Proper procedures in computer forensics must be followed in any investigation relying on computer or electronic information, regardless.

Computer Forensics – Overcoming the “after-the-fact” approach

Dr. P Dennis Newsom, CIS © March, 2006

Computer forensics is the art and science of retrieving, validating, and analyzing information to a computerized device. Although the common personal computer is an obvious data source, automated devices such as PDA’s digital cameras, cash registers, cell phones, fax machines and security systems are all potential data sources pertinent to expert witnesses in many fields. Experts are accustomed to verifying the data used in making conclusions, but the data derived from computerized devices presents forensic challenges unfamiliar to many experts. Expertise in computer forensics, or at least familiarity with the concept, is therefore a valuable credential on any expert's résumé.

Here are some examples: a labor relations expert questions wage data obtained from an electronic time clock; an accounting expert deciphers financial data retrieved from a damaged computer disk; or an engineering expert analyzes configuration data extracted from an industrial automation system. As each of the cases evolve, electronic data will be obtained and combined to form conclusions that later may be challenged as "bad data." The subject-matter experts may be well versed in labor or finance or engineering, but what are their skills in verifying computer data? Any attorney engaging an expert should address this concern long before the opposing attorney addresses it in deposition.

One traditional approach to verifying data sources has been incorporation of a computer forensics expert to augment the subject-specific expert. This after-the-fact approach presents at least two problems: 1) engagement of the forensics expert often comes too late to salvage verifiable data, and 2) forensics experts typically have a narrow focus that limits their value in the non-computer matter under investigation. A more efficient solution in the era of computerization is to engage a subject matter expert who also has adequate credentials in computer forensics.

The engineering example listed above is a typical area. Similar situations involving automated equipment failures should encourage the engineer to seek and obtain formal credentials in computer forensics to augment his or her engineering pedigree. Given proper forensic training, the “engineer” will now consider the "chain of evidence" procedures before addressing the case's technical aspects that may be totally unrelated to the attached computers. Attorneys should realize that the seemingly unimportant computers and their vast resource of data might eventually become more important than the technical findings they produced. Computer forensics is therefore a useful tool for an expert to carry in their toolbox.

Although every state issues engineering licenses, there are no equivalent certifications in computer forensics. This statutory void is currently being filled by academic organizations that set their own computer forensics standards, and also provide software and training to meet them. These programs generally target computer technicians in law enforcement and government, but qualified applicants from other fields can qualify if they meet the security requirements and demonstrate an adequate technical background. Investigators, engineers and others with extensive low-level computer experience are welcome candidates for forensics training.

After researching available programs, you may chose from a number of leading computer forensics programs at a major university or from software developers such as AccessData, or Encase; each has an abundant, diverse mix of technical and procedural content. If you have reached this point, you will then need to invested the

necessary time and expense to attend the program, study and pass the examinations, and procure the specialized hardware and software required to implement what you have learned. As a properly trained computer forensics expert you will not simply copy disks and concentrate only on their contents. Instead, you will apply proper computer forensic procedures to ensure that the data obtained, and the results produced, can withstand rigorous scrutiny long after the chance to "do it over" is gone.

Don't overlook computer forensics in any matter involving electronic data. Either engage a computer forensics expert on Day One, or even better, engage a subject-specific expert who can also apply proper forensics procedures as part of their overall service.

The Devil's Advocate:
Computer Forensics Can Support Both Sides of Computer Litigation

Dr P Dennis Newsom © March, 2006

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. Computer specialists can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information. Any or all of this information may help during discovery, depositions, or actual litigation.

GIVE THE DEVIL'S ADVOCATE HIS DUE

Just as statistics are often used on both sides of many arguments, so are computer specialists. Although the experts sometimes present diametrically opposing positions, it is more likely that the lawyers involved in the case choose to elicit differing but not truly conflicting statements. Experts can readily help on either side of a case, either to identify helpful prosecutorial facts or to suggest alternative possibilities to create reasonable doubt. Experts are counseled not to be advocates, and they need not be when the facts alone offer sufficient material for legal presentation. Experts are told to answer Yes or No and not give any more than is asked. However, experts are also expected to know when to refuse to give a simple Yes or No when a more expanded answer is truly necessary to clarify a response.

In Alabama recently, I testified for the defense in a military court martial trial in a case that involved possible use (or misuse) of the Internet for interstate trafficking in child pornography. Computer experts were engaged on both sides of the issue, and there was no contention between their expert opinions. The prosecution expert conducted the original forensic exploration of the defendant's computers. He presented his facts about files, both existing and deleted, that were found there. No argument there. However, the Defense was able to note some degree of inattention to the Federal guidelines for search and seizure of computer evidence. This led to discussions of the ease with which anybody can change the various dates and times associated with computer files. Reasonable doubt?

The prosecution presented lists of photographic images that were downloaded from the Internet. No argument there. Many thousands of images await interested viewers on the Internet, and an increasingly large percentage of those are pornographic. However, if more than one person has access to the same Internet account via a common password (and a girlfriend in this case did have that kind of easy access to the defendant's computer), who is to say which person was actually responsible for downloading the photographs found on this defendant's computer. Reasonable doubt?

Medical evidence was brought in by the prosecution to confirm the fact that some of the pornography was of women under the age of 18. In this case, a defense medical witness spoke to the uncertainty of age determination. The defense computer expert then spoke to the ease

with which photographic retouching can modify digital pictures. Not that any picture in the case was actually manipulated digitally, but only that it can and could have been done with alarming ease and subsequent difficulty in ever determining if it was ever done. More reasonable doubt?

The list can go on, and in some cases, it certainly does. The computer forensics expert can unearth incredibly damaging evidence on computer disks. It's the prosecution's job to use that evidence to cement their case. But the computer forensics expert can also help the defense to identify any weaknesses in procedure or results that can help cast reasonable doubt on the apparent findings. It's the defense counsel's job to ascertain where and what weaknesses may exist and bring them to the fore.

BENEFITS OF PROFESSIONAL FORENSIC METHODOLOGY

The impartial computer expert who helps during discovery will typically have experience on a wide range of computer hardware and software. This is always beneficial when your case involves hardware and software with which this expert is directly familiar. But fundamental computer design and software implementation is often quite similar from one system to another, and experience in one application or operating system area is often easily transferable to a new system.

Unlike paper evidence, computer evidence can often exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of their existence, even alternate formats of the same data can be discovered. The discovery process can be served well by a knowledgeable expert identifying more possibilities that can be requested as possibly relevant evidence. In addition, during on-site premises inspections, for cases where computer disks are not actually seized or forensically copied (see below), the forensics expert can more quickly identify places to look, signs to look for, and additional information sources for relevant evidence.

