Computer Forensics

Part 1: An Introduction to Computer Forensics

Information Security and Forensics Society (ISFS)
http://www.isfs.org.hk

April 2004

Overview

This document is designed to give non-technical readers an overview of computer forensics. It is not intended to offer legal advice of any kind. Specifically the following questions are addressed:

1. What is Computer Forensics?
2. Why do individuals and organizations need to pay attention to Computer Forensics?
3. What is digital data?
4. Why is knowledge of Computer Forensics so important?
5. What does a Computer Forensics specialist do?
6. What should a company do if an incident occurs?

1. What is Computer Forensics?

Computer Forensics is the science of obtaining, preserving, and documenting **evidence** from **digital** electronic storage devices, such as computers, PDAs, digital cameras, mobile phones, and various memory storage devices. All must be done in a manner designed to preserve the probative value of the evidence and to assure its admissibility in a legal proceeding[1].

You can think of it as the science of forensics applied in a digital environment. But where a traditional forensics specialist might collect and preserve fingerprints or other physical evidence, the computer forensics specialist collects and preserves *digital evidence*.

This collection of digital evidence must be done through carefully prescribed and recognized procedures so that the probative value of digital evidence is preserved to ensure its admissibility in a legal proceeding.

As traditional forensics may involve people with different specialties, computer forensics similarly involves a multitude of professional specialties working together to gather, preserve and analyze digital evidence.

1.1 Computer Forensics vs. Computer Security

Though Computer Forensics is often associated with Computer Security, the two are different.

- *Computer Forensics* is primarily concerned with the proper acquisition, preservation and analysis of digital evidence, typically after an unauthorized access or use has taken place.

- With *Computer Security* the main focus concerns the prevention of unauthorized access, as well as the maintenance of confidentiality, integrity and availability of computer systems.

Nevertheless, Computer Security and Computer Forensics are complimentary in that greater familiarity with Computer Forensics may lead to greater awareness of the importance of both computer security, in general, and proper procedural controls governing the access and use of computers, networks and other devices.

Furthermore, in the event of a breach of security, a great deal may be learned during the process of collecting digital data. This knowledge can be applied to improve system procedural controls, operations and staff capabilities.

[1] Steven M. Abrams and Philip C. Weis, "*Knowledge Of Computer Forensics Is Becoming Essential For Attorneys In The Information Age*", New York State Bar Journal February, 2003.

2. Why do individuals and organizations need to pay attention to computer forensics?

Nowadays, more and more people are using computers and devices with computing capability. For example, one can send and receive e-mail messages from handheld devices (such as mobile phones, or PDAs), participate in online computer games simultaneously with other game players over digital networks, or manage their finances over the Internet.

Today, many business and personal transactions are conducted electronically:

- Business professionals regularly negotiate deals by e-mail;
- People store their personal address books and calendars on desktop computers or PDAs.
- People regularly use the Internet for business and pleasure

According to a University of California study, 93% of all information generated during 1999 was generated in digital form, on computers; only 7% of information originated in other media, such as paper[2]. Moreover, a significant percentage of computer-created documents might never be printed on paper. Many messages and documents are exchanged over the Internet and are read on the computer screen but are not printed out.

2.1 Preservation of Evidence

As computers, computing devices (or other devices with computing capability such as mobile phones or PDAs) and networks become more widely used in general, the chance that crimes involving such networks and devices occur will increase.

It goes without saying that in order to prosecute such crimes, evidence must first be gathered both:

- in sufficient quantity to substantiate any criminal or civil charges, and
- handled properly so that the evidence will hold up in court.

But as much of this evidence will be in digital form the ability to extract the relevant digital evidence *in a manner that preserves the value and integrity of the data* is critical. This is the reason we need a careful, methodical process for gathering digital data in the first place; and this is why we need computer forensics.

2.2 Why do we need computer forensics?

Consider a hypothetical scenario where a criminal has broken into an organization's premises and stolen critical assets (money, data or reports). A responsible executive would have no hesitation in calling in profession forensics examiners and extending them all necessary cooperation.

Such cooperation might involve cordoning off the crime scene to ensure that:

- The area is not disturbed,
- Evidence is not accidentally contaminated or tampered with,
- Forensics professionals have access to the necessary information or locations.

[2] Mary Kay Brown and Paul D. Weiner, "*Digital Dangers: A Primer On Electronic Evidence In The Wake Of Enron*", Pennsylvania Bar Association Quarterly January, 2003.

