First Responder's Manual

Department of Energy
Computer Forensic Laboratory

DEPARTMENT OF ENERGY – COMPUTER FORENSIC LABORATORY

First Responder's Manual

U.S. Department of Energy
Computer Forensic Laboratory
P.O. Drawer A
Aiken, SC 29802
Phone: SRS-EOC (803) 725-1911   Fax (803) 725-2368

Table of Contents

First Responder's Manual

Appendices

Introduction

As computers become an integral part of our daily lives, there are going to be incidents where systems and individual computers are misused or potentially compromised. When a breach of security or criminal act involving a computer is suspected, it is essential that steps be taken to ensure the protection of the data within the storage media. The stored data is invaluable to determine the level of security breach and location of potential evidence concerning a criminal act.

Purpose

While this manual cannot address every scenario involving computer system misuse or compromise, it is designed as a guide concerning the initial response to a computer incident for both system administrators and security personnel.

Overview of First Response

Although this manual is being written with system administrators and security personnel in mind, it can be useful to anyone who suspects a computer was used, intentionally or unintentionally, in a security incident or criminal act. The initial response to such an incident is more important than later technical analysis of the computer system as actions taken by the first responder will greatly impact on the subsequent laboratory examinations of the questioned media. Simply put, the success of data recovery and potential prosecution is dependent on the actions of the individual who initially discovers a computer incident.

First Response for System Administrators

The role of a system administrator is vital in ensuring all aspects of network security and maintenance, but this individual also plays the most important role in the event a computer is used in a security incident or unlawful act. The system administrator will most likely be the primary point of contact for individuals wishing to make a report of computer use violations. In addition, a system administrator may come across a violation during the normal course of their duties. The actions taken by the system administrator after discovery of a potential computer violation will play a vital role in the investigation, forensic evaluation of the computer system, and potential prosecution or administrative actions.

From a forensic standpoint, the ideal situation is to isolate the computer from additional use or tampering. If you are dealing with a computer system which is a server supporting a vital mission function, isolation of the system may not be feasible. A suspected computer violation will result in difficult decisions in weighing the loss of potential evidence to the inability to utilize a computer system tied to the network.

In the event of a suspected computer incident, great care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, merely opening a file changes it. In a legal sense, it is no longer the original evidence and at that point may be inadmissible in any subsequent legal or administrative proceedings. Opening a file also alters the time and date it was last accessed. On the surface this may not be an important issue, however, it could later become extremely important in the determination of who committed the violation and when it occurred. Isolation of the computer system is ideal, but if this cannot be completed due to mission requirements, no attempts should be made to recover or view files at the local level.

Protecting the Integrity of Evidence

The isolation of a computer system so evidence will not be lost is of utmost importance. Consideration must also be given to other storage media, handwritten notes, and documents found in the area of the computer involved. These items could be of value to a subsequent investigation. Computer disks, CD-ROMs, tape storage media, additional hard drives found in the area of the computer also need to be protected and isolated.

No one, to include the individual suspected of committing the alleged computer violation, should be allowed contact with the storage media or the computer involved. Individuals with extensive computer experience can develop programs that, with a few keystrokes, will destroy all magnetic data on a hard drive.

As the system administrator and/or first responder to a suspected computer violation, it is very possible that you will be required to articulate the procedures used in protecting the questionable media to investigative personnel. You may also be called to testify at administrative or legal proceedings concerning the measures that were taken during the initial shutdown or isolation.

The manner the computer equipment and storage media is secured after a suspected computer incident is reported will be dependent on the facilities available and the computer system involved. In some instances, it may be impractical to seize the computer as in the case of a large mainframe, but it may be more appropriate to seize the back-up media. Once any item is seized, the physical integrity of the system and storage media must be protected. The ideal situation is to secure it in a manner where only the system administrator has access or to contact your local security force to collect the media as evidence.

Additional attention should be given to securing backup media storage devices. In many instances, systems are backed up on a daily basis. If the individual suspected in a security incident attempts to delete files from the primary storage device (hard drive), these files could still remain on the backup storage media.

The ideal situation would call for the system administrator to merely ensure no destructive programs are in operation, secure the scene and have security personnel trained in the seizure of computer systems respond to process the work station. As there are very few occasions where we will be faced with the “ideal situation”, an initial response guide is available at Appendix A.

Shut-Down Procedures

One of the most difficult decisions in dealing with a suspected computer violation is how to power-down a computer system in a manner that will not corrupt the integrity of the files. In most cases, the type of operating system employed on the computer will be the key in making this decision. With some operating systems, merely pulling the plug from the wall socket is the preferred method of shutting the system down. With other systems, disconnecting the power supply without allowing the operating system to initiate internal shutdown commands could result in everything from the loss of vital files to a hard drive crash.

