THE NEOTIA UNIVERSITY

Computer Science & Engineering

Digital Forensic Lab Manual

4th year, Semester – VII

1. Digital Forensic Laboratory Section Guidelines

1.1. Purpose

The procedures in this manual apply to examiners of the Digital Forensic Laboratory (DFL) when providing forensic services to customers. It is recognized that the digital data collection, recovery, and analysis field changes frequently therefore preventing the establishment of a rigid set of procedures to cover each and every case. This requires examiners to use their ingenuity, training, and experience to meet the requirements of the customers. These procedures establish the baseline for reliable technical services and are not intended to limit examiner's ingenuity when providing services to meet the customer's requirements.

When a technical procedure is dependent upon the use of a particular type of software and/or hardware, the step-by-step instructions on how to use the software/equipment or perform the analysis will not be included within the procedure. If vendor instructions are not sufficiently detailed, then additional instructions will be included in written procedures. User manuals will be available online, on the DFL internal server, or located in the proximity of forensic equipment.

There may be instances in which time-sensitive investigations/ threat to life situations require immediate processing and/or analysis of submitted evidence. For these instances, refer to the Exigency Procedure Section.

1.2. Responsibili

ties Technical

Supervisor

The Digital Forensics Laboratory may be directly managed by a Sergeant or civilian equivalent who acts as the Technical Supervisor for this section. His/her responsibilities include, but are not limited, to administrative, supervisory, and the operational functions of the DFL section. The technical supervisor responsibilities may include:

- Ensuring that new personnel are trained to the section's and quality standards.
- Conducting annual performance reviews of DFL personnel.
- Performing Administrative/Technical reviews of case records submitted by DFL personnel.
- Conducting Courtroom testimony evaluations.
- Serving as Training Liaison between the section, HFSC and personnel.
- Administering competency and proficiency tests to DFL personnel.
- Maintaining DFL personnel training file.
- Ensuring hardware, software and equipment are in proper working conditions.

- Ensuring that all quality standards are met as required for the section.
- Approving validation studies on hardware and software used for forensic casework.

- Recommending software and hardware to be implemented in the laboratory.

In the absence of the Technical Supervisor, another member of the DFL may be appointed to serve as a designee.

Digital Examiner

A Digital Forensic Examiner is a staff member who is authorized to examine digital evidence in assigned case work. Contingent on training and authorization, the duties of an examiner may include the following:

- Perform extraction and recovery of digital data from electronic devices.
- Write impartial test reports with details pertaining to their extraction and/or recovery of digital data.
- Perform technical reviews of case records submitted by DFL personnel. The reviewer is qualified through technical experience to conduct these reviews.
- Perform administrative reviews of case records submitted by DFL personnel.
- Respond to on-scene incident call outs and assist customers in identifying devices that may contain evidence.
- Provide expert testimony in court.
- Provide training and mentor guidance to new personnel.
- Ensure hardware, software and equipment is in proper working conditions.
- Validate and/or performance-check software and hardware to be used for forensic casework.

1.3. Digital Forensic Analysis Limitations

Digital data storage methodologies and systems vary. Variables include hardware, software and software operating systems, software release versions, and sometimes alternative use of hardware and software from original intent. Examiners apply their education, training, and experience to analyze data; and to use best scientific practices in that regard.

1.4. Safety

Examiners should be aware of their personal safety when handling test items.

Digital devices are powered by electricity. Devices should be disconnected from power sources when disconnecting and/or removing internal components (e.g., hard drives).

The internal components of digital devices, particularly desktop computers, are tightly configured with the potential for encountering sharp metal edges. Examiners should exercise caution when maneuvering inside devices. Gloves are an acceptable safeguard. Injuries should be reported to the section manager and the Health and Safety Specialist.

If biohazard substances are present on evidence, measures will be taken to sanitize and decontaminate the media as best as possible. While wearing rubber or latex gloves, use a bleach-solution sanitizing wipe(s) to remove visible biological materials present on the device. It is a good practice to sanitize all devices when unpackaging them and prior to ungloved handling to prevent contamination. When using bleach-wipes, care should be exercised to prevent cleaning solution from seeping into and possibly damaging electronic components. Please refer to the HFSC safety manual for further information for utilizing cleaning solutions.

Digital Forensic Laboratory
Evidence Handling

Forensic Analysis Division

2. Digital Forensic Laboratory Evidence Handling

2.1. Purpose

To establish guidelines for the receipt, tracking, protection, marking, handling, and return of evidence in the Digital Forensic Laboratory.

2.2. Scope

This procedure applies to all Digital Forensic Laboratory employees and administrative personnel who receive, handle, or process evidence.

2.3. Submission of Evidence

2.3.1. Examination requests are most commonly submitted via the Laboratory Information Management System (LIMS) for HPD-controlled evidence. HPD customers, in consultation with the DFL, may also submit their evidence directly to the lab for examination. For non-HPD customers, evidence is submitted via the HFSC Evidence Triage group utilizing their evidence submission guidelines.

2.3.2. Evidence is generally couriered by HFSC personnel to the DFL from the HPD Property Division, or from the HFSC Evidence Triage section.

2.3.3. At the DFL, submitted items shall be visually examined for damage prior to analysis at the time the evidence is unpackaged. Evidence should be photographed prior to examination and notations of damage recorded in the LIMS report.

2.3.4. Peripheral equipment not designed to store digital data (e.g. monitors and keyboards) will not be accepted unless those items are unique and are required to facilitate the examination.

2.3.5. Receipt of evidence from the customer will be documented at the time of transfer either electronically in the LIMS or on paper as part of the chain of custody.

2.3.6. Digital Forensic Laboratory personnel receiving evidence shall ensure the items are properly labeled and sealed.

2.3.6.1. If an existing seal is observed to be broken at the time of submission, the item should be rejected.

2.3.6.2. Exceptions can be made if an item is submitted with a deficient seal or lack of seals because of the size, the DFL examiner may accept the evidence, but it must be immediately and properly sealed prior to being placed into the evidence vault.

2.4. Evidence seized at response scene

2.4.1. Examiners who are requested to attend the on-scene incident call-outs may assist customers in identifying devices that may contain evidence.

2.4.2. Seized evidence will be documented electronically in the LIMS upon arrival to the Digital Forensic Laboratory or on paper at the crime scene as part of the chain of custody (this information will be transferred to the LIMS upon arrival at the lab).

2.4.3. Evidence seized at an on-scene incident response scene may be transported directly to the Digital Forensics Laboratory or to the HPD Property Division. In cases where it's impractical and/or unsafe to transport evidence back to the laboratory, the evidence shall by properly sealed and secured.

2.4.4. For circumstances that require on-site processing such as imaging or copying of data, refer to the appropriate procedure.

2.4.5. To expedite the imaging process at on-scene incident locations, the target forensic drives should be prepared prior to arriving at the scene.

2.5. Receiving Evidence

2.5.1. It is the responsibility of the examiner to maintain the integrity of the evidence at all times while in his/her custody. Evidence must be protected from loss, cross-transfer, contamination and/or deleterious change.

2.5.2. Evidence shall be sealed properly. Examiners will check the evidence container to ensure that proper seal(s) are in place whenever evidence is received. A proper seal is one in which there is no possibility that the contents of a container can be removed, altered or a substitution made without the seal being obviously disturbed.

2.5.2.1. NOTE: Some items of evidence may be too large to seal inside a container. However, every effort will be made to secure and store the item with its appropriate identifiers to ensure items are not confused with submitted evidence from other cases. For example, computers, at a minimum, should have evidence tape applied to the cover opening of the computer chassis. The intake technician should apply his or her initials and date of receipt on the evidence tape.

2.5.3. Receipt of evidence will be documented at the time of transfer electronically in the LIMS or on paper as part of the chain of custody.

2.5.4. Cases that contain items that could represent a possible biohazard require special handling. While working with possible biohazards, proper precautions, such as wearing gloves and cleaning with a diluted bleach, solution may be needed. Contaminated items shall be sanitized as best as is practical and labeled to the effect that a potential biohazard may exist prior to placing into the evidence vault if received in an unsealed container. Likewise, contaminated items should be sanitized prior to being introduced into the examiners workstation area.

2.5.5. Evidence items contained within a case will be labeled. This also includes media device(s) containing the extracted data from the original physical evidence or digital evidence data source (e.g. evidence CD/DVD created for the customer).

2.5.5.1. Some items of evidence may be too small to be marked or labeled with unique identifiers directly on the item. If so, it shall be marked on its proximal container.

2.5.5.2. For groups of like evidence such as CD's/DVDs, the groups of items may be labeled with one unique identifier as long as the items of evidence are securely packaged and sealed together.