I was a designated prosecution expert earlier this year in a case in Las Vegas, Nevada. During Discovery, the attorneys for the prosecution were going to ask for most of the obvious things about the subject software that had allegedly performed inadequately. But they hadn't planned to ask for any earlier versions of the software in question; these versions may have still existed on the computer systems of the developing programmers or on the backup tapes of the developing software firm. These historical versions could have included helpful historical comments or earlier code that might have helped the determination of current software inadequacy. Similarly, any forensics exploration of a computer system should consider the existence and relevance of earlier versions of data files (eg. memos, spreadsheets) 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 (eg. word processing, spreadsheet, e-mail, timeline, scheduling, or graphic).

Protection of evidence is critical. A knowledgeable computer forensics professional will ensure that a subject computer system is carefully handled to ensure that:

- No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
- No possible computer virus is introduced to a subject computer during the analysis process.
- Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage.
- A continuing chain of custody is established and maintained.
- Business operations are affected for a limited amount of time, if at all.
- Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

STEPS TAKEN BY COMPUTER FORENSICS SPECIALISTS

The computer forensics specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system. These steps include:

- Protecting the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
- Discovering all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
- Recovering all (or as much as possible) of discovered deleted files.
- Revealing (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.
- Accessing (if possible and if legally appropriate) the contents of protected or encrypted files.
- Analyzing all possibly relevant data found in special (and typically inaccessible) areas of a disk.
- This includes but is not limited to what is called '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 once again may be a possible site for previously created and relevant evidence).
- Printing out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data. Further, provides 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.
- Providing expert consultation and/or testimony, as required.

Recovering and Examining Computer Forensic Evidence

Dr P Dennis Newsom, CIS ©

Introduction

The world is becoming a smaller place in which to live and work. A technological revolution in communications and information exchange has taken place within business, industry, and our homes. America is substantially more invested in information processing and management than manufacturing goods, and this has affected our professional and personal lives. We bank and transfer money electronically, and we are much more likely to receive an E-mail than a letter. It is estimated that the worldwide Internet population is 349 million (Commerce Net Research Council 2000).

In this information technology age, the needs of law enforcement are changing as well. Some traditional crimes, especially those concerning finance and commerce, continue to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulations of data are detected daily. Crimes of violence also are not immune to the effects of the information age. A serious and costly terrorist act could come from the Internet instead of a truck bomb. The diary of a serial killer may be recorded on a floppy disk or hard disk drive rather than on paper in a notebook.

Just as the workforce has gradually converted from manufacturing goods to processing information, criminal activity has, to a large extent, also converted from a physical dimension, in which evidence and investigations are described in tangible terms, to a cyber dimension, in which evidence exists only electronically, and investigations are conducted online.

Computer Forensic Science

Computer forensic science was created to address the specific and articulated needs of law enforcement to make the most of this new form of electronic evidence. Computer forensic science is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media. As a forensic discipline, nothing since DNA technology has had such a large potential effect on specific types of investigations and prosecutions as computer forensic science.

Computer forensic science is, at its core, different from most traditional forensic disciplines. The computer material that is examined and the techniques available to the examiner are products of a market-driven private sector. Furthermore, in contrast to traditional forensic analyses, there commonly is a requirement to perform computer examinations at virtually any physical location, not only in a controlled laboratory setting. Rather than producing interpretative conclusions, as in many forensic disciplines, computer forensic science produces direct information and data that may have significance in a case. This type of direct data collection has wide-ranging implications for both the relationship between the investigator and the forensic scientist and the work product of the forensic computer examination.

Background

Computer forensic science is largely a response to a demand for service from the law enforcement community. As early as 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence. To properly address the growing demands of investigators and prosecutors in a structured and programmatic manner, the FBI established the Computer Analysis and Response Team (CART) and charged it with the responsibility for computer analysis. Although CART is unique in the FBI, its functions and general

organization are duplicated in many other law enforcement agencies in the United States and other countries. An early problem addressed by law enforcement was identifying resources within the organization that could be used to examine computer evidence.

These resources were often scattered throughout the agency. Today, there appears to be a trend toward moving these examinations to a laboratory environment. In 1995, a survey conducted by the U.S. Secret Service indicated that 48 percent of the agencies had computer forensic laboratories and that 68 percent of the computer evidence seized was forwarded to the experts in those laboratories. As encouraging as these statistics are for a controlled programmatic response to computer forensic needs, the same survey reported that 70 percent of these same law enforcement agencies were doing the work without a written procedures manual (Noblett 1995). Computer forensic examinations are conducted in forensic laboratories, data processing departments, and in some cases, the detective's squad room. The assignment of personnel to conduct these examinations is based often on available expertise, as well as departmental policy. Regardless of where the examinations are conducted, a valid and reliable forensic examination is required. This requirement recognizes no political, bureaucratic, technological, or jurisdictional boundaries. There are ongoing efforts to develop examination standards and to provide structure to computer forensic examinations. As early as 1991, a group of six international law enforcement agencies met with several U.S. federal law enforcement agencies in Charleston, South Carolina, to discuss computer forensic science and the need for a standardized approach to examinations. In 1993, the FBI hosted an International Law Enforcement Conference on Computer Evidence that was attended by 70 representatives of various U.S. federal, state, and local law enforcement agencies and international law enforcement agencies. All agreed that standards for computer forensic science were lacking and needed. This conference again convened in Baltimore, Maryland, in 1995, Australia in 1996, and the Netherlands in 1997, and ultimately resulted in the formation of the International Organization on Computer Evidence. In addition, a Scientific Working Group on Digital Evidence (SWGDE) was formed to address these same issues among federal law enforcement agencies.

A New Relationship

Forensic science disciplines have affected countless criminal investigations dramatically and have provided compelling testimony in scores of trials. To enhance objectivity and to minimize the perception of bias, forensic science traditionally has remained at arms length from much of the actual investigation. It uses only those specific details from the investigation that are necessary for the examination. These details might include possible sources of contamination at the crime scene or fingerprints of individuals not related to the investigation who have touched the evidence. Forensic science relies on the ability of the scientists to produce a report based on the objective results of a scientific examination. The actual overall case may play a small part in the examination process. As a case in point, a DNA examination in a rape case can be conducted without knowledge of the victim's name, the subject, or the specific circumstances of the crime.

Conversely, computer forensic science, to be effective, must be driven by information uncovered during the investigation. With the average storage capacity in a personally owned microcomputer approaching 30 gigabytes (GB;

Fischer 1997), and systems readily available that have 60-GB storage capacity or more, it is likely to be impossible from a practical standpoint to completely and exhaustively examine every file stored on a seized computer system. In addition, because computers serve such wide and varied uses within an organization or household, there may be legal prohibitions against searching every file. Attorney or physician computers may contain not only evidence of fraud but probably also client and patient information that is privileged. Data centrally stored on a computer server may contain an incriminating E-mail prepared by the subject as well as E-mail of innocent third parties who would have a reasonable expectation of privacy. As difficult as it would be to scan a directory of every file

on a computer system, it would be equally difficult for law enforcement personnel to read and assimilate the amount of information contained within the files. For example, 12 GB of printed text data would create a stack of paper 24 stories high. For primarily pragmatic reasons, computer forensic science is used most effectively when only the most probative information and details of the investigation are provided to the forensic examiner. From this information, the examiner can create a list of key words to cull specific, probative, and case-related information from very large groups of files. Even though the examiner may have the legal right to search every file, time limitations and other judicial constraints may not permit it. The examination in most cases should be limited to only well-identified probative information.

