DIGITAL FORENSIC UNIT PROCEDURES MANUAL

INDIANA STATE POLICE LABORATORY DIVISION
DIGITAL FORENSIC PROCEDURES MANUAL

TABLE OF CONTENTS

INDIANA STATE POLICE LABORATORY DIVISION
DIGITAL FORENSIC PROCEDURES MANUAL

1. Introduction

1.1. The Digital Forensics Unit (DFU) is a part of the Laboratory Division that provides the preservation, repair, acquisition, processing, analysis, and reporting of information stored on evidence in an analog or digital format.

1.2. Purpose

1.2.1. The Digital Forensics Procedures Manual is a resource for Indiana State Police (ISP) Digital Forensic Examiners (DFE's) on common digital forensic examination procedures. This manual should not be considered an all-inclusive procedure manual for every situation involving digital forensic examinations. Nor is intended to supersede ISP Rules, Regulations, Standard Operating Procedures (SOP's), Laboratory Division policies and procedures, or Physical Evidence Bulletins (PEB's).

1.2.2. Minor Deviations from the procedures in this manual shall be approved by the Digital Forensics Supervisor (DFS) before use. The deviation used, justification, and DFS's approval shall be documented in the Laboratory Inventory Management System (LIMS).

1.3. Scope

1.3.1. The DFU encompasses the preservation, repair, acquisition, processing, analysis, clarification, and reporting of information stored on evidence in an analog or digital format. The DFU is divided into sub-disciplines:

1.3.1.1. Computer and Mobile Device Analysis

1.3.1.1.1. DFE's analyze electronically stored information on a wide variety of devices, including computers, mobile phones and any digital storage device that contains memory.

1.3.1.2. Video and Image Analysis

1.3.1.2.1. DFE's analyze analog or digital video recordings or print or digital images to clarify details or intelligibility and provide data that is not readily apparent within an original multimedia or video recording or image. These recordings and images can originate from a variety of sources including video and digital cameras, surveillance systems, or other means.

2. Facilities

2.1. The DFU maintains its workspace facilities to ensure that environmental conditions do not adversely affect the outcome or reliability of technical procedures and results and that appropriate safety precautions are maintained.

2.2. Environmental Conditions

2.2.1. The workspace is air conditioned to prevent equipment overheating.

2.2.2. HVAC filters are changed regularly to reduce dust and indoor particulate matter.

2.2.3. The laboratory has sufficient electricity to support technical services.

2.2.4. Computer hardware equipment shall be connected to Uninterruptible Power Supplies (UPS's) when in use, if available in the workspace building infrastructure.

2.2.5. Any environmental conditions that impact a forensic process are documented in the Technical Notes.

2.3. Effective Separation

2.3.1. Technical services in the DFU workspace are generally conducted on forensic tower computers, or laptop computers, utilizing hard drives, mobile phones, other removable digital media, and/or other hardware.

2.3.2. Non-laboratory administrative functions, including access to agency networks, are conducted on separate computers that are not used for providing technical services.

2.3.3. Technical processes are performed in a designated area of each DFE's workspace. Work performed in any other area requires prior approval from the Digital Forensic Supervisor.

3. Safety

3.1. DFU workspaces should be equipped and maintained to help minimize safety risks to DFE's. Listed below are some risks and hazards unique to providing examination services for analog and digital evidence.

3.2. Biohazards

3.2.1. Physical devices submitted to the DFU may contain biohazardous material. Examiners are responsible for wearing proper Personal Protective Equipment (PPE), such as latex gloves and eye protection, when handling evidence that may contain biohazards. PPE, germicides, and hand sanitizers may be obtained from a Regional Laboratory or the Quartermaster Section and shall be used when appropriate.

3.2.2. If an item of evidence contains biohazardous material the DFE shall make attempts to clean the device before examination and clean their workspace after handling the evidence.

3.2.3. Examiners are also responsible for using appropriate evidence handling procedures to protect their workspace and limit biohazard exposure to themselves and others.

3.3. Sharp Objects

3.3.1. Some procedures require DFE's to disassemble devices with sharp edges, while some devices are submitted with damage exposing the DFE to sharp edges. Caution, and proper PPE, shall be used to minimize the potential for injury.

3.4. Lithium Batteries

3.4.1. In certain situations, DFE's may encounter lithium batteries. In the event of encountering a damaged lithium battery, or if a lithium battery becomes damaged during handling, DFE's shall be aware that a lithium battery can enter an uncontrolled, self-heating state that can release gas, cause a fire, or even an explosion. Each workspace shall maintain a container, filled halfway with sand, and a fire extinguisher suitable for electrical fires.

3.5. Electric Shock

3.5.1. DFE's shall be familiar with proper methods to disassemble items that may be capable of electrical shock. Devices should not be connected to power and the batteries of portable devices should be disconnected as soon as practical during disassembly.

4. Limitations

4.1. Device diversity and the rapid evolution of technology:

4.1.1. The constant influx of new devices and the rapid evolution of technology pose a challenge for DFE's to keep pace with all hardware and software variations. Many devices use closed systems and have proprietary interfaces that limit access to critical data, necessitating specialized tools or reverse engineering techniques.