2.6. Evidence Security

The Digital Forensic Laboratory personnel will ensure that evidence integrity is not compromised. Access to evidence within the Digital Forensic Laboratory is controlled by several different means. The Digital Forensic Laboratory operational area is controlled with restricted access. Access to the restricted area is only available through key cards issued to personnel assigned to the laboratory. Visitors will be escorted into the evidence facility only by a member of the Digital Forensic Laboratory or administrative staff with proper keycard access. A visitors log documenting visitor's purpose, date, and time is maintained for each visitor. Access controls allow examiners to process and examine evidence while maintaining the integrity of the evidence.

Most digital evidence examinations can be conducted at the examiner's desk. Any area where there is evidence being actively worked or where evidence is kept to permit ready access for examination is considered to be an operational area. The short term evidence storage room and the server room are located in, and considered an operational area.

2.7. Return of Evidence to the Customer

2.7.1. All items and sub-items within a case will be packaged to protect from loss, cross-transfer, and/or deleterious change. Whenever possible, evidence will be packaged in the same condition and/or containers as it was received.

2.7.2. Outer evidence containers will be sealed according to the Quality Manual handling of evidence procedures.

2.7.3. The return of evidence will be documented at the time of transfer either electronically in the LIMS or on paper as part of the chain of custody.

2.7.4. Evidence artifacts extracted from the source media provided to the customer, generally on CD/DVD, will be assigned an item# in LIMS. The CD/DVD or other media shall be labeled on the media or on its sealed container with the case identifying information and have its own chain of custody documented in LIMS.

2.7.5. Upon completion of the forensic examination, original media evidence along with the controlled exported evidence exhibits will be either directly released to the customer, or couriered via the HFSC evidence triage group. Proper chain of custody documentation will be completed.

Digital Forensic Laboratory Reporting Guidelines

Forensic Analysis Division

3. Digital Forensic Laboratory Reporting Guidelines

3.1. Purpose

The purpose of this procedure is to provide guidance for reporting case analysis results.

3.2. Scope

This procedure describes the steps to be taken when reporting case analysis results to ensure consistency within the Digital Forensic Laboratory. The LIMS report is the official reporting mechanism for the DFL.

Forensic software-generated reports are supplemental exhibits that are often not user-configurable to enable the insertion of header/footer or page numbering, etc. Some software-generated report content concerning forensic imaging of devices, where applicable, shall be copied into the LIMS report record (see Physical and Logical Imaging Procedure). Forensic software-generated reports are provided to the customer on DVD and controlled by issuing a LIMS barcode and affixing the barcode to the DVD in order to maintain a chain-of-custody.

3.3. Equipment

- Forensic Computer
- Administrative workstation with LIMS program

3.4. Overview

LIMS reports shall address examination requests and provide the customer with all relevant information in a clear and concise manner. The case analysis results shall include accurate statements to ensure a consistent interpretation of the actual case results of the examination. The following LIMS Report statements are common for all computer and mobile device cases regardless of the type of case being examined. There may be certain situations in which the provided standard LIMS report statements may not address the nature of the case and/or data being analyzed. In these situations, the examiner will consult with the Section Manager or designee for appropriate wording for the report statement.

3.5. Case Reviews

All cases will be submitted to a qualified supervisor or examiner for a Technical Review. A technical review consists of reviewing the case record notes in LIMS, forensic software generated reports, and photographs of submitted evidence:

Technical Review

- Conclusions are accurate and supported by the examination records.
- Verify that the Quality Control Checks and performance verifications were performed.
- The appropriate technical procedures (test methods) were used.
- The accuracy of report results and conclusions are supported by the technical data.

- Proper recording of actions, evidence description, and software version utilized are documented correctly.
- Ensure that derivative evidence exported to DVD was issued a unique identifying number and that evidence was properly documented in LIMS.

If the reviewer finds that the report and case records are deficient, they will be returned to the examiner for corrections and resubmission for TR.

Administrative Review

All cases will be submitted to another qualified supervisor or examiner for an Administrative Review. An Administrative Review consists of reviewing the case record notes and examiner report in LIMS to ensure that:

- Case notes and report was technically reviewed by a qualified examiner.
- Grammar and spelling is correct.
- Page number, examiners initials, and other requirements are in the LIMS report.
- All necessary documentation has been recorded in the LIMS case record (i.e. photographs, results, imaging software report, derivative evidence documentation for DVD, etc.).
- A review of all examination records to ensure that the unique case identifier and examiners initials are on each printed page.

If the reviewer finds that the case notes or the report is deficient, it will be returned to the examiner for corrections and resubmission.

3.6. Resolution of Differences of Opinion

If the reviewer disagrees with or has a difference of opinion regarding the conclusions stated in the case records and test report, then the issue will be brought to the Technical Supervisor or designee who will review the issue(s) and decide on the correct resolution for the matter. The resolution of differing conclusions will be recorded in the case record.

3.7. Report Modification

It is sometimes necessary to modify a report after it has been issued. This may be necessary to correct an error in the report, to document additional information conducted after the issuance of the report, at the request of the customer, or for various other reasons.

If it becomes necessary to amend a signed report, then the new report will be clearly identified, it will contain a reference to the original report that it is replacing, and will clearly state why an amended report was issued. The original report must be maintained within the case record.

Exigency Exception:

Whenever a customer requests expedited processing due to a threat-to-life situation, the supervisor may authorize the examiner to release some or all *derivative evidence* content to the customer prior to

it being technically or administratively reviewed. The examiner may not issue an opinion concerning that information. Rather, the examiner is merely providing a data-dump of raw or formatted forensic software-generated content.

- This situation would generally involve an overnight callout situation where the supervisor would be notified of the customer request and would assign an examiner to process the evidence.
- The examiner is required to issue a LIMS barcode to any derivative evidence released and that evidence shall be controlled in LIMS. The customer is advised that the derivative content is evidence and should be handled as such. The chain-of-custody transaction shall be recorded in LIMS and also in the LIMS Report.
- The customer will be advised that the official LIMS report ***will not*** be issued until it is technically and administratively reviewed. A copy of the derivative evidence released to the customer shall be temporarily copied to the F-SAN for the purpose of the technical and/or supervisory review (See Technical Procedure for F-SAN Data Storage).
- The customer will be notified in the event the technical review of the derivative evidence reveals anomalies or supplemental information, and that information will be fully documented in the LIMS report.

Digital Forensic Unit
Technical Procedure for F-SAN Data Storage

Forensic Analysis Division

4. TECHNICAL PROCEDURE FOR F-SAN DATA STORAGE

4.1. Purpose

4.1.1. The purpose of this procedure is to establish guidelines for the temporary storage of forensic images, derivative evidence, or processed data extracted from submitted evidence and copied onto the Digital Forensic Lab server, or F-SAN.

4.1.2. This internal network is not accessible or connected to the HFSC network. The DFL server is only accessible to employees of the DFL. This separation is due to the fact that the DFL handles sensitive information and exports content that may contain child pornography, adult pornography, financial records, files that may be contaminated with computer viruses, etc. Limiting access to these files by physical separation of networks is best practice. Introducing contaminated or contraband files on the HFSC server would place the production HFSC server at-risk of infection.

4.2. Scope

4.2.1. This procedure delineates the steps necessary for the Digital Forensic Laboratory employees to store forensics images, derivative evidence, and/or processed data onto the DFL Server. All case related data copied to the F-SAN shall be stored using a uniquely identified folder naming system. The naming convention utilized should generally be the LIMS forensic case number, but in some instances may be the agency case number. For example, "2015-12345", or "00345815". Subfolders may then be created within the main folder to store categorized data as desired.

4.2.2. A copy of extracted derivative evidence exported onto DVD for the customer should be temporarily stored on the F-SAN for a minimum of six months (depends upon data storage space availability). This serves two purposes:

- To allow for the technical review and/or administrative review of the content for quality assurance purposes.
- To afford assessors the ability to review exported content that is provided to the customer (since the evidence DVD is controlled as evidence and returned to the requesting agency and otherwise unavailable for review).

4.2.3. There are several instances where derivative evidence may not be stored on the F-SAN or temporary retention period may be less than six months:

- Data extraction was not possible for the submitted evidence (password locked, damaged, etc).
- Technical difficulties with the network or physical failure of the F-SAN.
- Size of the data may make storage impractical for a specific examination.

4.2.4. The lab manager will make decisions on what content is stored and for what duration depending upon these factors.

4.2.5. Copies of forensic images, derivative evidence, or processed data may be stored as reference material for purposes described; however there are no requirements for archival or long-term storage on the F-SAN. The original evidence is retained by the customer. The LIMS report and/or a copy of the derivative evidence provided to the customer is the official record for the case.

4.3. Equipment

4.3.1. Forensic Computer

4.3.2. DFL networked F-SAN

4.4. Procedure

4.4.1. At the beginning of an examination, a case folder is created on the local forensic examination machine that will contain all extracted evidence files associated with this case. This data is stored in folders using the unique case numbering associated with the exam request.

