Scientific Working Group on Digital Evidence

SWGDE Model Standard Operation Procedures for Computer Forensics

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the user's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived for future reference, as needed, in accordance with that organization's policies.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

SWGDE Model Standard Operation Procedures for Computer Forensics
Version: 3.0

Table of Contents

SWGDE Model Standard Operation Procedures for Computer Forensics
Version: 3.0

1. Introduction

1.1 Purpose

The purpose of this document is to create a working sample document that organizations can utilize as a template for producing their own documented Standard Operating Procedures (SOPs).

1.2 Scope

It is designed to be functional for a single person operation as well as multiple person units and laboratory organizations.

1.3 Discussion

During the development of this document, SWGDE reviewed a variety of SOPs from a broad selection of federal, state and local organizations. Organizations having a requirement to document their procedures are encouraged to use this modular sample in construction their own SOPs. It should be noted that variations of this SOP design have been successful in several currently ASCLD/LAB and FQS accredited labs.

This modular approach will enable a lab to include sections they may choose to implement (e.g. Cell Phone Analysis or Macintosh Forensics). Each module of the SOP is focused on the methodology to conduct an exam properly. It is assumed that the examiner is properly trained and competent in digital forensic analysis (see SWGDE-SWGIT Guidelines and Recommendations for Training).

Note:
The sample SOPs are examples and should not be considered as mandatory step-by-step guides. This document must be revised to reflect your organization's policies and procedures (see SWGDE Best Practices for Computer Forensics).

Any references to hardware and/or software are for illustrative purposes only and do not constitute recommendation nor endorsement.

2. Minimum Exam Standards

2.1 Purpose

This section describes an overview of the examination process.

2.2 Scope

This is information defining the structure of the examination process for the individual examiner, unit or laboratory system.

2.3 Examination Requirements

2.3.1 Equipment Preparation

Hardware and software must be configured to prevent cross contamination.

2.3.2 Examination Request

All examinations must have a request. Communicate with requestor to determine the focus and parameters of the examination. A request for forensic services will include:

1. The type of examinations requested and necessary legal authority. Attention should be paid to whether the request requires examinations by other disciplines.

2. Any known safety hazards (e.g., chemical, blood borne pathogens, etc.).

3. The identity of the party requesting the services and the date of the request.

2.3.3 Evidence Preservation

Digital evidence submitted for examination must be maintained in such a way that the integrity of the data is preserved. Evidence must be handled in a manner preventing cross contamination. If other forensic processing will be conducted, consult with examiners in the appropriate disciplines.

2.3.4 Examination

Conduct examinations pursuant to the request and additional identified exams as necessary pending appropriate legal authority. At a minimum, an examination must consist of:

1. **Visual Inspection** – Determine the type of evidence, its condition and relevant information to conduct the examination.

2. **Forensic Duplication** – Conducting an examination on the original evidence media should be avoided if possible. Examinations should be conducted on forensic duplicates or forensic image files.

3. **Media Examination** – Examination of the media should be completed in a logical and systematic manner.

4. **Evidence Return** – Exhibit(s) are returned to appropriate location.

2.4 Documentation

While documentation may vary, the following items must be included:

2.4.1 Request

The examination request must be included

2.4.2 Chain of Custody

The chain of custody must include a description of the evidence and a documented history of each evidence transfer.

2.4.3 Notes

Notes stemming from the examination shall include at a minimum:

1. Examiner communications regarding the case.
2. Review of legal authority (if necessary)
3. Procedural steps of the examination (with date(s)) in sufficient detail to allow another forensic examiner, competent in the same area of expertise, to be able to identify what has been done and to assess the findings independently.
4. If multiple examiners, initials of examiner performing procedural step.

2.4.4 Examination Report

The report is to provide the reader with all the relevant information in a clear and concise manner using standardized terminology. The examiner is responsible for reporting the results of the examination.

Reports issued by the examiner must address the requestor’s needs and contain the following items:

1. Identity of the reporting organization.
2. Case identifier or submission number.
3. Identity of the submitter.
4. Date of receipt.
5. Date of report.
6. Descriptive list of items submitted for examination.
7. Identity and signature of the examiner.
8. Description of examination.
9. Results/conclusions/derived items.

3. Tool and Technique Testing

Tools and techniques are used to analyze digital data to find evidence regarding an incident. The tool output may result in evidence to be introduced in a court trial. It is necessary to have tools and techniques that provide reliable results. The preferred tools and techniques should be independently verified. (NIST Tool Test Results and NRDFI Tool Testing)

Methods, procedures, and tools shall be validated before being used on evidence. Testing can be performed by third parties if the application used within the laboratory falls completely within the scope of the validation testing. Validation testing should be performed whenever new, revised, or reconfigured tools, techniques or procedures are introduced into the forensic process.

Testing of new technical procedures shall be accomplished using known data sets so that the expected outcome shall be known. Procedure testing shall be conducted using the standard workstations and software found in the laboratory. A testing plan shall be developed to check that the procedure is suitable for the purpose intended and produces repeatable results. If the testing does not produce the expected results, the test documentation shall be compared to the procedure tested to ensure the procedure was followed. The results of testing shall be documented in a report. The report shall include but is not limited to: test requests, data sets used, test notes, review documentation, and test reports with appropriate signatures. Test records shall be retained.

The use of tools and techniques that have yet to be tested may be employed with performance verification and documentation as a deviation from your SOP.

4. Case Prioritization

4.1 Purpose and Scope

This policy discusses how digital evidence cases are received, triaged, prioritized, and assigned for forensic analysis and/or criminal investigation.

4.2 Case Prioritization

Once a digital evidence examination request is accepted, the supervisor/lab director is responsible for prioritization. Cases will be further prioritized within their individual agency classifications. Generally, the supervisor/lab director will prioritize examination requests based upon the facts known to him/her at the time of prioritization. Digital evidence examination requests will be prioritized as follows:

NOTE: This is an example of case prioritization. Each agency/lab should establish their own examination request priority.

