Computer Forensics (Finding & Preserving the Hidden Evidence)

John Mitchell

PhD, CEng, CITP MBA, FBCS, MBCS, CISA, FIIA, MIIA, QiCA, CFE

LHS Business Control
47 Grangewood
Potters Bar
Hertfordshire EN6 1SL
England
Tel: +44 (0)1707 851454
Fax: +44 (0)1707 851455
Mobile: +44 (0)7774 145638
John@lhscontrol.com
www.lhscontrol.com

Computer Forensics: finding and preserving the hidden evidence

John Mitchell

Introduction

'The moving finger writes and having writ moves on...' wrote Omar Khayyam some 900 years ago. What he did not foresee was the possibility of the text being composed on a device that could retain the imprint of the writing even after the paper on which it had been printed was destroyed. The role of forensic computing is very varied, but really falls into two main areas: criminal investigation and civil litigation.

Criminal cases usually require the retrieval of some information to support, or refute, a case being bought by the State. The most important part of any retrieved data item is usually the date and time it was created, the timestamp, as this usually ties in with some other evidence that is being presented. Proving the date and time is fraught with problems however, as we will discuss later. With the growth of the Internet, the problems associated with proving who originated something, from where and when, is becoming a major problem. With many international criminal organisations using the net for communication and data storage, the problem of decoding encrypted data is vexing the minds of the law enforcement bodies. This, coupled with the length of time that an investigation can take, often provides a warning to the perpetrators that allows them to move their activities to another part of the world and the whole investigative process may have to start again.

The *civil* cases usually revolve around contractual issues and requires the piecing together of what was intended and then comparing that with what has been provided. As the problem tends to be one of expectation it is not too surprising to find that the two sides have different views on what the deliverable should have been. The job of the investigator is firstly to decide what was reasonable and then to ascertain whether that marker has been met. This usually requires establishing the functionality of the system, its speed of response, the reliability of the documentation and the ongoing maintainability of the system. As the 'other side' will usually have their own expert there can be an interesting tussle in establishing the 'truth'. It never ceases to amaze me that the two sides can be well down the road of expensive litigation before they call in a couple of experts to advise them. It more often becomes a case of macho management, rather than sensible debate, with both sides hoping that 'their' expert can provide the coup de grace. In reality, the experts are there to guide the court and they usually reach agreement on what has happened and what should have been delivered long before their clients are ready to listen to reason.

The Evidence

Computer evidence exists on computer hard disk drives and other computer media (e.g. zip disks and floppy diskettes) at three different levels, two of which are not visible to the computer user. Such evidence is fragile and it can easily be destroyed through something as simple as the normal operation of the computer. Electromagnets and planted destructive Trojan horse programs are other hazards that can permanently destroy computer evidence in just a few moments.

Unlike paper evidence, computer evidence often exists in many different forms, with earlier 'draft' versions still retained on the same media as the final copy. Knowing the possibility of their existence means that alternate formats of the same data can be discovered. An expert identifying more evidence possibilities than originally requested can enhance the discovery process. In addition, during on-site premise inspections in cases where computers are not actually seized, the forensics expert can quickly identify places to look, signs to look for, and additional information sources for relevant evidence. These may take the form of earlier versions of data files that still exist on the computer's disk or on backup media, or differently formatted versions of data, either created or treated by other application programs (e.g. word processing, spreadsheet, e-mail, scheduling, or graphic).

Who Uses the Evidence?

Many types of criminal and civil proceedings make use of evidence revealed by computer forensics specialists:

- Criminal Prosecutors use computer evidence in cases where incriminating documents have been stored electronically;
- Civil litigators make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases;
- Insurance Companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and compensation cases;
- Corporations hire computer forensics specialists to ascertain evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information;
- Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of computer equipment;

- Individuals hire computer forensics specialists in support of possible claims of wrongful dismissal, sexual harassment, or age discrimination.