4.1.2. Counterfeit devices often lack proper documentation and compatibility with standard forensic tools, complicating data recovery efforts.

4.1.3. These factors may necessitate manual data extraction methods, which can be time-consuming and less reliable than automated tools.

4.2. Data Volatility:

4.2.1. Data can change during extraction and analysis due to device processes or background activities, even with write-blocking techniques.

4.2.2. Volatile data, like Random Access Memory (RAM) content or temporary files, may be lost or modified during the examination process. DFE's shall be aware of and document in the Technical Notes any adjustments made to the settings of a device during an examination.

4.3. Device Damage:

4.3.1. Extensive physical damage or liquid contamination can render data extraction impossible or significantly reduce recoverable data.

4.3.2. Internal hardware failures from faulty components or damage can prevent data access or corrupt stored information.

4.3.3. Software malfunctions such as operating system crashes or corrupted firmware can make data inaccessible. Prior assessment of device condition is essential. Data extraction may not be possible on severely damaged devices, and manual methods may be ineffective.

4.4. Software Limitations:

4.4.1. Not all forensic software tools support every device model or operating system version, which may lead to partial or failed extractions. Some tools may not offer comprehensive data recovery capabilities, requiring additional tools or manual techniques for specific data types.

4.4.2. New software versions may introduce compatibility issues or bugs, requiring ongoing evaluation and updates of forensic tools. DFE's shall be familiar with the limitations of their chosen tools and consider alternative methods when necessary.

4.5. Encryption and Passcodes:

4.5.1. Advanced encryption algorithms can make data decryption impossible without the proper key or brute-force techniques. Passwords, PIN codes, or other user-enabled locking mechanisms can prevent access to data even if it is not encrypted. As a result, data extraction may be completely blocked, and brute-force attempts carry risks of potential hardware damage or software corruption.

4.6. Audio and/or Video Limitations:

4.6.1. Clarification of some audio/video recordings may not significantly improve audio/video clarity due to the quality and characteristics of the original recording.

4.6.2. Some digital cameras may preserve data only so long as power is provided; therefore, care should be taken to examine these devices as soon after submission as possible to reduce the potential for data loss.

4.6.3. Other limiting factors include:

4.6.3.1. Low resolution.

4.6.3.2. Limited focal length.

4.6.3.3. Compression.

4.6.3.4. Media wear.

4.6.3.5. Extremely poor signal-to-noise ratio.

4.6.3.6. Severe distortion.

4.6.3.7. Insufficient bandwidth.

4.6.3.8. Technical limitations and proprietary files of the recording devices/systems used to make the original recording.

4.6.3.9. The physical environment where the original recording was produced.

5. Equipment, Maintenance, and Use

5.1. The reliability and performance of the equipment used in the examination of analog and digital evidence shall be monitored to ensure the equipment is operating properly.

5.2. The DFU uses methods that are widely accepted in the digital and multimedia evidence forensic disciplines. These are known to produce outcomes consistent with the technical services requested by the contributor.

5.3. Equipment and Maintenance

5.3.1. Equipment consists of hardware (such as computers, write-blockers, and audio/video players), and software (such as computer programs).

5.3.2. DFE's shall report and document any anomalous performance of the equipment immediately to the DFS.

5.3.3. Maintenance shall consist of upgrades or replacements of hardware or components, and major updates to Operating Systems (OS).

5.3.4. All equipment shall be maintained in accordance with the manufacturer's specifications and recommendations as per operating and warranty manuals.

5.3.5. All maintenance shall be documented on the Maintenance Log and retained in the DFU.

5.4. Use

5.4.1. DFE's can use equipment (hardware and software) to perform the examination of analog and digital evidence as described in this manual.

5.4.2. Computer system hardware equipment shall maintain active and current security software and utilize unique password or Personal Identification Number (PIN) code protection. Network access requires the use of a firewall.

5.4.3. Any equipment integrated into an OS, that is intended for routine consumer or commercial use is generally regarded as reliable by merit of the testing and validation conducted by the operating system developer, as well as by the widespread use within the computing industry as well as the digital and multimedia forensic community.

5.4.4. Equipment used to acquire, view, process, parse, or analyze data is generally regarded as reliable by merit of the testing and validation conducted by the developer, as well as by the widespread use in the digital and multimedia forensic community. Use may be necessary for data with proprietary formatting or encoding for which no other equipment has been developed or validated. However, performance verification may be required.

6. Validation

6.1. The purpose of validation testing is to ensure that methods produce reliable and consistent results, and that equipment and software identified in the methods are suitable for their intended purpose. Prior to starting validation testing, a validation plan must be submitted and approved by the DFS.

6.2. The equipment the DFU utilizes for casework is considered its "methods" and are either commercially available, non-commercially available, or laboratory created.

6.3. Commercially available equipment used within its designed application range can be considered sufficiently validated, however, may be subject to performance verification (as described in the Performance Verification section of this manual).

6.4. Non-commercially available equipment used within its designed application range is subject to performance verification (as described in the Performance Verification section of this manual).

6.5. All equipment used outside its intended scope shall undergo formal validation testing prior to being approved and placed into service for DFU use.

6.6. The validation process shall evaluate the equipment against specific requirements to determine its acceptance and suitability. The validation needs and requirements will depend on the equipment's purpose, the nature of the data analyzed, and whether any direct results will be reported.

