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

- **Target drive** – A sterile piece of media used to store forensic image(s) and case related data.
- **System drive** – The drive that contains the operating system (OS).
- **System Image** – Backup of the system drive that contains a clean install of the operating system (OS).
- **Forensic Image** – An exact copy of the original evidence.
- **Control Media** – A standard piece of media with a known hash value.
- **Hash value** – An alphanumeric value that uniquely represents a set of data.
- **Hash Value Set (File Filter)** – a list of hash values of known files used within a forensic software tool to show or mask files on a forensic image that have a hash value contained within the list. A file filter does not alter any data on a forensic image.

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 The system drive for the forensic computer shall be restored from a system image (see Technical Procedure for System Image Restoration).

5.2 Ensure the forensic computer is functioning properly after system image restore (see Technical Procedure for Computer Forensics Performance Verification).

5.3 Review the accompanying documentation for the evidence to determine the processes necessary to conduct the requested examination.

5.4 Select a target drive(s) of appropriate size for the case (see Technical Procedure for Target Drive Preparation).

5.5 If necessary, remove the hard drive(s) from the computer (see Technical Procedure for Hard Drive Removal). Remove all external media. Label items of evidence for identification.

5.6 Determine which procedure for acquisition will be required based on the type of evidence (see Technical Procedure for Evidence Acquisition in Computer Forensic Examinations). If necessary for the acquisition procedure, acquire the Control Media for the forensic computer or forensic tool (see Technical Procedure for Computer Forensics Performance Verification).

5.7 Acquire the evidence with an approved software or hardware tool using the proper acquisition procedure (see Approved Software and Hardware List for Computer Forensic Examinations).

5.8 Anti-virus programs may be run either on the original evidence using a write-blocker or on a forensic image mounted in forensic software unless the evidence drive is incompatible. Virus definitions for anti-virus software shall be checked for updates prior to running the program.

5.9 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

5.10 Ensure thorough analysis is conducted on the evidence in both allocated and unallocated space. Bookmark or tag pertinent files in the case.

5.11 Complete examination and create reports based on examination results (see Technical Procedure for Generating Results and Technical Procedure for Writing Results Statements).

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).

7.0 Calibrations – N/A

8.0 Maintenance – N/A

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 System Image Restoration
- Technical Procedure for Hard Drive Removal
- Technical Procedure for Computer Forensics Performance Verification
- Technical Procedure for Evidence Acquisition in Computer Forensic Examinations
- Technical Procedure for Generating Results
- Technical Procedure for Writing Results Statements
- Approved Software and Hardware List for Digital Evidence

15.0 Records – N/A

16.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
11/07/2016	1	Original Document
01/05/2018	2	Adjusted the header to reflect Digital Evidence Section 2.0 – Adjusted scope to reflect personnel in the Digital Evidence Section. 3.0 – Added a definition for "File Filter." 4.0 – Added "File Filter" to list. 5.3 – removed "Ensure legal authorization"; added "requested" to the type of examination. 5.8 – changed "shall" to "may;" clarified using a write-blocker when running anti-virus scans on original evidence. 5.9 – Changed "legal authorization" to "documentation supplied by the submitting agency;" added language to permit the use of file filters 5.11 – removed 5.12 – changed to new 5.11 and added "based on examination results." 14.0 – corrected citations for SWGDE references; changed "Approved Software and Hardware List for Computer Forensics" to "Approved Software and Hardware List for Digital Evidence."