The executive would do this because it is in the best interest of his or her organization because relevant evidence must be collected, the more the better, if the criminal is to be caught, assets are to be recovered or if court action is to be successful. Without this evidence, any chances of asset recovery or successful court prosecution will vanish.

Furthermore, this evidence must be collected and preserved in a proven, systematic manner to ensure admissibility in court.

Now, let's suppose the criminal had committed the theft electronically -- for example he hacked into an organization's computers to steal valuable data such as strategic business plans, secret formulae, customer data, account number or employee records. Or perhaps, the criminal is an insider committing a white-collar crime or fraud using the organization's computers.

A responsible executive similarly would know that it was in his or her best interest to call in the appropriate *Computer Forensics* specialists and extend them as much cooperative assistance as possible because if there is to be any chance of recovering property, locating and successfully prosecuting the criminal, there must be evidence of sufficient quantity and quality.

As with a physical crime scene, digital evidence must also be carefully and systematically collected and preserved to ensure admissibility in court. The locations where digital evidence might be found – for example, computer hard drives or digital media – should not be disturbed to minimize the chance of losing valuable evidence. Computer Forensics professionals should be extended the requisite cooperation and have access to the necessary information or locations.

But handling digital evidence differs in many ways from handling physical evidence and an investigator must know:

- Where to look for digital evidence
- The proper way to acquire this evidence
- How to handle and preserve this evidence in such a manner that preserves its probative value

To appreciate why digital evidence requires specialized management, we must first understand the nature of digital data.

3. What is Digital Data and where can it be found?

Understanding the nature of digital data involves knowing what types of digital data exist and where these data can be found.

3.1 Types of Data

A modern computer typically stores vast amounts of data. Some of these data are active others may be residual or back up data.

3.1.1 Active Data

Active data consists of user created data such as customer information, inventory data, word processing documents or spreadsheets, program and operating system files, including temporary files.

3.1.1.1 Metadata and other data

3.1.1.1.1 Metadata

Many users are aware of the important data kept within data files. However, many users may not be aware of the other information about the files – including the time of creation and the person creating it – that may also be useful in an investigation. This data is referred to as *metadata*.

For example, were one to open a Microsoft Word© document and check properties (by clicking on File then Properties in the top menu) one would find a wealth of information including the dates and times document was created, last modified and printed, the number of revisions, file size and editing time.

This metadata, which is stored within the document itself, can contain the history of the document, including all users who have modified and/or saved it, the directory structure of all machines it was saved on and names of printers it was printed on.

3.1.1.1.2 Operating System data

Data from the computer's operating system can be a rich source of details about what a user has been doing. From this data, a forensics specialist may retrieve information such as Web sites a user has visited; e-mail messages sent and received, etc.

While accessing the Internet, browsers keep records of the sites a user has visited. If a user permits cookies, which are small files used by browsers to keep track of, among other things, a user's visits, cookies may be a valuable source of information about the user's Internet practices storing all sorts of data including passwords. These records can be retrieved by forensics investigations if clear evidence of sites the user has visited is required.

3.1.1.2 Temporary Files

When a user runs a program, for example a word processor, data may be temporarily stored on the hard drive. For instance, Microsoft Word© saves changes to a document at set intervals in a separate, temporary recovery file when the AutoRecover feature is turned on. These temporary files may allow a Computer Forensics specialist access to documents not saved by a user.

This is something the 'Gap-Toothed Bandit' discovered in 1999. This thief, who had involved in 12 bank robberies in the San Diego area, wrote threatening notes on his computer. Even though he exited

his word processor without saving these notes, a forensic investigation of his computer yielded five of his demand notes[3].

3.1.1.3 Communications Data

Whenever a person uses a computer, mobile phone or other device to communicate, a digital trail is created that can yield information regarding whom the user communicated with, what was discussed, when it occurred, who was privy to it, what documents were transmitted, and even attempts to erase the record of that communication. All these would be electronically stored – and potentially discoverable.

Some of this data resides in a user's computer but other relevant data may reside in devices that form part of the network or are attached to the network such as routers or intrusion detection systems. Companies providing communications services, for example, Internet Service Providers (ISPs) maintain communications logs that are useful in investigative searches.