6.7. Validation testing is not required for equipment designed to decrypt encrypted data or identify, remove, or bypass security measures.

6.8. Prior to beginning a validation process, consult the DFS and available guidelines in order to develop an appropriate validation procedure. A validation procedure should consist of the following elements:

6.8.1. Introduction – State the purpose and a brief description of the method validated or the change(s) to an existing validated method.

6.8.2. Method – Include instructions for performing the method validated or changes to existing validated method including reagents, reference materials, quality control samples, instruments and equipment, and its performance or acceptance requirements.

6.8.3. Validation Process – Describe how the validation was performed including determination of the performance characteristics of the method.

6.8.4. Results – Summarize in text, tables, or graphs, the data collected during validation process. Discuss the meaning of the data and results in relation to the method validation. When applicable, determine the uncertainty of measurement.

6.8.5. Conclusion – Summarize the results of the validation and include a statement on the validity of the method, detailing its fitness for the intended use.

6.9. Validation testing completed by a reputable external entity can be used in lieu of internal testing if the validation procedure is deemed acceptable by the DFS.

6.10. It is not always possible to validate experimental approaches with unknown results, and in these instances, the final report shall not include the accreditation statement.

7. Performance Verification

7.1. Performance verification is a quality assurance measure used to assess the functionality of the equipment that may affect the accuracy of forensic examination results.

7.2. The performance verification process shall evaluate equipment against specific requirements in order to determine its acceptance and suitability. The performance verification needs and requirements will depend on the function of the equipment.

7.3. Relevant equipment is considered verified after a successful Power-On Self-Test (POST) and, if applicable, OS load.

7.4. Relevant software equipment is considered verified after a review of the available product documentation (e.g., release notes or specifications) confirms that the software can acquire, view, process, parse, or analyze data in a way that is applicable to a given task.

7.5. Performance verification is not required for equipment designed to decrypt encrypted data or identify, remove, or bypass security measures.

7.6. Additional specific performance verification requirements are listed below for certain equipment:

7.6.1. Write-blockers

7.6.1.1. Performance verification of write-protecting hardware shall consist of confirmation that the hardware's write-protect settings are enabled. Confirmation will be dependent on the method of indication employed by the device. Performance verification of write-protecting software shall consist of confirmation that the target device indicates a write-protected or read-only status and done on an annual basis.

7.6.2. Shielded Testing Enclosures

7.6.2.1. Performance verification of radio frequency shielded testing enclosures shall consist of the annual testing and documentation to ensure that cellular, Wi-Fi, and Bluetooth frequencies are successfully shielded.

7.6.3. Video Analysis

7.6.3.1. Analog performance verifications shall consist of a prerecorded color bar, frame counter and audio tone recording utilizing the proper media format per case requirements. The acceptable result is a visual display of the color bar, an audible tone, and visual display of the frame counter in frames per second to ensure frames are not being dropped.

7.6.4. Software

7.6.4.1. Software equipment used to acquire, view, process, parse, or analyze data shall undergo performance verification after a major release. For the purposes of this manual, a software release is considered major when there is a whole number change. The software version number indicates whether a software update is major or minor. A version changes from 7.1 to 7.2 is minor, while a change from 7.1 to 8.0 is major.

7.7. When equipment used for an examination is uniquely identified in the analytical notes, it should also indicate that it successfully passed performance verification unless otherwise noted.

7.8. Equipment verified and placed into service for DFU use shall be approved by the DFS or a qualified DFE in the applicable sub-discipline and documented in the appropriate log.

7.9. Subsequently released versions of previously verified equipment shall be approved for DFU use after the DFS or a qualified DFE in the applicable sub-discipline reviews the available release notes and either determines that additional performance verification is not required or completes the additional validation or performance verification.

7.10. Performance verification of existing equipment returned to service after repair, modification, maintenance, or calibration shall be documented in the appropriate log.

8. Evidence and Intake

8.1. This procedure ensures that submitted items are properly documented, including their condition upon submission to the DFU.

8.2. Devices submitted to the DFU could include laptop or desktop computers; external or portable hard disk drives; portable flash-type memory storage devices; mobile devices such as mobile phones or tablets; various audio/video recording devices such as security digital video recording devices; small Unmanned Aerial Systems (sUAS's); vehicle infotainment systems, among other items not listed here.

8.3. When handling evidence items, consider that there might be a need for other forensic analyses such as DNA or latent print examination, and determine the proper order of analyses. Wear PPE when appropriate.

8.4. Procedure

8.4.1. Upon receiving an item for examination, inspect the item to document the condition of the make, model, serial number (or some such unique identifying number), and other unique features. Record this information, as well as other information contained in the appropriate Technical Notes form and include it in the case.

8.4.2. The DFE shall photograph and document any damage or abnormalities that may affect the examination in the Technical Notes. Upload photographs of such abnormalities to the case file.

8.4.3. Photographs may also be used to supplement the Technical Notes.

8.4.4. If an item submitted to the DFU for examination has more than one storage source that can be examined for data, subdivide the item as follows:

8.4.4.1. Computers with more than one hard disk drive or additional removable storage devices. Consider the first hard drive to be the same number as the item number (e.g., Item 1). Subdivide the second hard drive or other storage devices with the parent item as Items 1A, 1B, and so on.