1. Imminent credible threat of serious bodily injury or death to persons known or unknown, including examinations of evidence necessary to further the investigation of an at-large or unknown suspect who poses an imminent threat of serious bodily injury or death to persons known or unknown.
2. Potential threat of serious bodily injury or death to person(s).
3. Sexual crimes against children.
4. Imminent credible risk of loss of or destruction to property of significant value including identity and financial theft, as well as system intrusions.
5. Immediate pending court date, or non-extendable legal deadline.
6. Potential risk of loss of or destruction to property, or exam needed to further an investigation.

4.3 Exceptions and Modifications to Case Prioritization

On a case-by-case basis, the supervisor/lab director may authorize an examination request be given priority outside of this policy.

4.4 Triage

Casework may be triaged to identify primary evidentiary items for examination and eliminate items having no evidentiary interest to an investigation. Triage may involve several methods including; review of item locations within the scene, on-site preview, lab preview, etc. (e.g., Item location within a scene can be used to determine the highest probability that the subject was using a computer, which was found in his bedroom, where a computer found in a box in his basement may have little value. Using on-site and lab preview can eliminate items not associated with the incident.)

5. Recommendation

The accompanying modules are intended to be selected to meet an organization's needs and operational focus. These modules are examples and should be edited to comply with the organization's methodology. The modules currently relate to two areas of interest: the scene and the lab.

6. Model Standard Operating Procedures

<Organization>
<Lab>

Standard Operating Procedures (SOP)

Revision X
Issue Date: mm/dd/yyyy

Standard Operating Procedures Manual
Authorization and Approval Hierarchy

This authorization and approval section is designed to outline the authorization for the use of Standard Operating Procedures (SOP) and the methods used to deviate from or implement changes to an SOP. In this document, the term Laboratory Director is used for the role of the laboratory's responsible authority.

The technical responsibility for the SOPs resides with the Laboratory Director. Annual review of SOPs shall include review of deviations. Recurrent deviations should be considered for incorporation into the affected SOP. Changes shall be documented and disseminated to affected personnel.

Approved:

Supervisor/Laboratory Director _______Signature on file________ Date: xx/xx/xx
<typed name>

Document Title	Revision Number	Issue Date
Onsite/Scene Based Procedures		
Scene Module 1: Evidence Preservation: Crime Scene / Field Response	1	xx/xx/xx
Scene Module 2: Live Memory Imaging and Analysis	1	xx/xx/xx
Scene Module 3: Onsite Imaging and Preview	1	xx/xx/xx
Scene Module 4: Mobile Device Collection	1	xx/xx/xx
Laboratory Based Procedures		
Lab Module 1: Exam Preparation: Workstation	1	xx/xx/xx
Lab Module 2: Physical Inspection	1	xx/xx/xx
Lab Module 3: Write Protecting Media	1	xx/xx/xx
Lab Module 4: Wiping Media	1	xx/xx/xx
Lab Module 5: Hard Drive Removal and BIOS Check	1	xx/xx/xx
Lab Module 6: Hard Drive Imaging Protocol Using Windows	1	xx/xx/xx
Lab Module 7: Imaging Protocol Using Linux	1	xx/xx/xx
Lab Module 8: Imaging a Macintosh Computer	1	xx/xx/xx
Lab Module 9: Cable Acquisition Protocol	1	xx/xx/xx
Lab Module 10: Handheld/Mobile Devices	1	xx/xx/xx
Lab Module 11: Examination and Analysis	1	xx/xx/xx
Lab Module 12: Image Restoration	1	xx/xx/xx

Scene Module 1: Evidence Preservation: Crime Scene / Field Response

Purpose:
The purpose of this procedure is to secure digital evidence located at a non-laboratory location to preserve its integrity for further forensic processing.

Scope:
This SOP describes procedures to follow when providing digital forensics assistance at non-laboratory locations.

Equipment:

- A digital forensics field response kit may contain some of the following:
    1. Digital camera
    2. Sterilized removable media
    3. Forensic computer
    4. Hardware write-blocking devices
    5. Forensically sound boot disks
    6. Mobile device acquisition tools
    7. Tool kit (screw drivers, etc.)
    8. Evidence packaging materials

Definitions:

- **Handheld Digital Devices** – Portable devices that have digital storage, network connectivity (see SWGDE-SWGIT Glossary).
- **Removable Media** – digital storage media such as: CDs, DVDs, Zip disks, Jazz disks, floppy disks, external hard drives, memory cards, thumb drives, SIM cards, etc.

Limitations:

- **Computers:**
    a. Networked:
        1. Unplugging a suspect computer from a network may cause data loss and could potentially damage other computers on the network.
        2. Computer networks can be technically complex and may prevent collection of evidence in a timely manner. *Note: If the system administrator is a suspect in the case, assistance should be sought from personnel knowledgeable in the network's operation.*

    b. Non-networked:
        1. Powering down a suspect's computer may cause data loss and potentially damage the operating system.
        2. While securing the computer, if the analyst believes that evidence may be destroyed or manipulated, the computer should be forcibly shut down.
- **Removable Media:**

1. Most removable media is very small and often hard to locate and is often overlooked.
2. Thumb drives may be obfuscated to thwart detection.
3. Some removable media is susceptible to immediate physical destruction.

- **Handheld Digital Devices:**
    1. Active devices are susceptible to data destruction due to network communication.
    2. Mobile devices may lose data or initiate additional security measures once discharged or shut down.
    3. Blocking RF signals: may drain the battery, may be expensive, are not always successful and may result in the alteration of data.
    4. Some components and devices are susceptible to immediate physical destruction and should be physically secured.
    5. A device may be protected with a password, PIN, token or other authentication mechanism, the suspect may be queried for this information during the initial interview.