Although it is strongly recommended coordination be made with the Department of Energy Computer Forensic Laboratory (DOE-CFL) prior to shutting down a system that will later undergo forensic examination, it is recognized this is not always feasible. Appendix B contains a quick reference guide that will provide you with information regarding how to shutdown most current operating systems with the least amount of data loss.

Department of Energy Computer Forensic Laboratory

The Department of Energy Computer Forensic Laboratory (CFL) is located at the Savannah River Site in Aiken, SC. CFL support is available to all inquiry officials and system administrators in DOE who require or request forensic evaluation of computer equipment for unauthorized disclosure of classified information. The CFL is also available to review computer media for evidence of fraud, waste, abuse and other criminal or administrative infractions. These services can also be requested by other federal, state and local government law enforcement agencies on a space available basis.

The CFL can assist system administrators with advice on preserving data and if necessary, can dispatch a fly-away team that will perform data imaging. If warranted the media or an image of the media will be transported to the CFL for detailed analysis.

The CFL has state of the art computer forensic tools that enable computer specialists to conduct examinations of computer media without compromising the integrity of the original files. Using the most current forensic tools, in most instances, deleted files, printed documents and hidden directories/files, can be viewed even if they are password protected. The laboratory currently has the ability to conduct forensic analysis on most storage media operating with MS-DOS, MAC, WIN3.1, 95 and 98, LINUX, Windows NT, and UNIX. A detailed, factual, unbiased computer forensic report that will clearly detail the evidentiary content of the questionable storage media will be provided upon completion of the forensic analysis.

Requesting Computer Forensic Support

Requests for support can be made at anytime after a suspected computer violation is detected. It is highly recommended coordination be made with the DOE-CFL immediately prior to collection of computer equipment or storage devices and prior to operating system shut-down. Our specialists are constantly available and can provide advice, laboratory analysis or a flyaway team to assist in the collection or imaging of computer media for forensic evaluation.

In the event your organization requires forensic computer support or has questions regarding evidence collection, please contact the DOE-CFL at (803) 725-0722 or e-mail at forensic@srs.gov. If you have an emergency after duty hours, call the Emergency Operations Center, Savannah River Site at (803) 725-1911 and ask that they notify a member of the CFL.

First Response for Security/Inquiry Officials

In today's environment, there is no doubt that you will be faced with an incident where a computer was used to commit either a security violation or a criminal act. The initial response to a situation where a computer is suspected to be involved should be handled as any other crime scene with the primary emphasis being on the security and protection of potential evidence. The only difference is, that in most instances, the majority of the evidence will be latent in nature and will require forensic laboratory analysis to retrieve it. Files detailing the security incident or criminal act may have been deleted from a computer system but often these can be recovered.

Under no circumstances should anyone, with the exception of laboratory personnel, make any attempts to restore or recover information from a computer system. It must be remembered that the data present within the storage media is potential evidence and should be treated accordingly. Any attempts to retrieve data by unqualified individuals should be avoided as these attempts could either compromise the integrity of the files or result in files being inadmissible in legal or administrative proceedings.

The entire workstation or office is a potential crime scene, not just the computer itself. The workstation/office should be secured and protected to maintain the integrity of the scene and the storage media. Under no circumstances should anyone be allowed to touch the computer, to include shutting the computer down or exiting from any programs/files in use at the time inquiry and/or security personnel arrive. In addition, no one should be allowed to remove any items from the scene. All individuals present at the scene should be fully identified and briefly interviewed to determine their access to the computer and office or workstation involved before asking them to depart.

Once initial security has been established, the scene should not be left unattended or unsecured for any reason until the processing of the scene is completed. Instructions should be provided to any individuals guarding the scene concerning access. Only inquiry/security officials should be allowed to enter and the numbers of individuals involved in processing should be kept at a minimum. Notes should be maintained regarding how scene security was established to include the identification of security personnel involved.

Detailed notes should be maintained during all aspects of the scene processing. This not only includes the usual who, when, what, why and how, but your overall observations of the scene. Notes should articulate to the reader exactly what the scene looked like upon your arrival. This would include items of furniture within the room and their locations, the condition of the room (clean, dirty, etc.), locations of any computer equipment, disks, tapes, etc., along with the locations and descriptions of potential evidence.