8.4.4.2. Mobile devices with internal non-removable storage and more than one removable internal storage device (e.g., removable SIM card, removable flash memory card, etc.). Consider a cell phone with internal non-removable storage to be the same number as the item number (e.g., Item 1). Only subdivide a SIM card, Micro SD card, or other storage devices as Items 1A, 1B, etc. if it is to be separated from the parent item for an external provider.

8.4.4.3. Multiple items of loose media within the same packaging (e.g., multiple USB thumb drives, hard drives, or other flash media). Consider the packaging that the items were contained in to be the same number as the item number (e.g., Item 1), then subdivide the items themselves as Items 1A, 1B, and so on.

9. Computer/Mobile Device Data Preservation & Acquisition

9.1. Computer and mobile device analysis is the scientific examination of electronically stored information originating from a variety of computer, mobile and digital storage devices. Due to the vast number and types of legacy, current and emerging devices, there are inherent qualities that prohibit the establishment of a rigid set of procedures to cover every case; therefore, it is acceptable for the examiner to select the appropriate course of action. Regardless, careful documentation and meticulous handling are crucial to preserve data integrity and ensure accurate analysis.

9.2. In certain situations, the repair or replacement of part(s) may be necessary for data acquisition to occur. In these circumstances, document the repair or replacement in the Technical Notes. Photographs may also be suitable and should be included in the case file.

9.3. Computers and Other Digital Storage Devices

9.3.1. Conducting an analysis directly on the original submitted digital evidence should be avoided whenever possible.

9.3.2. Data Preservation

9.3.2.1. To ensure evidence integrity, write-protection is crucial for devices to be examined. Whenever possible, devices with original data or recordings receive write-protection upon entering the examination process. If a physical write-blocker is unavailable, software write-protection may be used.

9.3.2.2. Not all devices can be accessed read-only, or utilizing write-protection, so if an eligible device is accessed as read-write, the reason shall be documented in the Technical Notes.

9.3.2.3. Read-only and write-protecting mechanisms are not required for mobile devices, or other devices where their internal storage is not removable, and/or is not accessible or recognizable by available equipment.

9.3.2.4. For devices with network capabilities, precautions are to be taken to preserve user data. Manually enter the device into an offline mode (commonly referred to as airplane mode), if possible. If possible or applicable, a shielded testing enclosure can be utilized.

9.3.3. Data Acquisition

9.3.3.1. This procedure describes creating a forensically sound image (a bit-for-bit copy, also referred to as a forensic image) of digital media evidence. In case of damaged or failing media, attempts to image and the reason for failure shall be documented in the Technical Notes.

9.3.3.2. Adapt measures and equipment used to obtain the forensic image based on the device type and given circumstances.

9.3.3.3. Document any abnormal conditions in the Technical Notes. If the imaging process fails or hash values mismatch, attempt imaging again.

9.3.3.4. Generate and document a hash value for the acquired forensic image. Verify image integrity by comparing acquisition and verification hash values.

9.3.3.5. A post-acquisition hash is not required for a mobile device, or other devices where their internal storage is not removable or is not accessible or recognizable by available equipment.

9.3.3.6. DFE's do not have the authority to access or acquire evidence source data that is stored on a cloud source; however, cloud data already obtained from a cloud source may be submitted for analysis.

9.4. Mobile Devices

9.4.1. Mobile devices present unique challenges for DFE's due to their rapid technological advancement, diverse operating systems, and potential for data loss during examination. It may be necessary to utilize several different equipment, software, and acquisition methods in order to extract as much data as possible.

9.4.2. Data Preservation

9.4.2.1. If the mobile device is submitted powered on, attempts should be made to completely isolate the device from all cellular, Bluetooth, and WiFi signals. This can be achieved through several methods such as manually enabling the offline mode or by placing the device in a shielded enclosure.

9.4.2.2. If the mobile device is powered off at the time of submission, any removable media such as a SIM card or some sort of solid-state memory card should be removed and examined before powering on.

9.4.3. Data Acquisition

9.4.3.1. Approved hardware and software should be utilized for data extraction. However, not all forensic software tools support every device model or operating system version, which may lead to partial or failed extractions. The chosen method and any anomalies that occur during the process should be documented in the Technical Notes.

9.4.3.2. An advanced data extraction technique, commonly referred to as "chip-off", may be necessary to acquire data. The chip-off process is destructive by nature and will render a device inoperable. There is also the possibility of destroying potential evidence.

9.4.3.3. Use heat or the process of material reduction to separate the memory micro-chip from the Printed Circuit Board (PCB).

9.4.3.4. All chip-off examinations will require legal authority. Likewise, thorough research shall be conducted prior to performing the chip-off to determine the level of support. The chip off procedure shall be documented in the Technical Notes.

9.4.3.5. Physical or software-based brute-forcing may be necessary to unlock a mobile device so that the most data can be acquired. Brute-forcing is a trial-and-error type attack on PIN codes and passwords.

