Duplication and Preservation of Digital Evidence

- **Computer evidence is odd, It lurks on computer hard disk drives, zip disks, and floppy diskettes at three different levels.**
- **Two of these levels are not visible to the computer user, such evidence is fragile and can easily be destroyed by something as simple as the normal operation of the computer.**
- In the old days, defense lawyers didn’t know much about computer evidence. As a result, cross-examination by the defense wasn’t as strong a few years ago as it is today.
- However, things are changing because lawyers are becoming educated because of the current popularity of electronic document discovery in the legal community.
- Times have changed and it is all the more important to do things by the book

- Nevertheless, computer forensic evidence is frequently challenged in court.
- Some judges accept it with little question because they want to crack down on computer criminals, and others reject it because they hold to a fairly technophobic view of the Fourth Amendment.
- **There’s also some confusion over the legal classification of computer evidence. Is it documentary evidence (which would require reams of printout under the best evidence rule) or is it demonstrative evidence (which would require a true-to-life sample of the reconstructed evidence.**

- **The three criminal evidence rules to gain admissibility are**
- **1. Authentication**
- **2. The best evidence rule**
- **3. Exceptions to the hearsay rule**
- **Authentication means showing a true copy of the original; best evidence means presenting the original; and the allowable exceptions are when a confession or business or official records are involved.**
- Authentication appears to be the most commonly used rule, but experts disagree over what is the most essential, or most correct, element of this in practice.
- Some say documentation (of what has been done); others say preservation (the integrity of the original); still others say authenticity (the evidence being what you say it is).
- Good arguments could be made for the centrality of each, or all, as the standard in computer forensic law

- If your documentation is poor, it will look like your processing procedures were poor, and when you testify in court, you will look ridiculous since you have no good written record to refresh your memory.
- **In general, the condition of all evidence has to be documented. It has to be photographed, weighed, and sketched.**
- **Then, the laboratory worker (forensic scientist or criminalist) figures out what tests are appropriate, decides on what part of the evidence to examine first, dissects or copies the part to be tested (specimen = dissection; exemplar = copying), and prepares the testing ground, all the while documenting each decision step.**
- Only then does any testing begin, and that’s heavily documented with bench notes that are subject to discovery and review by experts from the other side

- If your preservation is poor, it becomes fairly evident that your collection and of evidence gives rise to numerous possibilities for error in the form of
- destruction, mishandling, and contamination. Problems in the preservation area have
- implications for the integrity of law enforcement and crime labs. The basic chain of
- custody, for example, involves at least three initial sources of error. Evidence has to be
- discovered (police), it has to be collected (crime scene technician), and then it has to
- be packaged, labeled, and transported (police supervisor). Once it gets to the lab, it
- has to be logged in, assigned an identification number, placed in storage, and kept
- from intermingling with other evidence. All workplaces must be clean and contamination
- free. Some workplaces are required to meet the standards of professional accrediting
- organizations. Written policies have to be in place. The quality assurance
- policy, for example, must act as a check on quality control. Some employee job titles
- must be held by those with college degrees in the appropriate field

- Some workplaces are required to meet the standards of professional accrediting
- organizations. Written policies have to be in place. The quality assurance
- policy, for example, must act as a check on quality control. Some employee job titles
- must be held by those with college degrees in the appropriate fieldexplain, for example, how an “MD5 Hash algorithm” works. Computer evidence,
- like computer simulations, hasn’t fared all that well under the rigorous standards of
- admissibility for scientific evidence. The old common law standard is *oculis subjecta*
- *fidelibus*, as it is for any piece of demonstrative evidence (like a plaster cast model;
- if the scale is 1:10, an average person ought to be able to visualize the larger thing
- to scale). Case law, however, varies by jurisdiction. Only the Marx standard resembles
- the old common law standard, and it’s only found in a handful of jurisdictions.
- Here’s a list of all the scientific evidence standards