Forensic Results

Forensic science has historically produced results that have been judged to be both valid and reliable. For example, DNA analysis attempts to develop specific identifying information relative to an individual. To support their conclusions, forensic DNA scientists have gathered extensive statistical data on the DNA profiles from which they base their conclusions. Computer forensic science, by comparison, extracts or produces information. The purpose of the computer examination is to find information related to the case. To support the results of a computer forensic examination, procedures are needed to ensure that only the information exists on the computer storage media, unaltered by the examination process. Unlike forensic DNA analysis or other forensic disciplines, computer forensic science makes no interpretive statement as to the accuracy, reliability, or discriminating power of the actual data or information.

Beyond the forensic product and the case-related information needed to efficiently perform the work, there is another significant difference between most traditional forensic science and computer forensic science. Traditional forensic analysis can be controlled in the laboratory setting and can progress logically, incrementally, and in concert with widely

accepted forensic practices. In comparison, computer forensic science is almost entirely technology and market driven, generally outside the laboratory setting, and the examinations present unique variations in almost every situation.

Common Goals

These dissimilarities aside, both the scientific conclusions of traditional forensic analyses and the information of computer forensic science are distinctive forensic examinations. They share all the legal and good laboratory practice requirements of traditional forensic sciences in general. They both will be presented in court in adversarial and sometimes very probing proceedings. Both must produce valid and reliable results from state-of-the-art procedures that are detailed, documented, and peer-reviewed and from protocols acceptable to the relevant scientific community (ASCLD/LAB 1994). As laboratories begin to examine more computer-related evidence, they must establish policies regarding computer forensic examinations and, from these policies, develop protocols and procedures. The policies should reflect the broad, community-wide goal of providing valid and reproducible results, even though the submissions may come from diverse sources and present novel examination issues. As the laboratory moves from the policy statement to protocol development, each individual procedure must be well-documented and sufficiently robust to withstand challenges to both the results and methodology. However, computer forensic science, unlike some of its traditional forensic counterparts, cannot rely on receiving similar evidence in every submission. For instance, DNA from any source, once cleared of contaminants and reduced to its elemental form, is generic. From that point, the protocols for forensic DNA analysis may be applied similarly to all submissions. The criminal justice system has come to expect a valid and reliable result using those DNA protocols. For the following reasons, Computer forensic science can rarely expect these same elements of standardized repetitive testing in many of its submissions: Operating systems, which define what a computer is and how it works, vary among manufacturers. For example, techniques

developed for a personal computer using the Disk Operating System (DOS) environment may not correspond to operating systems such as UNIX, which are multi-user environments.

Applications programs are unique.

Storage methods may be unique to both the device and the media. Typical computer examinations must recognize the fast-changing and diverse world in which the computer forensic science examiner works.

Examining Computer Evidence

Computer evidence represented by physical items such as chips, boards, central processing units, storage media, monitors, and printers can be described easily and correctly as a unique form of physical evidence. The logging, description, storage, and disposition of physical evidence are well understood. Forensic laboratories have detailed plans describing acceptable methods for handling physical evidence. To the extent that computer evidence has a physical component, it does not represent any particular challenge. However, the evidence, while stored in these physical items, is latent and exists only in a metaphysical electronic form. The result that is reported from the examination is the recovery of this latent information. Although forensic laboratories are very good at ensuring the integrity of the physical items in their control, computer forensics also requires methods to ensure the integrity of the information contained within those physical items. The challenge to computer forensic science is to develop methods and techniques that provide valid and reliable results while protecting the real evidence—the information—from harm. To complicate the matter further, computer evidence almost never exists in isolation. It is a product of the data stored, the application used to create and store it, and the computer system that directed these activities. To a lesser extent, it is also a product of the software tools used in the laboratory to extract it. Computer forensic science issues must also be addressed in the context of an emerging and rapidly changing environment. However, even as the environment changes, both national and international law enforcement agencies recognize the need for common technical approaches and are calling for standards (Pollitt 1998). Because of this, a model (see Figure 1) must be constructed that works on a long-term basis even when short-term changes are the rule rather than the exception. The model that we describe is a three-level hierarchical model consisting of the following: An overarching concept of the principles of examination,

Policies and practices, and Procedures and techniques.

Principles of examinations are large-scale concepts that almost always apply to the examination. They are the consensus approaches as to what is important among professionals and laboratories conducting these examinations. They represent the collective technical practice and experience of forensic computer examiners. Organizational policy and practices are structural guidance that applies to forensic examinations. These are designed to ensure quality and efficiency in the workplace. In computer forensic science, these are the good laboratory practices by which examinations are planned, performed, monitored, recorded, and reported to ensure the quality and integrity of the work product. Procedures and techniques are software and hardware solutions to specific forensic problems. The procedures and techniques are detailed instructions for specific software packages as well as step-by-step instructions that describe the entire examination procedure (Pollitt 1995). As an overall example, a laboratory may require that examinations be conducted, if possible and practical, on copies of the original evidence. This requirement is a principle of examination. It

represents a logical approach taken by the computer forensic science community as a whole, and it is based on the tenet of protecting the original evidence from accidental or unintentional damage or alteration. This principle is predicated on the fact that digital evidence can be duplicated exactly to create a copy that is true and accurate.

Creating the copy and ensuring that it is true and accurate involves a subset of the principle, that is, policy and practice. Each agency and examiner must make a decision as to how to implement this principle on a case-by-case basis. Factors in that decision include the size of the data set, the method used to create it, and the media on which it resides. In some cases it may be sufficient to merely compare the size and creation dates of files listed in the copy to the original. In others, it may require the application of more technically robust and mathematical rigorous techniques such as a cyclical redundancy check (CRC) or calculating a message digest (MD).

CRC and MD are computer algorithms that produce unique mathematical representations of the data. They are calculated for both the original and the copy and then compared for identity. The selection of tools must be based on the character of the evidence rather than simply laboratory policy. It is likely that examiners will need several options available to them to perform this one function.

An examiner responsible for duplicating evidence must first decide an appropriate level of verification to weigh time constraints against large file types. The mathematical precision and discriminating power of these algorithms are usually directly proportional to the amount of time necessary to calculate them. If there were 1 million files to be duplicated, each less than 1 kilobyte in size, time and computational constraints would likely be a major determining factor. This circumstance would probably result in a decision to use a faster, but less precise and discriminating, data integrity algorithm.