9.4.3.6. DFE's should be aware that continuous running of brute-force processes can generate excessive heat, leading to component failures or permanent damage. Plus, overburdening device resources can cause crashes, restarts, or data loss. At a minimum, on a yearly basis, if the device is actively brute-forcing, then the DFE shall check with the investigating officer to see if the examination is still necessary.

10. Computer and Mobile Device Examination and Analysis

10.1. The purpose of this procedure is to establish a guideline and framework for the baseline examination and analysis of submitted digital media.

10.2. The specific examination techniques and data recovered may be dependent on the type of device submitted, the contributor's request, legal authority, and other factors that are to be applied to each examination. These procedures should be adapted as necessary based upon the type of device, and the equipment and software to be used to facilitate the examination and analysis processes.

10.3. 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.

10.4. Below is a list of possible analytical processes that DFE may conduct in an examination. DFE's can extract, recover, identify, or analyze:

10.4.1. Passwords and encryption.

10.4.2. Deleted or hidden partitions, folders, or files.

10.4.3. File signatures and file headers.

10.4.4. Internet history.

10.4.5. Databases.

10.4.6. Location data.

10.4.7. Operating system and program artifacts.

10.4.8. Registry hives.

10.4.9. User accounts.

10.5. DFE's can also:

10.5.1. Identify picture and video files related to the examination request.

10.5.2. Analyze communications such as email or native or third-party chat messages.

10.5.3. Analyze document files such as text files or spreadsheets.

10.5.4. Carve data from unallocated space, unused space, or file slack.

10.5.5. Conduct keyword or text string or regular expression searches.

10.5.6. Use hash databases to include or exclude known data.

10.5.7. Detect evidence of system compromise, if needed, or anti-forensic programs or artifacts.

10.5.8. Conduct timeline searches.

10.6. If necessary, a manual examination of the device should be conducted to capture non-extractable data or verify extracted data against observable content. The process and captured data should be documented in detail in the Technical Notes.

10.7. The extracted data may be compared against the viewable content on the device whenever possible. Any discrepancies or inconsistencies should be documented in the technical notes. Any deviations from approved hardware, software, or procedures require written approval from the DFS and thorough documentation in the technical notes.

11. Forensic Audio/Video Examination and Analysis

11.1. The purpose of this document is to provide an overview of methods for the examination and analysis of audio/video recordings.

11.2. This procedure applies to DFE's tasked with the duplication, analysis, or clarification of audio and or video recordings. Various equipment and computerized hardware and software may be used.

11.2.1. Forensic Video Analysis (FVA) is defined as the scientific examination, comparison, and/or evaluation of video in legal matters.

11.2.2. Audio clarification is the processing and filtering of audio recordings to improve the signal quality and intelligibility of the signals of interest, such as speech, by attenuating noise or otherwise increasing the signal-to-noise ratio.

11.3. Due to the vast number and types of legacy, current, and emerging devices there are inherent qualities that prohibit the establishment of a rigid set of procedures to cover every case; therefore, it is acceptable for the DFE to select the appropriate course of action.

11.4. Due to the rapid development and release of digital devices capable of producing audio/video recordings, it may be necessary to deviate from the standard processes. Prior approval by the DFS shall be obtained and documented in the technical notes.

11.5. Audio/Video Data Acquisition

11.5.1. For original digital recordings or images submitted on a computer or mobile device, or their associated digital storage devices, follow any applicable guidelines, listed in this manual.

11.5.2. For original analog recordings or images, and derivative digital recording or images, conduct a physical examination of the analog or digital storage device and document identifying information, unusual markings, and defects. If defects are present, the item may require cleaning and/or repair prior to any analysis. If available and necessary, obtain any applicable manuals or documentation for the device.

11.6. Audio/Video Examination and Analysis

11.6.1. When handling requests for audio/video analysis, qualified DFE's shall generally:

11.6.1.1. Examination priority, integrity, and protection of the original recording.

11.6.1.2. Review the contributor's report and supporting documentation.

11.6.1.3. Consider anti-malware or virus scans, when applicable.

11.6.1.4. Consider physical or software write-protection.

11.6.1.5. Once a working copy has been made, perform the requested services.

11.6.1.6. Create a report of findings, if applicable.

11.6.1.7. Document the relevant processes in the Technical Notes.

11.6.1.8. Return original recording and findings to the contributor.

12. Examination Documentation and Reporting of Results

12.1. It is the duty of DFE personnel to document and report the results of each examination in a manner that is not only accurate and clear, but also objective. All reports and Technical Notes shall contain details about the examinations that were conducted and any additional information that might be required for interpreting the results.

12.2. The process of documenting these reports is an integral part of the DFE's responsibilities.

12.3. Content and Accuracy

12.3.1. The role of the DFE is to provide an objective analysis of the data found on the device in question. The DFE's findings are strictly limited to the interpretation of this data and do not extend to opinions on the broader investigation.

12.3.2. The data retrieved from the device has been extracted using industry-standard digital forensic tools and methodologies. The findings are presented in this report with the aim of providing clear information about the state, authenticity, and relevance of the digital evidence.

12.3.3. It is important to note that any opinions or conclusions about the implications of these findings for the overall investigation are outside the scope of this report. Such determinations should be made by the contributor, who has a comprehensive understanding of the broader context and details of the case.

12.3.4. The DFE's role is to ensure the integrity and reliability of the digital evidence, and as such, any opinions expressed in this report are confined to these areas of expertise.