- **Relevancy test (FRE 401, 402, 403):** This is embodied in the Federal Rules of Evidence
- and some state versions that liberally allow anything that materially
- assists the trier of fact to be deemed relevant by the trier of law.
- **Frye standard (Frye v. U.S., 1923):** For the results of a scientific technique to be admissible,
- the technique must be sufficiently established to have gained general
- acceptance in its particular field. This is a "general acceptance" test.
- **Coppolino standard (Coppolino v. State, 1968):** The court allows a novel test or
- piece of new, sometimes controversial, science on a particular problem at hand
- if an adequate foundation can be laid, even if the profession as a whole isn't familiar
- with it.
- **Marx standard (People v. Marx, 1975):** The court is satisfied that it did not have to
- sacrifice its common sense in understanding and evaluating the scientific expertise
- put before it. This is a "common sense" or "no scientific jargon" test.
- **Daubert standard (Daubert v. Merrell Dow, 1993):** This rigorous test requires
- special pretrial hearings for scientific evidence and special procedures on discovery
- where the rules are laid out beforehand on validity, reliability, benchmarking,
- algorithms, and error rates [1]

- The federal courts were the first to recognize that files on computers were similar,
- but unlike, files kept on paper. The best evidence rule has also, in recent years,
- seen the growth of a standard known as representational accuracy, which means
- you don’t have to present all the originals. Therefore, a modern clause exists in the
- Federal Rules of Evidence (FRE 1001-3) that states, If data are stored by computer
- or similar device, any printout or other output readable by sight, shown to reflect
- the data accurately, is an original

- This exception to the best evidence rule has found a mostly welcome reception
- in state courts, and you should argue that it’s more appropriate to consider digital
- evidence as demonstrative than documentary. The history of computers in the
- courtroom ties in with demonstrative standards, and computer forensics, after all, is
- about reconstructing the crime, or criminalistics. You see how apparent this is once
- you realize that investigators and technicians always work from a copy, duplicate, mirror, replica, or exemplar of the original evidence. Digital evidence is the most
- easily lost evidence. There’s nothing in criminal justice more easily damaged, corrupted,
- or erased

- You need to be able to demonstrate that the evidence is what you
- say it is, came from where you say it did, and has not been modified in any way since
- you obtained it. How you go about that depends on the circumstances and the computer
- systems you’re dealing with. It’s futile to talk about any one correct way to do
- it, or any perfect printout. There’s no “silver bullet” standardized checklist, and
- there’s no “magic” software to produce the perfect printout [1].
- Now let’s look at some of the emerging principles of duplication and preservation
- of digital evidence collection and handling. Many regard this as the skillset of
- computer forensics.

PRESERVING THE DIGITAL CRIME SCENE

- The computer investigator not only needs to be worried about destructive process
- and devices being planted by the computer owner, he or she also needs to be concerned
- about the operating system of the computer and applications. Evidence is
- easily found in typical storage areas (spreadsheet, database, and word processing
- files). Unfortunately potential evidence can also reside in file slack, erased files, and
- the Windows swap file. Such evidence is usually in the form of data fragments and
- can be easily overwritten by something as simple as the booting of the computer or
- the running of Microsoft Windows

- When Windows starts, it potentially creates
- new files and opens existing ones as a normal process. This situation can cause
- erased files to be overwritten, and data previously stored in the Windows swap file
- can be altered or destroyed. Furthermore, all of the Windows operating systems
- (Windows 2000, XP and especially 2003) have a habit of updating directory entries
- for files as a normal operating process. As you can imagine, file dates are important
- from an evidence standpoint.
- Another concern of the computer

- the subject computer. Criminals can easily modify the operating system to destroy
- evidence when standard operating systems commands are executed. Perpetrators
- could modify the operating system such that the execution of the DIR
- command destroys simulated evidence. Standard program names and familiar
- Windows program icons can also be altered and tied to destructive processes by a
- crafty high-tech criminal.

