Jim McMillan
May 1, 2000

## Why use a standard methodology?

Following a standard methodology is crucial to successful and effective computer forensics. Just as professional programmers use a thorough programming methodology, computer forensic professionals should use a thorough investigative methodology.

Computer design and software implementation is very similar from one system to the next. With this in mind, similar concepts can be applied from one system to another. Computer evidence can exist in many forms, and often in many different versions. The investigator having knowledge of many storage techniques and methods can quickly identify places to look for signs of evidence. Many times evidence will not escape the case by being overlooked. Subsequently, due to the many types of hardware and software available for storing information, the investigator must have access to a wide variety of equipment.

A standard methodology will provide for protection of evidence and some common steps that should be followed in the investigation process.

## Why is it important to protect evidence?

Many cases are lost or don't even make it to court because of compromised evidence. Evidence must be handled very cautiously to avoid any circumstances that would cause it to be dismissed from court. You must be very careful to ensure that evidence is not destroyed or altered. The slightest change or mishap could cost you the case. Computer evidence can be very sensitive, diskettes and hard drives can be destroyed or rendered useless by electromagnetic forces, improper handling and storage, etc. The computer forensic professional must handle the computer and it's media in a way to ensure that no possible evidence is damaged, destroyed, or altered.

Some potential threats that could compromise evidence during the seizure or investigation of computer equipment:

- Viruses – These programs lay dormant waiting for execution. When the malicious code is executed the possibility of file deletion or corruption is possible
- Computer cleanup procedures – There is a possibility of the existence of programs or scripts that delete files when the computer is shutdown or started up. The computer forensic professional must realize this to understand why it is important not to use the operating system's shutdown method or boot using the suspect drive or operating system.
- Even external threats can destroy evidence. Storing media in an environment that is not suited for it to be stored can cause damage or loss of evidence. Avoid places that are too hot, cold, dry, or moist. Computer media is best suited for a controlled comfortable environment.

Some other factors that are not physically associated with the seizure or investigation of the evidence or its surroundings include:

- Chain of custody – The chain of custody is a record of evidence handling from the time of seizure to the court case. The custody of evidence should be closely documented. This documentation should show who, what, where, when, why, and how. The more detailed the events the better.
- Time constraints – Timeliness can be crucial in some investigations. Especially cases that involve human life. There may be a time when evidence that you have not discovered may lead to the plans of a terrorist attack or similar event. Time is of essence, but sometimes time constraints placed on the investigator could force quick and possible compromise or missed evidence.
- Divulged information – Information that is inadvertently acquired such as client-attorney respected information.

Collecting evidence is very time consuming and tedious. A lot of the evidence is encrypted (I.E. PGP – Commonly used to encrypt e-mail messages and files) or hidden in a way that it looks as another type of file (I.E. Steganography – which hides secret data with other data, such as secret company data with a graphic image). If you are stumped on an encrypted file, try looking around the crime scene for a paper copy of the encrypted file in it's decrypted printed copy. Don't let encrypted data be the cause of not prosecuting. Several software applications have a key or password recovery system that is protected by a trusted agent of the software's company. Third-party software is also available to exploit known weaknesses in some systems. Many of these software packages are downloadable from the Internet; others are only obtainable by law enforcement agencies.

Files are sometime stored with a deceptive extension, sometimes images will be stored to look like a text document. For example, someone with a child pornography image may save it as a README.TXT file in a program setup folder. Remote file storage may be utilized to hide data, so be aware of remote file servers, or data that may be stored on removable media and kept off-site. Remember when it comes to computer storage avenues, locally is not always used.

For these reasons many cases are not even prosecuted. According to the "Crime Seen" article by Bill Betts (referenced below), "A recent study by the Electronic Privacy Information Center (EPIC) demonstrates just how serious this problem is: Since 1992, the number of computer crime cases sent to federal prosecutors has tripled, while the number of cases actually prosecuted has remained the same. Of the 419 cases referred to prosecutors, only 83 were prosecuted. The rest were dismissed due to… you guessed it… lack of evidence."

Evidence is essential to successfully apprehending and convicting the criminal of their offense. Thus, protecting the evidence and being thorough is very crucial to the investigation. Since some cases may not go to trial for several years, this task can be somewhat tedious and space consuming. But if it is done correctly, the benefits will pay off in the long run.

## Some common steps found among computer forensic professionals.

Below are some steps that many of the computer forensic professionals have in common and consider to be steps in the right direction.