During your observations, a determination should be made concerning the possibility that potential evidence is at immediate risk of destruction (i.e. disk format or upload of information in progress). This may require an immediate decision to disconnect the power supply. All factors, such as the potential loss of data, need to be taken into consideration when making this decision, but it must be made quickly. (See Appendix B)

Other things that should to be noted and discussed with CFL personnel prior to the processing of the scene include the number and type of CPUs involved; the location of the CPUs and peripherals; the type and topology of the network operating system; the size and nature of storage media; and the existence of any back-up media.

Depending on access to the scene and the nature of the crime, fingerprint evidence could be important during a later phase in the investigation. Inquiry officials should consider wearing surgical gloves prior to touching anything within the office or workstation.

A step-by-step guide concerning the processing or a workstation involving computer evidence is located at Appendix C. An additional guide concerning evidence collection and marking is available at Appendix D. Instructions for evidence documentation are at Appendix E.

Questions raised during the processing of a scene involving a computer can be directed to the DOE-CFL. The DOE-CFL technicians can provide you with advice for scene processing and evidence collection involving computer media, laboratory analysis of your evidence, or on-scene assistance if requested.

The DOE-CFL conducts computer forensics data recovery and analysis only. Examination of latent fingerprints or other physical evidence must be coordinated with DOE Headquarters inquiry officials.

Appendix A – Initial Response Guide

Notification:

Detailed notes should be maintained regarding the time and date of notification; who provided the notification and the type of computer incident suspected to have been committed.

Individuals providing the notification should be instructed to deny use of the computer or workstation until cleared by authorized personnel (system administrator/investigative personnel).

Immediately determine if the system performs critical functions that make shutdown difficult or impossible and if classified information is processed on the system.

Appropriate inquiry/security personnel should be notified immediately.

Response:

If you are unsure of what actions to take at any point during your preliminary computer response contact the DOE-CFL.

Ensure the security of the computer and workstation. All individuals should be kept clear of the computer until a determination has been made regarding the disposition of the system.

All external data connections should be removed (review Appendix B). If the computer is part of a network system, it should be disconnected from the network to eliminate the transfer between other computers on the system.

If the computer is operational upon arrival, check to make sure that a self-destruct program, such as Norton Wipe-Info, is not running. If such a program is found to be operational, immediately pull the power cord from the wall socket.

Warning: Before disconnecting or shutting down a system, first ensure that the action will not jeopardize a critical safety or operational function.

Initial Observations/Actions

Handwritten notes, loose magnetic storage media to include computer disks, tapes and CD-ROM's should be collected for later evaluation.

Any "personal organizers" (e.g. HP Palm Pilot, Sharp's Wizard, etc.), desk/personal calendars and/or address books should be identified.

A search for potential passwords and website/IP addresses written on scraps of paper within the workstation should be completed. Most passwords will be at least six digits in length.

Do not overlook the trashcan as an area where potential items of evidence may be located.

Determine occupancy of the workstation by documents and/or personal effects found within the room.

If the type of report or initial inquiry determines the workstation should be processed as a crime scene, refer to Appendix C as a guide for overall processing and Appendix D as a guide to evidence collection and marking.

Power Down the System:

Determine the type of operating system involved (e.g. WIN98, UNIX, LINUX).

Refer to Appendix B concerning shut down procedures. The manner the computer is shut down is dependent on the operating system involved.

Additional Actions:

Locate and secure any backup storage media concerning the system. In some instances files that are deleted from the hard drive will be present within the backup on the backup storage media.

If within a DOE facility, contact the DOE telecommunications officer and attempt to obtain a printout of phone numbers dialed from the workstation. This should include information from a fax and/or data line if one is available.

Conduct interviews of individuals with access to the system or network.

Determine the type and security classification of the work normally performed on the questionable computer system. If unclassified, would there be any logical reason for classified information to be present on the hard drive or other storage media?

Determine the identity of all individuals with both physical and password access to the computer involved.

Determine if the computer is a part of a network and the type of network system involved.

Determine if the system requires "log on" identification and if available, obtain password information concerning the computer.

Determine if the computer system is also used as a fax and/or a telephone-answering device.

Attempt to determine, through interviews, the types of computer programs present on the computer. If a non-standard program is used, attempt to obtain a working copy or installation disk.

Appendix B: Operating System Shutdown Procedures

(Note: This section is being presented as a guide and should not be considered all-inclusive. Some operating systems such as LINUX and UNIX have numerous versions and different operating commands. To ensure correct procedures are being utilized, contact the DOE-CFL.)