- Even trusted word processing programs such as Microsoft Word and Word-
- PerfectTM can become the enemy of the cyber cop. It works this way: When word
- processing files are opened and viewed, the word processing program creates temporary
- files. These files overwrite the temporary files that existed previously, and
- potential evidence stored in those files can be lost forever. There's a point to all ofthis. Computer evidence processing is risky business and is fraught with potential
- problems. Of course, any loss of crucial evidence or exculpatory material falls on
- the shoulders of the computer investigator. What will your answer be if the defense
- attorney claims the data you destroyed proved the innocence of his or her client?
- You had better have a good answer

- Many inherent problems associated with computer evidence processing vanish
- when tried and proven processing procedures are followed. The objective of this
- section is to keep Murphy’s law from ruining your case. When it comes to computer
- evidence processing, Murphy is always looking over your shoulder. He stands
- ready to strike at just the wrong moment.

- Your first objective, after securing the computer, should be to make a complete
- bit stream backup of all computer data before it is reviewed or processed. This
- should normally be done before the computer is operated. Preservation of evidence
- is the primary element of all criminal investigations, and computer evidence is certainly
- no exception. These basic rules of evidence never change. Even rookies know
- that evidence must be preserved at all costs. As stated previously, evidence can reside
- at multiple levels and in bizarre storage locations

- These levels include allocated
- files, file slack, and erased files. It is not enough to do a standard backup of a hard
- disk drive. To do so would eliminate the backup of file slack and erased file space.
- Without backing up evidence in these unique areas, the evidence is susceptible to
- damage and modification by the computer investigator. Bit stream backups are
- much more thorough than standard backups. They involve copying of every bit of
- data on a storage device, and it is recommended that two such copies be made of
- the original when hard disk drives are involved. Any processing should be performed
- on one of the backup copies. As previously recommended, the original evidence
- should be preserved at all costs. After all, it is the *best eviden*

- The importance of bit stream image backups cannot be stressed enough. To
- process a computer hard disk drive for evidence without a bit stream image backup
- is like playing with fire in a gas station. The basic rule is that only on rare occasions
- should you process computer evidence without first making an image backup. The
- hard disk drive should be imaged using a specialized bit stream backup product

- hard disk drive should be imaged using a specialized bit stream backup product.
- To avoid getting too technical for the purposes of this chapter, specifics regarding
- the uses of these backup programs will be avoided. However, instruction
- manuals should be studied thoroughly before you attempt to process computer evidence.
- Ideally, you should conduct tests on your own computers beforehand and
- compare the results with the original computer evidence. Being comfortable with
- the software you use is an important part of computer evidence processing. Know
- your tools. Practice using all of your forensic software tools before you use them for
- processing of computer evidence. You may only get one chance to do it right

COMPUTER EVIDENCE PROCESSING STEPS

- Computer evidence is fragile by its very nature, and the problem is compounded by
- the potential of destructive programs and hidden data. Even the normal operation
- of the computer can destroy computer evidence that might be lurking in unallocated
- space, file slack, or in the Windows swap file. There really are no strict rules
- that must be followed regarding the processing of computer evidence. Every case is
- different, and flexibility on the part of the computer investigator is important.

- With that in mind, the following general computer evidence processing steps
- have been provided. Remember that these do not represent the only true way of processing
- computer evidence. They are general guidelines provided as food for thought:
- 1. Shut down the computer.
- 2. Document the hardware configuration of the system.
- 3. Transport the computer system to a secure location.
- 4. Make bit stream backups of hard disks and floppy disks.
- 5. Mathematically authenticate data on all storage devices.
- 6. Document the system date and time.
- 7. Make a list of key search words.
- 8. Evaluate the Windows swap file.
- 9. Evaluate file slack.
- 10. Evaluate unallocated space (erased files).
- 11. Search files, file slack, and unallocated space for keywords.
- 12. Document file names, dates, and times.
- 13. Identify file, program, and storage anomalies.
- 14. Evaluate program functionality.
- 15. Document your findings.
- 16. Retain copies of software used [2].