Procedures:

These procedures should be adapted as necessary based upon the situation.

- **General:**
    1. Ensure the safety of all individuals at the scene.
    2. Protect the integrity of evidence.
    3. Evaluate the scene and formulate a search plan.
    4. Identify potential evidence.
    5. All potential evidence should be secured, documented, and/or photographed.
    6. Conduct interviews.
    7. Any item to be removed from the scene should be properly packaged and secured.
- **Computers:**
    1. The scene should be searched to determine if any wireless networks or networking devices exist.
    2. If the evidence computer or device is connected to a network:
        a. Assistance should be sought from the system administrator in isolating the computer or device from the network, presuming the administrator is not a suspect in the case. *Note: If the system administrator is a suspect in the case, assistance should be sought from personnel knowledgeable in the network's operation.*
        b. Isolate and remove the evidence computer or device from the network immediately.
    3. Document the location and condition of all computers and/or devices.
    4. Document and preserve any open file(s) on the computer.
    5. Capture live memory (see Live Capture SOP Module).

    6. Document all connections to the computer.
    7. Shutdown procedures.
        a. Pull the plug from the back of the computer, or when necessary normal shutdown procedures should be utilized. When forcibly shutting down a computer, the plug should be pulled from the back of the unit, not from the outlet.
        b. For laptops you must either push the power button until the system shuts off or remove the battery.
        c. Do not unplug an Uninterruptable Power Supply (UPS) backup unit to cut power to a computer, because the battery in the UPS could power the computer long enough to complete any destructive processes.
    8. Search the scene for passwords, account numbers, or other pertinent information.

- **Removable Media:**
    1. Document the location and condition of all removable media.
    2. Remove any connected external media (e.g. external drives or thumb drives) after the computer has been powered down.
- **Handheld Digital Devices:**
    1. Document the location and condition of all handheld digital devices including on-screen data.
    2. If possible, physically remove the battery from the device, otherwise power off the device in the appropriate manner.
    3. Search the scene for removable media, passwords, or other pertinent information.

References:

1. Electronic Crime Scene Investigation: A Guide for First Responders, US Dept. of Justice, NCJ187736, July 2001, URL: http://www.ncjrs.org/pdffiles1/nij/187736.pdf

2. Guidelines on Cell Phone Forensics, NIST Special Publication 800-101, May 2007, URL: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

3. Best Practices for Mobile Phone Examinations, SWGDE, May 2009, URL: https://www.swgde.org/pdf/Current%20Documents/5c180858-0785-3bea-aaad-c02477886dc56.pdf

4. Best Practices For Seizing Electronic Evidence v.3: A Pocket Guide for First Responders, US Secret Service, October 2006, URL: http://www.forwardedge2.usss.gov/pdf/bestPractices.pdf

Scene Module 2: Live Memory Imaging and Analysis

Purpose:
The purpose of this procedure is to describe the steps to acquire data stored in Random Access Memory (RAM).

Scope:
This procedure shall be followed when the acquisition of RAM is desired.

Equipment:

- Removable media (USB thumb drive or USB hard drive)
- Memory acquisition software for the target operating system (e.g., "Win32dd.exe" for a Windows operating system or other approved software)
- Memory acquisition software user manual or documentation

Limitations:

- Inserting USB drives will change the configuration files of the operating system of the subject computer.
- Running a computer program will cause a portion of RAM to be overwritten. Sacrificing a small portion of RAM by running a memory-capturing tool may potentially yield several gigabytes of data stored in RAM that would not otherwise be recoverable.
- Due to the dynamic nature of RAM, authentication of acquired memory is not possible.

Procedure:

1. Determine amount of RAM in the subject computer.
2. Wipe and format removable media larger than the amount of RAM in the subject computer.
3. Copy "Win32dd.exe", or other approved software, to the removable media.
4. Insert the prepared removable media into the subject computer and run the memory acquisition software in accordance with the software's user documentation.
5. Safely eject the USB drive from the subject computer.

References:

1. Memory acquisition software user documentation

Scene Module 3: Imaging and Preview

Purpose:
The purpose of this procedure is to describe the steps for previewing and imaging computers and digital media on-scene.

Scope:
This procedure shall be followed when previewing and imaging computers and digital media on-scene.

Equipment:

- Linux boot media with preview/imaging software (Helix, SPADA, Knoppix, etc.)
- Forensic computer
- Windows preview/imaging software (FTK Imager, EnCase, etc.)
- Hardware write blocker for various hard drive interfaces (EIDE, SATA, SCSI, etc.)
- Wiped and formatted "destination" hard drive if imaging using evidence files (.E01 files)
- Wiped "destination" hard drive if imaging using a RAW data dump (forensic clone of drive)

Limitations:

- Failure to control the boot order of the computer may result in unintentional writes to the computer's hard drive.
- Laptop drives may require special hard drive interface adapters.
- Hard drive removal from a computer may not be easily accomplished.
- Previewing data on hard drives should be used for triage and not as an alternative to a full forensic examination.
- The quantity of data and the time to process digital media can be limiting factors.

Procedures:

- **Linux preview:**
  1. Ensure the boot order of the subject computer is set to boot to the Linux media.
  2. Boot the subject computer to the Linux media and preview the computer's hard drive for evidence related to the case.
  3. Document the findings of the preview.
- **Linux imaging:**
  1. Ensure the boot order of the subject computer is set to boot to the Linux media.
  2. Boot the subject computer to the Linux CD.
  3. Image the computer's hard drive to the destination drive.