MS DOS Operating System

Characteristics

- Text on solid background (usually black)
- Prompt contains drive letter and uses backslashes
- Prompt usually ends with a greater than sign (>)

Shutdown Procedures:

- Photograph screen and annotate any programs running
- Pull power cord from wall

Windows 3.X Operating System

Characteristics:

- Program Manager
- Colored tile bar
- Standard menu options

Shutdown Procedures:

- Photograph screen and annotate any programs running
- Pull power cord from wall

Windows NT 3.51 Operating Systems

Characteristics:

- Program Manager
- Colored tile bar
- Standard menu options
- Icons have computers or people added

Shutdown Procedures:

- Photograph the screen and annotate any programs running
- Pull power cord from wall

Windows 95/98/NT 4.0 Operating Systems

Characteristics:

- Start button with Windows symbol

Shutdown Procedures:

- Photograph screen and annotate any programs running
- Pull power cord from wall

UNIX/Linux Operating Systems

Characteristics:

- Start button with UNIX/Linux version symbol

Shutdown Procedures:

- Photograph screen and annotate any programs running
- Right click to menu
- From menu, Click **Console**

    a. Root user prompt is set to **#** sign. If not present, change user to root (type **su -**). At that point you will be prompted for the root password. If password is available enter it. At the **#** sign type **sync;sync;halt** and system will shutdown. If you do not have root password, pull cord from wall

b. If when at console **#** sign is displayed, type id and press enter. If you see that your user ID is root, type **sync;sync;halt** and press enter. This will shutdown the system. If your user ID is not root, pull cord from wall.

MacOS Operating System

Characteristics:

- Apple symbol in upper left corner
- Small horizontal lines on windows menu bar
- Single button in each corner of window
- Trash icon

Shutdown Procedures

- Photograph screen and annotate any programs running
- Record time from menu bar
- Click **Special**
- Click **Shutdown**
- The window will tell you it is safe to turn off the computer
- Pull power cord from wall

Appendix C- Scene Processing Guide

Initial Search

The initial seizure conducted within a computer related scene is much like any traditional crime scene. The area of primary importance should be the location and identification of any fragile evidence that could be altered if not immediately collected. In dealing with a computer related scene, it is possible that the perpetrator initiated a self-destruct program (e.g. Norton Wipeinfo) or is in the process of reformatting the storage media upon your arrival. In the event such activities are taking place, immediately pull the power cord that connects to the Central Processing Unit from the wall.

Photographing the Scene

The old adage of crime scene processing, “you cannot take too many pictures” is also true when processing a scene where computer evidence is involved. Photographing a scene should be the first step taken by any inquiry official upon arrival at a potential crime scene. This will accurately depict the condition of the scene prior to any evidence collection or disruption that will occur during processing.

Detailed notes should be taken concerning each photograph exposed to include the camera height (i.e. eye level or measurement), distance from specific items within the scene, time exposed, type of camera, a flash attachment utilized if any, etc. The easiest way to accomplish this is through the use of a photograph log. This log can be locally generated and should contain general information concerning the camera, film type (if wet photography is used), lens type, any type of filters used along with detailed information concerning each photo. The following is an example of a photograph log:

Time	Photo #	Type	Depicting	Distance	Remarks
0900	#1	Overall	Doorway of Room 45, Bldg 718	5’3	1/60 w/Flash
0905	#2	Entry	Entry into room 45	6’4”	1/60 w/Flash
0907	#3	360	Shot from West wall	8’10”	1/60 w/Flash
0908	#4	360	Shot from North wall	8’10”	1/60 w/Flash
0909	#5	360	Shot from East wall	8’10”	1/60 w/Flash
0910	#6	360	Shot from South wall	8’10”	1/60 w/Flash

The above should continue to include evidence photographs, etc.

The order photographs are taken should be done in a manner that will not corrupt the scene. The ideal situation is to first take several photographs that will establish the location of the scene (i.e. building, office number), followed by an entry photograph (what you are seeing as you enter the room), followed by "360 degree" photographs. "360 degree" photographs are simply overlapping photographs depicting the entire crime scene. The key to remember in crime scene photography is to go from the overall scene down to the smallest piece of evidence. This all should be completed prior to any evidence collection taking place or the scene being disturbed in any manner. At this point there should be no attempt to search the contents of desks or any other containers within the scene. The initial set of photographs should depict exactly the condition of the scene as you found it.

If the CPU is operational upon your arrival, photographs should be taken of the monitor screen depicting what is currently displayed. In the event a "screen saver" is being utilized, press the "down arrow" key to redisplay the open file. Other than touching that one key, DO NOT make any other keystrokes and DO NOT turn the computer off unless a self-destruct program is running. The manner to properly shut down the computer is addressed within Appendix B of this manual.