Having decided how best to ensure the copy process will be complete and accurate, the next step is the actual task. This is a subset of the policy and practice, that is, procedures and techniques. These most closely represent the standard cookbook approach to protocol development. They are complete and contain required detailed steps that may be used to copy the data, verify that the operation was complete, and ensure that a true and accurate copy has been produced.

Again, as Figure 1 illustrates, a principle may spawn more that one policy, and those policies can accept many different techniques. The path an examiner takes in each case is well-documented and technologically sound for that particular case. It may not, however, be the same path the examiner takes with the next case. Traditional forensic examinations, such as the DNA examination of blood recovered from a crime scene, lend themselves to a routine and standardized series of steps that can be repeated in case after case. There is generally no such thing as generic computer evidence procedures. The evidence is likely to be significantly different every time a submission is received by the laboratory and will likely require an examination plan tailored to that particular evidence. Although this situation may present a recurrent consideration of management checks and controls within the laboratory setting, it is a consideration that must be addressed and improved if this emerging forensic discipline is to remain an effective and reliable tool in the criminal justice system.

Conclusion

Valid and reliable methods to recover data from computers seized as evidence in criminal investigations are becoming fundamental for law enforcement agencies worldwide. These methods must be technologically robust to ensure that all probative information is recovered. They must also be legally defensible to ensure that nothing in the original evidence was altered and that no data was added to or deleted from the original. The forensic discipline of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media is computer forensic science. This article examined issues surrounding the need to develop laboratory protocols for computer forensic science that meet critical technological and legal goals. Computer forensic scientists need to develop ongoing relationships with the criminal justice agencies they serve. The

reasons for these relationships include the following: In their efforts to minimize the amount of data that must be recovered and to make their examinations more efficient and effective, computer forensic scientists must have specific knowledge of investigative details. This is a clear requirement that is generally more demanding than traditional forensic science requests, and it places more reliance on case information.

Courts are requiring that more information rather than equipment be seized. This requires cooperative efforts between law enforcement officers and the computer forensic scientist to ensure that the technical resources necessary for the execution of the search warrant are sufficient to address both the scope and complexity of the search.

Computers may logically contain both information identified in the warrant as well as information that may be constitutionally protected. The computer forensic scientist is probably the most qualified person to advise both the investigator and prosecutor as to how to identify technical solutions to these intricate situations. Developing computer examination protocols for forensic computer analysis is unique for several reasons: Unlike some traditional forensic analyses that attempt to gather as much information as possible from an evidence sample, computer forensic analysis attempts to recover only probative information from a large volume of generally heterogenous information.

Computer forensic science must take into account the reality that computer forensic science is primarily market driven, and the science must adapt quickly to new products and innovations with valid and reliable examination and analysis techniques.

The work product of computer forensic science examinations also differs from most traditional forensic work products. Traditional forensic science attempts to develop a series of accurate and reliable facts. For example, the DNA extracted from blood found at a crime scene can be matched to a specific person to establish the fact that the blood was shed by that person to the exclusion of all other individuals. Computer forensic science generally makes no interpretive statement as to the accuracy or reliability of the information obtained and normally renders only the information recovered.

Computer forensic science protocols should be written in a hierarchical manner so that overarching principles remain constant, but examination techniques can adapt quickly to the computer system to be examined. This approach to computer forensic protocols may differ from those developed for many traditional forensic disciplines, but it is necessary to accommodate a unique forensic examination.

References

American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB). ASCLD/LAB Manual. American Society of Crime Laboratory Directors/Laboratory Accreditation Board, Garner, North Carolina, 1994, pp. 29–30.

CommerceNet Research Council. 2000 Industry Statistics. Available at http://www.commerce.net/research/stats/wwstats.html

Fischer, L. M. I.B.M. plans to announce leap in disk-drive capacity, New

York Times (December 30, 1997), p. C-2.
Noblett, M. G. Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence. In: Proceedings of the 11th INTERPOL Forensic Science Symposium, Lyon, France. The Forensic Sciences Foundation Press, Boulder, Colorado, 1995.
Pollitt, M. The Federal Bureau of Investigation report on computer evidence and forensics. In: Proceedings of the 12th INTERPOL Forensic Science Symposium, Lyon, France. The Forensic Sciences Foundation Press, Boulder, Colorado, 1998.
Pollitt, M. Computer Evidence Examinations at the FBI. Unpublished presentation at the 2nd International Law Enforcement Conference on Computer Evidence, Baltimore, Maryland, April 10, 1995.

Forensic Examination Procedures

These procedures are established as the IACIS® Forensic Examination standards to ensure that competent, professional forensic examinations are conducted by IACIS® members. We promote and require that these standards be used by IACIS® members.

It is acknowledged that almost all forensic examinations of computer media are different and that each cannot be conducted in the exact same manner for numerous reasons, however there are three essential requirements of a competent forensic examination. These are:

- **Forensically sterile examination media *must be* used.**
- **The examination *must* maintain the integrity of the original media.**
- **Printouts, copies of data and exhibits resulting from the examination *must be* properly marked, controlled and transmitted.**

Hard Disk Examination

The following are the IACIS® recommended procedures for conducting a complete examination of computer Hard Disk Drive (HDD) media:

Forensically sterile conditions are established. All media utilized during the examination process is freshly prepared, completely wiped of non-essential data, scanned for viruses and verified before use.

All forensic software utilized is licensed to, or authorized for use by, the examiner and/or agency/company.

The original computer is physically examined. A specific description of the hardware is made and noted. Comments are made indicating anything unusual found during the physical examination of the computer.

Hardware/software or other precautions are taken during any copying or access to the original media to prevent the transference of viruses, destructive programs, or other inadvertent writes to/from the original media. We recognize that because of hardware and operating system limitations and other circumstances, this may not always be possible.

The contents of the CMOS, as well as the internal clock are checked and the correctness of the date and time is noted. The time and date of the internal clock is frequently very important in establishing file creation or modification dates and times.

The original media is not normally used for the examination. A bitstream copy or other image of the original media is made. The bitstream copy or other image is used for the actual examination. A detailed description of the bitstream copy or image process and identification of the hardware, software and media is noted.

The copy or image of the original HDD is logically examined and a description of what was found is noted.

The boot record data, and user defined system configuration and operation command files, such as, the CONFIG.SYS file and the AUTOEXEC.BAT file are examined and findings are noted.

All recoverable deleted files are restored. When practical or possible, the first character of restored files are changed from a HEX E5 to “-”, or other unique character, for identification purposes.