4. Verify and document the integrity of the image file(s) by comparing the acquisition and verification hash values.

- **Windows preview:**
    1. Remove the hard drive from the subject computer.
    2. Attach the subject hard drive to the appropriate hardware write blocker.
    3. Attach the write blocker to the forensic computer.
    4. Boot the forensic computer and run the Windows preview/imaging software.
    5. Preview the computer's hard drive for evidence related to the case.
    6. Document the findings of the preview.
- **Windows imaging:**
    1. Remove the hard drive from the subject computer.
    2. Attach the subject hard drive to the appropriate hardware write blocker.
    3. Attach the write blocker to the forensic computer.
    4. Boot the forensic computer and run the Windows preview/imaging software.
    5. Image the computer's hard drive to the destination drive.
    6. Verify and document the integrity of the image file(s) by comparing the acquisition and verification hash values.

References:

1. Preview/Imaging software user manual

2. Hardware write blocker user manual

Scene Module 4: Mobile Device Collection

Purpose:
The purpose of this procedure is to describe the steps to collect mobile devices.

Scope:
This procedure shall be followed when collecting mobile devices on-scene.

Equipment:

- RF shielding device (e.g. Faraday bag, etc.)
- Shielded power cable for mobile device

Limitations:

- Placing a mobile device in an RF shield may cause the mobile device to increase its transmit power in a search for a cell tower signal.
- Removing power from a mobile device may prevent the extraction of data from the device without the PIN or pass code.

Procedure:

1. Physically secure the mobile device.
2. Perform any other forensic examinations (biological testing, fingerprints, DNA, etc.).
3. Block the mobile device from receiving RF signals by placing the phone in Airplane mode or using an RF shielding device.
4. Turn off the mobile device if unable to block the RF signals.
5. Submit the mobile device for examination as quickly as possible.
6. Remove the battery from the mobile device, if possible, if storing it for an extended time. This will prevent the battery from corroding the inside of the mobile device.

References:

1. User manual for the mobile device

Lab Module 1: Exam Preparation: Workstation

Purpose:
The purpose of this procedure is to prepare workstation system drives used in forensic casework to a default state in order to ensure that no cross contamination occurs between cases.

Scope:
This procedure applies to personnel who prepare workstation system drives used in forensic examinations.

Equipment:

- Forensic Workstation
- Software for creating and restoring system images
- System Image

Definitions:

- **System Drive** – the drive that contains the operating system (OS).
- **System Image** – factory default or user created image of the drive that is used to restore the hard drive(s) on the forensic workstation.

Limitations:
Failure to sanitize the information from a previously used hard drive can lead to potential contamination of a new case.

Procedure:

1. If a previously created system image is available, skip to step 5.
2. If no previously created system image is available use the original system restoration discs.
3. Install necessary software and configure the new system.
4. Use a backup utility to create the image of the system.
5. Restore the system drive using the prepared system image.

References:
None

Lab Module 2: Physical Inspection

Purpose:
The purpose of this procedure is to properly catalogue and document the condition of digital evidence.

Scope:
This procedure applies to all submitted digital evidence.

Equipment:

- Tool kit (screw driver, etc.)
- Camera.

Limitations:

- Some manufacturers of computers have mechanisms that alert the user the computer case has been opened.

Procedure:
It is recommended that the examiner become familiar with computers or devices before taking the following steps.

1. Assess the potential for a destructive device, biological contaminant or hazardous material and take appropriate action.
2. Photograph evidence items if necessary.
3. Label submitted evidentiary items in accordance with quality assurance manual.
4. If applicable, remove the cover from the case in order to:
    a. Locate and identify internal components.
    b. Document serial/model numbers if necessary.
    c. Check power leads and cabling and document abnormalities.
5. Upon completion of the hardware examination, replace the cover and secure the case, if applicable.

References:

1. See user manuals for specific software and hardware.

2. Quality Assurance Manual: Practices for Evidence Control.

Lab Module 3: Write Protecting Media

Purpose:
The purpose of this procedure is to preserve the integrity of the evidence during examination by preventing alterations.

Scope:
This procedure applies, when possible, to all digital storage media and/or devices that have been submitted for examination.

Equipment:

- **Hardware:**
  a. Write protection hardware
  b. Internal or external hard drive
  c. Removable media (e.g., flash media, floppy disk or tapes)
- **Software:**
  a. Write protection software utilities
  b. Hard Disk Write Lock (HDL RCMP Tool)
  c. Forensic boot CD
  d. Write Blocker XP/2K (ACESLE Tools)
  e. Unix/Linux command mount -r (Read only: all Unix/Linux recognized file systems)

Limitations:

- **General:**
  a. Write protection software may not protect against programs using direct access writes to media.
  b. Write protection software in a network/RAID environment may not be applicable.
- **Specific:**
  a. **Write Blocker XP**: Not recommended for use with USB floppy drives or USB CD/DVD writers.
  b. **Unix/Linux Command mount –r:** Only effective for the file system(s) mounted as read only. Will not provide protection at the device level. May not mount all file systems. May not provide full protection when mounting a journaled file system.
  c. **IDE Jazz and Zip drives**: None of the write protection hardware above has been verified to effectively write protect this type of media.

Procedures:
Original evidence must be write-protected when possible. Built-in write protection mechanisms must be utilized whenever available to complement hardware and software write protection. If write protection is not possible, this must be documented.

- For hard disk drives and solid-state storage devices (e.g. USB thumb drives, memory or flash cards) the following two methods can be used together or separately:
  a. Follow the manufacturer's instructions when using a hardware write-protect device.
  b. Use the appropriate operating system or boot media when using software write-protection. If write protection software was not started during the boot process, initiate write protection software prior to attaching the media.
- For Iomega Zip and Jazz disks:
  a. Iomega Zip and Jazz disks utilize a proprietary software utility that changes a storage location on the media to indicate a write protected or "read only" state. Use the appropriate OS version of Iomega Tools to make the disk read only. Whenever possible, use software write protection.

References:

1. See user manuals for listed software and hardware.

Lab Module 4: Wiping Media

Purpose:
The purpose of this procedure is to overwrite all data on media (commonly known as "wiping"). Wiping is used to sanitize target media prior to the examination process and ensures that no cross-contamination occurs between cases.

