Sally Ramage
United Kingdom: British Businesses Beware! Digital Evidence is Coming to a Courtroom Near You!
07 August 2006
Article by Sally Ramage

This is the type of digital evidence report that is valid in a
court of law and which can be used in court, the digital evidence expert having used such scrupulous procedures, that his report is utterly valid and carries great weight…..

Developments worldwide have made it simple to acquire all sorts of information through the use of computers. Criminal activity is a major one. In an effort to fight an exponentially increasing fraud wave, law enforcement agencies, financial institutions, investment firms and insurance firms are incorporating computer forensics into their infrastructure. From network security breaches to corporate money laundering, the common bridge is the demonstration that the particular electronic media contained **the incriminating evidence**.

Supportive examination procedures and protocols are used in order to show that the electronic media contains the incriminating evidence. The computer investigation process expands from the crime scene through analysis and finally into the courtroom. This summary of procedures attempts to inform about digital evidence reports.

Examination Of Digital Evidence.

Technology is advancing at a rapid rate, nevertheless, each case is unique and the judgment of the examiner should be given deference in the implementation of any particular procedures. Circumstances of individual cases and relevant laws may also require actions other than those described here.

When dealing with digital evidence, the following general forensic and procedural principles apply.

1. Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
2. Persons conducting an examination of digital evidence should be trained for that purpose.
3. Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review. The aim is to conduct an accurate and impartial examination of the digital evidence.

Digital evidence is processed by assessment and computer forensic examiners assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take. Digital evidence, by its very nature, is fragile and can be altered, damaged or destroyed by improper handling or examination. Therefore, examination is best conducted on a *copy* of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence. The purpose of the examination process is to extract and analyze digital evidence. Here, extraction refers to the recovery of data from its media and analysis refers to the interpretation of the recovered data and presenting it in a logical

and useful format. All actions and observations should be rigorously documented throughout the forensic processing of evidence. This will conclude with the preparation of a written report of the findings. A well-trained examiner understands that documentation is continuous throughout the entire examination process.

Computer forensics as a discipline demands specially trained personnel in order to produce sound digital evidence recovery techniques. These computer digital examiners must have policies and procedures a Mission statement in order to establish the parameters for operation and function. Their Mission Statement would incorporate the core functions of high-technology crime investigations, evidence collection, or forensic analysis. All such personnel must meet minimum qualifications and job descriptions. They must ensure that all software they use is properly licensed and must prove that they have maintained their skill and competence through ongoing training.

Firstly, when a digital evidence report is required, the nature of the crime, court dates, deadlines, potential victims, legal considerations, volatile nature of the evidence, and available resources must all be considered. Established guidelines for receiving, processing, documenting, and handling evidence will be to hand. Other forensic disciplines might be able to recover some other evidence, such as fingerprints on the hard drive, hair or fibres in the keyboard, and handwritten disk labels or printed material.

Even if the examiner is from a one-man expert concern, he must have developed processes for preserving and processing digital evidence and should never attempt to look for files on the original media because this will change the date and time stamps associated with those files and possibly affect other data on the media. Procedures to guide the technical process of the examination of evidence should be tested prior to their implementation to ensure that the results obtained are valid and independently reproducible. The steps in the development and validation of the procedures must be documented and include identifying the task or problem, proposing possible solutions, testing each solution on a known control sample and evaluating the results of the test and finalizing the procedure. *Original evidence should never be used to develop procedures.*

The digital evidence should be thoroughly assessed by reviewing case detail, nature of hardware and software, potential evidence sought, and the circumstances surrounding the acquisition of the evidence to be examined and there should be a discussion as to the possibility of pursuing other investigative avenues to obtain additional digital evidence, identifying remote storage locations and email addresses.

Consideration must be made of the relevance of peripheral components to the investigation. *For example, in forgery or fraud cases consider noncomputer equipment such as laminators, credit card blanks, cheque paper, scanners, and printers*.

A determination must be made of the potential evidence being sought (e.g., photographs, spreadsheets, documents, databases, financial records). A determination needs to be made of any additional information regarding the case (e.g., aliases, e-mail accounts, e-mail addresses, ISP used, names, network configuration and users, system logs, passwords, user names. This information may be obtained through interviews with the system administrator, users, and employees. There must be an assessment of the skill levels of the computer users involved. Techniques employed by skilled users to conceal or destroy evidence may be

sophisticated (e.g., encryption, booby traps, steganography). A priority is established of the order in which evidence is to be examined, determining the equipment needed. This assessment might uncover evidence pertaining to other criminal activity. In some cases, the examiner may only have the opportunity to do the following while onsite: identify the number and type of computers; determine if a network is present; interview the system administrator and users; identify and document the types and volume of media, including removable media; document the location from which the media was removed; identify offsite storage areas and/or remote computing locations; identify proprietary software; evaluate general conditions of the site; determine the operating system in question; determine the need for and contact available outside resources, if necessary and establish and retain a phone list of such resources.