4.4.2. Derived evidence, exported to CD/DVD will have an assigned Item # in LIMS and will be properly sealed, labeled, and returned to the customer. A quality control file copy of the exported CD/DVD containing the exported exhibit items and/or forensic software record should be copied to the F-SAN for technical and/or administrative review purposes using appropriate uniquely identifying naming conventions.

4.4.3. After successful upload of the derivative evidence to the F-SAN from the local forensic machine, the local copy can then be deleted from local storage.

4.4.4. Upon successful completion of the required review(s), the copy may be deleted from the F-SAN. However, dependent upon available storage space, the derivative evidence should be retained for at least six months to allow for future review. The original CD/DVD provided to the customer is considered the official record.

4.4.5. Where appropriate, the evidence CD/DVD returned to the customer shall be labeled to reflect the following: "Warning: this disk is provided for evidentiary purposes only and may contain child pornography. Personal possession of child pornography for non-law enforcement purposes is a crime."

4.5. Limitations

4.5.1. The F-SAN is a mechanical, electronic device. As such, it is subject to failure. Data storage may be impacted by unexpected events outside the control of the DFL. Therefore, original evidence is the best evidence and should be retained by the customer along with derivative evidence produced on CD/DVD media for courtroom purposes.

Digital Forensic Unit
Validation, Performance Verification and Quality Control Checks

Forensic Analysis Division

5. VALIDATION, PERFORMANCE VERIFICATION AND QUALITY CONTROL CHECKS

5.1. Purpose

5.1.1. The purpose of this procedure is to establish guidelines for the validation and/or performance verification of forensic hardware and software.

5.2. Scope

5.2.1. This procedure applies to the forensic tools, hardware, and software used in the Digital Forensic Laboratory Section.

5.3. Equipment and Software

5.3.1. Refer to Approved Forensic Software and Hardware list for Forensic Digital Examination Section.

5.4. Overview

5.4.1. The Digital Forensic Laboratory uses technical procedures, hardware, and software that are widely used in the digital forensic discipline. These are known to produce outcomes consistent with the technical services requested by the customer.

5.4.2. The Digital Forensic Laboratory shall be responsible for determining whether a new method, software, and/or hardware are categorized as a forensic tool.

5.4.3. New forensic tools and methodologies introduced for use in the laboratory that have not been tested by a reputable scientific, law enforcement, or educational organizations, laboratory-developed methods, or the use of approved tools outside of their approved scope are to be internally validated prior to being used in evidence testing. This internal validation study is documented in the DFL Forensic Software/Hardware Internal Validation Form prior to casework use. After successful testing and documentation, each examiner desiring to utilize the new method or tool is required to conduct a performance check before placing it into service.

5.4.4. Forensic applications to be used by the Digital Forensic Laboratory that have been tested and validated by reputable scientific, law enforcement, or educational organizations require performance verification. These performance verifications will be documented in the equipment spreadsheet where such software/hardware will be labeled as a forensic tool. Administrative and interpretative tools do not require validation study nor performance verification. Subsequently released sub-versions of previously verified software may be approved for lab use by the section manager after a review of the available release notes. If the released version impacts core forensic services, then it must undergo performance verification before use.

5.4.5. Both Internal Validations and Performance Verifications are performed on the individual forensic functionality of the software/hardware rather than treating the software as a single entity. The validation and performance verification of specific functions allow the software/hardware in use to be partially utilized for active examinations rather than having to undergo validation of each individual functionality component. Equipment used for administrative or interpretative purposes, as well as equipment solely designed to decrypt data and/or identify, remove, or bypass security measures, does not require validation.

5.4.6. Performance verifications must be successfully performed before the forensic software or hardware are placed in service.

5.5. Equipment and Forensic Software Inventory

5.5.1. Each piece of technical equipment and forensic software is uniquely identified and recorded on the DFL inventory spreadsheet.

5.5.2. Equipment and forensic software licenses, including dongle license numbers where applicable, are recorded in the Equipment/Software Inventory which is maintained by the Section Manager. The inventory log may include the following:

- Identity of the item of equipment and/or software (i.e. workstation, write blocker, etc.);
- Manufacturer's name, make, model, and serial number and/or laboratory inventory number;
- Location (i.e. workstation, computer, laptop, etc.);
- Dates, actions, examiners identity, and results of performance verifications, and the due date of next performance verification;
- Applicable software release installations;
- Firmware updates;
- Hardware maintenance carried out and dates, as well as upgrades;
- Damage, malfunction, modification or repair to the equipment; and
- Date taken out of service if applicable.

5.6. Data Set(s)

5.6.1. A known test data set developed in-house, or obtained from a reputable scientific organization (e.g., NIST) or vendor, is used to facilitate performance verification of certain types of digital devices or components. The test data set may be the same data set used for conducting test and validation of methods, software, and hardware.

5.6.2. A test data set may include one or multiple of the following types of data for testing digital data equipment and software:

- Logical file (document and spreadsheet)
- Folder

- Photo
- Web-based email
- Outlook .pst file
- Deleted files (document, spreadsheet, and photo)
- Deleted folder

5.6.3. A test data set(s) is maintained and controlled by the Section's manager as a tool for performance verification. An inventory of the contents of the test data set(s) and associated hash value(s) is retained with the test data set, if applicable.

5.7. Internal Validation Procedure

5.7.1. Prior to the implementation of a forensic tool such as software and/or hardware with no externally validated method, an internal validation study shall be performed.

5.7.2. An internal validation study should consist of the following elements:

- Purpose and Scope (a description of the method being tested).
- Requirements (equipment specific function being validated).
- Methodology (the hardware/software, settings and test details).
- Test data sets description (used to evaluate the specific function).
- Expected Results
- Usage requirements (tool usage conditions required to compensate for any identified limitations).
- Results and Conclusions (requirements satisfied or not satisfied, observations, anomalies, concerns, or limitations).

5.7.3. Use the appropriate developed class test data set(s).

5.7.4. If relevant, hash the test data set(s) and compare the recorded values to its original creation value. This will establish that they have not been altered by the methodology.

5.7.5. Record all observations, findings, and recommendations in the DFL Forensic Software/Hardware Internal Validation Form.

5.7.6. Validation records shall be approved by the Section Manager or designee and the Quality Director. These records shall be maintained by the Section Manager or designee.

5.7.7. The Approved Forensic Software and Hardware for Forensic Digital Examination Section and appropriate technical procedures should be updated or a new procedure written if the method validated has not been used in the laboratory previously.

5.8. Performance Verification

5.8.1. Prior to the implementation of an externally validated standard method, software and/or hardware, the reliability shall be demonstrated with an appropriate class test data set against its performance characteristics before its placed into service and annually thereafter.

5.8.2. Class data sets are tracked in the LIMS and its chain of custody is updated prior and after the performance verification testing.

5.8.3. Performance verification testing of the internal test data shall be documented in the DFL inventory spreadsheet for each item tested. The chain of custody of those test data sets shall be recorded in LIMS.

5.8.4. At a minimum, any procedure taken directly from reference sources shall be demonstrated and documented to be effective when performed by the Digital Forensic Laboratory Examiners.

5.8.5. The Approved Software for Forensic Digital Examination Section and appropriate technical procedures shall be updated if new forensic imaging software and hardware is added to the section.

5.9. Forensic Workstations and Laptops Performance Verification – No Integrated Write Protection

5.9.1. The laboratory establishes the performance of forensic workstations and laptops (with or without integrated write protection) in several ways. First, when forensic workstations are used with associated forensic software or other data collection techniques, those methods are validated, verified, or adopted from reputable scientific organizations. When a laboratory method is developed in-house or approved methods are used for an alternate purpose, a validation or verification of the results is conducted. The forensic image and files contained within that/those images are hashed for verification to establish the integrity of the evidence output. These factors and activities establish the accurate performance of computers (workstations) used to support technical services.[1]

5.9.2. For standard forensic workstations and laptops without integrated write protection devices, a successful Power On - System Test (POST) will meet the requirement for performance verification. This performance verification requirement applies to workstations used to process physical devices (physical evidence – computers, peripheral devices, video, or mobile devices). This section does not apply to administrative computers.

5.10. Forensic Workstations Performance Verification with Integrated Write Protection

5.10.1. For forensic workstations with integrated write protection devices installed, a successful Power On System Test (POST) meets the requirement for performance verification. Additionally, each internal write protection device must be performance verified to include installed forensic imaging software. This performance verification

[1] Laboratory management has incorporated by reference the Scientific Working Group for Digital Evidence "SWGDE Standards and Controls Position Paper," Version 1.0 issued January 30, 2008.

requirement applies to workstations used to process physical devices (physical evidence – computers, peripheral devices, video, or mobile devices). Performance verification is required for each individual write protection unit installed in the forensic workstation to ensure that the units function as intended.