- **Shut Down the Computer**
- Depending on the computer operating system, this usually involves pulling the
- plug or shutting down a network computer using relevant commands required by
- the network involved. At the option of the computer investigator, pictures of the
- screen image can be taken. However, consideration should be given to possible destructive
- processes that may be operating in the background. These can be in memory
- or available through a connected modem. Depending on the operating system
- involved, a password-protected screen saver may also kick in at any moment. This
- can complicate the shutdown of the computer. Generally, time is of the essence,
- and the computer system should be shut down as quickly as possible.

- **Shut Down the Computer**
- Depending on the computer operating system, this usually involves pulling the
- plug or shutting down a network computer using relevant commands required by
- the network involved. At the option of the computer investigator, pictures of the
- screen image can be taken. However, consideration should be given to possible destructive
- processes that may be operating in the background. These can be in memory
- or available through a connected modem. Depending on the operating system
- involved, a password-protected screen saver may also kick in at any moment. This
- can complicate the shutdown of the computer. Generally, time is of the essence,
- and the computer system should be shut down as quickly as possible.

- **Document the Hardware Configuration of the System**
- It is assumed that the computer system will be moved to a secure location where a
- proper chain of custody can be maintained and evidence processing can begin. Before
- dismantling the computer, it is important that pictures are taken of the computer
- from all angles to document the system hardware components and how they
- are connected. Labeling each wire is also important, so that it can easily be reconnected
- when the system configuration is restored to its original condition at a secure
- location

- **Transport the Computer System to a Secure Location**
- This may seem basic, but all too often seized computers are stored in less than
- secure locations. War stories can be told about this one that relate to both law
- enforcement agencies and corporations. It is imperative that the subject computer
- is treated as evidence and stored out of reach of curious computer users.
- All too often, individuals operate seized computers without knowing that theyare destroying potential evidence and the chain of custody. Furthermore, a
- seized computer left unattended can easily be compromised. Evidence can be
- planted on it and crucial evidence can be intentionally destroyed. A lack of a
- proper chain of custody can make a savvy defense attorney's day. Lacking a
- proper chain of custody, how can you say that relevant evidence was not planted
- on the computer after the seizure? The answer is that you cannot. Don't leave
- the computer unattended unless it is locked up in a secure location.

- **Make Bit Stream Backups of Hard Disks and Floppy Disks**
- The computer should not be operated, and computer evidence should not be
- processed until bit stream backups have been made of all hard disk drives and floppy
- disks. All evidence processing should be done on a restored copy of the bit stream
- backup rather than on the original computer. The original evidence should be left untouched
- unless compelling circumstances exist. Preservation of computer evidence is
- vitally important. It is fragile and can easily be altered or destroyed. Often such alteration
- or destruction of data is irreversible. Bit stream backups are much like an insurance
- policy and are essential for any serious computer evidence processing.

- **Mathematically Authenticate Data on All Storage Devices**
- You want to be able to prove that you did not alter any of the evidence after the
- computer came into your possession. Such proof will help you rebut allegations
- that you changed or altered the original evidence. Since 1989, law enforcement and
- military agencies have used a 32-bit mathematical process to do the authentication
- process. Mathematically, a 32-bit validation is accurate to approximately one in 4.3
- billion. However, given the speed of today's computers and the vast amount of storage
- capacity on today's computer hard disk drives, this level of accuracy is no longer
- accurate enough. A 32-bit CRC can be compromised.

- **Document the System Date and Time**
- The dates and times associated with computer files can be extremely important
- from an evidence standpoint. However, the accuracy of the dates and times is just
- as important. If the system clock is one hour slow because of daylight-savings time,
- then file timestamps will also reflect the wrong time. To adjust for these inaccuracies,
- documenting the system date and time settings at the time the computer is
- taken into evidence is essential.