Photographs should also be taken of the immediate work area to include computer disks, handwritten notes, and other computer equipment (printers, external drives, etc…). Photographs should also be taken of the rear of the computer to accurately display how the cords are connected if this can be accomplished without moving the CPU. In the event the CPU cannot be moved to expose these photographs, they can be taken later during evidence collection. At this point in the processing, overall photographs should only be taken.

Sketching the Scene

A crime scene sketch should be prepared which details the overall scene. This should include the locations of items within the office area. Again, the rule of thumb for crime scene sketching is to go from the overall scene to the smallest piece of evidence. This may require several sketches to accurately depict the scene. An overall sketch could be completed, followed by a sketch of the top of a desk detailing where items of evidence are present, followed by a projection sketch of the rear of the CPU detailing where different cords are plugged in.

In the event the crime scene is a workstation within a large office area or in an office where more than one individual has access, consideration should be given to the preparation of a sketch detailing the location of the scene in relation to other offices or workstations.

Initial Interviews

The identification of personnel at the scene and initial interviews are extremely important. In some instances more than one individual, as in a location where shift work is conducted, may use a computer system. Identification of all parties who have access and normal shift times could play a key role in a determination of who committed the actual offense. In addition, during initial interviews, the potential suspect has not had sufficient time to formulate any denials or an alibi concerning any information that is later received. The fact that their initial account of the events may not match subsequent interviews could be extremely important during the investigation. If the system administrator is available at the scene, this individual could also provide valuable information concerning the computer system involved, user identification and password information.

Evidence Collection/Search of Scene

As items that need to be evaluated as evidence are collected, care must be taken to note their position at the time of processing and to ensure they are not altered from their original state. Under no circumstances should any investigative personnel tamper with any items which could be evidence. This deals primarily with any computer storage media (disks, tapes, etc.) that are identified during processing. They should be collected in the state they are found. Do not make efforts to determine what is present on this media prior to collection. Trained technicians from the Computer Forensics Laboratory (CFL) should be contacted for forensic analysis of the storage media.

When processing a scene where a computer is suspected to have played a part in a security incident or criminal act, the natural instinct is to seize the CPU as the first item of evidence. In reality, due to the time involved and the number of items involved in seizing the CPU, this should be one of the last items removed from the office/workstation. The CPU should be left in the position it was found. If the computer was already shut down prior to arrival at the scene, no attempts should be made to make the CPU operational.

The scene should be searched in a circular motion with the concept of the CPU being at the center of the circle. Items of evidence, as located, should be photographed, identified within notes and then collected. Detailed information concerning the marking, care and transportation of computer evidence is present within Appendix D of this manual.

Entries within the evidence/property document should contain a description of the item (to include model and serial number if the item is a piece of hardware), any visible markings present on the item, the condition of the item, the manner it was marked for evidence and the location from within the scene it was seized (i.e. "from on top of desk” or “from trash can”). Typical evidence listings within the evidence/property custody document could be documented as follows:

Item #	Quantity	Description
1	1	3.5 computer disk, black in color, no labels present engraved at the top with manufacturer marking of “MF 2HD Maxwell”. Marked with scribe for ID “MFR, 1100, 15 Sep 99” Sealed in static free bag and seal marked with same markings (top right hand corner of desk)
2	1	White in color plastic box with green in color plastic lid containing a total of fifteen 3.5 computer disks, all with various markings and labels. Box has locking device on the front, which is in the open position. Box sealed with evidence tape and seal marked for ID “MFR, 1107, 15 Sep 99 (top left hand corner of desk)
3	1	Central Processing Unit (CPU), white in color, tower type design, with marking on front of “Dell Dimension XPS T600” and label on top with the words “Property of US Department of Energy Computer Forensics Laboratory”. Serial number information is on a white label affixed to the bottom of the CPU. Serial number listed is “YX2451MN94J”. CPU was marked for ID on rear with scribe “ “MFR, 1243, 15 Sep 99” (on floor, right hand side of desk)

Note: This is not all-inclusive. Every item of evidence has its own characteristics, but should be identified within the evidence/property custody document in a manner where you can easily identify it at a later date and if required, testify that it is the same item you seized at the scene. As noted above, items should be collected as found. If you find a disk or a piece of paper lying on a desk, it should be collected as an individual item. If you discover a box or container (as in the example above), seize the entire container as one item of evidence containing a specific number of items.