5.10.2. It is understood that there is no standard forensic software build common to each forensic computer used by examiners in the lab due to operating system and forensic license copyright restrictions. Each forensic computer will have a forensic software inventory log of the forensic imaging software installed according to licenses associated with that specific machine. This log will be maintained by the section manager along with performance verifications of that software.

5.10.3. The integrated write protection units of a forensic workstation are performance verified annually.

5.11. Write Protection Devices Performance Verification Procedure

- The following steps are followed to verify performance of write protection devices:

5.11.1. The controlled data set will be restored to a wiped digital device. The restored data volume will be hashed along with the logical files and compared with the stored hash values for the associated logical files on the controlled data set. Note: The volume hash values from the source will not match the destination volume hash value as a result of the restore process due to differing drive geometry, make, model and manufacturer of each device. The restore function in EnCase will verify a hash value after replication over the identical number of sectors that are being examined. If a separate MD5 hash is run on the target media, the hash values will only match if it computes the value over the exact number of sectors included from the source drive. However, the logical files resulting from this process should always match.

5.11.2. The write protection device will be connected to the restored digital device and to the workstation in accordance with the manufacturer's instructions.

5.11.3. Each device will be powered on.

5.11.4. An attempt will be made to read the data on the digital device attached to the write blocker.

5.11.5. An attempt will be made to delete a file from the digital device attached to the write blocker.

5.11.6. An attempt will be made to save a known data file (write attempt) to the digital device attached to the write blocker.

5.11.7. At the conclusion of these steps (1-6), the data on the original digital device will be hashed and the resulting hash will be compared with the controlled test data hash value to verify no data has been altered.

5.11.8. Successful performance verification will be documented in the equipment's spreadsheet.

5.11.9. Unsuccessful performance verification will be documented in the equipment's spreadsheet. The Section Manager will be promptly notified when a write protection device fails.

5.12. Imaging Devices Performance Verification Procedure

- The following steps are followed to verify performance of imaging devices:

5.12.1. The controlled data set will be loaded onto a wiped digital device. The data will be hashed and compared with the stored hash for the controlled data set.

5.12.2. The imaging device will be connected to the loaded digital device. A wiped target device will be used to capture the image.

5.12.3. Each device will be powered on.

5.12.4. An attempt will be made to image the test data set to the target device following the manufacturer's instructions for imaging and hashing. The resulting hash will be noted.

5.12.5. At the conclusion of these steps, the data on the test digital device will be hashed and the resulting hash will be compared with the controlled data set hash value and the image hash to confirm there are matches between all three indicating data on the test device has not been altered and the image was successful.

5.12.6. Successful performance verification will be documented in the equipment's performance verification spreadsheet maintained by the section manager.

5.12.7. Unsuccessful performance verification will be documented in the equipment's spreadsheet. The section manager will be promptly notified when a write protection device fails.

5.13. Wiping Devices Performance Verification Procedure

- The following steps are followed to verify performance of wiping devices:

5.13.1. A destination hard drive will be used.

5.13.2. The wiping device will be connected to the media device containing the data and to the workstation in accordance with the manufacturer's instructions.

5.13.3. Each device will be powered on. The manufacturer's instructions will be followed for configuring the wiping device.

5.13.4. An attempt will be made to wipe the data from the digital device using the wiping device.

5.13.5. At the conclusion of the wiping process, the wiped device will be examined with a hex editor or forensic software to visually observe the data has been wiped using "00" or other hex value specified by the examiner.

5.13.6. Each step will be documented. A comparative hash value is unnecessary, since the before and after values will not match if the wiping process was successful. The success of the wiping function will be documented in the equipment's database.

5.13.7. The section manager will be promptly notified when a wiping device fails.

5.14. Performance Verification of Forensic Software

5.14.1. Due to ubiquitous acceptance within the forensic community, the full features and functionality of forensic software applications will not undergo complete performance verification. Software applications which will not be fully tested include, but are not limited to, EnCase and Forensic Toolkit (FTK). However, each of these tools will be performance verified for:

- Physical imaging
- Wiping media (EnCase only)

5.14.2. Tools which are considered interpretive or administrative (e.g., Windows OS, Microsoft Office Suite, Adobe Reader, etc.) will not undergo performance verification.

5.15. Performance Verification of Physical Imaging Software

- The following procedures are used to verify performance of physical imaging software:

5.15.1. The controlled data set will be loaded onto a wiped digital device. The data on the digital device will be hashed and compared with the stored hash for the controlled data set.

5.15.2. The digital device to be imaged will be connected to a forensic workstation with an approved write blocker. A second wiped digital device, or a wiped partition on a workstation or forensic storage area network, will be designated as the target drive for the creation of an image of the digital device.

5.15.3. Each device will be powered on and the forensic software that is to be used to image the data on the digital device with the copy of the controlled data set to the target drive or partition will be launched. Imaging software will be configured to hash the imaged data.

5.15.4. An attempt will be made to image the data on the digital device and record the hash value of the image created to the target drive or partition.

5.15.5. At the conclusion of these steps, the data on the target drive will be hashed again and the resulting hash will be compared with the original test data hash value and the image hash to confirm matches. If the hashes match, indicating no data has been altered, the performance of the imaging software is considered verified.

5.15.6. Successful performance verification will be documented in the equipment's database.

5.15.7. Unsuccessful performance verification will also be documented in the equipment's database. The section manager will be promptly notified when a write protection device fails. The equipment will not be used on casework until verification is successful.

5.16. Performance Verification of Wiping Software

- The following procedures are used to verify performance of wiping software:

5.16.1. A drive that needs to be sanitized/wiped shall be identified and used for this process.

5.16.2. The digital device to be wiped will be connected to the workstation.

5.16.3. Each device will be powered on. Configuration of the software to wipe the digital device is performed.

5.16.4. An attempt will be made to wipe the data from the digital device using the software.

5.16.5. At the conclusion of the wiping process, the digital device will be examined with a hex editor or forensic software to visually observe that all data has been wiped.

5.16.6. Successful performance verification will be documented in the equipment's database.

5.16.7. Unsuccessful performance verification will be documented in the equipment's database. The Section's Manager will be promptly notified when a write protection device fails.

5.17. References

- Validation and Verification of Computer Forensic Software Tools-Searching Function
- Digital Forensics: Validation and Verification in a Dynamic Work Environment
- National Institute of Standards and Technology, Computer Tool Testing Program (www.cftt.nist.gov)
- Scientific Working Group on Digital Evidence (SWGDE), SWGDE Recommended Guidelines for Validation Testing, version 1.1, January 2009. (www.swgde.org)

Digital Forensic Laboratory Approved Software for Forensic Digital Examination

Forensic Analysis Division

6. APPROVED SOFTWARE FOR FORENSIC DIGITAL EXAMINATION

6.1. Purpose

6.1.1. This section describes software currently approved for use in computer and cellphone forensic examinations by the Digital Forensic Laboratory.

6.2. Scope

6.2.1. This section serves as a reference to denote forensic imaging and forensic examination software utilized in casework by examiners in the Digital Forensic Laboratory. Some forensic software is capable of both forensic imaging and forensic examination. The forensic imaging functionality of the forensic software must be performance checked on an annual basis and prior to being placed into service. Forensic examination software is considered analytical and/or interpretive and does not require performance checks.

6.3. Approved Forensic Imaging Software

6.3.1. Imaging

- EnCase/ EnCase Imager
- FTK Imager
- EnCase LinEn
- MacQuisition

6.4. Approved Forensic Wiping Software

6.4.1. Data Wiping Utilities

- EnCase

6.5. Forensic Examination Software In General Use

6.5.1. Digital Forensic Lab employees may be authorized to utilize one or more of the following forensic software products, dependent upon their individual authorization memos:

6.5.2. Computer Forensic Software

Guidance Software EnCase Forensic
Access Data Forensic Toolkit
FTK Imager
EnCase Imager
EnCase SE Write Blocker
EnCase LinEn
Magnet Forensics Internet Evidence Finder (IEF)
MacQuisition
SubRosaSoft MacForensic Lab

ADF Triage Examiner

6.5.3. Mobile Forensic Software

Cellebrite UFED4PC
Cellebrite Physical Analyzer
Access Data MPE+
Guidance Software EnCase
Katana Forensics Lantern
Oxygen Forensic Suite
Micro Systemation XRY/XACT
Blacklight
Magnet Forensics Internet Evidence Finder (IEF)

6.6. File Viewers

6.6.1. Digital Forensic examiners are free to utilize 3rd party file viewers or interpretive software that is necessary to examine and represent the file examined in an intelligible format. Successful results are self-evident.

6.6.2. It is recognized that numerous products exist that replicate capabilities to view assorted file types. For example, MS Windows has picture viewing software that displays .jpg files. IrfanView also properly displays .jpg images. There are numerous freeware and commercial software that accurately displays file content of various types. The specific file viewer utilized by the examiner is at the examiner's discretion, as long as the software utilized does not violate licensing or copyrights.