Scope:
This procedure applies to media authorized to be wiped.

Equipment:

- Forensic Workstation or other hardware wiping device
- Wiping Software
- Digital Media

Limitations:
None

Procedure:

1. Connect the target media to the forensic workstation or hardware wiping device.
2. Use wiping software or device to overwrite all sectors of the hard drive.
3. Ensure media is successfully wiped prior to use for examination purposes.

References:

1. See user manuals for wiping software and hardware.

Lab Module 5: Hard Drive Removal and BIOS Check

Purpose:
The purpose of this procedure is to describe the steps to remove the hard drive(s) from computers submitted for examination and checking the BIOS settings.

Scope:
This procedure shall be followed when the removal of a hard drive is required.

Equipment:

- Tool kit (screw driver, etc.)
- Digital camera

Limitations:

- Removing hard drives from some devices may not be an option.
- The hard drives removed from laptop computers can be imaged using the same procedures as those removed from desktop computers. An adapter may be necessary to connect a laptop hard drive to the forensic workstation.
- Some laptop hard drive/motherboard combinations may have security devices that do not allow them to be accessed outside of the laptop computer. Image these computers using a cable acquisition procedure or by booting the laptop using a forensic operating system environment.
- On some older or proprietary BIOS/CMOS chips, a setup disk (floppy) provided by the manufacturer is needed to access the BIOS.
- On some systems, accessing BIOS with the drives disconnected may change the boot sequence.
- Access to BIOS/CMOS can be protected by a password. Some manufacturers can provide a master password.
- Precautions should be used to guard against electrostatic discharges.

Procedure:

1. Open the case on the computer and photograph the hard drive(s) of the computer.
2. Mark the power cords and data ribbons/connectors connecting the hard drive to the evidence computer.
3. Remove the hard drive(s) from the evidence computer.
4. Label the hard drive(s) removed from the evidence computer with appropriate case information.
5. Document the drive information such as make, model, serial number, capacity, etc.
6. With all hard drives removed, boot the evidence computer into the BIOS and document the BIOS and actual date/time.

References:
None

Lab Module 6: Hard Drive Imaging Protocol Using Windows

Purpose:
The purpose of this procedure is to use a Microsoft Windows operating system to create a forensically sound image of evidence hard drives.

Scope:
This is the procedure to be utilized by all personnel who image digital evidence while using the Microsoft Windows operating systems.

Equipment:

- Forensic workstation.
- Prepared target media.
- Validated forensic imaging hardware or software.

Limitation:
There may be instances when an evidence hard drive cannot be forensically imaged. In these instances, attempts to properly image the hard drive must be completely documented.

Procedure:

1. Attach the evidence hard drive to the forensic workstation using a write-blocking device.
2. Boot the forensic workstation into the Windows OS.
3. Obtain a hash value of the evidence item before imaging.
4. Image the evidence to the target drive using imaging software.
5. Remove the evidence hard drive from the forensic workstation.
6. Verify and document the integrity of the image file(s) by comparing the acquisition and verification hash values.

References:
None

Lab Module 7: Imaging Protocol Using Linux

Purpose:
The purpose of this procedure is to use a Linux operating system to create a forensic image of evidence items without altering the data.

Scope:
This procedure describes the steps to image digital evidence using Linux.

Equipment:

- Forensic workstation
- Prepared target media
- Bootable Linux operating system
- Software for forensic imaging

Definitions:

- **Forensic OS drive** – Hard drive containing the operating system and all of the forensic software that will be used in the examination.
- **Forensically Sound Linux Operating System** – A bootable Linux operating system that runs entirely in the computer's memory and has been specifically modified to mount all devices connected to the system in a read-only state (e.g. Helix, Knoppix, etc.).
- **MD5 hash** – A 128 bit number that uniquely describes the contents of a file or hard drive. This is the standard hash value used in computer forensics.
- **Target Media** – The media that will be used in casework to receive forensic images upon and upon which the processing of casework may be performed.

Limitations:
The examiner must be aware of the Linux mounting process. Linux operating systems must be tested to ensure all devices are mounted in a read-only state before use.

Procedures:

- **Using a Linux Boot disc in an evidence computer:**
  1. Boot the computer into its BIOS setup program.
  2. Set the boot order to allow the Linux media to load first.
  3. Insert the forensically sound Linux operating system (CD/USB device, etc.) and boot the evidence computer.
- **Using a Linux workstation:**
  1. Boot the forensic workstation into the Linux OS.
  2. Attach the evidence media to the forensic workstation.
- **Image with Linux:**
  1. Obtain a hash value of the evidence item before imaging.
  2. Attach target media and allow read and write permissions.
  3. Image the evidence to the target media using imaging software.

4. Remove the evidence hard drive.
5. Verify and document the integrity of the image file(s) by comparing the acquisition and verification hash values.

References:

1. Linux Desk Reference

2. Quality Manual

Lab Module 8: Imaging a Macintosh Computer

Purpose:
The purpose of this procedure is to properly create a forensic image of a device running the Apple Macintosh operating system without altering the data. This procedure covers imaging of Macs when the hard drive can be removed, as well as in situations when the hard drive cannot be removed.

Scope:
This procedure applies to Macintosh computers.