Securing the Evidence

Law enforcement officials normally seize computers during the execution of a search warrant. Depending on the circumstances and scope of the search warrant, all computer hardware, software and manuals should be taken for evaluation as potential evidence. Some prosecutors may view this as overly broad. However, the ability to process and examine the evidence may be directly tied to special hardware, software and/or written instructions contained in manuals. Because computer technology changes so quickly, it may be impossible to obtain similar or outdated hardware or instruction manuals from other sources. Printers, tape drives, optical drives, hardware manuals and software manuals, should all be taken. Pay particular attention to possible passwords that may have been written down near the computer. Encrypted files can cause serious difficulties and finding a password scrawled on a desk calendar may help make the case.

Many corporations and government agencies are becoming involved with computer evidence relating to internal investigations and internal audits. Corporate computer specialists should follow the same procedures used in criminal investigations, because it is usually unknown if criminal proceedings will follow. Following accepted computer evidence processing procedures will ensure that the case meets the requirements for both civil and criminal trial purposes. In a corporate or government setting, the ability to seize a computer and evaluate its data will be governed by corporate policy and privacy laws. For this reason, it is essential that corporate legal counsel be consulted before taking any steps to seize or process a corporate computer. In the absence of a corporate policy covering computer evidence and privacy issues, corporate computer specialists could be exposing themselves and the corporation to litigation.

Caution should always be used in the shutdown and transport of the subject computer. To preserve the image on the screen, a photograph or camcorder image of the screen display may be appropriate. Then a decision has to be made as to whether or not the computer should be unplugged from the power supply, or shut down systematically based on the requirements of the operating system. Unfortunately, there is no correct answer and there are risks in taking either course of action. The decision will depend on the particular facts involved, the operating system involved, and judgement. On balance, I consider it safer to disconnect the computer from its power supply, whether it is stand alone, or networked. If the system is protected by an uninterruptible power supply disconnect the power to the machine from the machine side of the UPS to ensure an immediate break of power.

Care should be taken when using the keyboard to enter operating system commands. One press of a key may trigger destructive memory resident programs that have been planted on the computer.

If seizure of the computer is carried out when the system is attended, any individual attending the computer should be immediately removed from the vicinity. One press of a pre-arranged key combination can destroy all evidence stored on a hard disk. Consider using a subterfuge to remove the operator from the computer to eliminate the possibility of the destruction of potential evidence. Seizure planning is very important and this is especially true if the probability of destructive processes exist.

Evidence Gathering Concerns

The initial and primary job is to preserve the computer evidence and to transport the computer to a safe location where a complete bit stream backup can be made. You also want to ensure that the computer system can be reconfigured to match the configuration in which it was found. For this purpose, it is wise to take pictures of the complete computer system from all angles. Wires should be marked so that they can be correctly reconnected. Also, the computer should be clearly marked as evidence and stored out of reach of inquiring co-workers. Chain of evidence is as relevant when it comes to computers as any other form of evidence. Be sure to document the time, date and circumstances surrounding the actual seizure of the computer. Every effort must be made to show that no one could have made changes to the information contained on a seized computer system. Without such an assurance, countless hours of processing effort may be wasted and the case lost.

The computer investigator needs to be worried about destructive software planted by the computer owner. He also needs to be concerned about the operating system and applications. Evidence is easily found in typical storage areas, e.g., spreadsheet, database and word processing files, but evidence can also reside in slack space, erased files, the Windows swap file, email files and Internet temporary files. Such evidence is usually in the form of data fragments and it can be easily overwritten by something as simple as the booting of the computer and/or the running of the operating system. For example, when Windows starts, it 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 to be altered or destroyed. Furthermore, Windows has a habit of updating directory entries for files as a normal operating process. These file dates are very 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. Standard program names and familiar Windows program icons can also be altered and tied to destructive processes.

When it comes to computer evidence, paranoia is a good personality trait to have. Do not operate a suspect computer until a complete backup has been made of all storage devices. Standard computer backups won't do and a full bit stream backup is necessary. In the bizarre world of computer evidence, you should always assume that things will go wrong. Once computer evidence has been destroyed or altered, it is unlikely that it can ever be reconstructed.