- **Make a List of Key Search Words**
- Because modern hard disk drives are so voluminous, it is all but impossible for a
- computer specialist to manually view and evaluate every file on a computer harddisk drive. Therefore, state-of-the-art automated forensic text search tools are
- needed to help find the relevant evidence. Usually some information is known
- about the allegations, the computer user, and the alleged associates who may be involved.
- Gathering information from individuals familiar with the case to help compile
- a list of relevant keywords is important. Such keywords can be used in the
- search of all computer hard disk drives and floppy diskettes using automated software.
- Keeping the list as short as possible is important and you should avoid using
- common words or words that make up part of other words. In such cases, the
- words should be surrounded with spaces.

- **Evaluate the Windows Swap File**
- The Windows swap file is a potentially valuable source of evidence and leads. In
- the past, this tedious task was done with hex editors, and it took days to evaluate
- just one Windows swap file. With the use of automated tools, this process
- now takes only a few minutes. When Windows 2000, XP, and 2003 are involved,
- the swap file may be set to be dynamically created as the computer is operated.
- This is the default setting, and when the computer is turned off, the swap file is
- erased. However, all is not lost, because the content of the swap file can easily be
- captured and evaluated

- **Evaluate File Slack**
- File slack is a data storage area of which most computer users are unaware [5]. It is
- a source of significant *security leakage* and consists of raw memory dumps that
- occur during the work session as files are closed. The data dumped from memory
- ends up being stored at the end of allocated files, beyond the reach or view of the
- computer user. Specialized forensic tools are required to view and evaluate the file
- slack; file slack can provide a wealth of information and investigative leads. Like the
- Windows swap file, this source of ambient data can help provide relevant keywords
- and leads that may have previously been unknown.

- On a well-used hard disk drive, as much as 1.1 billion bytes of storage space
- may be occupied by file slack. File slack should be evaluated for relevant keywords
- to supplement the keywords identified in the previous steps. Such keywords should
- be added to the computer investigator’s list of keywords for use later. Because of the
- nature of file slack, specialized and automated forensic tools are required for evaluation.
- File slack is typically a good source of Internet leads. Tests suggest that file
- slack provides approximately 80 times more Internet leads than the Windows swap
- file. Therefore, this source of potential leads should not be overlooked in cases involving
- possible Internet uses or abuses.

- **Evaluate Unallocated Space (Erased Files)**
- On a well-used hard disk drive, billions of bytes of storage space may contain data
- associated with previously erased files. Unallocated space should be evaluated for
- relevant keywords to supplement the keywords identified in the previous steps.
- Such keywords should be added to the computer investigator’s list of keywords for
- use in the next processing step. Because of the nature of data contained in unallocated
- space and its volume, specialized and automated forensic tools are required
- for evaluation. Unallocated space is typically a good source of data that was previously
- associated with word processing temporary files and other temporary files
- created by various computer applications.

- **Search Files, File Slack, and Unallocated Space for Keywords**
- The list of relevant keywords identified in the previous steps should be used to
- search all relevant computer hard disk drives and floppy diskettes. Several forensic
- text search utilities are available in the marketplace. Some of these tools are designed
- to be state-of-the-art and have been validated as security review tools by the
- federal government intelligence agencies.
- It is important to review the output of the text search utility and equally important
- to document relevant findings. When relevant evidence is identified, the
- fact should be noted and the identified data should be completely reviewed for additional
- keywords. When new keywords are identified, they should be added to the
- list, and a new search should be conducted using the text search utility. Text search
- utilities can also be used effectively in security reviews of computer storage media

- **Document File Names, Dates, and Times**
- From an evidence standpoint, file names, creation dates, and last modified dates
- and times can be relevant. Therefore, it is important to catalog all allocated and
- “erased” files. The file should be sorted based on the file name, file size, file content,
- creation date, and last modified date and time. Such sorted information can provide
- a timeline of computer usage. The output should be in the form of a wordprocessing-
- compatible file that can be used to help document computer evidence
- issues tied to specific files.