3.1.1.3.1 Tracking and Tracing through the Internet

Tracing and tracking e-mails and other communications through the Internet is possible because the communications protocol upon which Internet communications is based, TCP/IP, assigns a four-byte identifier to every device connected to the Net. This identifier is referred to as an *IP address*. An IP Address is often represented as four decimal numbers separated by dots, such as 143.89.56.78.

Each ISP is assigned a range of IP addresses that it, in turn, assigns ("leases") to its subscribers. Some subscribers have static IP addresses that never change while others are assigned different IP addresses each time they connect to the Internet (i.e. 'Dynamic IP Addresses'). ISPs maintain log files that show who was assigned any given IP address at a given date and time.

The IP address of a sender is usually found in the header information that is sent with each e-mail message. Therefore, using relatively simple network tools, it is possible to get the name and contact information for the ISP, who is assigned the IP address.

3.1.2 Residual Data

Most users assume that deleting files from a computer actually removes the files but in fact a computer's operating system keeps a directory of the name and location of each file.

When a user deletes a file, the operating system does not remove the file data. Rather the operating system only indicates that the space is available. The content of a deleted file remains in place until specialized programs overwrite them. A person who knows how to access these released-but-not-erased areas, and who has the proper tools, can recover their contents.

Residual data can also include portions of files distributed on the drive surface or embedded within other files. These files are commonly referred to as *file fragments* and *unallocated data.*

3.1.2.1 Slack Space

Data can also be found in what is known as the *slack area* of a hard drive. *Slack space* is an area at the end of the space allocated to a file not occupied by the data belonging to that file. For instance a file 4Kilobytes (KB) in length may be allocated 32KB of disk space. The space of 28KB between the end of the file and the allocated space is the slack space.

[3] Johnette Hassell and Susan Steen, "Demystifying Computer Forensics", Louisiana Bar Journal, December 2002 / January, 2003

3.1.3 Backup Data

Much business data and communications are preserved on back-up tapes on a routine basis. Individual users can also create their own backups – for instance, Microsoft Word© allows users to automatically save a backup copy of a document if the backup feature is turned on.

Backup data typically consists of information copied to portable media (usually tapes, diskettes or CDs) to provide users with access to their data in the event of a system failure. The frequency of these backups and the data backed up generally are set by organizational policy though networked systems are normally backed up on a routine schedule. Typically network backups capture only the data that are saved to the centralized storage systems but not data stored on individual users' hard drives.

3.2 Sources of Data

One obvious source of data is a user's computer; yet potential sources of digital data within a computer are not always obvious.

While digital data obviously exists on a computer's hard drive, digital data may also be located on media devices attached or inserted to a computer such as a CD Rom, floppy diskettes, backup tapes and memory cards as well as within the cache memories of the computer.

Data may also be located on shared drives, also referred to as network drives or file servers. These shared drives act as centralized data repositories for user data that can be thought of as an electronic file room, with files indexed to facilitate access by individuals and groups. In many business environments, users save their work data, including word processing documents, e-mail messages, accounting and spreadsheet files to shared drives.

Data may also be found in other locations:

- Smart cards may contain valuable information that may be of use to a computer criminal.
- PDAs may be used to store password or other useful data.
- Mobile phone handsets reveal the callers' identities
- Whenever a person enters a building the building security system creates an electronic record

Even printouts from a computer, phone lists, access logs or procedural documentation may prove valuable in an investigation.

4. Why is knowledge of Computer Forensics so important?

As we have seen, computers and networks are becoming more widely used therefore the opportunity for criminals to employ these same facilities to commit crimes is growing.

4.1 Preservation of Evidence

The ability to retrieve and preserve data plays a pivotal role in the prosecution of a case and it is important that anyone gathering data know:

a. Where to find
b. How to properly handle
c. Gather and
d. Preserve such evidence

In order to ensure that digital evidence is admissible in a court of law, it must generally be proved that the evidence is both authentic and has not been modified[4].

There are several reasons why a *specially trained*, *qualified* Computer Forensics specialist should be called in to investigate a potential cyber crime:

- to handle issues specific to digital data
- to maintain the chain of custody
- to avoid the dangers of mishandling digital data.

4.2 General challenges posed by digital evidence

As electronic data differ from traditional paper documents, they need to be handled accordingly.

4.2.1 Electronic v Paper documents

Electronic documents are created at much greater rates than paper documents. Today nearly 6.8 trillion e-mail messages are generated in the United States each year in addition to other electronic files that are generated, such as word processing documents, spreadsheets, databases, graphic files and voice mail files[5].