Tools of the Trade

Computer forensic tools are basically computer software. Computer forensic specialists guarantee accuracy of evidence by using time tested evidence processing procedures and the use of multiple software tools developed by different developers. The use of different tools to validate results is important in order to avoid inaccuracies introduced by software design flaws and. It is a mistake for a computer forensics specialist to put all of his eggs in the same basket by using just one tool to preserve, identify, extract and validate the computer evidence. Cross validation through the use of multiple tools and techniques is standard in all the forensic disciplines. When this procedure is not used, it enables lawyers to challenge the efficacy of the software tool used and thus the integrity of the results.

Many inherent problems associated with computer evidence gathering disappear when tried and proven procedures are followed. The very first objective after securing the computer is to make a complete bit stream backup of all computer data before it is reviewed or processed. This should normally be done before the computer is operated. Preservation of evidence is the primary element of all criminal investigations and computer evidence is no exception. Evidence can reside at multiple levels and in strange locations. These levels include allocated files, slack space and erased files. It is not enough to do a standard backup of a hard disk drive. To do so would eliminate the slack and erased file space (see later). Without backing up evidence in these areas, the evidence is susceptible to damage and/or modification by the computer investigator. Bit stream backups are much more thorough than standard backups. They involve the copying of every bit of data on a storage device and usually two copies are made of the original. Any processing should be performed on only one of the backup copies. The original evidence should be preserved at all costs. After all, it is the 'best evidence' available.

Forensic Computing Rules

The computer forensics specialist will take into considerations the following areas when attempting to identify and retrieve evidence from a system computer system:

- Protect the suspect computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction;
- Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files;
- Recover all, or as much as possible, of discovered deleted files;
- Reveal, to the extent possible, the contents of hidden files as well as temporary, or swap files used by both the application programs and the operating system;
- Access, if possible and if legally appropriate, the contents of protected or encrypted files;
- Analyse all relevant data found in special and typically inaccessible areas of a disk. This includes unallocated space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as 'slack' space in a file (the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data, but which may be a possible site for previously created and relevant evidence);
- Prepare an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data;
- Provide an opinion of the system layout, the file structures discovered, any discovered data and authorship information, any attempts to hide, delete, protect, encrypt information, and anything else that has been discovered and appears to be relevant to the overall computer system examination;
- Provide expert consultation and/or testimony, as required.

The main processes are expanded below.

Main Computer Forensic Processes

Shut Down the Computer

Depending upon the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved. Ideally, a digital camcorder can be used to record the shutdown process in real-time. Consideration should be given to possible destructive processes that may be operating in the background. These can be in memory, or available through a network, or connected modem. Depending on the operating system involved, a password

protected screen saver may also kick in at any moment. This can complicate the shutdown of the computer. 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
It is assumed that the computer system will be moved to a secure location where a proper chain of evidence can be maintained and evidence processing can begin. 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. Again, the use of a digital camcorder is ideal. Labelling 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
This may seem basic but all too often seized computers are stored in less than secure locations. It is imperative that the suspect computer is treated as evidence and it should be stored out of reach of curious computer users. All too often, individuals operate seized computers without knowing that they are destroying potential evidence and the chain of evidence. Furthermore, a seized computer left unintended can easily be compromised. Evidence can be planted on it and crucial evidence can be destroyed. A lack of a proper chain of evidence can make inadmissible any evidence collected. Lacking a proper chain of evidence, how can it be argued that relevant evidence was not planted on the computer after the seizure?

Make Bit Stream Backups of Hard Disks and Other Media
The computer should not be operated and computer evidence should not be processed until bit stream backups have been made of all hard disk drives and other media. All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. The original evidence should be left untouched unless compelling circumstances exist. Preservation of computer evidence is vitally important. It is fragile and it can easily be altered or destroyed. Often such alteration or destruction of data is irreversible. Bit stream backups 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. Such proof will help you rebut allegations that you changed or altered the original evidence. Forensic tools will calculate a check sum for the original data and append this to the bit stream copy for subsequent verification. Modern software authenticates data using a 128-bit level of accuracy. Such a large key provides a good degree of certainty that the data has not been subsequently modified.