- **Evaluate Program Functionality**
- Depending on the application software involved, running programs to learn their
- purpose may be necessary. When destructive processes that are tied to relevant evidence
- are discovered, this can be used to prove willfulness. Such destructive
- processes can be tied to *hot keys* or the execution of common operating commands
- tied to the operating system or applications.

- **Document Your Findings**
- As indicated in the preceding steps, it is important to document your findings as issues
- are identified and as evidence is found. Documenting all of the software used
- in your forensic evaluation of the evidence, including the version numbers of the
- programs used, is also important. Be sure you are legally licensed to use the forensic
- software. Software pirates do not stand up well under the rigors of a trial. Smart
- defense lawyers will usually question software licensing; you don’t want to testify
- that you used unlicensed software in the processing of computer evidence. Technically,
- software piracy is a criminal violation of federal copyright laws.
- When appropriate, mention in your documentation that you are licensed to use
- the forensic software involved. Screen prints of the operating software also help document
- the version of the software and how it was used to find or process the evidence

- **Retain Copies of Software Used**
- Finally, as part of your documentation process, it is recommended that a copy of the
- software used be included with the output of the forensic tool involved. Normally,
- this is done on an archive Zip disk, Jazz disk, or other external storage device (external
- hard disk drive). When this documentation methodology is followed, it eliminates
- confusion (about which version of the software was used to create the output)
- at trial time. Often it is necessary to duplicate forensic-processing results during or
- before trial. Duplication of results can be difficult or impossible to achieve if the software
- has been upgraded and the original version used was not retained.

- **Identify File, Program, and Storage Anomalies**
- Encrypted, compressed, and graphic files store data in binary format. As a result,
- text data stored in these file formats cannot be identified by a text search program.
- Manual evaluation of these files is required and, in the case of encrypted files, much
- work may be involved. Depending on the type of file involved, the contents should
- be viewed and evaluated for its potential as evidence.

- Reviewing the partitioning on seized hard disk drives is also important. When
- hidden partitions are found, they should be evaluated for evidence and their existence
- should be documented. If Windows 2000, XP, and 2003 are involved, it
- makes sense to evaluate the files contained in the Recycle Bin. The Recycle Bin is
- the repository of files selected for deletion by the computer user. The fact that they
- have been selected for deletion may have some relevance from an evidentiary
- standpoint. If relevant files are found, the issues involved should be documented
- thoroughly.

Legal aspects of collecting and preserving computer forensic evidence

- Some of the most common reasons for improper evidence collection are poorly
- written policies, lack of an established incident response plan, lack of incident response
- training, and a broken chain of custody. For the purposes of this chapter,
- the reader should assume that policies have been clearly defined and reviewed by
- legal counsel, an incident response plan is in place, and necessary personnel have
- been properly trained. The remainder of this chapter focuses on the procedure a
- private organization should follow in collecting computer forensic evidence to
- maintain chain of custody.

- **Definition**
- In simple terms, a chain of custody is a roadmap that shows how evidence was collected,
- analyzed, and preserved in order to be presented as evidence in court. Establishing
- a clear chain of custody is crucial because electronic evidence can be
- easily altered. A clear chain of custody demonstrates that electronic evidence is
- trustworthy. Preserving a chain of custody for electronic evidence, at a minimum,
- requires proving that:
- No information has been added or changed.
- A complete copy was made.
- A reliable copying process was used.
- All media was secured

- **Legal Requirements**
- When evidence is collected, certain legal requirements must be met. These legal requirements
- are vast, complex, and vary from country to country. However, thereare certain requirements that are generally agreed on within the United States. U.S.
- Code Title 28, Section 1732 provides that log files are admissible as evidence if they
- are collected *in the regular course of business*. Also, Rule 803(6) of the Federal Rules
- of Evidence provides that logs, which might otherwise be considered hearsay, are
- admissible as long as they are collected *in the course of regularly conducted business*
- *activity*. This means you'd be much safer to log everything all the time and deal with
- the storage issues than to turn on logging only after an incident is suspected. Not
- only is this a bit like closing the barn door after the horse has fled, but it may also
- render your logs inadmissible in court.