12.4. Examination Documentation

12.4.1. Documentation may be accomplished through handwritten or electronically generated technical notes, photographs or other documents stored electronically in the case file.

12.4.2. Examination documentation shall contain sufficient detail to allow another qualified examiner to repeat the analysis under conditions as close as possible to the original and interpret the data.

12.4.3. The end date on the first page of the technical notes reflects the date when the examination was completed.

12.5. Reporting of Results

12.5.1. Reports shall include, at a minimum:

12.5.1.1. Reporting for all items received. Including items on which no work was performed but was requested.

12.5.1.2. Items collected or created and preserved for future testing.

12.5.1.3. Reporting for all work performed, both partial and complete.

12.5.1.4. Explanation of any anomalies, if applicable.

12.5.1.5. The DFE's name, title, and address of the facility in which they are located.

12.5.1.6. A unique identification number of the completed report.

12.5.1.7. Contributor information. This should include the contributor's name, agency, case number, and potentially their contact information.

12.5.1.8. Descriptions and conditions of the submitted items.

12.5.1.9. Any results from external providers, if applicable.

12.5.1.10. Examination starting and ending date.

12.5.1.11. Examination testing methods used.

12.5.1.12. Results for each item examined.

12.5.1.13. Any deviations or exclusions utilized.

12.5.1.14. The identification of the person authorizing the report.

12.6. The DFE shall make use of LIMS to prepare the summary report. Any relevant Technical Notes shall also be given to the contributor and documented if included on a Report Drive or other media for review.

12.7. Once a DFU report has been approved, any amendments shall be made in the form of an amended report following the same reporting requirements stated above. Any change of information shall be clearly identified and, where appropriate, the reasons for change included.

12.8. Digital Forensics Software Generated Reports

12.8.1. Software-generated reports may be available to the contributor. The contributor can always seek further assistance of clarification, verification, or additional analysis from the DFE.

12.8.2. Forensic Software Generated Report allow for:

12.8.2.1. Independent exploration:

12.8.2.1.1. Contributors with relevant knowledge about the investigation can conduct their own searches within the provided data.

12.8.2.2. Collaboration opportunities:

12.8.2.2.1. Reports facilitate informed discussions and collaboration between the DFE and the contributor.

12.8.2.2.2. There are limitations of Digital Forensic Software Generated Reports, such as potential for misinterpretation or missing context. The DFE's expertise remains crucial for interpreting complex data and ensuring its accurate use in the case so this can be testified in court.

13. Administrative and Technical Reviews

13.1. The DFE is responsible for preparing accurate, complete, and organized Technical Notes.

13.2. The DFE shall review documentation constituting the case file (examination records and administrative records) for compliance with laboratory policy and procedures and technical accuracy prior to submitting the case for administrative or technical review.

13.3. Administrative Review

13.3.1. At the completion of an examination and, if possible, prior to returning the evidence to the contributor, an administrative review shall be conducted by a member of the DFU, who has been trained and authorized to perform administrative reviews on all DFU Summary Reports, prior to the release to the contributing agency. The individual completing administrative reviews shall indicate in LIMS that the Administrative Review has been completed. Administrative reviews shall not be conducted by the author of the DFU Summary Report.

13.3.2. The Administrative Review shall include:

13.3.2.1. A review of the DFU Summary Report for spelling and grammatical accuracy.

13.3.2.2. A review of all technical notes associated with the DFU Summary Report to ensure that the records are uniquely identified according to laboratory policy and procedure.

13.3.2.3. A review of the DFU Summary Report to ensure that all key information is included.

13.4. Technical Review

13.4.1. A technical review is an evaluation of the DFU Summary, Technical Notes, and the appropriate administrative records which comprise a DFU examination. This review consists of determining whether the appropriate examinations have been performed, and whether or not the conclusions are consistent with the recorded data and are within the scope of the discipline or category of examination.

13.4.2. The DFS shall be notified of any substantive nonconformance related issues identified during a technical review. The severity and significance of the nonconformance issues shall determine the nature of the corrective action taken by the Digital Forensic Supervisor.

13.4.3. If the reviewer finds an error in the examination record, the reviewer shall notify the DFE. The DFE shall make the necessary corrections to the electronic examination record. The corrected pages of the electronic examination record shall be uploaded as an attachment in LIMS. All pages of the original electronic examination record shall be retained.

13.4.4. The reviewer shall ensure all necessary corrections were made by the DFE in the examination record before approving the case.

13.4.5. Technical reviews shall be conducted by individuals authorized by the Division Commander and have expertise gained through training and experience in the category of testing being reviewed. In addition, the technical reviewer shall have knowledge of the DFU examination methods. The reviewer shall complete the DFU Technical Review Checklist and upload the completed checklist to LIMS.

13.4.6. The DFU shall conduct a technical review on a minimum of one (1) case from each DFE on a quarterly basis. Technical reviews shall not be conducted by the DFE issuing the DFU Summary Report under review.

14. Authorized Casework and Proficiency Testing

14.1. Full-Time DFE's can be authorized to work on casework after approval from the Laboratory Division Commander.

14.2. Each DFE conducting examinations in the Digital Forensic Unit shall participate in the Laboratory Division's proficiency testing program. Participation, evaluation, documentation, and any necessary corrective actions shall comply with procedures listed in the Laboratory Division Quality Assurance Manual.