Digital Forensic Unit
Hard Drive Removal Technical Procedure
Forensic Analysis Division

7. HARD DRIVE REMOVAL TECHNICAL PROCEDURE

7.1. Purpose

7.1.1. The purpose of this procedure is to remove the hard drives from computers submitted for examination for the purpose of creating a forensic duplicate while maintaining the integrity of the evidence.

7.2. Scope

7.2.1. This procedure describes the essential steps needed to be taken by Digital Forensic Laboratory examiners in removing hard drives submitted as evidence.

7.3. Equipment

7.3.1. Computer repair tool kit
7.3.2. Permanent markers
7.3.3. Camera

7.4. Overview

7.4.1. This procedure can also be used to remove hard drives from laptop computers. Some laptop hard drives can only be removed by trained service personnel and others have security hardware or software features which do not allow them to be used outside the laptop computer. For these types of cases, imaging should be done by following the Cable Acquisition Procedure.

7.5. Procedure

7.5.1. Photograph the condition of the evidence device prior to the forensic examination of the device. Visible damage shall be documented, photographed, and noted in the case record.
7.5.2. With the computer powered off and power cord and/or battery disconnected, open the case on the computer to access the internal drive(s).
7.5.3. Photograph the internal contents of the evidence computer prior to removing the hard drive(s).
7.5.4. For non-cable acquisitions, disconnect the data and power cords connecting the hard drive to the evidence computer.
7.5.5. Remove the hard drive(s) from the evidence computer.
7.5.6. With an indelible marker, label the hard drive removed from the evidence computer or label the proximal container so it is properly identified. These markings will include the lab case number, evidence item number, and examiner's initials.
7.5.7. Photograph the hard drive to include the identification information.

7.5.8. Record the drive information from the hard drive label in the forensic lab report. This may be either an automated software report derived from the imaging process, or a manual record. In cases where the hard drive is not accessible (cable acquisition method employed), recording this information may not be feasible. Drive information may include:

- Make
- Model
- Serial number
- Storage capacity

7.5.9. Where possible or practicable, reconnect the power source to the computer and boot the evidence computer into the BIOS with the hard drive removed. If the date and time differ from the actual date and time, record the difference in the case record notes. Document instances where obtaining BIOS information is not feasible.

7.5.10. Record the BIOS information in the case record. BIOS information may include:

- Date and time the BIOS settings were verified
- The key or key sequenced invoked to display the BIOS
- BIOS date and time settings
- BIOS manufacturer and version
- Boot sequence settings
- Failure to access the BIOS and reasons why, if applicable

7.5.11. Image the hard drive(s) in accordance with approved procedures for write protection and imaging.

7.5.12. Reassemble the computer.

7.6. Limitations

7.6.1. Care shall be exercised to guard against electrostatic discharges which can damage or destroy the evidence hard drive. In cases where internal storage consists of flash memory only, drive labels may not exist. This will impact the approach taken to document the storage medium for examination. Traditional methods may not apply and the examiner should do their best to photograph and record the drive component. If the drive is not removable, please refer to the Cable Acquisition Procedure.

Digital Forensic Unit
Cable Acquisition Technical Procedure

Forensic Analysis Division

8. CABLE ACQUISITION TECHNICAL PROCEDURE

8.1. Purpose

8.1.1. This procedure is for situations in which the hard drive(s) cannot or is not easily removed from the evidence computer without risk of damaging the device.

8.2. Scope

8.2.1. This procedure delineates the essential steps needed to be taken by Digital Forensic Laboratory examiners for imaging hard drives using various cable connectors. This section is not intended to cover or delineate all possible scenarios an examiner may encounter. Rather, this describes steps most commonly used.

8.3. Equipment

8.3.1. Forensic Tower or Portable Forensic Workstation

8.3.2. Prepared Target drive

8.3.3. Appropriate EnCase software

8.4. Overview

8.4.1. This procedure provides steps for imaging computers and laptops without making changes to the data on the evidence drive. Imaging using a parallel cable is a slow method of data acquisition that may take several days to complete. For situations in which time is of importance, a network crossover cable provides a faster method for imaging compared to using a parallel cable. USB, Firewire, and Lightning connectors are faster technologies. Examiners are encouraged to utilize the most appropriate methods and connectivity suitable for the acquisition.

8.4.2. EnCase is the primary imaging tool used by the Digital Forensics Laboratory for cable acquisitions. There may be situations in which other forensic software or devices may be required. Using other tools is at the discretion of the examiner, in consultation with the section's manager. However, all methods must be documented.

8.4.3. The cable acquisition method is not a primary method DFL examiners utilize in day to day operations. Therefore, examiners must review software documentation directly from the product manufacturer's website prior to conducting a cable acquisition. This is to ensure the methods used are still recommended and that newer procedures or faster connectivity options are not available prior to the procedure being conducted.

8.4.4. Described below are some common methods utilized by DFL examiners to conduct cable acquisitions. These are not the only methods or techniques available and do not cover every possible scenario. Examiners should research the Guidance Software website (for

EnCase acquisitions) to determine the suitable method to employ depending upon the device encountered.

8.5. Procedures

8.5.1. LinEN Boot Disk or Drive Method

8.5.1.1. Summary:

8.5.1.1.1. When trying to perform a physical acquisition of a device, sometimes EnCase is unable to acquire the device. This may be an operating system issue or a physical issue where the source drive is not readily accessible (hard to remove). An example would be trying to acquire Macintosh computer where hard drive access is difficult, or other non-Windows based systems. In this case, a cable acquisition is necessary using EnCase LinEN.

8.5.1.1.2. With various virtualization platforms or virtual systems, EnCase may not be able to parse the virtual hard disk files. It may be necessary to acquire the files using LinEN which created an E01 file that EnCase can read.

8.5.1.2. Prerequisites:

8.5.1.2.1. You have downloaded the LinEN ISO and burned the image to a CD/DVD or a bootable USB flash drive.

8.5.1.2.2. You are able to boot the physical machine or virtual machine from the LinEN boot disk/USB flash drive.

8.5.1.2.3. You have a compatible internal or USB attached external hard drive that is FAT32 formatted.

8.5.1.2.4. The internal or USB external is detected by the system BIOS and/or operating system.

8.5.1.2.5. The amount of space on the USB external hard drive is greater than the source device. Target Drive Size (in GB) > Source Drive Size (in GB).

8.5.1.3. Procedure:

8.5.1.3.1. In order to successfully use LinEN, you must have either burned the ISO to a bootable DVD or USB Flash Drive. In addition, the destination drive must be formatted in FAT32.

8.5.1.3.2. Insert the LinEn Boot CD or USB Flash Drive and configure your system to either boot from the device through BIOS or hotkey. You will have to check your manufacturer for the appropriate hotkey or BIOS setting. Once booted, you should receive the main LinEN boot prompt asking for default settings. Choose the appropriate keyboard, time zone, and display.

***** Note: Make sure you have also connected your FAT32 formatted USB target media (USB flash drive/external hard drive etc.) to a spare USB port. *****

8.5.1.3.3. After selecting the default configuration, LinEN will load into the system memory and detect the hardware on the subject computer. This process can take several minutes depending on the speed and complexity of the subject machine.

8.5.1.3.4. When LinEN finishes detecting hardware, you will see the main command window. There are several options to choose from, but for a disk-to-disk acquisition, select the appropriate menu item.

8.5.1.3.5. LinEN will prompt a summary of detected/mountable target hard drives of which the user can specify where they want the evidence files stored. Please note that each disk has a unique name (i.e. /dev/sda, /dev/sdb, /dev/sdb1). Pay close attention as not to write over the source hard disk. LinEN will prompt for the destination drive. A sample entry input would follow this syntax "/dev/sdb1". Note: the drive will be mounted to "/dest"

8.5.1.3.6. Under "Mounted Drives" you will see your destination device "/dev/sdb1" labelled as "vfat" with "rw" which means read-write mode. If your device is not mounting or does not contain "vfat" and "rw" as part of the description, LinEN will not work and additional troubleshooting is required. Consider whether the target drive is FAT32 formatted or if your target drive is connected to a valid USB port. You might have to adjust settings within the BIOS or try another USB port. Once you have confirmed your target drive is mounted, type "Y" for yes and press enter to run LinEN (application).

8.5.1.3.7. The main application of LinEN will list all available devices/drives. Pay close attention to what is our source drive and what is our target.

8.5.1.3.8. Next, select the source drive you wish to acquire.

8.5.1.3.9. The next screen will ask where to store this image. Remember we noted that the destination/target drive labeled “/dev/sdb1" is mounted as "/dest". In order to use the drive we declared/mounted in the previous step, simply type "/dest/" and add the folder name/file name desired to deposit the image. For the filename, use the Lab#, Device#, and HD# (HD1 or HD2) to identify the E01 Image.