- Have a legal right to seize and investigate the suspect computer. Have appropriate approval, search warrants, subpoenas, etc.
- Protect the crime scene – Access to the area around the suspect computer should be restricted to only the individuals involved with the investigation. The scene should be documented in great detail. Photograph the computer from all angles and the surrounding area. In addition to photography, diagram the computer configuration on paper and by labeling which cables are attached and what they attach to.
- Kill the computer's power source - Do not shut the computer down through the normal shutdown process. As previously mentioned, there could be cleanup procedures implemented to delete data. Unplug the computer from the power source. This should be a direct source of power such as a wall outlet, power strip, or UPS if one is present.
- Transport the seized equipment to a secure and controlled environment that is trusted to be free of any thing that could modify or destroy the evidence.
- Disconnect hard drive – You should never use the suspect computer's hard drive to boot from or it's operating system to perform investigative tasks. You do not know what type of cleanup procedures are waiting in the boot process. Disconnect the hard drive and boot from a floppy disk (the BIOS may need to be modified to allow boot from a floppy). Once you are sure you can boot from the floppy drive, the hard drive can be reconnected for investigative purposes. Another good solution is to put the suspect's hard drive in a trusted computer as a slave drive.
- Make bit stream image of all disk space – You should make a bit stream image of the suspect hard drive before anything else.
- Examine free space and file slack, which can contain deleted information and/or hidden data. Free space comes from the available sectors that have not been written to or have been made available from hidden files. File slack is the area of space in an occupied cluster that spans the point where file data

ends to the end of the cluster. This area is sometimes used to hide data or where deleted data may remain.

- Be aware of swap files that may contain valuable data. Some systems have files that are used to cache information between memory and the hard drive; these files are known as swap files.
- Mathematically authenticate the data – use a hash algorithm to generate a numeric expression and compare this to the same hash algorithm on the data that was backed up. This is used as proof that the file has not changed.
- Discover all files – Use disk utilities such as undelete to recover as much of the deleted data as possible. When recovering data with the undelete utility, you should avoid using the real first character. It is recommended to use a common character that is not typical to any filenames. This way you can identify what files were recovered by being undeleted. In addition, use utilities to search the disk for hidden files.
- Search the contents of the hard drive for any incriminating evidence. Make a list of key words that pertain to the investigation. This could help narrow down some of the data that is pertinent.
- Analyze all of the relevant data that was found from your search.
- Document all processes in detail as they are being performed. From the beginning notification of possible illegal activity to the very end of the investigation.
- Prepare to make and defend your accusations in a court of law. You should be confident in your accusations and your knowledge of computer operations.

Remember that good detailed documentation can always benefit you, especially when the case may go to court in three to five years!

## What to look for in a computer forensic professional.

In addition to a using a good methodology, the following characteristics may be desired when looking for a computer forensic professional.

- Be a computer knowledgeable person that can back their comments and accusations with the proof that they are experts at what they do. Education, experience, and certifications are all good qualifications for a well-rounded computer forensic professional. The education with experience provides the confidence needed to make decisions and know the decisions made were the right ones. Certification shows that the education and experience of the person is of a high standard and understanding.
- Be confident in their decisions and actions. They must be confident enough to testify in court and withstand a harsh cross-examination.
- Be thorough on all processes involved.
- Have vast knowledge of how to recover data from several types of media.
- Be able to break the passwords of several different applications and operating systems, as well as understand the available tools and their uses for computer investigation.
- Be wary of an unqualified or under-qualified person. Without the proper knowledge of the computer technology involved, this person can make mistakes that will make the evidence inadmissible in a court. The evidence can be damaged, altered, or valuable data completely missed due to not understanding the process. Other than the possibility that the evidence is inadmissible in a court, there is the possibility of other lawsuits arising due to incompetence.
- Be objective and unbiased. The person must be fair and impartial to the person or people being investigated. The facts must be accurate and complete.
- Be innovative, outgoing, and possess good interpersonal skills.
- Have good verbal and oral communication skills.
- Be inquisitive and able to use logic.

When making a selection, be wary of an unqualified or under-qualified person. Without the proper knowledge of the computer technology involved, this person can make mistakes that will make the evidence inadmissible in a court. The evidence can be damaged, altered, or valuable data completely missed due to not understanding the process. Other than the possibility that the evidence is inadmissible in a court, there is the possibility of other lawsuits arising due to incompetence.

## Sources:

Judd Robbins, “An Explanation of Computer Forensics.”
URL: http://computerforensics.net/forensics.htm (April 27, 2000)

Berryhill Computer Forensics, “Choosing a computer forensics specialist for a criminal case.”
URL: http://www.computerforensics.com/law-enforce.htm (April 27, 2000)

Data Discovery, “Computer Forensics and Law Enforcement.”
URL: http://www.teleport.com/~peterc/law.html (April 27, 2000)

Kirk from Kompukirk Services, “Computer Forensics for the 21st Century is HERE!”
URL: http://www.compukirk.com/kk00007.html (April 27, 2000)

Kirk from Kompukirk Services, “Can you do Computer Forensics without Expert Help?”
URL: http://www.compukirk.com/kk00008.html (April 27, 2000)

David Morrow of Ernst and Young LLP, “The IT Security Professional as Investigator.”
URL: http://www.gocsi.com/sec.pro.htm (May 1, 2000)

Bill Betts, “Crime Seen”
URL: http://www.infosecuritymag.com/march2000/forensics.htm (May 1, 2000)

Bill Betts, “Storage Media Primer”
URL: http://www.infosecuritymag.com/march2000/forensics_box.htm (May 1, 2000)

Dorothy E Denning and William E Baugh Jr., “Hiding Crimes in Cyberspace.”, July 1999
URL: http://cryptome.org/hiding-db.htm (May 1, 2000)