The search of the scene should not be limited to areas on, in and around an individual’s desk. Trashcans are often a place where valuable evidence is located. Do not overlook items such as handwritten notes, especially if they are in close proximity to the CPU workstation. These could contain password information, IP addresses concerning web sites the individual has visited and a wealth of other information that could be invaluable to examiners attempting data recovery. Check under desk blotters for handwritten notes, “sticky notes” around the area of the computer along with other areas. If you are not sure an item has any evidentiary value, seize it. The item can always be returned to the owner later, but if missed during the initial search, chances are that if it was evidence, it will be gone during any subsequent visits.

"If in doubt concerning the value of something as potential evidence, seize it since in most cases you will not get the chance to come back later"

Seizure of CPU

If the CPU is found operational, prior to shutting the system down or exiting any programs, coordination should be made with the CFL. This is due to the type of operating systems currently available. In some instances, merely pulling the power cord from the wall would be sufficient, but with some operating systems, this could result in the loss or destruction of potential evidence. Some CPUs may require that the shut down procedures need to be accomplished by the operating system before the power supply is disconnected. A guide concerning shutdown procedures for different operating systems is present at Appendix B within this manual.

All connectors and plugs should be labeled and marked for evidence prior to disassembly. It is critical that the cabling be documented precisely. This is accomplished by using tape and/or tags to mark each end. A corresponding tape is placed on the device to which it is connected. Each cable, with the exception of the power cord, should have a label on each end. An example would be a printer cable attached to a CPU. The printer port on the CPU could have a label marked with "Port 1", the cable where it connects to the printer port would be labeled with "Port 1" and the other end could be labeled with "Printer". Whatever type of system is used, it should be kept simple and easily explained in subsequent reports as not only may you have to discuss it with the technician completing the data recovery, you also may be required to testify concerning the manner the CPU and peripherals were set up when you arrived at the scene. There are many non-standard cables and there may be multiple combinations that will fit, but will not work correctly. As a result, all cables that connect to peripherals to be seized must also be collected.

If more than one system is involved, this may require additional information being placed on individual labels. An example of something which could be used for multiple systems would be the label for the printer port at the CPU to read "1 (indicating CPU #1) – Port 1" and the cable where it connects to the port to be labeled "1-Port 1". Again, the system should be best suited for the scene you are processing, but should be kept simple and easy to explain.

Prior to disassembly, it is also very useful to do close-up photography of all the connections between individual pieces of hardware. This will provide an additional record of how the system was connected and labeled. It will also aid in the reconstruction of the system in a laboratory setting. It should be remembered that the individual doing the examination of the storage media at a later date would most likely not have the advantage of being present at the search scene.

After the labeling of all ports and cables has been completed and all close up photography, exposed, it is time to disassemble the equipment. It is best to work slowly and carefully. It is probably best to start with the peripherals and then to the CPU. Do not be in a rush and double check to make sure that all ports and cables are labeled as the disassembly process continues.

During a search of a scene where more than one CPU is seized as evidence, it is important to keep each system separate from others. All of the peripherals should be labeled to indicate which CPU they were connected to. If items get mixed together, it may be difficult to separate them at a later date.

Secondary Search of Scene

Once all evidence has been collected, it is recommended that an additional search be conducted of the scene. In the event additional evidence is located during this second search, it should be noted, photographed and collected.

Release of Scene

Upon completion of processing, the scene can be released. It is recommended the scene be released to the system administrator or supervisor for the area of the workstation. A copy of the evidence/property documents listing items removed from the scene should be provided to this individual.

Appendix D – Evidence Collection Guide

It is extremely easy to alter or damage information/evidence stored on a computer if proper shutdown procedures are not followed. If the computer is running and the agent performing the collection has not had formal training in handling computer evidence, coordination should be made with the DOE-CFL. If coordination is not possible, examine the screen and document (note, photograph, etc.) what programs are running. Refer to Appendix B for a guide to proper shutdown procedures concerning different operating systems. Once completed, unplug the CPU power cord from the wall or surge protector. Ensure a complete record is made of every step taken prior to shutdown.

All evidence collected should be marked so it can be easily identified at a later date. The minimum markings should at least contain the time and date the evidence was collected and the initials of the individual seizing the property (e.g. "MFR, 1020, 15 Sep 99"). This should be done in a permanent manner, but not in a way that will deface an expensive piece of equipment. Central Processing Units could be marked on the rear with either a scribe or permanent marker for later identification. The need for a permanent marking is to aid the investigator in the identification of the property during legal proceedings. Both tags identifying the previous connection and permanent markings should be on cables as one is for later identification and the other is for reassembly purposes.

Note: If you see what appears to be a destructive process running on the system, such as formatting of the disk drives, immediately disconnect the power.