A listing of all the files contained on the examined media, whether they contain potential evidence of not, is normally made.
If appropriate, the unallocated space is examined for lost or hidden data.
If appropriate, the “slack” area of each file is examined for lost or hidden data.
The contents of each user data file in the root directory and each sub-directory (if present) are examined.
Password protected files are unlocked and examined.
A printout or copy is made of all apparent evidentiary data. The file or location where any apparent evidentiary data was obtained is noted on each printout. All exhibits are marked, sequentially numbered and properly secured and transmitted.
Executable programs of specific interest should be examined. User data files that could not be accessed by other means are examined at this time using the native application.
Properly document comments and findings.

Floppy Disk Examination
The following are the IACIS® recommended procedures for conducting a complete examination of a Floppy Diskette (FD) or similar media:
Forensically sterile conditions are established. All media utilized during the examination process is freshly prepared, completely wiped of non-essential data, scanned for viruses and verified before use.
All forensic software utilized is licensed to, or authorized for use by, the examiner and/or agency/company.
The media is physically examined. A specific description of the media is made and noted.
The media is marked for identification.
Hardware/software precautions are taken during any copying process or access to the original media and examination to prevent the transference of viruses, destructive programs, or other inadvertent writes to/from the original FD or to/from the examination equipment.
The write-protect capability of the floppy disk drive (FDD) on the examining machine is tested.
A duplicate image of the original write protected FD is made to another FD. The duplicate image is used for the actual examination. A detailed description of the process is noted.
The copy of the examined FD is logically examined and a description of what was found is indicated. Anything unusual is noted.
The boot record data, and user defined system configuration and operation command files (if present) are examined and findings are noted.
All recoverable deleted files are restored. When practical or possible, the first character of restored files are changed from a HEX E5 to “-”, or other unique character, for identification purposes.
The unallocated space is examined for lost or hidden data.
The “slack” area of each file is examined for lost or hidden data.
The contents of each user data file in the root directory and each sub-directory (if present) are examined.
Password protected files are unlocked and examined.

If the FD holds apparent evidentiary data that is to be utilized, a listing of all the files contained on the FD, whether they contain apparent evidentiary data or not, is made. The listing will indicate which files were printed, copied or otherwise recovered.
A printout or copy is made of all apparent evidentiary data. The file or location where any apparent evidentiary data was obtained is noted on each printout. All exhibits are marked, sequentially numbered and properly secured and transmitted.
Executable programs of specific interest should be examined. User data files that could not be accessed by other means are examined at this time using the native applications.
Properly document comments and findings.

Limited Examinations

In many instances a complete examination of all of the data on media may not be authorized, possible, necessary or conducted for various reasons. In these instances, the examiner should document the reason for not conducting a complete examination. Some examples of limited examinations would be:
The scope of examination is *limited* by the search warrant or the courts.
The equipment *must* be examined on premises. (This may require the examination of the original media. Extreme caution must be used during this type of examination.)
The *media size* is so vast that a complete examination is not possible.
The *weight of the evidence* already found is so overwhelming that a further search is not necessary.
It is just *not possible* to conduct a complete examination because of hardware, operating systems or other conditions beyond the examiner's control.

Evidence Do's and Don’ts

Steps to take and things to consider if you think a computer may have been misused or involved directly or indirectly in a crime.

Don't Panic

If possible sit back and make a plan of action, it is rare that steps need to be taken immediately. A thorough and properly implemented plan will serve you well in the long term.

Don't do anything to arouse suspicion and don't tell anyone who does not need to know

Don't confront the suspect or do anything to arouse his or her suspicion. Consider carefully who needs to be told, crime is most often perpetrated by trusted individuals in positions of authority.

Identify the evidence

Establish what media is likely to contain data, think about:

- The suspects desktop or laptop computer
- The secretaries or colleagues computers
- Electronic organisers or Personal Digital Assistant (PDA)
- The company server especially the e-mail server
- Backup tapes (local and server)
- Telephone call logs and voice mail
- Fax logs
- Floppy disks, CD's, removable hard disks, Compact Flash cards, Memory Sticks, USB storage etc...
- Home computers
- Consider third party computers, do you need a court order to preserve evidence on a computer located elsewhere.

Secure and protect the integrity of the evidence

It is imperative that a forensic copy of the computers and associated media is secured at the earliest opportunity. If the investigation is to be overt and arousing suspicion is not an obstacle then consider the following:

- If the computer is switched off: leave it switched off - simply powering a computer on can cause irreparable damage to data and deleted data
- If the computer is a PDA then connect it to the mains - some computers of this type will lose data if the batteries are allowed to discharge
- If the computer is currently switched on, then give thought to leaving it on - depending on the type of case evidence may be in unsaved documents or in memory
- Disconnect the computer from the network and any phone lines - modern computers, if suitably configured, can be powered up by telephone or across a network
- Does the employee or his/her colleagues have remote access to the system - many a time an employee has been suspended only to find that they have accessed their computer or a server remotely after the event
- If it is considered 'safe' to involve the IT manager think about changing passwords

If possible secure the evidence under lock and key until it can be dealt with properly, 'chain of evidence' is an important concept, a court will want to know 'who did' and 'who could' have had access to the evidence

Don't be tempted to investigate yourself

Many well meaning IT departments have fallen into this trap and have contaminated or destroyed evidence. Unless you know exactly what is required, have the correct tools to do the job and understand the legal requirements of computer based evidence then don't be tempted. Failure to secure evidence in line with current accepted standards could rule the evidence inadmissible in court.

Always suspect the worst

Digital Evidence:
Standards and Principles
Proposed Standards for the Exchange of Digital Evidence

The Scientific Working Group on Digital Evidence (SWGDE) was established in February 1998 through a collaborative effort of the Federal Crime Laboratory Directors. SWGDE, as the U.S.-based component of standardization efforts conducted by the International Organization on Computer Evidence (IOCE), was charged with the development of cross-disciplinary guidelines and standards for the recovery, preservation, and examination of digital evidence, including audio, imaging, and electronic devices.

The following document was drafted by SWGDE and presented at the International Hi-Tech Crime and Forensics Conference (IHCFC) held in London, United Kingdom, October 4-7, 1999. It proposes the establishment of standards for the exchange of digital evidence between sovereign nations and is intended to elicit constructive discussion regarding digital evidence. This document has been adopted as the draft standard for U.S. law enforcement agencies.

Purpose

The latter part of the twentieth century was marked by the electronic transistor and the machines and ideas made possible by it. As a result, the world changed from analog to digital. Although the computer reigns supreme in the digital domain, it is not the only digital device. An entire constellation of audio, video, communications, and photographic devices are becoming so closely associated with the computer as to have converged with it.

From a law enforcement perspective, more of the information that serves as currency in the judicial process is being stored, transmitted, or processed in digital form. The connectivity resulting from a single world economy in which the companies providing goods and services are truly international has enabled criminals to act transjurisdictionally with ease. Consequently, a perpetrator may be brought to justice in one jurisdiction while the digital evidence required to successfully prosecute the case may reside only in other jurisdictions.

