Technical Procedure for Computer Forensic Examinations

1.0 Purpose – This procedure describes the processes and best practices of computer forensic examinations.

2.0 Scope - This procedure applies to computer forensic examinations conducted by personnel of the Digital Evidence section. The case specifics and legal authorization will determine which techniques and processes shall be required for examination.

3.0 Definitions – See Digital Evidence Dictionary

4.0 Equipment, Materials and Reagents

- Forensic computer
- Forensic software or hardware from the Approved Software and Hardware List
- Target drive
- Write-Blocker
- Hash Value Set (file filter) from the Approved Software and Hardware List for Digital Evidence

5.0 Procedure

5.1 Review the accompanying documentation for the evidence to determine the processes necessary to conduct the requested examination. Ensure proper legal authorization.

5.2 In order to avoid damage to the computer and its internal components from electrostatic discharge (ESD), place the computer on an anti-static bench mat, and attach the anti-static strap to a grounded source. The examiner shall also attach the anti-static wrist strap prior to opening the case on the computer.

5.3 Label the evidence in accordance with the Laboratory Procedure for Evidence Management. Avoid placing identifying marks on removable labels present on the evidence.

5.4 Inspect the evidence for physical damage. All damage must be documented in the analyst's case notes.

5.5 Information specific to the evidence (e.g., type/size of media, manufacturer, labels, and status of any write protection feature) must be documented in case notes.

5.6 Some computers require the hard drive to remain installed in order to image. The following steps for hard drive removal may be omitted. If the device supports hard drive removal, follow the steps included below. In all cases external media shall be removed for processing.

5.6.1 Photograph the external condition of the evidence computer. (e.g. any unique identifying numbers, damage, etc.).

5.6.2 Check for external media connected to the evidence computer. Check for media inside optical drive(s), flash memory slots, and all other external media connections. Remove all external media from the evidence computer and sub-item for identification. Complete labeling as provided in the Laboratory Procedure for Evidence Management.

5.6.3 If the device is opened, photograph the internal contents of the evidence computer prior to removing the hard drive(s).

5.6.4 If necessary, mark the cords connecting the hard drive(s) to the evidence computer to facilitate proper reassembly.

5.6.5 Remove the hard drive(s) from the evidence computer.

5.6.6 Label the hard drive(s) removed from the evidence computer for identification. Sub-item any hard drives removed as necessary in Forensic Advantage. Complete labeling as provided in the Laboratory Procedure for Evidence Management.

5.6.7 Record the drive information (e.g., make, model, serial number, number of sectors, number of heads, and jumper settings).

5.6.8 With the hard drive(s) removed, boot the evidence computer into the BIOS. If the date and time differ from the actual date and time, record the difference.

5.7 Ensure the forensic computer is functioning properly after system image restore and POST completed successfully. (see Technical Procedure for Computer Forensics Performance Verification).

5.8 Select a target drive(s) of appropriate size for the case (see Maintenance).

5.9 Determine which procedure for acquisition will be required based on the type of evidence.

5.10 Acquire the Control Media for the forensic computer or forensic tool (see Technical Procedure for Computer Forensics Performance Verification).

5.11 Perform an initial hash calculation of the evidence drive.

5.12 Acquire the evidence with an approved software or hardware tool using the proper acquisition. Compare the acquisition forensic image hash value to the initial hash value.

5.13 At the conclusion of the acquiring process, obtain a post-image hash value of the evidence drive, verify that it matches the initial hash value, and reassemble the computer.

5.14 Add forensic image(s) into approved forensic software tool(s) for evidence processing. Processing and analysis on the forensic image(s) shall be based on documentation supplied by the submitting agency. Based on training and experience, the Forensic Scientist shall run the appropriate processing options for each tool utilized in the case, along with utilizing the appropriate file filter(s). The processing options chosen shall be within the scope stated in the documentation provided by the submitting agency. Processing and analysis may include but is not limited to the following:

- Deleted or hidden partitions
- File Signature Analysis
- Hash Analysis
- Index Text
- Expand Compound Files
- Recover/bypass passwords
- Internet History Analysis
- Picture and Video Analysis
- Email Analysis
- Document Analysis
- System Information

- Deleted data
- Data from unallocated space and file slack
- Archives
- Databases
- Keyword and Pattern searches

5.15 Ensure thorough analysis is conducted on the evidence based on the computer supplemental form completed by the submitting agency. Bookmark or tag pertinent files in the case.

5.16 Complete the examination and create reports based on examination results. Transfer the recovered data and the software tool(s) report onto digital media of the appropriate size.

5.17 Obtain a post-examination hash of the forensic image.

5.18 Laboratory Reports must contain information specific to the requested examination(s) and must provide the reader with information in a clear and concise manner. Any analysis contained within a report must include an accurate interpretation of the actual results of the examination in a manner approved by the Forensic Scientist Manager or his/her designee.