Completion of an examination must take place in a controlled environment, such as a dedicated forensic work area or laboratory. Whenever onsite, the examiner must attempt to control the environment by considering the time needed onsite to accomplish evidence recovery and the impact on the business. Then he will prioritize the evidence (e.g., distribution CDs versus user-created CDs); determine how to document the evidence (e.g., photograph, sketch, notes), evaluate storage locations for electromagnetic interference, ascertain the condition of the evidence as a result of packaging, transport, or storage and assess the need to provide continuous electric power to battery-operated devices always remembering that digital evidence is fragile and can be altered, damaged, or destroyed by improper handling or examination.

Therefore he must document hardware and software configuration of the system; verifying operation of the computer system to include hardware and software and take care to ensure equipment is protected from static electricity and magnetic fields. He must also identify storage devices that need to be acquired. These devices can be internal, external, or both. He must document internal storage devices and hardware configuration and disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.

He must perform a controlled boot to capture CMOS/BIOS information and test functionality of boot sequence (this may mean changing the BIOS to ensure that the system boots from the floppy or CD-ROM drive), time and date and passwords. He must then perform a second controlled boot to test the computer's functionality and the forensic boot disk. He must boot the computer and ensure the computer will boot from the forensic boot disk. He must reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS. He must ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices. He must remove the subject storage device and perform the acquisition. When attaching the subject device to the examiner's system, he must configure the storage device so that it will be recognized. Removing the disks and acquiring them individually may not yield usable results. In laptop systems, the system drive may be difficult to access or may be unusable when detached from the original system. Older drives may not be readable in newer systems.

He must ensure that his storage device is forensically clean when acquiring the evidence. Write protection must be initiated to preserve and protect original evidence. He must investigate the geometry of any storage devices to ensure that all space is accounted for,

including host-protected data areas. He must capture the electronic serial number of the drive and other user-accessible, host-specific data.

To extract and analyse digital evidence, he must prepare working directory/directories on separate media to which evidentiary files and data can be recovered or extracted. The physical extraction phase identifies and recovers data across the entire physical drive without regard to file system. The logical extraction phase identifies and recovers files and data based on the installed operating system, file system, and application.

During the physical extraction stage, the extraction of the data from the drive occurs at the physical level regardless of file systems present on the drive. This will include keyword searching, file carving, and extraction of the partition table and unused space on the physical drive. Performing a keyword search across the physical drive will be useful as it allows the examiner to extract data that may not be accounted for by the operating system and file system.

The logical extraction of the data from the drive is based on the file system present on the drive and may include data from such areas as active files, deleted files, file slack, and unallocated file space. He must extract the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location. Analysis is the process of interpreting the extracted data to determine their significance to the case. Some examples of analysis that may be performed include timeframe, data hiding, application and file, and ownership and possession.

Timeframe analysis is useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual at the time the events occurred. By reviewing the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) files of interest can be linked to the timeframes relevant to the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed. By reviewing the system and application logs that may be present, ie. error logs, installation logs, connection logs, security logs, etc. may indicate when a user name/password combination was used to log into a system. Concealed data on a computer can be revealed by correlating the file headers to the corresponding file extensions to identify any mismatches. *The presence of mismatches may indicate that the user intentionally hid data.*

By gaining access to all password-protected, encrypted, and compressed files, an attempt to conceal the data from unauthorized users may be revealed. He must analyze *the file metadata*, the content of the user-created file containing data additional to that presented to the user, typically viewed through the application that created it and placing the subject at the computer at a particular date and time that may help determine ownership and possession. Files of interest may be located in nondefault locations . Hidden data may indicate a deliberate attempt to avoid detection .If the passwords needed to gain access to encrypted and password-protected files are recovered; the passwords themselves may indicate possession or ownership. Contents of a file may indicate ownership or possession by containing information specific to a user.

Documentation is an ongoing process throughout the examination. It is important to

accurately record the steps taken during the digital evidence examination. All documentation must be complete, accurate, and comprehensive. Documentation must be contemporaneous with the examination, and retention of notes follows policy procedures.

The digital evidence reporter must take notes detailed enough to allow complete duplication of actions; including dates, times, and descriptions and results of actions taken; irregularities encountered and any actions taken regarding the irregularities during the examination; additional information, such as network topology, list of authorized users, user agreements, and passwords. He must document the operating system and relevant software version and current, installed patches. He must have documented information obtained at the scene regarding remote storage, remote user access, and offsite backups.

His report will include date of report, descriptive list of items submitted for examination, including serial number, make, and model, identity and signature of the examiner, a brief description of steps taken during examination, such as string searches, and graphics, image searches and recovering erased files and conclusions. The details of findings must describe in great detail the results of the examinations and include specific files related to the request; other files, including deleted files, that support the findings; string searches, keyword searches, and text string searches; internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity; graphic image analysis; indicators of ownership such as program registration data; data analysis; description of relevant programs on the examined items; techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.

A list of supporting materials must be included with the report, such as printouts of particular items of evidence and digital copies of evidence. A glossary will be included with the report to assist the reader in understanding any technical terms used, with a generally accepted source for the definition of the terms, including appropriate references.

Digital evidence is the best evidence. It cannot be fabricated as one step reveals another. It can be reconstructed. It can only be dubious if there is conspiracy, perjury, or forensic incompetence.