This situation requires that all nations have the ability to collect and preserve digital evidence for their own needs as well as for the potential needs of other sovereigns. Each jurisdiction has its own system of government and administration of justice, but in order for one country to protect itself and its citizens, it must be able to make use of evidence collected by other nations. Though it is not reasonable to expect all nations to know about and abide by the precise laws and rules of other countries, a means that will allow the exchange of evidence must be found. This document is a first attempt to define the technical aspects of these exchanges.

Organization

The format of this document was adopted in conformance with the format of the American Society of Crime Laboratory Directors/Laboratory Accreditation Board manual.

Definitions

Acquisition of Digital Evidence: Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collector of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.
Data Objects: Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.
Digital Evidence: Information of probative value stored or transmitted in digital form.
Physical Items: Items on which data objects or information may be stored and/or through which data objects are transferred.
Original Digital Evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure.
Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item.
Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Standards

Principle 1

In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.

Standards and Criteria 1.1

All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.
Discussion. The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are essential to the acceptance of results and conclusions by courts and other agencies. The development and implementation of these SOPs must be under an agency's management authority.

Standards and Criteria 1.2
Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.
Discussion. Rapid technological changes are the hallmark of digital evidence, with the types, formats, and methods for seizing and examining digital evidence changing quickly. In order to ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, management must review and update SOP documents annually.

Standards and Criteria 1.3
Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.
Discussion. Because a variety of scientific procedures may validly be applied to a given problem, standards and criteria for assessing procedures need to remain flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other agencies may be useful.
Standards and Criteria 1.4
The agency must maintain written copies of appropriate technical procedures.
Discussion. Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.
Standards and Criteria 1.5
The agency must use hardware and software that is appropriate and effective for the seizure or examination procedure.
Discussion. Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem. Hardware used in the seizure and/or examination of digital evidence should be in good operating condition and be tested to ensure that it operates correctly. Software must be tested to ensure that it produces reliable results for use in seizure and/or examination purposes.

Standards and Criteria 1.6
All activity relating to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.
Discussion. In general, documentation to support conclusions must be such that, in the absence of the originator, another competent person could evaluate what was done, interpret the data, and arrive at the same conclusions as the originator.
The requirement for evidence reliability necessitates a chain of custody for all items of evidence. Chain-of-custody documentation must be maintained for all digital evidence.

Case notes and records of observations must be of a permanent nature. Handwritten notes and observations must be in ink, not pencil, although pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems.

Standards and Criteria 1.7

Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.

Discussion. As outlined in the preceding standards and criteria, evidence has value only if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes.

International Principles for Computer Evidence

Introduction

The International Organization on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning computer crime investigation and other computer-related forensic issues. Comprised of accredited government agencies involved in computer forensic investigations, IOCE identifies and discusses issues of interest to its constituents, facilitates the international dissemination of information, and develops recommendations for consideration by its member agencies. In addition to formulating computer evidence standards, IOCE develops communications services between member agencies and holds conferences geared toward the establishment of working relationships.

In response to the G-8 Communique and Action plans of 1997, IOCE was tasked with the development of international standards for the exchange and recovery of electronic evidence. Working groups in Canada, Europe, the United Kingdom, and the United States have been formed to address this standardization of computer evidence.

During the International Hi-Tech Crime and Forensics Conference (IHCFC) of October 1999, the IOCE held meetings and a workshop which reviewed the United Kingdom Good Practice Guide and the SWGDE Draft Standards. The working group proposed the following principles, which were voted upon by the IOCE delegates present with unanimous approval.

IOCE International Principles

The international principles developed by IOCE for the standardized recovery of computer-based evidence are governed by the following attributes:

- Consistency with all legal systems;

- Allowance for the use of a common language;
- Durability;
- Ability to cross international boundaries;
- Ability to instill confidence in the integrity of evidence;
- Applicability to all forensic evidence; and
- Applicability at every level, including that of individual, agency, and country.

These principles were presented and approved at the International Hi-Tech Crime and Forensics Conference in October 1999. They are as follow:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Other items recommended by IOCE for further debate and/or facilitation included:

- *Forensic competency* and the need to generate agreement on international accreditation and the validation of tools, techniques, and training;
- Issues relating to practices and procedures for the examination of digital evidence; and
- The sharing of information relating to hi-tech crime and forensic computing, such as events, tools, and techniques.

An Explanation of Computer Forensics

By: Dr. P. Dennis Newsom, C.I.S.

Computer Forensics Overview Computer forensics is merely the application of computer examination and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crimes or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud, child pornography, disputes of ownership, prevention of destruction of evidence, etc. Computer specialists can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information. Any or all of this information may help during discovery, depositions, settlements, or actual litigation. **The Payoff for Using a Professional Process** The impartial computer expert who helps during discovery will typically have experience on a wide range of computer hardware and software. This is always beneficial when your case involves hardware and software with which this expert is directly familiar. But fundamental computer design and software implementation is often quite similar from one system to another, and experience in one application or operating system area is often easily transferable to a new system. Unlike paper evidence, computer evidence can often exist in many forms (temporary, volatile, semi-permanent, & permanent), with earlier versions still accessible on a computer disk. Knowing the likelihood of their existence, even different formats of the same data can be discovered. The detection process can be served well by a well-informed, educated expert identifying more possibilities that can be requested as possibly relevant evidence. In addition, during on-site premises inspections, for cases where computer disks are not actually seized or forensically copied (see below), the forensics expert can more 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 (e.g. documents, spreadsheets) 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, timeline, scheduling, project file or graphic). Safeguarding and protection of evidence is critical. A knowledgeable computer forensics professional will ensure that a subject computer system is carefully handled to ensure that: **no possible** evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer. **no possible** computer virus is introduced to a subject computer during the analysis process. **extracted** and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage. **a continuing chain** of custody is established and maintained. **business operations** are affected for a limited amount of time, if at all. **any client-attorney information** that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged. **The Process Normally Associated With the Forensic Expert** The computer forensics professional will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system: **Protects** the subject computer system during the forensic examination from any possible modification, damage, data corruption, or virus introduction. **Discovers** all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files. **Recovers** all (or as much as possible) of discovered deleted files. **Reveals** (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. **Accesses** (if possible and if legally appropriate) the contents of protected or encrypted files. **Analyzes** all possibly