14.3. Procedures used for analysis of proficiency samples shall be similar to the procedures used for casework examinations and shall follow best practices for digital evidence.

14.4. The DFS shall assign the annual external proficiency sample to one DFE at each DFU Office location. The DFE's are to complete the examination and forward the results and all notes and documentation to the DFS prior to the completion deadline.

14.5. All DFE's in the DFU shall participate in one open, external, or internal proficiency test in digital forensics annually. Exceptions to this procedure include DFE trainees released for casework after all proficiency samples have been distributed, and DFE's who are unavailable during the proficiency timeframe.

15. Appendix 1 Terms and Definitions

15.1. **After First Unlock (AFU)** - a state of a mobile device that has been powered on and the user has entered the passcode to unlock the device, even if the device is currently locked.

15.2. **Advanced Logical Extraction** - a logical extraction combined with a file system extraction which can contain deleted or hidden files within the databases as well as the user data stored within the files and folders of a device.

15.3. **Axiom** - Digital media forensic tool to find, analyze and report on digital evidence from computers, smartphones, and tablets. https://www.magnetforensics.com/products/magnet-axiom/

15.4. **Before First Unlock (BFU)** - a state of a mobile device that has been powered on and the user has not entered the passcode to unlock the device.

15.5. **BFU Extraction** - a limited file system extraction which may contain some deleted and hidden files in the databases. More data may be extracted from an AFU extraction than from a BFU extraction.

15.6. **Cellebrite** - Industry-leading mobile forensic tool for examining cell phones and other mobile devices. http://www.cellebrite.com

15.7. **Chip-Off Process** - Process that involves the removal of a memory chip from a printed circuit board to conduct analysis.

15.8. **Code-Division Multiple Access (CDMA)** - The mobile phones using this cellular system do not incorporate a card and the device's assigned phone number is stored on the mobile phone.

15.9. **CSAM** - United States federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (a person less than 18 years old). These images are also referred to as Child Sexual Abuse Material (CSAM) to most accurately reflect what is depicted the sexual abuse and exploitation of children. These images and videos depict actual crimes being committed against children. https://www.missingkids.org/

15.10. **Deleted File** - When a file is deleted, the data associated with the file may not be erased. The index entry associated with that file is slightly changed so that the operating system no longer sees the file as valid. Nearly all file attributes and data can be recovered from a deleted file until the file data or file index entry has been overwritten.

15.11. **Destination Media/Drive** - Used during an examination to store images, analysis output, or serve as a working copy of the data recovered from the original media submitted. Also referred to as "target drive" or "target media."

15.12. EXIF Metadata - EXIF (Exchangeable Image File) is a standard format for storing information in digital photography used by digital cameras, cell phones, camcorders, etc. Types of EXIF data may include: camera make/model, original thumbnail, date and time digitized, resolution, shutter speed, GPS coordinates, and more.

15.13. Filesystem Extraction - A filesystem extraction is a technique used in mobile forensics to acquire data from a mobile device. It works by copying the entire file system of the device, which includes all the files and folders present on it. This encompasses user data like documents, photos, videos, contacts, and messages. It also captures application data such as app settings, cached data, and potentially deleted information within apps. Additionally, system files like operating system files and configuration settings are included in the extraction.

15.14. Firmware - In computing, firmware is a specific class of computer software that provides low-level control for a device's specific hardware. Devices such as printers, scanners, cameras, and USB flash drives have internally stored firmware.

15.15. Forensic Computer or Forensic Workstation - Computer system used for the examination of digital evidence.

15.16. Forensic Operating System Drive - Hard drive containing the operating system and the approved forensic software that can be used in the examination of submitted media.

15.17. Forensically Sound Bootable Disk - Linux Operating System - Bootable Linux operating system that runs entirely in the computer's memory and can be configured to mount devices connected to the system in a read-only state (e.g., Sumuri Paladin).

15.18. Forensically Sound Bootable CD for Intel-based MAC hardware - Bootable CD for Intel-based MAC 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 since all media on the system is placed in read-only mode.

15.19. Full Filesystem Extraction - A full filesystem extraction is a more comprehensive version of a regular filesystem extraction. Its goal is to capture all possible data from the device's file system. This includes everything obtained in a regular extraction, along with deleted data that might not be readily accessible through standard techniques. Examples of such deleted data include fragments of deleted files, messages, or call history. Additionally, it aims to capture hidden data that applications or the operating system might conceal from traditional views.

15.20. Global Positioning System (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.

15.21. 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 this system do not store the device's assigned phone number.

15.22. **Hash Value** - A hash is a unique alphanumeric value that represents the data.

15.23. **Hierarchical File System (HFS)** - File system developed by Apple for use in computers running MAC operating systems. HFS is also referred to as MAC OS Standard.

15.24. **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-OS Extended.

15.25. **ICCID** - Integrated Circuit Card Identifier, uniquely identifies the SIM itself.

15.26. **IMSI** - International Mobile Subscriber Identity, identifies a subscriber's account with the cellular network provider.