These data files can be stored in a multitude of locations and though search terms can be formulated to overcome the random data storage problem, in many instances search terms are an imprecise and flawed solution at best. When broad and all-encompassing search terms are used, the resultant number of documents captured is often quite large[6].

In addition, electronic documents are more easily replicated and changed than paper documents. While paper documents can be copied, copying physical documents results in degradation with each copy. However, electronic information can be subject to rapid and large scale user-created and automated replication without degradation of the data.

---

[4] Casey Eoghan, "*Digital Evidence And Comptuer Crime*" Academic Press, p. 47.

[5] Johnson Larry, "*Gathering Electronic Evidence During Discovery*", Larry Johnson Legal Tech, Nov 2000, Vol. 18; No. 8; p.1.

[6] Jones, Loren D. "*Software Licensing in the New Age*," New Jersey Law Journal, Aug. 5, 2002, also cited in Legal Tech, Sept 2002, Vol. 20; No. 6; Pg. 10.

Unlike "paper file" discovery, electronic "documents" cannot be easily or inexpensively identified for production because the "documents" are stored randomly on an electronic medium. As a result investigators may need to review each document, not just each file.

Finally, computer information, unlike paper, has dynamic content that is designed to change over time even without human intervention. As an example, consider web pages that are constantly being updated with information fed from other applications or e-mail systems that reorganize and remove data automatically[7].

4.2.2 Handling issues with Digital Data

Digital data poses other challenges: digital data must be properly extracted and handled due to its perishability; digital data can be erased, corrupted or modified in any number of ways including:

- Improperly keyed commands,
- Booby traps,
- Improper procedures
- Stray magnetic fields or
- Merely starting a computer changes files.

Therefore it is imperative that the Computer Forensic specialist ensures that any collected digital evidence is not altered during and after its acquisition.

4.2.3 Chain of Custody

Throughout the process, the forensics specialist must also provide assurance of a proper chain of custody to ensure that the evidence obtained retains it probative value.

The importance of maintaining a proper chain of custody cannot be overemphasized. For any legal action to even have a chance of success*, there must be complete, thorough, and convincing evidence that has been protected through a secure chain-of-custody procedure* that tracks who has been involved in handling the evidence and where it has been stored.

The Computer Forensic specialist must take special care to protect digital evidence from deliberate or inadvertent changes or erasure. Otherwise, the information collected may not be considered as valid evidence in a legal proceeding.

4.2.4 The Dangers of Mishandling Data

When a problem with a computer system occurs (for instance, a system goes down, a website is defaced or the back-end server powering an e-commerce site crashes), there is frequently a temptation to simply fix the problem. But with the growth of cyber crime, the possibility that a computer problem is the result of a deliberate act, perhaps by a disgruntled customer or employee, cannot be dismissed.

Yet the typical reaction of most companies -- to quickly diagnose and remedy a problem -- may result in the loss of valuable evidence thereby making prosecution impossible. Even if some data can be preserved, its evidentiary value may be severely compromised if this data was not handled in a forensically proper manner.

Therefore it is important that professionals charged with the responsibility of overseeing computer

---

[7] Thesedona Principles: Best Practices Recommendations & Principles For Addressing Electronic Document Production, A Project of the October 2002 Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production March 2003.

systems recognize that if a problem with a computer system or network occurs that:

a. Such an event may be the result of a deliberate act.
b. It is vital that evidence be gathered and preserved by professionals *properly trained* in computer forensics.

These same responsible parties must also be aware of the potential sources of digital evidence within their installations and organizations.

4.3 Why we need Computer Forensics and the importance of gathering and preserving evidence

While the process of digital forensics examination may admittedly be time consuming and disruptive, the potential costs of *not* conducting a *proper* digital forensics examination may be substantial if not disastrous:

a. Loss of evidence may hamper any efforts to recover lost digital assets or affect the viability of the any future legal action. Even if the criminal were caught, without proper evidence he/she could not be charged.
b. By avoiding a proper examination, an organization risks losing a valuable opportunity to identify and correct security weaknesses. As a result, not only would an organization remain vulnerable to future attacks, such failure to take positive corrective action might also damage an organization's image and reputation potentially resulting in loss of customer confidence in the organization – and loss of business.
c. Loss of valuable information such as customer files, private data or other confidential information, may potentially render an organization vulnerable to legal or other action.
d. For companies whose business models depend on protection of intellectual properties, maintaining confidentiality or whose business data is a highly sought after commodity, such losses could be catastrophic particularly if the data were not recovered in a timely manner.