5.19 A narrative-driven reporting method shall be used. In order to establish consistency within laboratory reports with regards to digital forensic examinations, the following items shall be, at a minimum, included within a laboratory report:

- Item(s) examined, including sub-items
- What type of examination was requested (e.g. computer forensics, mobile device, security bypass, etc.)
- Under what authority the exam was performed (e.g. search warrant, consent, etc.)
- Results of the examination, regardless of outcome (e.g. data located, not located, data encrypted, etc.).
- The methodology used during the examination(s).

The following are examples for report wording. The examples may be modified based on the case circumstances:

5.19.1 Methodology: The following methodologies were used in the examination of this case: visual examination, forensic imaging, processing, and analysis of results

5.19.2 Initial examination: Examination of the (generic description of evidence item) found that it contained (enter internal or external pieces of media found with sub item numbers.)

5.19.3 Imaging/Processing: (Item number) was imaged, processed, and a user report was generated.

5.19.3.1 Positive results: Flagged in the report are files of interest for the agency to review in the following categories:

5.19.3.2 Negative results: No files of interest were flagged for review.

5.19.4 Container Information: (Container number) was created and contains the following: (enter report names)

5.19.5 In instances where suspected child pornography is recovered, a warning statement shall be added to the laboratory report that indicates the presence of contraband. Example:

The report contained in Container (number) may contain contraband and is intended for use by law enforcement in an official criminal investigation. It is highly recommended that any device used to view the report and the material it contains be disconnected from any network, including the Internet. Dissemination of this material may result in criminal prosecution.

5.19.6 The overall process used to identify recovered data or artifacts must be described within the Forensic Scientist's worksheet and is not necessarily needed for the Laboratory Report. The description must be detailed enough so that another digital forensic examiner could replicate the examination if necessary.

5.19.7 Any additional statements describing the examination results that do not match the criteria above shall be approved by the Forensic Scientist Manager prior to the release of the report.

5.20 The forensic image will be retained for a period of time as described in the disposition on the Laboratory Report in the event further analysis is required.

6.0 Standards and Controls

6.1 All forensic computers and forensic tools shall be functioning properly prior to beginning a computer forensic examination (see Technical Procedure for Computer Forensics Performance Verification).

6.2 At the completion of an examination, the forensic image shall be verified for integrity in order to ensure that the forensic image did not change during the course of the forensic examination. The verification shall be done within the forensic software tool used to conduct the forensic examination. If any changes are made to the forensic image during the examination, it will not verify within the forensic software tool. The verification of the forensic image shall be documented in the case notes. If the forensic image does not verify, this shall be reported to the Section Forensic Scientist Manager immediately and this step repeated.

7.0 Calibrations – N/A

8.0 Maintenance –

8.1 The system drive for the forensic computer shall be restored from a system image.

8.1.1 If a previously created system image is available, skip to step 8.1.5.

8.1.2 If no previously created system image is available or updates to the default system image are required, then use the original Restore Disk that came packaged with the Forensic computer or perform a fresh install of the operating system.

8.1.3 Install any software from the Approved Software and Hardware for Computer Forensic Examinations List to be included on the system image.

8.1.4 Use an approved backup utility to create an image of the system drive.

8.1.5 Restore the system drive using the system image.

8.1.6 The Forensic Scientist shall ensure that the system drive restored properly, and that the forensic computer completed its POST successfully after restore.

8.1.7 The case preparation notations shall be made in the worksheet/examiner's notes. The "Case Start" date shall be the day the case was initially started and when the case preparation process was completed.

8.2 The target drive shall be wiped prior to examination. This procedure shall be used for new target drives as well as target drives used in previous cases.

8.2.1 Select digital media to be used as target drive.

8.2.2 Use an approved software or hardware device for wiping data to overwrite all data from the target drive.

8.2.3 Format the target drive.

8.2.4 Name the target drive using the case number and any other identifiers (e.g., forensic image, target, etc.).

9.0 Sampling – N/A

10.0 Calculations – N/A

11.0 Uncertainty of Measurement – N/A

12.0 Limitations

12.1 Processes and results are dependent upon the capabilities of specific forensic software and hardware tools. The Forensic Scientist shall be aware of the capabilities and limitations of forensic tools to ensure that appropriate software and hardware tools are utilized to process evidence.

13.0 Safety – N/A

14.0 References

- Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Computer Forensics*, 2014, Version 3.1.
- Scientific Working Group on Digital Evidence, *SWGDE Model Standard Operating Procedures for Computer Forensics*, 2012, Version 3.0
- Technical Procedure for Computer Forensics Performance Verification
- Approved Software and Hardware List for Digital Evidence
- Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Handling Damaged Hard Drives*, 2014, Version 1
- Scientific Working Group on Digital Evidence, *SWGDE Mac OS X Tech Notes*, 2019, Version 1.3

15.0 Records – N/A

16.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
08/02/2024	3	Header – Updated issuing authority 5.0 – Updated order of steps for workflow and updated language throughout the procedure 5.1 thru 5.7 – Incorporated Technical Procedure for the Physical Inspection of Digital Evidence 5.10 – Incorporated Technical Procedure for Hard Drive Removal 5.18 thru 5.19 – Incorporated the Technical Procedure for Generating Results, Updated information included in lab reports, and examples 8.0 – Incorporated Technical Procedure for System Image Restoration. 14 – Updated references