Central Processing Unit

- Photograph the computer, including all components
- Using adhesive labels, label each of the computer connections (ports)
- Using adhesive labels, label each of the cables connected to the computer with numbers or letters corresponding to the computer connection they were attached to.
- Disconnect all the cables from the computer
- Photograph the location of manuals and documentation in relation to the computer. This may provide important information during analysis.

- Mark as evidence, wrap in static free bubble wrap. Place in a box or crate to prevent shifting. If available, pack in the original factory container.

Monitor

- If the computer is operational, photograph the screen (avoid using videotape to record data present on the monitor as a video will usually be of poor quality due to the refresh rate of the monitor).

- Disconnect the power source.

- If the monitor has removable cables, attach hand numbered adhesive labels to the cables and their associated connecting points on the computer monitor.

- Mark as evidence, wrap in static free bubble wrap. Place in box or crate to prevent shifting.

Keyboard

- If the keyboard has removable cables, attach hand numbered adhesive labels to the cables and their associated connecting points.

- If any other devices are attached to the keyboard or if the keyboard is attached to another device, label all connecting points and cables.

- Mark as evidence, wrap in static free bubble wrap. Place in a box or crate to prevent shifting.

Pointing Devices (mouse, light pen, wand, etc.)

- If the pointing device has removable cables, attach hand numbered adhesive labels to the cables and their associated connecting points.

- Mark as evidence. Typically, pointing devices can be boxed or bagged in static free containers.

Printers

- If the printer has removable cables, attach hand numbered adhesive labels to the cables and their associated connecting points.

- If any other devices are attached to the keyboard or if the keyboard is attached to another device, label all connecting points and cables.

- Mark as evidence, wrap in static free bubble wrap. Place in box or crate to prevent shifting.

Scanners

- If the scanner has removable cables, attach hand numbered adhesive labels to the cables and their associated connecting points.

- Mark as evidence. Some scanners are extremely fragile and care must be exercised when handling them. If the owner's manual for the scanner is available, determine the proper way to prepare the scanner for shipping.

External Drives

- If the external drive has removable cables, attach hand numbered adhesive labels to the cables and their associated connecting points.

- Mark as evidence. There are a number of different types of external drives. If the external drive uses removable media, the media should be removed prior to packaging the drive for shipping.

- Any media that was removed from the device should be marked as evidence, placed in a static free container and notes generated indicating it was removed from the external drive.

Other Devices

- If any other device not listed above is connected to a computer system, photographs of the item, along with detailed notes of its location, should be generated.

- If the device connected to the computer has removable cables, attach hand numbered adhesive labels to the cables and their associated connecting points.

- Mark the device for evidence, wrap in static free bubble wrap and prepare for shipping.

Floppy Diskettes and Other Removable Media

Floppy diskettes and other removable media require special attention during the collection phase. The media can be found in a variety of locations at a crime scene. It is important to note the location and other pertinent information about the collection of floppy diskettes and other removable media. If floppy diskettes or other removable media are stored in the diskette case, box or other storage container, it is recommended that the media remain in the storage container when it is collected.

Diskettes are covered with a fragile magnetic media. If they are packed loosely and allowed to strike each other repeatedly during transit, the data could be damaged. Make sure they are packed in a manner to reduce this possibility.

Protection and Marking of Floppy Diskettes and other Removable Media

- Write protect 5 ¼ inch disks by placing tape over the notch. Mark with initials, time, date on corners using laundry marker (permanent marker). Place in static free bags.

- Write protect 3 ½ inch disks by placing the write protect tab in the open position. Mark with initials, time and date with a laundry marker and place in static free bags.

- Write protect reel-to-reel tapes by pulling the small plastic write enable ring off (located on back of tape around hub). Write initials, time and date on first 10-13 feet (leader) of tape and place in static free bags.

- Write protect cassette tapes by removing the record tab. Mark with time, date and initials on plastic surface of tape case with laundry marker and place in static free bags.

- Write protect disk cartridges (removable hard drives) by placing tape over notch. Mark with time, date and initials with laundry marker and place in static free bags.

- Write protect cartridge tapes by turning the dial until arrow is aligned with "safe" mark or white dot is facing out. Mark initials, time and date on plastic surface or cartridge case or cartridge case with permanent marker and place in static free bags.

- Mark initials, time and date on ribbon containers, do not mark on the ribbon itself. Remember, printer ribbons, like typewriter ribbons, may contain the last document typed.

Cables and Wires

Label both ends of each cable describing connectors (to assist in reassembly at a later date). Label each connector. Mark with time, date and initials using permanent marker. Place coils in paper bag and seal.