As noted before, greater familiarity with Computer Forensics may lead to greater awareness of the importance of both computer security, in general, and proper procedural controls governing the access and use of computers, networks and other devices.

Finally, there is one other compelling issue to consider, *Corporate Governance.* With more corporate and organizational data being created and stored electronically, the need to gather and preserve this data, for example in the event of an investigation, is critical. Such data can be invaluable in proving collective organizational innocence or in identifying internal criminals.

Anyone doubting the potentially calamitous consequences of a failure to preserve electronic evidence should recall the scandal at Enron that resulted in the collapse of both the company and its outside auditors, Arthur Andersen. In the case of Enron, a key focus of the inquiry was whether Enron, Arthur Andersen, and its in-house lawyers took the appropriate steps to preserve relevant evidence, or permitted its intentional destruction and during the subsequent trial, e-mail became a star witness[8].

[8] Paul Wall, "*Enron, Anderson And E-Communications - A Wake-Up Call For E-Mail Users*", 2002 UCLA Journal of Law & Technology & Tech. Notes 25.

5. What does a Computer Forensics specialist do?

The job of a Computer Forensic specialist is to help determine if a computer disk, media or other device contains potential evidence and secure from any seized material, be it hard disks, floppy disks, tape or any other storage media, a true copy of the data contained therein[9]. If it does, he/she must oversee the extraction of information from the computer media to ensure that this process is conducted properly and that evidence is obtained without compromising the original data.

Once the data has been extracted and properly processed (more about this later) the Computer Forensics specialist (or members of his/her team) must evaluate the information for its evidentiary value.

All this should be done in accordance with internationally accepted best practices to ensure the probative value of the evidence obtained.

5.1 Evidence Handling Principles

According to the G8 recommendations relating to digital evidence, forensics specialists must follow certain principles.

First, the general rules of evidence should be applied to all digital evidence. It is important that forensics specialists, upon seizing digital evidence, ensure that the evidence is not changed and that only persons who are suitably trained should be allowed to access original digital evidence should the need arise.

There must be full documentation of all activities related to the seizure, access, storage or transfer of digital evidence. The documentation should be preserved and available for review[10].

Finally, there must be ownership: that is the person in charge of the investigation must have overall responsibility for ensuring that these principles (and the law) are adhered to[11].

All practices employed in the recovery of digital evidence recovery should fall within a defined and accepted framework and must comply with the above principles.

What does the recovery of digital evidence involve?

5.2 Initial Assessment

In the event that a Computer Forensics specialist must go to a site to acquire evidence, his or her first task is to attempt to determine the types of computer systems in use so that he or she can then bring the appropriate software and hardware tools to the scene.

---

[9] "*ACPO Good Practice Guide for Computer based Electronic Evidence"*, Association of Chief Police Officers of England, Wales and N. Ireland (ACPO).

[10] "*Guidelines For Best Practice In The Forensic Examination Of Digital Technology*", IOCE 2002 Digital Evidence Standards Working Group (www.ioce.org).

[11] "*ACPO Good Practice Guide for Computer based Electronic Evidence*", Association of Chief Police Officers of England, Wales and N. Ireland (ACPO).

5.2.1 Precautions

Forensic specialists attending the scene or may need to give advice to others attending the scene and recovering the evidence. Professional forensics specialists should be aware of any relevant jurisdictional guidelines and take all necessary precautions to minimize the chance of accidental contamination[12].

5.3 Evidence gathering considerations

In general, items for forensic examination should be preserved securely as soon as possible with all items taken, including image copies, examined in the laboratory or forensic work space rather than at the scene.

Wherever practicable, an image copy should be made of the entire target device though partial or selective file copying may be acceptable in certain circumstances (e.g. when the amount of data involved makes copying of an entire device impractical)[13].

All these should be performed in accordance with relevant jurisdictional guidelines. A recording of all items removed from the scene should be made, describing the exact locations where the items were taken. All evidence should be properly packaged, sealed and labeled.

5.4 Image copy

In most computer forensic examinations, the next step is to make an *exact* copy of the data residing on the evidence hard disk (or other electronic digital storage device). The need to create such a copy is consistent with the essential concern not to change the evidence.