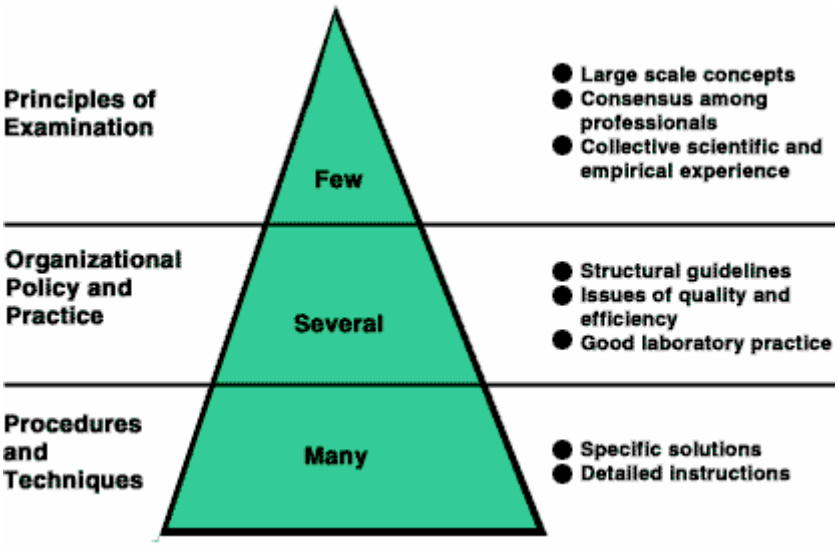
relevant data found in special (and typically inaccessible) areas of a disk. This includes but is not limited to what is called 'unallocated' space on a disk (currently unused, but possibly the storehouse of previous data that is significant evidence), as well as 'slack' space in a file (the leftover area at the end of a file, in the last assigned disk cluster, that is unused by current file data, but once again may be a possible site for previously created and relevant evidence). **Prints** out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data. Further, provides 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. **Provides** expert consultation and/or testimony, as required. Forensic Examination Procedures These procedures are established as the Forensic Examination standards to ensure that competent, professional forensic examinations are conducted. It is acknowledged that almost all forensic examinations of computer media are different and that each cannot be conducted in the exact same manner for numerous reasons, however there are three essential requirements of a competent forensic examination. These are: Forensically sterile examination media must be used. The examination must maintain the integrity of the original media, in as much as is possible. Printouts, copies of data and exhibits resulting from the examination must be properly marked, controlled and transmitted. **Add to these Ethics** Maintain the highest level of objectivity in all forensic examinations and accurately present the facts involved. Thoroughly examine and analyze the evidence in a case. Conduct examinations based upon established, validated principles. Render opinions having a basis that is demonstratively reasonable. Not withhold any findings, whether culpatory or exculpatory, that would cause the facts of a case to be misrepresented or distorted. **Hard Disk Examination** The following are the recommended procedures for conducting a complete examination of computer Hard Disk Drive (HDD) media: Forensically sterile conditions are established. All media utilized during the examination process is freshly prepared, completely wiped of non-essential data, scanned for viruses and verified before use. All forensic software utilized is licensed to, or authorized for use by, the examiner and/or agency/company. The original computer is physically examined. A specific description of the hardware is made and noted. Comments are made indicating anything unusual found during the physical examination of the computer. Hardware/software or other precautions are taken during any copying or access to the original media to prevent the transference of viruses, destructive programs, or other inadvertent writes to/from the original media. We recognize that because of hardware and operating system limitations and other circumstances, this may not always be possible. The contents of the CMOS, as well as the internal clock are checked and the correctness of the date and time is noted. The time and date of the internal clock is frequently very important in establishing file creation or modification dates and times. The original media is not normally used for the examination. A bitstream copy or other image of the original media is made. The bitstream copy or other image is used for the actual examination. A detailed description of the bitstream copy or image process and identification of the hardware, software and media is noted. The copy or image of the original HDD is logically examined and a description of what was found is noted. The boot record data, and user defined system configuration and operation command files, such as, the CONFIG.SYS file and the

AUTOEXEC.BAT file are examined and findings are noted. All recoverable deleted files are restored. When practical or possible, the first character of restored files are changed from a HEX E5 to "-", or other unique character, for identification purposes. A listing of all the files contained on the examined media, whether they contain potential evidence of not, is normally made. If appropriate, the unallocated space is examined for lost or hidden data. If appropriate, the "slack" area of each file is examined for lost or hidden data. The contents of each user data file in the root directory and each sub-directory (if present) are examined. Password protected files are unlocked and examined. A printout or copy is made of all apparent evidentiary data. The file or location where any apparent evidentiary data was obtained is noted on each printout. All exhibits are marked, sequentially numbered and properly secured and transmitted. Executable programs of specific interest should be examined. User data files that could not be accessed by other means are examined at this time using the native application. Properly document comments and findings. **Limited Examinations** In many instances a complete examination of all of the data on media may not be authorized, possible, necessary or conducted for various reasons. In these instances, the examiner should document the reason for not conducting a complete examination. Some examples of limited examinations would be: The search warrant or the courts limit the scope of examination. The equipment must be examined on premises. (This may require the examination of the original media. Extreme caution must be used during this type of examination.) The media size is so vast that a complete examination is not possible. The weight of the evidence already found is so overwhelming that a further search is not necessary. It is just not possible to conduct a complete examination because of hardware, operating systems or other conditions beyond the examiner's control. **The Use of Computer Forensic Evidence** Criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists: **Criminal Prosecutors** use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record keeping, and child pornography. **Civil litigations** can readily make use of personal and business records found on computer systems revolving from litigation 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 workman's compensation cases. **Corporations** often 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 i n pre-search warrant preparations and post-seizure handling of the computer equipment. **Individuals** sometimes hire computer forensics specialists in support of possible claims of: wrongful termination, sexual harassment, or age discrimination.

Recovering and Examining Computer Forensic Evidence

Figure 1

A Three-Level Hierarchical Model for Developing Guidelines for Computer Forensic Evidence


Principles of Examination
Few
Large scale concepts
Consensus among professionals
Collective scientific and empirical experience
Organizational Policy and Practice
Several
Structural guidelines
Issues of quality and efficiency
Good laboratory practice
Procedures and Techniques
Many
Specific solutions
Detailed instructions

Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972)

Anti-Monoply, Inc. v. Hasbro, Inc., 94 Civ.2120, 1995 U.S. Dist. LEXIS 16355 (S.D.N.Y. 1995)

Armstrong v. Executive Office of the President, 821 F. Supp. 761, 773 (D.D.C. 1993)

Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993)

Ball v. State of New York, 101 Misc. 2d 554, 421 N.Y.S. 2d 328 (Ct.Cl. 1979)

Bills v. Kennecott, 108 F.R.D. 459, 462 (D. Utah 1985)

City of Cleveland v. Cleveland Electric Illuminating Co., 538 F. Supp. 1257 (N.D. Ohio 1980)

Daewoo Electronics Co. v. United States, 650 F.Supp. 1003, 1006 (Ct.Int'l Trade 1986)

Easley, McCaleb & Associates, Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994)

First Technology Safety Systems, inc. v. Depinet, 11 F. 3d 641 (6th Cir. 1993)

Gates Rubber Co. v. Bando Chemical Industries, Ltd, 167 F.R.D. 90, 112 (D. Colo. 1996)

Pearl Brewing Co. v. Joseph Schlitz Brewing Co., 415 F. Supp. 1122 (S.D. Tex. 1976)

PHE, Inc. v. Department of Justice, 139 F.R.D. 249, 257 (D. D.C. 1991)

Pink v. Oregon State Board of Higher Education, 816 F.2d 458 (C.A. 9, 1987)

Playboy Enterprises, inc. v. Terry Welles, 60 F. Supp 2 1050; 1999 U.S. Dist. LEXIS 12895 (S.D. Cal. 1999)

Quotron v. Automatic Data Processing Inc., 141 F.R.D.