Equipment:

- **Hardware**
    a. Forensic Tower, Laptop, Portable Forensic Workstation, or Macintosh laptop specifically used for Mac forensics analysis
    b. Prepared external target drive
- **Software (approved and appropriate version)**
    a. Forensically sound, bootable CD for Power PC-based Macintosh hardware
    b. Forensically sound, bootable CD for Intel-based Macintosh hardware

Definitions:

- **FireWire Target Disk Mode** – FireWire Target Disk Mode allows a Mac system to act as if the entire computer were an external FireWire hard drive for another system. This mode works at the firmware level before the operating system is engaged and booted. It is entered by holding down the "T" key on the Mac system during the boot process.
- **Forensically sound, bootable CD for Power PC Macintosh hardware** – A forensically sound, bootable CD for Power PC Macintosh hardware is a Linux operating system variant on a CD that has been specially constructed for forensic examination of live Macintosh systems that have the Power PC processor chips. The CD is forensically sound due to the fact that all media on the system is placed in read-only mode.
- **Forensically sound, bootable CD for Intel-based Macintosh hardware** – A forensically sound, bootable CD for Intel-based Macintosh hardware is a Linux operating system variant on a CD that has been specially constructed for forensic examination of live Macintosh systems that have the Intel processor chips. The CD is forensically sound due to the fact that all media on the system is placed in read-only mode.
- **fstab –** fstab is a configuration file that contains information for all of the partitions and storage devices in a Linux-based computer. fstab contains information concerning how and where the partitions and storage devices in a Linux-based system should be mounted.
- **HFS** – Hierarchical File System (HFS) is a file system developed by Apple for use in computers running Mac OS. HFS is also referred to as Mac OS Standard.

- **HFS+** – HFS Plus or HFS+ is a file system developed by Apple to replace their Hierarchical File System (HFS) as the primary file system used in Macintosh computers (or other systems running Mac OS). HFS Plus is an improved version of HFS, supporting much larger files (block addresses are 32-bit length instead of 16-bit) and using Unicode for naming the file items. HFS Plus also uses a full 32-bit allocation mapping table, rather than HFS's 16 bits. HFS Plus is also referred to as Mac OS Extended.
- **MD5 hash** – A 128 bit number that uniquely describes the contents of a file or hard drive. This is the standard hash value used in computer forensics.
- **Target Drive** – The hard drive that will be used in casework to receive forensic images upon and upon which the processing of casework may be performed.

Limitations:

- **Macintosh Computers:**
  a. Be sure to plug in a power cable to any MacBook or other Macintosh laptop to be previewed. Do not allow a laptop to run on battery power during a preview or acquisition if the appropriate AC power cord is available.
  b. If an Intel based Macintosh in dual boot firewire mode is attached to a Windows system, the Windows partition, if present, will be mounted.
  c. If an open firmware password is enabled, it will not be able to be accessed while the HDD is connected to that computer.
  d. An Intel based Macintosh does not have open firmware; the only way to determine if there is a boot password is to boot with the "option" key depressed.
  e. If you are using another Mac as the examination platform, make sure that you turn off DiskArbitration otherwise there may be inadvertent writes to the evidence Mac system.
- **Linux Boot CD:**
  a. Will only work with an Intel based Macintosh.
- **Windows Computers:**
  a. NEVER use a Microsoft Windows operating system to preview or image a live Macintosh system. Microsoft operating systems "touch" drives during the boot sequence and hence modify the data of the evidence computer.

Procedures:

Macintosh computers that have an open firmware password enabled will prevent booting with external media and target disk mode from working properly. The examiner must then remove the hard drive for imaging or be able to obtain or defeat the open-firmware password on the evidence computer.

- **Booting using external media:**
  Note: If using external media with OS X, disable auto-mounting or disk arbitration.

1. Verify that computer is powered off.
2. Insert a boot disc in the evidence computer. Attach wiped and formatted media to the evidence computer to store the forensic image.
3. While holding down the appropriate key(s), boot the evidence computer.
4. Observe the bootable external media device and display screen carefully to make sure that system is accessing the boot media. If there are no indications that the computer is accessing the boot media, turn off power to the computer immediately.
5. When the forensically sound Linux environment has fully loaded, open up a terminal session.
6. Navigate to the /etc directory.
7. Edit the fstab file using "vi" or another text editor. Navigate to the entry in the fstab file that corresponds to the HFS partition on the evidence computer's hard drive and change the partition type from "hfs" to "hfsplus".
8. If there is a need to copy data off of the evidence computer during the preview, the target drive must be mounted as read/write in the fstab file by changing the "ro" characteristic (Read-Only) to "rw" (Read-Write). Be cautious to ensure that only the target drive is mounted as Read-Write.
9. Save the changes to the fstab file and close the terminal session. The changes to the fstab file allow the forensically sound Linux environment to properly read the file system on newer Macintosh systems while remaining in a read-only state. Because this file remains in the active memory of the computer it remains forensically sound and does not "touch" the suspect computer.
10. If using the GUI, click once on the Mac hard drive icon to mount the drive. Repeat this process for the target drive (if used) to mount the target drive. If using the command line, mount both the suspect drive and the target drive.
11. Use a hashing program to obtain the MD5 hash value of the evidence item before imaging.
12. Image the evidence computer to the target drive.
13. If the examiner desires to analyze the data from the evidence computer in the native (Mac) format then the image file must be saved in raw/DD format as a single file.
14. Verify the forensic image was successfully completed.
15. Shut down the evidence and forensic computers and disconnect the Firewire cable.

- **Target Disk Mode:**
    1. Boot the evidence computer while holding down the "Option" key until the selection dialog is presented. If the evidence computer presents a lock icon and a password dialog box (Figure 1), there is a firmware password in place and the drive cannot be imaged without the password. If icons for

bootable partitions are visible, then there is no firmware password and the drive may be imaged.

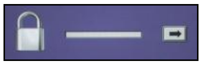

Figure 1

2. If no firmware password is installed, reboot the evidence computer while holding down the "T" key until a FireWire logo is displayed (Figure 2). Selecting this boot option will place the evidence computer into Target Disk mode.