Identify File, Program and Storage Anomalies
Encrypted, compressed and graphic files store data in binary format. As a result, a text search program cannot identify text data stored in these file formats. Manual evaluation of these files is required and in the case of encrypted files, much work may be involved. Reviewing the partitioning on seized hard disk drives is also important. The potential exists for hidden partitions and/or partitions formatted with other than a DOS compatible operating system. When this situation exists it is comparable to finding a hidden hard disk drive and volumes of data and potential evidence can be involved. The partitioning can be checked with any number of utilities including the DOS FDISK program or Partition Magic[1]. When hidden partitions are found, they should be evaluated for evidence and their existence should be documented. If Windows 95 or upward is involved, it makes sense to evaluate the files contained in the Recycle Bin. The Recycle Bin is the repository of files selected for deletion by the computer user. The fact that they have been selected for deletion may have some relevance from an evidentiary standpoint. If relevant files are found, the issues involved should be documented.

Document the System Date and Time
The dates and times associated with computer files can be extremely important from an evidence standpoint. However, the accuracy of the dates and times is just as important. If the system clock is one hour slow because of daylight-saving time, then file time stamps will also reflect the wrong time. The operator may have set the date/time of the computer incorrectly to start with, or may have access to powerful utility programs that allow the subsequent alteration of the timestamp. The software itself may timestamp the transaction incorrectly and the computer's clock may have been altered several times to cloud the issue. To adjust for these inaccuracies, documenting the system date and time settings at the time the computer is taken into evidence is essential.

Depending on the forensic tools being used it may be necessary to boot the suspect computer under controlled conditions in order to obtain the internal date and time settings. This is usually achieved by booting the machine from a floppy diskette containing a controlled version of an operating system. It may be necessary to load the system configuration option to achieve this as some machines are configured not to boot from the floppy drive. The use of a camcorder to record the event is desirable as it could be held that changing the computer's configuration could have changed the data content. Hence the need to obtain a bit stream image *before* doing anything else.

Prepare a List of Key Search Words
Modern hard disk drives are so large that it is all but impossible for a computer specialist to manually view and evaluate every file on a computer's hard drive. Therefore, automated forensic text search tools are needed to help find the relevant evidence. Usually, some information is known about the allegations, the computer user and the alleged associates that may be involved. Gathering information from individuals

[1] PowerQuest Corporation

familiar with the case to help compile a list of relevant key words is important. Keeping the list as short as possible is important and common words or words that make up part of other words should be avoided.

Examine the Windows Swap File
The Windows swap file is potentially a valuable source of evidence and leads. In the past this tedious task was done with hex editors and the process took days. By using automated tools, that process now takes just a few minutes. Where Windows 95 upward is involved, the swap file may be set to be dynamically created as the computer is operated. This is the default setting and when the computer is turned off, the swap file is erased. However, not all is lost because the content of the swap file can easily be captured and evaluated in much the same way as any other erased file can be recovered.

Evaluate File Slack
File slack is a data storage area of which most computer users are unaware. It consists of raw memory dumps that occur during the work session as files are closed. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or the view of the computer user. Specialised forensic tools are required to view and evaluate file slack and it can provide a wealth of information and investigative leads. Like the Windows swap file, this source of data can help provide relevant key words and leads that may have previously been unknown. Such keywords should be added to the computer investigator's list of key words for use later. Because of the nature of file slack, specialised and automated forensic tools are required for evaluation.

Evaluate Erased Files
The DOS and Windows delete function does not completely erase file names or file content. Many computer users are unaware the storage space associated with such files merely becomes unallocated and available to be overwritten with new files. Unallocated space is a source of significant 'security leakage' and it potentially contains erased files and file slack associated with the erased files. Often the operating system’s undelete program can be used to restore the previously erased files. Like the Windows swap file and file slack, this source of data can help provide relevant key words and leads that may have previously been unknown to the computer investigator. Because of the nature of data contained in unallocated space and its volume, specialised and automated forensic tools are required for evaluation.

Identify Email Storage Areas
If the computer has been used for email, then it is likely that relevant correspondence will be held in the email folders.