Handling/Transportation

It is extremely important that computer equipment be handled gently. The condition of the equipment is not known when you seize it. Any disturbance could result in connections coming loose. In addition, not all fixed magnetic media is self-parking. Head parking moves the electromagnetic equipment inside a disk away from the magnetic media. The "parking" of the heads provides some protection, but should never be substituted for careful handling. It should always be assumed that the heads are not parked. Any significant trauma to the CPU could result in hard drive failure.

The ideal packing material for a CPU is the original factory container. If this cannot be located, the CPU should be packed and carried as it was set up. Avoid turning the CPU upside down or laying it on its side during transport.

When transporting a CPU or other computer devices, they should not be placed in a trunk or like area where there will be drastic changes in temperature. In a vehicle, the idea place for transport would be on the rear seat, placed in a manner where the computer will not fall during sudden stop or quick maneuver.

Appendix E – Evidence Documentation

Evidence Chain of Custody

Chain of custody refers to a written account of individuals who had sole physical custody of a piece of evidence from the time it was seized until final disposition. In becoming a "link" of the chain by assuming possession for a piece of evidence, an individual has the responsibility to secure it in a manner which can later stand legal scrutiny in the event claims are raised that the evidence was tampered with. A piece of evidence is only as good as the chain of custody accompanying it. An item could be seized which has great evidentiary value, but unless the manner it was secured and accounted for can be articulated, it may be worthless in legal or administrative proceedings.

An individual who assumes physical possession of a piece of evidence is responsible for the security of it. Evidence should be secured a manner where only the individual who has signed for it can gain access to it. Security can be maintained by placing the item in a safe, locked container or room that only the responsible individual has the ability to enter.

Chain of Custody Documentation

DOE has no standard form for the chain of custody on a piece of evidence or property. The following page contains a blank Property Custody Document utilized by the DOE-CFL that can be reproduced. All transfers of a piece of evidence should be recorded on a form of this nature. In an effort to make the completion of this document as easy as possible, the following block-by-block steps are provided:

Case Number – If a unique case number is assigned by your agency or laboratory, place the number within this block, otherwise leave blank.

Name and Title from Whom Received - The full name and title of the individual releasing the item to inquiry personnel should be placed in this block. In the event the item is seized from a common office area or crime scene the words "N/A Crime Scene" should be placed in this block.

Address and Telephone Number - Self-explanatory if received from an individual. If from a crime scene or a common office area the words "N/A Crime Scene" should be placed in this block.

Location from Where Obtained - Place the physical location where the evidence was obtained. If from an individual, the entry may be "From Jones while in room 211, Bldg

703-A, SRS, Aiken, SC 29802". From a crime scene or common office area, place the specific location within this block.

Reason Obtained - The entry "Evaluation as Evidence" or "Safekeeping" as appropriate.

Date/Time Obtained - Self-Explanatory

Item Number/Quantity/Description of Items - Items should be numbered beginning with "1" and continue until the last item. The description of items should be specific so that the piece of evidence cannot be confused with another item of property. This could include serial and model numbers or any markings placed on the property by the individual first assuming legal custody.

Chain of Custody - Item Number and Date of change of custody are self-explanatory. In the event the item was received from an individual, the first "Released By" block should contain the name and signature of this individual. In the event the item was seized from a crime scene or common office area, the entry "N/A" within the signature block and "Crime Scene" within the Name/Title block would be entered. Within the first "Received By" block, the name and signature of the first individual taking legal custody of the property should be present. The reason for this initial change of custody should be placed in the "Reason" block (normally "Evaluation as Evidence"). The written chain of custody should be continued as the items of evidence are transferred between individuals.

DEPARTMENT OF ENERGY
COMPUTER FORENSICS LABORATORY
PROPERTY AND CHAIN OF CUSTODY DOCUMENT

Case Number

Name and Title from Whom Received	Address and Telephone Number

Location from Where Obtained	Reason Obtained	Date/Time Obtained

Item #	Quantity	Description of Articles

Chain of Custody

Item #	Date	Released By	Received By	Reason
		Signature	Signature	
		Name/Title	Name Ttitle	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	

Location ______________________ Property Number ______________________

Page 2 - Evidence Property Custody Document Chain of Custody (Continued) Property Document Number ________________

Item #	Date	Released By	Received By	Reason
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	

FINAL RELEASE AUTHORITY

Item(s) ________________________ on this document pertaining to the investigation involving ____

_________________________ (is)(are) no longer required as evidence and may be disposed of as indicated below.

____

(Printed Name/Title) (Signature) (Date)

FINAL DISPOSAL ACTION

Released to Owner or Other (Name/Addess) ____

Destroyed by (describe) ____

Other (Explain) ____