15.27. **Internet Browser History** - When using an Internet web browser, the history is an index of websites the user has visited. The history also lists the files on the local machine which have been viewed. Depending on the type of history index, the entry will record the website (or file) visited, the user account logged in at the time, and the date and time.

15.28. **LNK Files** - Files that contain pointers to other files, usually to make access to them faster or more convenient for the user without having to move the original file. For example, a LNK file associated with an executable program can be created or present on a user's desktop so that the user does not have to navigate to the specific location for a program each time they want to use it. When the shortcut file is selected or run it points to the location the executable is stored in and the executable will run.

15.29. **Logical Acquisition Copy or Logical Copy** - An accurate reproduction of information contained within a logical volume (e.g., mounted volume, logical drive assignment, etc.)

15.30. **Logical extraction** - Extracted data like contacts, messages, and photos. It's faster than the other types of extractions but can't recover deleted information or access locked devices. This method is ideal for grabbing readily available data quickly and preserving its integrity for investigations.

15.31. **Manual Data Extraction** - When used to describe mobile phone examinations, this is a process that involves manually using the keypad and handset display to document data present in the mobile phone's internal memory.

15.32. **Manual Examination** - A manual examination is performed during a forensic examination when data extraction techniques are unsuccessful or unavailable. This may occur when a device is not supported by the laboratory's forensic tools, damage to the device prevents data extraction, or when a forensic examiner observes additional data on the device that was not observed in the extraction report. A manual examination consists of a forensic examiner powering on the device and manually navigating through it in a controlled environment. Any notable data observed throughout a manual examination is photographed or otherwise recorded. During this process the device is fully isolated from cellular, WiFi, and Bluetooth signals, when applicable.

15.33. **Metadata** - File metadata is additional information about the file such as author(s), dates and times, revisions, hidden text, file properties, comments, company, or organization name, and more.

15.34. **Mobile Device** - A portable device that has an embedded system architecture, processing capability, on-board memory, and may have telephony capabilities (e.g., cell phones, tablets, and smartphones). Mobile or 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 computers which allow users to store information e-mail, and install programs, photographs, and other data in one device.

15.35. **MSISDN** - Mobile Subscriber ID, normally illustrates the number dialed to make contact with the device.

15.36. **Physical Extraction** - a bit-for-bit copy of the flash memory of a device which can include deleted and hidden data.

15.37. **Secure Folder** - Samsung Secure Folder is an encrypted space on your smartphone for storing files, images, videos, and apps for your eyes only.

15.38. **Slack Space** - A hard drive is comprised of many small allocation blocks. Unallocated space consists of all the allocation blocks not currently assigned to a valid file. These blocks are available to be written to. Data can reside in unallocated space if a file has been deleted and its index entries have been overwritten. When a new file is written, a certain number of these allocation blocks are used depending on the size of the file. The new file's data will overwrite any old data in the allocation blocks; however, it is not likely that the new file will completely fill the entire portion of the last allocation block. The area from the end of the new file data to the end of the last allocation block is called the swap space of the file. Since this area has not been overwritten, data from a previous file can reside in the swap space.

15.39. **Swap File/Page File** - Swap files are relied upon by Windows to create "virtual memory"; i.e., using a portion of the hard disk drive for memory operations. These files are used as a "scratch pad" to write data when additional Random Access Memory is needed.

15.40. **Temporary Internet Files** - Temporary internet folders are the location on a user's hard disk in which a web browser stores the data from a web page or URL address that the user visits. When the web server sends the web page files to the browser, they are stored in a file so that the next time the user visits the same web site the browser takes the data from the temporary Internet file. With this method, the page quickly displays in the browser instead of having to wait for a response from the website's server again. Temporary internet files are downloaded to the user's computer automatically and the process does not require the consent or even the knowledge of the user. One web page or URL address can download numerous temporary internet files to the user's hard drive.

15.41. **Unallocated Space** - A hard drive consists of allocated space and unallocated space. Allocated space is the portion of the drive containing the operating system and accessible user files. Unallocated space, also known as free space, is the unused portion of a drive where space is available for data to be written.

15.42. Time Zones:

15.42.1. Eastern Standard Time (EST), when observing standard time (autumn/winter), are five hours behind Coordinated Universal Time (UTC−05:00). Eastern Daylight Time (EDT), when observing daylight saving time (spring/summer), are four hours behind Coordinated Universal Time (UTC−04:00).

15.42.2. Central Standard Time (CST) is six hours behind Coordinated Universal Time (UTC). During summer, most of the zone uses daylight saving time (DST), and changes to Central Daylight Time (CDT) which is five hours behind UTC.

15.42.3. Coordinated Universal Time or UTC is the primary time standard by which the world regulates clocks and time. It is within about 1 second of mean solar time at 0° longitude and is not adjusted for daylight saving time. It is effectively a successor to Greenwich Mean Time (GMT).

15.43. **VCF File - vCard**, also known as VCF (Virtual Contact File), is a file format standard for electronic business cards. vCards can be attached to e-mail messages, sent via Multimedia Messaging Service (MMS), on the World Wide Web, instant messaging or through QR code.

15.44. **X-Ways** - X-Ways Forensics is an advanced work environment/tool for computer forensic examiners. www.x-ways.net