8.5.1.3.10. You will be prompted for several entries, such as examiner name, case number, evidence number, etc., before the imaging process begins. This information is stored within the E01 file.

8.5.1.3.11. The next 4 options toggle whether compression is enabled, whether an acquisition hash is performed and whether to password protect the E01 file,

and the total sector count. As a general rule, do not password protect the E01 file.

8.5.1.3.12. The next option is to configure the size of the file segments. Due to limitations in the FAT32 format, files that are larger than 2 GB (Gigabytes) are not supported. For large source/subject devices, the E01 file is divided into user specified chunks. Please consult the below table and make a decision based on how you intend to store the E01 files or what media type you plan to use. By default, LinEN will use 640 MB (megabytes) segments. Remember, the MAX is 2000 MB. The following are generic file segment sizes for various types of destination media:

File Segment Size	Destination Media Type	Reason	Recommended By
490 MB	USB Flash Drive / Media	2 segments per 1 GB	Technical Services
640 MB (Default)	CD / CDR / CDRW	1 segment per CD	Product Management
1440 MB	DVD / DVD-DL / Blue-Ray	3 segments per DVD	PSD
2000 MB (MAX)	Non-Flash or Optical Device	Less segments	Maximum for FAT32

8.5.1.3.13. The next six steps allow the user to configure Granularity, Block Size, Worker Threads, Hashing, and Verification. It is recommended to leave these at default settings.

8.5.1.3.14. The next page is a confirmation of settings. Represented is a summary of some of the values entered. These values will be locked inside the evidence file and cannot be changed.

8.5.1.3.15. Upon pressing enter, the acquisition will start. It can take several minutes before you see source/subject and/or target hard disk activity. Note: LinEN will automatically "blank" the screen if there is no user activity (moving the mouse). In order to resume reviewing the process, press the control key (ctrl).

8.5.1.3.16. Once the acquisition is complete, LinEN will ask if you wish to create a text file with the acquisition information/metadata. Select “Yes”. Utilize this text file for documenting your process in your report.

8.5.1.3.17. LinEN will then prompt where you wish to store the text file. Remember that our target/destination drive is mounted as "/dest". We can simply type “/dest/<unique file name>.txt” and press enter.

8.5.1.3.18. LinEN will then return to the main application/device selection screen. Select "Quit" and press enter to Exit. You will see the "command window menu", where you can shut down the system. Once the system is shutdown, you can disconnect the target/destination media into which the E01 files have been written.

8.5.1.3.19. You can verify the E01 files by connecting your external USB FAT32 hard drive containing the E01 files to your forensic machine utilizing a hardware or software write-blocker.

8.5.1.3.20. Acquisition is complete. Treat these E01 files as any other evidence E01 files and begin your examination.

8.5.2. Firewire Target Disk Mode for Macintosh Method

8.5.2.1. FireWire Target Mode works at the firmware level before the Mac OS starts to boot. You can connect the Mac computer to your PC over a Firewire. When booting a Mac, hold down the "T" key until you see a blue screen with a yellow FireWire logo floating around the screen. This process ensures the internal drive in the Mac computer will act like an external hard drive connected to the PC.

8.5.2.2. Firewire Target mode will not write to the internal drive unless the PC it is connected to attempts to mount the HFS partition (most PCs will not know what to do with the HFS partitions). Ensure your Windows based examination machine does not support HFS.

8.5.2.2.1. With both systems off, connect the Mac to the forensic PC over FireWire.

8.5.2.2.2. Boot up the Mac and hold down the [T] key, holding it down until you see the blue screen. Make sure you press the "T" key immediately after the Mac boots. NOTE: The user may have created a firmware password. Check this by first holding down the "Option" key. If a firmware password has been set, you will get a screen with a password prompt (at this point shutdown the Mac and look at removing the drive from the computer). If no password is set, you will get a screen showing each bootable drive and you can select them from here (at this point you want to shut down the computer). Once you reboot the Mac hold down the "T" and follow from Step 2.

8.5.2.2.3. Boot the forensic machine.

8.5.2.2.4. Identify the drive connected to the PC; it should look like an external FireWire drive.

8.5.2.2.5. Image the Mac.

8.5.2.2.6. Once imaging is complete, save the image and shutdown the PC, reversing the original process.

8.5.2.2.7. Shutdown the Mac.

8.5.2.2.8. Disconnect the FireWire cables from the Mac and the PC.

*****Note: If the Mac has more than one drive, only the main drive, zero, will be seen.**

8.5.3. Thunderbolt Target Disk Mode for Macintosh

8.5.3.1. Thunderbolt is an interface, exclusively offered on newer Macintosh desktops and laptops, which combines both PCI Express and Display Port technology into a serial data interface. Some of Apple's products, such as the Mac Book Air, no longer offer a FireWire port to support TDM.

8.5.3.2. Apple will include TDM (target disk mode) on the Thunderbolt interface. This functionality is added to Thunderbolt capable models through the release of new firmware, otherwise known as "EFI updates", for machine specific models.

8.5.3.3. Check Apple's web site for machine specific information for the specific model being examined. Search on Mac's support pages for keywords "EFI and/or TDM".

Digital Forensic Unit
Technical Procedure for Write Protection of Media

Forensic Analysis Division

9. TECHNICAL PROCEDURE FOR WRITE PROTECTION OF MEDIA

9.1. Purpose

9.1.1. The purpose of this procedure is to protect original evidence from deleterious change during the imaging or previewing processes.

9.2. Scope

9.2.1. This procedure applies to the Digital Forensic Laboratory examiners who image digital devices or preview digital data using external hardware write protection devices, integrated write protection devices (e.g., F.R.E.D. workstations) or application write protection software, and where the integrity of the electronically stored information must be preserved.

9.3. Equipment

9.3.1. Hardware

- Forensic workstation or notebook
- Data cable adapters (may be required to properly connect write blockers to devices being write protected)
- Write blocker forensic bridges
- Internal write blockers

9.3.2. Software

- FTK Imager and EnCase for previewing
- EnCase Software write-blocker (Fast Bloc SE)

9.4. Overview

9.4.1. Write protection of media devices should be tested in accordance with the performance verification procedures prior to being placed in service and annually throughout the life cycle of the device in accordance with the Validation and Performance Verification Procedure. In those instances where a hard drive cannot be removed, or it is impractical to remove, examiners should utilize a cable acquisition procedure as appropriate for the type of device being examined.

9.5. Procedure

9.5.1. Computers

9.5.1.1. Photograph, label and document the evidence as described in Hard Drive Removal Technical Procedure at the appropriate times during the process.

9.5.1.2. With the original source computer powered off, disconnect the power and data cables from the hard drive.

9.5.1.3. Remove the hard drive from the drive bay.

9.5.1.4. Connect power and data cables from the write protection device to the source drive to be examined.

9.5.1.5. Connect the write protection device to the appropriate connection on the forensic workstation or notebook. If using a disk duplicating device with integral write blocking features (i.e., Tableau TD2), connect it to the drive to be duplicated.

9.5.1.6. Connect a power cable to the write blocker and power on. If utilizing software write blocker, enable the write protection feature prior to connecting the device.

9.5.1.7. The device to be write-protected should be displayed as a device in the "My Computer" view if using a Windows-based computer to perform the examination. In some instances, the device may display as the name of the forensic write blocker, such as "Fastblock." The forensic disk duplicators should also display data specific to the disks (i.e. disk to be copied and disk to receive the image) attached. The device is ready for imaging or preview.

9.6. Eternal Media (e.g., USB Device)

9.6.1. When using a software-based write blockers (i.e. Fastblock SE) for USB/Firewire and/or SCSI ports, initiate the software write blocking function in EnCase.

9.6.2. Connect power and data cables from the write protection device to the external media.

9.6.3. Connect the write protection device to the appropriate connection on the forensic workstation or notebook.

9.6.4. Connect a power cable to the write blocker and power on.

9.6.5. The source hard drive or the forensic device should be displayed in the "My Computer" or "Computer" view if using a Windows-based computer to perform technical service. The device is ready for imaging or preview.

9.7. Technical Record

9.7.1. The examiner shall ensure the following information is documented in the LIMS report.

- Date and time the forensic copying or preview was initiated;
- The unique identifier for the device;
- Failure of the device, if applicable; and
- Date and time the forensic imaging process was completed.

9.8. Limitations

9.8.1. Some write blockers and disk duplicators may not recognize a host protected area (HPA) or dynamic disk overlay (DDO) and thus will not copy the data residing in the HPA or DCO. Refer to the manufacturer's manual to determine if this limitation exists for the device being used.

9.8.2. Since write protection of cellular systems is not feasible, this procedure does not apply.

9.8.3. System files accessed over a network- which are typically logical files stored in a RAID environment- is not be applicable to write protection procedures, as this is considered live, volatile data. Hard drives must be physically accessible in order to write protect them. Documentation of the circumstances of why a logical image or capture was performed must be documented in the examination notes.