- Another factor in the admissibility of log files is the ability to prove that they
- have not been subject to tampering. Whenever possible, digital signatures should be
- used to verify log authenticity. Other protective measures include, but are not limited
- to, storing logs on a dedicated logging server and encrypting log files. Log files
- are often one of the best, if not only, sources of evidence available. Therefore, due
- diligence should be applied in protecting them.
- One other generally accepted requirement of evidence collection is a user’s expectation
- of privacy. A key to establishing that a user has no right to privacy when
- using corporate networks or computer systems is the implementation of a log-on
- banner.

- CERT Advisory CA-1992-19 suggests the following text be tailored to a
- corporation’s specific needs under the guidance of legal counsel:
- This system is for the use of authorized users only. Individuals using this computer
- system without authority, or in excess of their authority, are subject to having all
- of their activities on this system monitored and recorded by system personnel.
- In the course of monitoring individuals improperly using this system, or in the
- course of system maintenance, the activities of authorized users may also be
- monitored.
- Anyone using this system expressly consents to such monitoring and is advised
- that if such monitoring reveals possible evidence of criminal activity, system personnel
- may provide the evidence of such monitoring to law enforcement officials

- Furthermore, security policy can play a key role in establishing a user’s expectation
- of privacy. The Supreme Court ruling in O’Connor v. Ortega, 480 U.S. 709
- (1987) implies that the legality of workplace monitoring depends primarily on
- whether employment policies exist that authorize monitoring and whether that
- policy has been clearly communicated to employees. To prove that the policy has
- been communicated, employees should sign a statement indicating that they have
- read, understood, and agreed to comply with corporate policy and consent to system
- monitoring.

- **Evidence Collection Procedure**
- When the time arrives to begin collecting evidence, the first rule that must be followed
- is *do not rush*. Tensions will probably be high and people will want to find answers
- as quickly as possible. However, if the investigators rush through these
- procedures, mistakes will be made and evidence will be lost

- The investigation team will need to bring certain tools with them to the incident
- site. They will need a copy of their incident-handling procedure, an evidence
- collection notebook, and evidence identification tags. Depending on the type of incident
- and whether the team will be able to retrieve an entire system or just the data,
- they may also need to bring tools to produce reliable copies of electronic evidence,
- including media to use in the copying process. In some cases, legal counsel will
- want photographs of the system prior to search and seizure. If this is something
- your legal counsel wants as part of the evidence, then also include a Polaroid camera
- in the list of tools.

- Policy and procedure should indicate who is to act as incident coordinator.
- When an incident is reported, this individual will contact the other members of the
- response team as outlined in the Incident Response Policy. Upon arrival at the incident
- site, this individual will be responsible for ensuring that every detail of the
- incident-handling procedure is followed. The incident coordinator will also assign
- team members the various tasks outlined in the incident-handling procedure and
- will serve as the liaison to the legal team, law enforcement officials, management,
- and public relations personnel. Ultimate responsibility for ensuring that evidence
- is properly collected and preserved, and that the chain of custody is properly maintained,
- belongs to the incident coordinator.

- One team member will be assigned the task of maintaining the evidence notebook.
- This person will record the who, what, where, when, and how of the investigation
- process. At a minimum, items to be recorded in the notebook include
- Who initially reported the suspected incident along with time, date, and circumstances
- surrounding the suspected incident.
- Details of the initial assessment leading to the formal investigation.
- Names of all persons conducting the investigation.
- The case number of the incident.
- Reasons for the investigation.
- A list of all computer systems included in the investigation, along with complete
- system specifications. Also include identification tag numbers assigned to
- the systems or individual parts of the system.
- Network diagrams.
- Applications running on the computer systems previously listed.

