
0ED898100  08 02 43 00 4F 00 4D 00  4D 00 4F 00 4E 00 7E 00  ..C.O.M.M.O.N.~.
```

Sector 7783616 of 8401928 | Offset: ED898000 | = 73 | Block: ED898092 - ED8980A9 | Size: 18

Drive H: 53% free
Xp NTFS

State: original
Undo level: 0
Undo reverses: n/a

Used space: 1.9 GB
2.026.643.456 bytes
Free space: 2.1 GB
2.275.143.680 bytes
Total capacity: 4.0 GB
4.301.787.136 bytes

Bytes per cluster: 4.096
Free clusters: 555.455
Total clusters: 1.050.241
Bytes per sector: 512
Total no. of sectors:8.401.928

Last scanned: 1 min. ago
Cluster No.: 972952
Program Files
H:\

Window #: 4
No. of windows: 4
Mode: Text

Data Interpreter
8 Bit (±): 73
16 Bit (±): 20041
32 Bit (±): 1480871497

FIGURE 1 **Forensic search for "common files."**

forensic experts involved, hourly rates can vary widely between $100 and $500 per hour. When dealing with electronic data it is imperative that the processes utilized do not compromise the value of the data under examination. Chain of custody and proper, defensible tools and procedures are critical to establish the credibility of the information found. Computer forensics experts are expensive, but don't be fooled into thinking that a computer technician is a viable substitute. A technician may find what you are looking for but in the process contaminate the hard drive and render the evidence inadmissible or invalid. Be assured that the validity or authenticity of the "smoking gun" will be challenged.

ADMISSIBILITY OF DATA FOUND?

Electronic data and the associated metadata (generally defined as data about data) make electronic evidence more valuable than hard-copy evidence. Often multiple versions of a single email or word-processed document can be located on a hard drive. The date and time the document was created can be validated by the date and time stamp on the electronic file and attempts to manipulate the system's data and time stamp can be found in system files maintained by the operating system. With hard-copy documents the date on the document is much more difficult to crosscheck. Further, with electronic data it may be possible to establish the context of a single document.

Certainly electronic data can be fabricated, deleted, or manipulated, but it is not easily done. Computer forensic information can also be misinterpreted. In a recent case, experts for opposing counsel interpreted the presence of a very large amount of zeros (or blank space) as evidence of data spoliation. It was unusual to see such a large amount of unused disk space, but careful examination of the data on the drive and a few questions to the user of the computer established a provable and entirely innocent explanation for all the blank space.

Dates of when an agreement was made, correspondence sent, and receipt or payment of funds are often the subject of dispute. If electronic records are maintained, the computer's method of logging, organizing, and sequencing information can provide an option for independent validation. Email or other computer records when printed can be manipulated to substantiate the position of one party. The electronic version of the very same record provides information not available in the printed form, which may enable information in the record or the entire record to be validated.

LIKELIHOOD OF SUCCESS

Setting an expectation for the success of electronic discovery examinations is akin to setting an expectation for non-electronic evidence; however, estimates are as high as 90% of documents created on a computer are never printed. Not looking for electronic evidence may mean you are looking at only 10% of documents produced. Information on a computer hard drive can be used to establish that an employee was at work, what they were working on on a particular day, whether they were using company time for non-work-related activities, and a host of other information not otherwise available.

WHEN TO CONTACT THE FORENSIC EXPERT?

The first rule of evidence is to preserve. Since electronic data is very volatile, the best time to preserve is immediately. You may not get everyone to agree on what is relevant and how to screen out privileged or private data, but that should not stop a preservation effort. Hard drive data can be preserved and handed over to a neutral party to hold until a procedure for extracting relevant data can be established. The courts recognize the criticality of preserving electronic data at the earliest point possible. Preservation must be done properly, documented, and a chain of custody established. If this is not done by an experienced professional, expect your findings to be challenged. An experienced professional can also be helpful in providing guidance on what to examine, providing questions for technical personnel, and help in establishing a discovery plan and priorities.

Computer forensic investigations are both art and science. The art involves how to get to the core documents, the smoking gun. Individual disk drives, in and of themselves, are very large reservoirs of information. The investigator's job is to assist counsel in establishing priorities for searching drives, directories, and document types. This is where the experience of the examiner and the art of forensic examinations come in. The science involves the tools that capture, sort, and select the data for review by counsel. Further, there exists a wealth of knowledge about how computers operate and where programs and operating systems store data or encode information about where and when information was placed on a computer's hard drive. Experts who excel at combining the science with the art are the ones who are most helpful in assisting counsel making arguments that win court decisions.