Figure 2

3. Attach the evidence computer to the forensic computer via a Firewire connection.
4. Boot the forensic computer into a forensically sound operating system environment. If using a Windows computer, the forensic computer must be booted with a forensically sound Linux variant. If using a forensic Mac computer, the examiner must mount the evidence computer in read-only mode. Disk Arbitration must be turned off in the forensic computer.
5. Use an hashing program to obtain the MD5 hash value of the evidence item before imaging.
6. Make a forensic image of the evidence computer onto the target drive. A single disk image file (raw or DD format) must be used to view Mac data natively.
7. Verify the forensic image was successfully completed.
8. Shut down the evidence and forensic computers and disconnect the Firewire cable.

- **Removing HDD from the evidence computer:**
    1. Remove the hard drive or drives from the evidence computer and image.
    2. If the examiner desires to analyze the data from the evidence computer in the native (Mac) format then the image file must be saved in raw/DD format as a single file.

References

(In progress)

Lab Module 9: Cable Acquisition Protocol

Purpose:
This procedure describes the steps to be taken in obtaining a forensic image using a network crossover cable. The purpose of this procedure is to forensically image an evidence hard drive still installed in the evidence computer when the evidence hard drive is impossible to remove. This protocol provides a procedure for imaging these evidence hard drives without making changes to the data on the evidence drives.

Scope:
This procedure applies to computers that have been submitted for examination.

Equipment:

- **Hardware**
  a. Forensic computer
  b. Network crossover cable or parallel (laplink) cable
  c. Wiped and formatted target media
- **Software**
  a. Forensic software

Limitations:

- **General**
  a. Media that has sustained physical or mechanical damage and/or electronic failure may not successfully or completely image.
  b. Examiners should note that in order to use a network crossover cable, the evidence computer must be equipped with a network interface card, and the forensic boot disk must contain the DOS drivers for that network interface card.

Procedure:
This procedure requires the use of a forensic tool that can function in a DOS or Linux environment. (Examples include, but are not limited to, EnCase, LinEn, Raptor, and SPADA.)

1. The evidence computer's BIOS/CMOS settings should be checked in a way that will not access or boot the installed evidence hard drive. During this process, the evidence hard drive can be removed from the evidence computer, or the power cable and data cable can be removed from the evidence hard drive.
2. Check the BIOS/CMOS settings to be sure that the evidence computer will boot from attached removable media devices, changing if necessary. This may not be possible or obvious as some computers do not display the required key(s) or may require a proprietary disk utility to gain access to the BIOS/CMOS. If the BIOS/CMOS cannot be accessed, the examiner should perform research on a way to access the BIOS/CMOS (i.e., reference materials, contacting the manufacturer, etc.).

3. Disable any power-saving features in the BIOS, as available.
4. Once the BIOS/CMOS settings have been checked and changed, as necessary, turn off the evidence computer and reconnect the evidence hard drive to the evidence computer..
5. Prepare a hard drive for storage of the forensic image and install it in/connect it to the forensic computer.
6. Set up the evidence computer in server mode by booting into DOS/Linux using a forensic tool that allows this (for example, EnCase, SPADA, LinEn, etc.). Server mode is the mode that the evidence computer is put into to enable it to send data to a forensic computer in a forensically safe manner for imaging. Always set up the evidence computer in server mode first before setting up the forensic computer.
7. Connect the evidence computer and forensic computer using a network crossover cable between the network interface cards, or connect the laplink cable from the parallel port of the evidence computer to the parallel port of the forensic computer (running through the dongle if a parallel port dongle is required).
8. Once the evidence computer has booted, run the forensic utility on the evidence computer according to the tool's instructions.
9. Set up the forensic computer in client mode by booting the forensic computer into DOS/Linux. Client mode is the DOS/Linux mode that the forensic computer is put into to enable it to receive data from an evidence computer in a forensically safe manner for imaging.
10. Prior to imaging the evidence hard drive, use a hashing program to obtain the MD5 hash value of the evidence drive.
11. When imaging is complete, follow the prompts to terminate the server/client mode and power down the evidence computer.

Lab Module 10: Handheld/Mobile Devices

Purpose:
This procedure may be used for examinations of Handheld/Mobile Devices to extract and/or recover data that may have value as evidence in criminal investigations. The purpose of these procedures is to establish a basic methodology for personnel conducting examinations of Handheld/Mobile Devices. The primary reason for the establishment of these standards is to ensure the techniques used conform to common industry practices.

Scope:
This document applies to the forensic examination/data extraction of Handheld/Mobile Devices, which may include mobile phones, personal digital assistants (PDA) and Global Positioning System (GPS) devices.

Equipment:

- Forensic Computer Workstation
- Forensic Analysis Software
- RF shielding
- Hardware Extraction Devices
- Hardware/Software Write-blockers
- SIM card reader
- Appropriate charging cables and universal battery charging kit
- Data cables or cradles
- Manufacturer & 3rd Party software
- Blank and/or Sterile Media (HD/CD/DVD or other removable devices)
- Digital camera and camcorder

Definitions:

- **Chip-Off** – A process that involves the removal of a memory chip to conduct analysis.
- **Code-Division Multiple Access (CDMA)** – The mobile phones using this cellular system do not incorporate a SIM card, and the device's assigned phone number is stored on the mobile phone.
- **GPS Device** – A device utilizing the worldwide satellite navigational system formed by 24 satellites orbiting the earth and their corresponding receivers on the earth. These devices come in a variety of styles which may include vehicle-mounted, portable, handheld, and wristband.
- **Global System for Mobile Communications (GSM)** – The mobile phones using this cellular system utilize a Subscriber Identity Module (SIM) card to store carrier specific information and some user information such as text (SMS) messages, call history and phonebook information. The mobile phones utilizing GSM do not store the device's assigned phone number.