- A copy of the policy or policies that relate to accessing and using the systems
- previously listed.
- A list of administrators responsible for the routine maintenance of the system.
- A detailed list of steps used in collecting and analyzing evidence. Specifically,
- this list needs to identify the date and time each task was performed, a description
- of the task, who performed the task, where the task was performed, and the
- results of the analysis.
- An access control list of who had access to the collected evidence at what date
- and time

- Another team member (or members) will be assigned the task of evidence collection.
- To avoid confusion, the number of people assigned this task should be
- kept to a minimum. This member (or members) should also be highly proficient
- with copying and analysis tools. This person will tag all evidence and work with the
- person responsible for the evidence notebook to ensure that this information is
- properly recorded. Next, the person will also be responsible for making a reliable
- copy of all data to be used as evidence. The data will include complete copies of drives
- on compromised or suspect systems, as well as all relevant log files. This can be
- done on-site or the entire system can be moved to a forensics lab, as needs dictate.

- simple file copy is not sufficient to serve as evidence in the case of compromised
- or suspect systems. A binary copy of the data is the proper way to preserve evidenceTwo copies of the data should be made using an acceptable tool. The original
- should be placed in a sealed container. One copy will be used for analysis and the
- other copy can be put back in the system so the system can be returned to service
- as quickly as possible. Once all evidence is collected and logged, it can be securely transported to the
- forensics lab. A detailed description of how data was transported and who was responsible
- for the transport, along with date, time, and route, should be included in
- the log. It is required that the evidence be transported under dual control.

- **Storage and Analysis of Data**
- Finally, the chain of custody must be maintained throughout the analysis process.
- One of the keys to maintaining the chain is a secure storage location. If the corporation
- uses access control cards or video surveillance in other parts of the building,
- consider using these devices in the forensics lab. Access control cards for entering
- and exiting the lab will help verify who had access to the lab at what time. The video
- cameras will help determine what they did once they were inside the lab. At a minimum,
- the lab must provide some form of access control; a log should be kept detailing
- entrance and exit times of all individuals. It is important that evidence never
- be left in an unsecured area. If a defense lawyer can show that unauthorized persons
- had access to the evidence, it could easily be declared inadmissible.

- Pieces of evidence should be grouped and stored by case along with the evidence
- notebook. In an effort to be as thorough as possible, investigators should follow
- a clearly documented analysis plan. A detailed plan will help prevent mistakes
- (which could lead to the evidence becoming inadmissible) during analysis. As
- analysis of evidence is performed, investigators must log the details of their actions
- in the evidence notebook. The following should be included at a minimum:
- The date and time of analysis
- Tools used in performing the analysis
- Detailed methodology of the analysis
- Results of the analysis [

- Pieces of evidence should be grouped and stored by case along with the evidence
- notebook. In an effort to be as thorough as possible, investigators should follow
- a clearly documented analysis plan. A detailed plan will help prevent mistakes
- (which could lead to the evidence becoming inadmissible) during analysis. As
- analysis of evidence is performed, investigators must log the details of their actions
- in the evidence notebook. The following should be included at a minimum:
- The date and time of analysis
- Tools used in performing the analysis
- Detailed methodology of the analysis
- Results of the analysis [

- Finally, once all evidence has been analyzed and all results have been recorded
- in the evidence notebook, a copy of the notebook should be made and given to the
- legal team. If the legal team finds that sufficient evidence exists to take legal action,
- it will be important to maintain the chain of custody until the evidence is handed
- over to the proper legal authorities. Legal officials should provide a receipt detailing
- all of the items received for entry into evidence