5.4.1 The Importance of Forensically Sterile Media

This copy is made on media that is *forensically sterile*. This means that any previous data must be removed from the copy media with a software tool that is proven to remove all data from the drive. Merely reformatting a hard drive does not actually remove all files from the drive.

By using forensically sterile media, the Computer Forensics specialist ensures that the media itself will not contaminate the evidence.

5.4.2 Exactness

The image copy is important because the search will be conducted on the copy, not the original. One reason this is done is because a search conducted on the original creates both the actual and perceived problem that the original has been corrupted or altered by the person performing the analysis, therefore rendering vulnerable to a disqualifying objection in court.

As noted above, this image copy is what is actually evaluated but *this copy must be exact*. To ensure this exactness, the computer forensics specialist employs special tools to maintain the integrity of the original media during the copy process.

5.4.3 Time

Another consideration concerns time. Once the copy is made, the forensic examination is performed using any of a number of tools that can dramatically cut the amount of time required.

---

[12] "*Guidelines For Best Practice In The Forensic Examination Of Digital Technology Draft V1.0*", International Organization of Computer Evidence May 2002.

[13] "*ACPO Good Practice Guide for Computer based Electronic Evidence*", Association of Chief Police Officers of England, Wales and N. Ireland (ACPO).

5.4.3.1 Using a hash to save time

A computer forensics specialist will run files through what is called a *hash algorithm*, a one-way (meaning that the original value cannot be determined from the hashed value) mathematical formula that computes a unique value – in a sense creating a digital fingerprint uniquely identifying a particular file. The MD5 (Message Digest 5) hash and SHA-1 (Secure Hash Standard) hash are among the most common hash algorithms in use today.

This hash process serves two functions. First, it helps ensure the integrity of the file – if the file is altered its hash value will be changed. Therefore any tampering would be quickly discovered.

Second, by computing a hash code from each file on the evidence drive, and comparing the hash value against a database of hash values for all known commercial software and operating system components, the forensic specialist can readily identify which files can be safely ignored (obviously, this is done through the use of specialized tools) and thus save time.

After this has been done, the forensics specialist must then analyze the evidence and produce the appropriate reports.

In some cases, some files are not immediately available because they may be password-protected. In such cases, special tools must then be employed to crack the passwords.

5.5. Analysis

With the image copy, the forensics specialist can now commence his/her examination following Standard Operating Procedures (SOPs)[14].

In performing the analysis, the forensics specialist needs to consider, among other things:

- The urgency and priority of the need for information
- Time constraints
- Which items have the potential to provide the most information, the best choice of target data, in terms of evidential value

When evaluating and interpreting case findings, the forensics specialist must consider the background information available about the case and the original expectations formulated during case assessment[15].

5.5.1 Reporting and Review

After the examination and interpretation are complete, the forensics specialist must now present his findings in a clear, concise, structured and unambiguous report.

Ideally, all work undertaken should be subjected to both technical review, conducted by a qualified agency to assess whether the conclusions drawn are justified by the work done and the information available, and administrative review top ensure that the requester's needs have been properly addressed, editorial correctness and adherence to policies.

[14] "*ACPO Good Practice Guide for Computer based Electronic Evidence*", Association of Chief Police Officers of England, Wales and N. Ireland (ACPO).

[15] "*Guidelines For Best Practice In The Forensic Examination Of Digital Technology Draft V1.0*", International Organization of Computer Evidence May 2002.

6. Incident Response

In case an organization falls victim to a suspected cyber crime what should it do?

Generally, an organization should resist the temptation to implement a quick fix by itself. Instead, it should contact the proper Computer Forensics specialists and leave the scene (i.e. the computers, networks, etc.) *undisturbed* until the appropriate professionals arrive:

- Screen displays should not be changed
- Printouts should be left in place
- Systems and access logs should not be deleted
- Personnel should be instructed not to perform any activities on the affected devices until the Computer Forensics specialist is finished with his/her work
- Devices already running on should be left on, it should be left to the Computer Forensics specialist to determine whether to shut down any devices and when.
- Restoration from back up files *should not* be done until after the Computer Forensics specialist has finished with his/her initial investigation and has indicated that restoration work can safely begin.

To maximize the efficiency of the investigation the organization should be prepared to provide the Computer Forensics specialists any relevant information that might be required such as the types of machines and operating systems used, contact lists, process documentation, system configurations and identify all potential sources of digital data.