- **Hex Dump** – A process that provides a physical acquisition of a mobile phone's file system. This may provide access to deleted data that has not been overwritten.
- **Logical** – A process that provides access to the user accessible files. This process will not provide access to deleted data.
- **Manual** – A process that involves manually using the keypad and handset display to document data present in the mobile phone's internal memory.
- **MicroRead** – A process that involves the use of a high-power microscope to provide a physical view of the electronic circuitry of memory. This would typically be used when acquiring data from physically damaged memory chips.
- **Mobile phones** – This category includes both the traditional cellular phones and smartphones. Cellular phones can provide voice communications, Short Message Service (SMS), Multimedia Message Service (MMS), and newer phones may also provide Internet services such as Web browsing, instant messaging capabilities and e-mail. Smartphones are a combination of cellular phones and PDA's, which allow users to store information, e-mail, and install programs, along with using a mobile phone in one device.
- **PDA** – Traditionally designed to be a personal organizer, but may include other features such as web browsing.

Limitations:

- Mobile phones present a unique challenge to examiners due to rapid changes in technology. There are numerous models of mobile phones in use today. New families of mobile phones are typically manufactured every three to six months. Many of these phones use closed operating systems and proprietary interfaces making it difficult for the forensic extraction of digital evidence.
- Some software tools do not capture all of the data in a device. This limitation may be identified through comparison of user records displayed on the device with records extracted by the tool.

Procedure:

1. Conduct examination pursuant to the request of the submitter and within the search authorization/warrant or consent to search limitations and/or scope.
    a. If possible, determine make and model of the device and acquire the user manual. Research the user manual before removing the battery and/or powering on device to ensure proper handling. Charge the device when required to prevent data loss.
    b. Remove any media storage, such as a memory or SIM card,process separately. Protect device from external signals by placing in Faraday bag (or other approved device) before powering on. If airplane mode is available, engage immediately. Turn any wireless communication features off if the option is available.
    c. Determine software/hardware that supports data extraction from the device and SIM. Extract data using software tested and authorized for use.

d. Extracted data is verified by manually reviewing data on the device. Any deviations must be documented.

References:

- Owner’s Manuals
- User’s Manuals
- Software manuals for specific equipment and operating instructions

Lab Module 11: Examination and Analysis

Purpose:
This procedure pertains to the extraction and/or recovery of data from digital media that may have evidentiary value in criminal investigations.

Scope:
This procedure applies to the examination and analysis of a forensic duplicate (image) or write protected digital media. The request, case specifics and search authority will determine which techniques are used during the examination.

Equipment:

- **Hardware:**
    a. Forensic computer
- **Software:**
    a. Forensic software

Limitations:

- Results are dependent on a tool's capabilities and limitations (refer to NIST CFTT test results).

Procedure:
Procedural steps of the examination shall be documented in sufficient detail to allow another forensic examiner, competent in the same area of expertise, to be able to identify what has been done and to assess the findings independently.

1. Recover Data
    a. Identify deleted or hidden partitions, folders, and/or files
    b. Decompress files
    c. Recover/bypass passwords and encryption
    d. Identify file signatures and file headers
    e. Carve data from unallocated space, unused space, or file slack
    f. Extract Internet history
2. Conduct Searches
    a. Conduct keyword/text string and/or regular expression searches
    b. Use hash databases to include or exclude known data
    c. Detect malware programs or artifacts
    d. Detect evidence of system compromise
    e. Detect counter/anti-forensic programs or artifacts
3. Identification and Analysis
    a. Image restoration (see Module 12)
    b. Conduct registry analysis
    c. Identify user accounts
    d. Analyze communications (email, chat messages, instant/private messaging, newsgroups)

e. Analyze document files (text files, spreadsheets, databases, presentations)
f. Analyze graphics and multimedia files
g. Analyze program files
h. Conduct timeline analysis

References:
None

Lab Module 12: Image Restoration

Purpose:
The purpose of this procedure is to restore media to observe it in its native state.

Scope:
This procedure applies to the restoration of a forensic duplicate (image).

Equipment:

- **Hardware**
  a. Forensic computer
  b. Subject computer
  c. Target drive
- **Software**
  a. Forensic software
  b. Restoration software
  c. Virtualization software (VMWare)
  d. Forensic duplicate (image)

Limitations:

- Hardware configuration may prevent access to restored media.
- Only the logical file system will be accessible.
- Licensing may be required to load an operating system properly.
- Virtualization utilities may be needed for a successful boot process.

Procedures:

- **Restoration**
  At times it may be necessary to view the evidence in its native state. It is acceptable to restore the evidence media using a forensically prepared media of the same storage capacity. Restored media can then be inserted into the original device and used to boot the hardware.
  1. Connect forensically prepared target drive to the workstation.
  2. Open forensic image in restoration software.
  3. Clone (dd) or restore (forensic compressed file e.g., .E01, .AFF, etc.) all files of a forensic image. Document the method used.
  4. Determine the hash value of the restored image and compare it to the hash value of the original evidence item, for verification if applicable.
- **Virtualization**
  Another option is to utilize virtual imaging technology to spawn a virtual computer using the forensic image of the computer as the basis for the virtual machine. This will allow the examiner to examine the suspect's computer in a virtual environment that simulates the "users" computer in its native state.
- **Locally/Virtually attached drive**

1. Mount a forensic clone or forensic image files as a virtual drive on the forensic machine (EnCase or FTK Imager will allow this).
2. Run Virtual Machine software.
3. Attach the virtual drive to the virtual machine.
4. Boot a virtual image of the computer in the virtual machine software.

- **Live View**
    1. Make a DD image of the subject’s hard drive.
    2. Open Live View and create a virtual machine using the DD image.
    3. Save the virtual machine to the analysis machine.
    4. Boot the virtual machine in the virtualization software.

History
Model Standard Operation Procedures for Computer Forensics

Revision	Issue Date	Section	History
1.0	01/14/2011	All	Creation
2.0	06/17/2011	Modules	Addition of SOP Lab Modules through Module 12
3.0	06/06/2012	All	Formatting and initial publication as Public Draft
3.0	09/13/2012	All	Voted to publish as Approved document, no changes made