9.9. References

- Weibe Tech User Guides
- Digital Intelligence User Guides
- Tableau TD2 Manual
- FTK Imager User Manual
- EnCase User Manual

Digital Forensic Laboratory
Technical Procedure for Wiping Media

Forensic Analysis Division

10. TECHNICAL PROCEDURE FOR WIPING MEDIA

10.1. Purpose

10.1.1. The purpose of this procedure is to completely wipe digital media from destination drive when applicable in order to restore a source forensic image to that drive. The intent is to ensure that the destination drive contains no remnant files that may contaminate the source files copied to the destination media. The destination drive can then be inserted into the original device for native examination of the source content, if needed. This process prevents contamination or deleterious changes to the original source media by using a substitute drive for the examination.

10.2. Scope

10.2.1. This procedure describes the steps taken for the secure wiping of data on target drives by Digital Forensic Laboratory examiners.

10.3. Equipment

- Forensic workstation, or external stand-alone media wiping device
- Approved software or hardware device(s) for wiping data
- Device to be wiped

10.4. Procedure

10.4.1. Select an appropriate forensic target drive of suitable size and characteristics to be wiped.

10.4.2. Attach the forensic target drive to be wiped to the appropriate forensic workstation.

10.4.3. Use an approved hardware wiping device or wiping software to remove all information from the target drive.

10.4.4. Note that EnCase will wipe a target hard drive prior to restoring a forensic image as part of the process.

10.4.5. The following information should be documented in the technical case record:

- Date and time the forensic wiping was initiated
- Hardware and software (include version) used to wipe the target device
- Unique identifier for the forensically wiped media (i.e. drive characteristics, make, model, serial number or lab designator written in indelible marker on the label)
- Record if the wipe fails.

10.5. Limitations

10.5.1. Due to media architecture limitations, software wiping utilities likely will not be successful or possible on tape drives, CDs/DVD, Blu-ray or other media. Reuse of this media for forensic purposes is not recommended.

10.5.2. Wiping is generally only performed on hard drives.

10.5.3. Damaged hard drives that cannot be completely or successfully wiped should be physically destroyed. Absent a successful wiping process, data overlap contamination may occur. Wiping must be properly completed to safeguard the process.

10.6. References

- EnCase Forensic User Manual
- EnCase Intermediate Analysis and Reporting Course Guide
- EnCase Advanced Computer Forensics Course Guide
- Tableau User Guide for TDW1 and TD2

Digital Forensic Laboratory
Physical and Logical Imaging Technical Procedure

Forensic Analysis Division

11. Physical and Logical Imaging Technical Procedure

11.1. Purpose

11.1.1. The purpose of this procedure is to avoid damage and alterations to original evidence when creating forensic copies of digital media.

11.2. Scope

11.2.1. This procedure applies to Digital Forensic Laboratory examiners tasked with capturing or recovering data from physical and logical digital media devices such as a hard drives or external media.

11.3. Equipment

- Forensic workstation
- Approved write protection hardware or software
- Forensic disk duplicator, if applicable
- Target forensic media

11.4. Overview

11.4.1. The original source media is best evidence. Forensic examiners conduct their forensic examinations utilizing forensic copies of the source media to safeguard and preserve original evidence from deleterious change. Verification of the forensic image is accomplished by hashing the image files during the imaging phase and post processing, if applicable, using a hash algorithm and/or cyclical redundancy checks (CRC) to ensure the forensically copied data matches the original data. Upon completion of the examination, the original evidence is returned to the customer and any forensic images are then deleted from examination machines to prepare for the next examination.

11.4.2. Whenever possible, original digital media should be imaged and the data analysis should be conducted on the image rather than the original device. The original media is imaged to a separate device, such as a hard drive, which is used to temporarily store the image.

11.4.3. If the number of devices are such that the total storage volume of exceeds the capacity of the storage capabilities on the forensic examination machine, the forensic images can be copied to the F-SAN or a NAS device. Should the original media be copied to or directly imaged to a Forensic SAN or NAS, the image shall be uniquely identified and stored within a uniquely identified folder. Upon completion of the forensic examination, the forensic working copies shall be deleted.

11.5. Physical Imaging Procedure

11.5.1. Connect the forensic target drive.

11.5.2. Use an approved hardware write blocking device, such as Weibetech or Digital Intelligence Write Blockers.

11.5.3. Attach the media to be imaged to a write blocking device, if applicable, noting that certain workstations are equipped with built in write blockers. A software write blocker such as FastBlock SE may also be utilized.

11.5.4. Power on or enable the write-blocking device.

11.5.5. Begin the imaging process.

11.5.6. At the conclusion of the imaging process, verify the image integrity using a hash algorithm. For FTK Imager and EnCase, this is an integrated and automated function. Save the output summary bookmark into the software forensic data report. Copy that log to the LIMS report.

11.5.7. Power down equipment and remove the media. Secure the original device by re- installing it into the computer or other housing, if applicable.

11.5.8. The following information should be documented in the lab report:

- Date and time the imaging was initiated.
- Hardware and software (include version) used to create the image.
- Unique identifier for the forensically wiped media used to store the image.
- The hash values verifying the image integrity, when applicable.
- Automated logs, if possible.
- Record if the imaging fails.

11.6. Logical Imaging Procedure

11.6.1. Connect the forensic target drive.

11.6.2. If a network acquisition is being employed to capture network-stored data, the forensic workstation will connect to the network and the forensic software will be directed by the examiner to the network storage location of the evidence data to be retrieved.

11.6.3. Launch the approved forensic imaging software to capture the logical data.

11.6.4. Direct the software to the file, folder, mounted volume, or attached network drive to be acquired.

11.6.5. Begin the imaging process, being sure to choose the option to hash the source during acquisition (if not enabled by default).

11.6.6. At the conclusion of the imaging process, verify the image integrity using a hash algorithm. For the DFL-approved software and devices, this is an integrated and automated function.

11.6.7. Unmount and detach the target drive and secure it as described.

11.6.8. The following information should be documented in the technical record notes:

- Date and time the imaging was initiated.
- Hardware and software (include version) used to create the image.

- Unique identifier for the forensic image folder used to store the logical files or logical images.
- The hash values verifying the image integrity, when applicable.
- Automated logs, if enabled, that document success or process failures.

11.7. Quality Control Checks

11.7.1. The forensic computer used in casework shall be performance verified (POST check) annually to ensure that the forensic computer is functioning properly. The procedure for this verification process can be found in the Validation and Performance Verification Procedure.

11.8. Limitations

- Attempts to image damaged media may not be successful. Files and or file fragments may be the only information recoverable.
- Improperly invoked commands or incorrect connection of the source media may result in destruction of data or deleterious change.
- Forensic imaging may or may not capture data in a Host Protected Area or Dynamic Disk Overlay/Dynamic Configuration. This is dependent upon the write blocker being used and its capabilities or settings.
- The use of virtualized forensic processing may require different procedures than those set out herein.
- This procedure does not apply to cellular devices in general, but does apply to the devices' internal storage media (SD) cards when so equipped.
- Unallocated clusters, deleted files and folders, file slack, volume slack, alternate data streams, and other data areas that are normally acquired with physical imaging are not obtained using logical acquisitions.

11.9. References

- Technical Manual – Procedure for Write Protection
- Access Data FTK Imager User Manual
- Guidance Software EnCase User Guide
- Weibetech and Digital Intelligence Write Blocker User Guides
- Tableau User Manual

Digital Forensic Laboratory
Mobile Device Data Extraction

Forensic Analysis Division

12. MOBILE DEVICE DATA EXTRACTION PROCEDURE

12.1. Purpose

12.1.1. The purpose of this procedure is to extract data from mobile devices and/or removable media utilizing the most appropriate examination tool.

12.2. Scope

12.2.1. This procedure describes an overview of the steps taken by DFL examiners in extracting data from various types of mobile devices submitted for examination.

12.3. Equipment

- Forensic workstation
- Appropriate examination tool for mobile devices (software and/or hardware)
- Forensic storage drive/flash drive for data storage
- Shielding enclosure (Faraday device)
- Digital camera

12.4. Overview

12.4.1. Mobile devices are designed to communicate with cellular networks, but also may be capable of connecting wirelessly to other devices via Wi-Fi, Bluetooth, or infrared connections. Allowing a device to receive a signal from a network or wireless connection can result in a change in the data contained on the internal memory of the device. Remote wiping is also a concern.

12.4.2. While powered on, cellular devices are always attempting to establish asynchronous communication with cell towers or other wireless channels to enable the devices to perform as designed. Therefore, mobile devices should be powered OFF when submitted for examination. If, during processing and/or transportation, it is necessary to power on the mobile device, the device should not be allowed to connect to surrounding networks. The device should be placed into airplane mode if possible. Faraday enclosures are utilized to prevent external connectivity if airplane mode is not enabled.