R.J. Reynolds, et al v. Minnesota, et al, U.S. Court Docket number 95-1611, cert. Denied May 28, 1996

Santiago v. Miles, 121 F.R.D. 636, 640 (W.D.N.Y. 1998)

Seattle Audubon Society v. Lyons, 871 F. Supp. 1291 (W.D. Wash. 1994)

Simon Property Group v. mySimon, Inc., 2000 WL 963035 (S.D. Ind)

Williams v. E.I. du Pont de Nemours and Co., 119 F.R.D. 648 (W.D. Ky. 1987)

Fennell v. First Step Design, Ltd, 83 F.3d 526 (1st Cir. 1996)

Hoffman v. United Telecommunications, Inc., 117 F.R.D. 436 (D. Kan 1987)

IBM Peripherals EDP Devices Antitrust Litigation, MDL #163-RM (ND Cal Feb. 10, 1975)

International Business Machines v. Comdisco, Inc., 91-C-67-194, 1992 Del. Super LEXIS 67 Mar 11, 1992

Lawyers Title Ins. Co. v. U.S.F. & G., 122 F.R.D. 567 (N.D.Cal. 1988)

Leeson v. State Farm Mutual Automobile Insurance Company, 190 Ill. App. 3rd 359, 546 NW2d 782, (1989, 1st Division)

Munoz-Santana v. U.S. Immigration and Naturalizaton Service, 742 F.2d 561 (C.A. 9, 1984)

Strausser v. Yalamachi, 669 So.2d 1142, 1144-45 (Fla. App. 1996)

U.S. v. Kupka, 57 F.3d 1078 (C.A. 9, California 1995)

ABC Home Health Services, Inc. v. International Business Machines Corp., 158 F.R.D. 180 (S.D. Ga. 1994)

American Banker Insurance Co. v. Caruth, 786 S.W. 2d 427 Texas Ct. App. 1990 & 430

Computer Associates International v. American Fundware, Inc., 133 F.R.D. (D. Colo. 1990)

Crown Life Insurance Company v. Kerry P. Craig, US Court of Appeals, 7th Circuit #92-3180

Lauren Corp v. Century Geophysical Corp., 1998 Colo. App. LEXIS 12 (No. 96CA0554, Jan. 22, 1998)

Linnen v. A.H. Robins Co. Inc., 10 Mass. L. Rptr. 189 (1999)

National Association of Radiation Survivors v. Turnage, 115 F.R.D. 543 (N.D. Cal. 1987)

Prudential Ins. Co. of America Sales Practices Litigation, 169 F.R.D. 598 (1997)

Shaw v. Hughes Aircraft, Orange County Superior Court (1996)

Wm. T. Thompson Co. v. General Nutrition Corp., 593 F.Supp. 1443 (1984)

Adams v. Dan River Mill, Inc. 54 F.R.D. 220 (W.D. Va. 1972)

Greyhound Computer Corp., Inc v. IBM 3 Computer L. Serv. Rep. 138, 139 (D. Minn. 1971)

In re Air Crash Disaster, 130 F.R.D. 634 (E.D. Mich. 1989)

State of New York and UDC-Love Canal Inc. v. Hooker Chemicals and Plastics Corp, Order, CIV-79-990 (W.D.N.Y. Nov. 30, 1989)

Minnesota v. Philip Morris Inc., No. CI-94-8565 (Dist. Ct. Minn.)

National Union Electric Corp. v. Matsushita Electric Industrial Co., 494 F. Supp. 1257 (E.D. 1980)

Williams v. Owens-Illinois, Inc., 665 F.2d 918 (C.A. 9, 1982)

Blakey v. Continental Airlines (2000) 751 A.2d 538 (NJ Sup. Ct.)

Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993)

Smyth v. Pillsbury Co., 1996 WL 32892 (E.D.Pa. 1/23/96 Weiner J.)

7 ALR 4th 8, Admissibility of Computerized Records
8 Federal Procedural forms Section 23:277
12 Federal Procedural Forms Section 45:122
16 AM JUR Proof of Facts Section 273
32B AM JUR 2nd Federal Rules of Evidence Section 235

Acierno v. New Castle County, 1997 U.S. Dist. LEXIS 11437, Robinson, J. (D. Del. May 28, 1997)

Burleson v. Texas, 802 S.W.2d 329 (Tx. App. 2d Dist. 1991)

Casey v. Zeneca Inc., 1995 U.S. Dist. LEXIS 5656, Schwartz, J. (D. Del. Mar 31, 1995)

Hahnemann University Hospital v. Dudnick, 292 N.J. Super. 11 (App. Div. 1996)

Harley v. McCoach, 928 F.Supp. 533 (E.D. Pa. 1996)

Knox v. State of Indiana, 93 F. 3d 1327 (7th Cir. 1996)

Mesquite v. Moore, (1990 Texas App. Dallas) 800 SW2nd 617

The Monotype Corporation, PLC v. International Typeface Corp., 41 F.R. Evid Serv. 86 (9th Cir. 1994)

National Union Electric Corp. v. Matsushita Electric industries Co., 494 F. Supp. 1257

N.C. Electric Membership Corp. v. CP&L Co. 110 F.R.D. 511, 517 (M.D.N.C. 1986)

Parsons v. Jefferson Pilot Corp., 141 F.R.D. 408 (M.D.N.C. 1992)

People v. Holuwko, 109 Ill.2d 187, 486 N.E.2d 877 (1985)

Quality Auto Serv. V. Fiesta Lincoln-Mercury Dodge, Inc., No. 04-96-00967-CV, 1997 WL 563176 (Tex. App. Sept. 10, 1997)

Somerset Pharmaceuticals, Inc. v. Shalala, 1997 U.S. Dist. LEXIS 11461, Robinson, J. (D. Del. June 13, 1997)

Stender v. Lucky Stores, Inc., 803 F. Supp. 259 (D.C. N.D., California 1992)

Wesley College v. Pitts, 874 F. Supp. 375 (D. Del. 1997)

U.S. v. Catabran, 836 F.2d 453 (9th Cir. 1988)

U.S. v. Kim, 595 F.2d 755 (D.C. Cir. 1979)