Identify Internet Storage Areas
If the computer has been used for accessing the Internet, then it is likely that a wealth of information will be held in Internet folders, favourites and temporary Internet files. The

'cookie' repository should not be overlooked, as information here will reveal some of the sites visited.

Search All Areas for Key Words
The list of relevant key words identified in the previous steps should be used to search all relevant computer hard disk drives and other media. There are several forensic text search utilities available in the marketplace. It is important to review the output of the text search utility and equally important to document relevant findings. When relevant evidence is identified, the fact should be noted and the identified data should be completely reviewed for additional key words. When new key words are identified, they should be added to the list and a new search should be conducted.

Stegnographic Awareness
Stegnography is the process by which data can be hidden in images. A key protects the data so hidden and a casual browse of the image will show nothing amiss. Indeed, the only sign that stegnography is being is used may be the existence of a stegnographic application on the disk. The investigator needs to be aware of the names of these programs, but also aware that they are easily renamed to something innocuous. In some cases the only indication that a program is of the stegnographic school comes when it is run.

Document File Names, Dates and Times
From an evidence standpoint, file names, creation dates, last modified dates and times can be relevant. Therefore, it is important to catalogue all allocated and 'erased' files.

Document the Findings
As indicated in the preceding steps, 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.

Retain Copies of Software Used
As part of your documentation process, ensure that a copy of the software used is included with the output of the forensic tool involved. Normally this is done on an archive Zip disk, Jazz disk or other external storage device, such as an external hard disk drive. When this documentation methodology is followed, it eliminates confusion as to which version of the software was used to create the output. Often it is necessary to duplicate forensic processing results during or before trial. Duplication of results can be difficult or impossible to achieve if the software has been upgraded and the original version used was not retained. There is a high probability that you will encounter this problem because most commercial software is upgraded routinely but it may take years for a case to go to trial.

Only Use Licensed Forensic Software!
Be sure that you are legally licensed to use the forensic software. Software pirates do not stand up well under the rigours of a trial. Lawyers may question software licensing and you do not want to testify that you used unlicensed software in the processing of computer evidence, as software piracy is a criminal violation of copyright laws. Where appropriate, mention in your documentation that the forensic software used was licensed

Conclusions

The preservation of computer evidence is the most important element of computer evidence processing. However, the proper documentation of the steps taken during the evidence processing also ranks as a top priority. Good documentation tied to sound processing procedures is essential for success. Without the ability to reconstruct accurately what has been done, crucial evidence may be subject to question. More importantly, the qualifications of the expert witness can become an issue if the computer evidence processing was done haphazardly. Shortcuts should be avoided at all costs.

One of the main problems associated with criminal cases is that the burden of proof is so great that extensive investigation is required. A further problem is that with the increasing use of personal computers, everyone tends to consider themselves experts in computing. It is important that the forensic investigator can present a case in a way that will not antagonise a jury, but which at the same time eliminates the likelihood of misinterpretation, due to misguided knowledge.

Forensic computing, whether of a criminal, or civil nature, requires attention to detail, a methodical approach and good record keeping. It brings together many skills: computing; auditing; the law, interviewing, report writing, but above all, patience. This last skill is the most difficult to learn, as it is easier to destroy evidence by switching on a suspect computer without realising that the very act of switching it on may contaminate the evidence, than it is to retrieve it by careful thought and thorough analysis.

The evidence is one thing, interpretation is another. Two experts will often agree on the accuracy of the evidence, but will disagree on its interpretation. Now that is where the fun really starts!

Bibliography

Investigating Computer-Related Crime, Peter Stephenson, CRC Press, 1999

Computer evidence: A Forensic Investigations Handbook, Edward Wilding, Sweet & Maxwell, 1997

The Expert Witness and his evidence, M P Reynolds & P S D King, Blackwell Scientific Publications, 1992

John Mitchell
Managing Director
LHS Business Control
47 Grangewood
Potters Bar
Hertfordshire
EN6 1SL
England
Tel: +44 (0)1707 851454
Fax: +44 (0)1707 851455
Mobile: +44 (0)7774 145638
Email: john@lhscontrol.com
Internet: www.lhscontrol.com