12.4.3. Mobile devices are produced by a variety of manufacturers, each utilizing their own unique operating system, version or implementation of an operating system, applications, data storage services, peripherals, and file structure systems. Due to this, it may be necessary to utilize several different acquisition tools in order to extract and document the desired data from a mobile device. Qualified examiners determine the best acquisition tool(s) to be utilized to conduct an examination.

12.4.4. Mobile devices often contain removable storage devices such as media cards. These removable devices are processed via normal computer forensic imaging procedures. See Physical and Logical Imaging Procedures section for processing instructions.

12.5. Procedure

12.5.1. The examiner should visually examine and photograph the mobile device and document the following:

- Appearance
- Condition
- Presence of any removable digital storage devices (e.g., integrated circuit cards, flash memory, etc.)
- Identifying information (e.g., manufacturer, model number, etc.)
- Unusual markings and defects

12.5.1.1. It is preferred to do this prior to the imaging process, but circumstances may dictate doing so after the image extraction is completed. All steps, where applicable, must be documented.

12.5.2. If the target device is submitted in a powered-on state, place the device into airplane mode, if possible.

12.5.3. If powered off, place the device into a shielded enclosure, power on, and place into airplane mode, if airplane mode is supported.

12.5.4. If this is not supported, examination shall be performed inside the shielded enclosure.

12.5.5. Attach the device with appropriate connectors for data extraction.

12.5.6. The tools that are appropriate for the examination of a mobile device will be determined by factors such as the examination request, the type of mobile device to be examined, and the presence of any external storage capabilities.

12.5.7. A communication channel must be established between the evidence device and the examination machine. The device must be detected successfully before the examiner may proceed with an automated examination.

12.5.8. It may be necessary to utilize various acquisition methods in order to extract as much data as possible.

12.5.8.1. If the evidence device cannot be successfully connected to an examination machine, but the device contents are accessible by visual examination, the requested evidence may be extracted manually by photographing the content of individual screens.

12.5.8.2. If evidence is visually observed on the device, but automated software extraction does not support the specific task to extract that visual evidence, then those specific screens may be photographed to supplement the automated extraction report.

12.5.9. Analyze the device and resident data to identify and recover specific data that addresses the customer extraction request. Document the details of the analysis.

12.5.10. Discrepancies noted during the examination must be documented in the case record.

12.5.11. The following information if applicable, should be documented in the LIMS report:

- Shielding method(s) employed
- Hardware(s) and software(s) (include version) used for the extraction.
- Record if the imaging fails and/or other recovered data discrepancies.
- Devices that are not supported by software may have the display content photographed through manual extraction, as described above.

12.5.12. The forensic copy and work product may be exported to the forensic server into an appropriately labeled case folder structure for temporary backup purposes. See F-SAN storage procedure section for further details.

12.6. QC Verifications

12.6.1. After processing mobile devices, examiners shall always verify the accuracy of the data extracted from the device where possible:

12.6.1.1. The examiner shall ensure that the identified and recovered data is an accurate depiction of what is on the submitted mobile target device through visual comparison. This comparison may be accomplished by randomly picking extracted data and comparing it to the data displayed in the mobile device. Another way to confirm an accurate data extraction is to verify that the mobile device has the same phone number from the SIM card (and/or serial #/IMEI).

12.7. Limitations

12.7.1. It may not be possible to bypass securities to obtain information from a mobile device or to utilize forensic examination software to successfully connect to the device to obtain intelligible, stored data. Furthermore, the device may be physically damaged, preventing connection and/or manual review of device content.

12.7.2. Currently there is no forensic product that acquires or parses all electronically stored information from every type of mobile device. Multiple forensic products and/or manual preservation (photography, video recording and/or transcription) may be necessary to document the information observed on the mobile device's display, where possible.

12.7.3. Forensic examination devices or software may not identify or recover all electronically stored information on all devices. This limitation can be identified through a manual review of identified and recovered data, unless a visual review is not possible (password lock, damaged screen, etc.).

12.7.4. There is no HASH verification required for cell phone and portable device imaging due to the volatile nature of memory storage and due to the fact that communication channels

must be established between the forensic examination device and mobile device. Therefore, some writing to the device is required to access the internal memory.

Digital Forensic Laboratory
Exigency/Non-Validated Procedures Exception

Forensic Analysis Division

3. EXIGENCY/NON-VALIDATED PROCEDURES EXCEPTION

3.1. Purpose

3.1.1. The purpose of this procedure is to acknowledge the necessity of releasing derivative evidence (generally exported to CD/DVD) to the customer prior to formal review of the LIMS report in some time-sensitive digital investigations.

3.1.2. This section also acknowledges instances where non-standard approaches to digital investigations may be required to examine new or emerging technologies where no formalized or validated procedures exist.

3.2. Overview

3.2.1. DFL examiners should use approved equipment, software, and procedures when processing evidence. However, due to the rapid development and release of new software and technology, there may be instances where non-validated procedures or devices, or examiner ingenuity must be employed to facilitate the examination of submitted devices to meet customer needs.

3.2.2. In exigent circumstances, it is understood there are instances where derivative evidence may be shared with customers prior to technical or administrative review of the LIMS report. The derivative evidence may contain investigative leads immediately necessary to safeguard lives or property. In these instances, by customer request, derivative evidence may be released prior to formal review, with lab supervisor authorization.

3.2.3. Regardless of the exigent circumstances involved, the official LIMS report will undergo technical and/or administrative review prior to being released to the customer. Non- validated procedures will be fully documented in the formal LIMS report.

3.2.4. Non-validated forensic software will undergo a validation in a timely manner.

3.2.5. In situations where non-validated procedures are used, the lab report will not claim accredited status nor utilize the ANAB logo symbol.

Digital Forensic Laboratory
Definitions and Abbreviations

Forensic Analysis Division

14. DEFINITIONS AND ABBREVIATIONS

14.1. Purpose

14.1.1. This procedure contains definitions and abbreviations used in the Digital Forensic Laboratory.

14.2. Scope

14.2.1. These abbreviations are used for all Digital Forensic Technical procedures.

14.3. Definitions And Abbreviations

- **Forensic Imaging Software**- software capable of creating a forensic "bitstream" copy, or exact duplicate of the submitted media.
- **Interpretive Software**- Software capable of reading file structure and intelligibly interpreting the files into a logical presentation. Most computer forensic software is capable of both forensic imaging and presentation of the content. The presentation of content is considered interpretive (a document file will appear with legible results, etc.) Non-forensic software, such as media players, MS Word, etc., are also considered interpretive when representing data.
- **Administrative Software**- Software used for administrative purposes, such as writing reports. The Laboratory Information Management System (LIMS) and MS Word are examples of administrative software.
- **Validation** – A performance confirmation of a tool, technique, or procedure through examination and the provision of objective evidence that it functions correctly and as intended.
- **Performance Verification –** The DFL internal confirmation that an externally validated tool, technique, or procedure performs as expected.
- **Quality Control Checks –** The periodic confirmation of the reliability of the equipment, software, and/or hardware such as towers and virtual machine.
- **BIOS** – Basic Input Output System. Program that manages computer system startup and data flow between the computer operating system and attached devices such as keyboard, mouse, and printer. The BIOS stores system and configuration settings for a computer including date, time, boot sequence, chipset information, attached hardware, and onboard interrupt handlers.
- **Target Drive** – Destination drive to store data transferred from submitted evidence drives.
- **Digital Media** - Any storage device that holds digital data.
- **EnCase boot**– CD/DVD or USB Drive
- **Wipe –** The act of completely erasing digital data from media.
- **F-SAN** – Storage device attached to the DFL internal server.
- **Hash Values:**

    - **MD5 –** Message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value commonly used to verify data integrity. Hash functions are commonly used to guard against malicious changes to protected data in a wide variety of software, Internet, and security applications, including digital signatures and other forms of authentication
    - **SHA-1 –** Secure Hash Algorithm is another cryptographic hash function. Its result is usually expressed as a 160 bit hex number. This algorithm was developed by the NSA.
- **Logical vs. Physical Imaging** – A logical image captures an evidentiary image of all, or a targeted subset, of the active data on a logical partition of a hard drive. This active (or visible) data is what one would find if you were to browse through the drive with My Computer on Windows or with the Finder on a Mac. A logical image doesn't include deleted files, file fragments, and deleted or clear space from a drive partition. Physical imaging creates an exact copy/bit stream image of the source media that is inclusive of logical files, along with deleted content, file fragments, and other content that may not be apparent to the casual user. Thus, physical imaging is the preferred method for data acquisition.
- **Portable Electronic Device** – Device such as a tablet, GPS unit, cellphone, etc., meant to be portable and stores digital data.
- **Ramsey Faraday Enclosure** – Device that shields its contents from cellular, Bluetooth, and WiFi signals.