Form	Deviation Request Form
Title	DFR for Computer Forensics Performance Verification
Laboratory Location	Raleigh Lab
Discipline/Section	Digital Evidence
A. Requested deviation applies to:	5.2.3 Technical Procedure for Computer Forensics Performance Verification
B. Requested deviation:	5.2.3.1 Prior to beginning the imaging process for an item, the Control Media shall be acquired for each forensic hardware device being utilized. The write-blocker shall be tested using the WiebeTech WriteBlocking Validation Utility.
C. Necessity for the deviation:	To clarify when the hardware verification need to be preformed during the imagining process.

D: Technical Review and Authorization

Technical Authorization	Yes - Authorized
Technical Authorizer	☐ Trevillian, Jim
Duration	1 year / next procedure revision

E: Quality Assurance Authorization

Acceptable within general QA guidelines and good laboratory practice?	Yes
Significant negative impact to Crime Laboratory Quality System?	No
QA Authorization	Yes - Authorized
QA Authorizer	☐ Suggs, Timothy
Effective Date:	9/27/2024

Version: 2.0
Created at 9/20/2024 11:51 AM by ☐ Trevillian, Jim
Last modified at 9/26/2024 1:25 PM by ☐ Suggs, Timothy

Close

Technical Procedure for Computer Forensics Performance Verification

1.0 Purpose – The purpose of this procedure is to ensure that forensic computers and forensic tools utilized in casework are functioning properly prior to use in case work and at the beginning of an examination.

2.0 Scope - This procedure describes the steps to be taken prior to beginning a computer forensic examination by personnel in the Digital Evidence Section to determine that forensic computers and forensic tools are in proper working order.

3.0 Definitions – See Digital Evidence Dictionary

4.0 Equipment, Materials and Reagents

- Forensic Computer
- Software from the Approved Forensic Software and Hardware List for Digital Evidence
- Control Media
- Control Image

5.0 Procedure

5.1 Initial Verification

5.1.1 Prior to use in casework, all software tools intended for use in casework must be verified to ensure the software performs in a manner that provides accurate results.

5.1.1.1 Verification shall be completed on all initial versions of software intended for use in casework, and all major revisions of software (e.g. x.0 to y.0) used thereafter.

5.1.1.2 Verification will not be required on "dot" revisions (e.g. 8.x to 8.y) of software tools.

5.1.1.3 Verification of software tools shall be performed using a piece of control media.

5.1.1.4 The verification process and results shall be documented. Documentation shall be maintained by the Technical Leader of the respective subdisciplines in the Digital Evidence Section.

5.1.2 Prior to use, all hardware tools intended for use must be verified prior to use in order to ensure the hardware performs in a manner that is expected.

5.1.2.1 Verification shall be completed on all new hardware tools.

5.1.2.2 Verification of hardware tools shall be performed using a piece of Control Media.

5.1.2.3 The verification process and results shall be documented. Documentation shall be maintained by the Technical Leader of the respective subdiscipline in the Digital Evidence Section.

5.2 Verification Prior to Examination

5.2.1 The forensic computers used in casework shall be restored to a clean system image before beginning a new case. The Forensic Scientist shall ensure that the computer restored and completed its POST successfully.

5.2.1.1 Forensic tools for acquisition that are standalone hardware devices do not need to be restored between cases; however, a Control Media shall be acquired prior to acquiring evidence items.

5.2.2 The forensic computer or forensic tool shall successfully complete its POST without errors. If the POST reports an error, then the forensic computer or forensic tool shall not be used in casework until the error has been corrected and POST completes successfully.

5.2.3 Prior to evidence media examination the write-blocker shall be tested using the WiebeTech WriteBlocking Validation Utility and a control media with known hash value shall be examined. The Control Media shall be acquired as stated below. If more than one item of evidence is acquired in the same day with the same tool, then it is only necessary to acquire the Control Media before the first item.

5.2.3.1 The Control Media shall be acquired each day that items of evidence are imaged for each forensic hardware device being utilized. The write-blocker shall be tested using the WiebeTech WriteBlocking Validation Utility.

5.2.3.2 The Control Media shall be acquired for each forensic software tool utilized after the forensic software tool is installed. This performance verification is only needed once per forensic software tool installation.

5.2.4 The acquisition hash value of the Control Media must match the known hash value for the acquisition tool to be functioning properly. If the hash values do not match, then the forensic computer or forensic tool shall not be used in casework until the source of the error in the hash values has been determined and corrected.

5.2.5 The Forensic Scientist shall ensure that the acquisition hash value matches the known hash value for the Control Media. If the hash values match, then the acquisition tool is functioning properly on the forensic computer or forensic tool.

5.2.6 A notation shall be made in the Forensic Scientist's case notes.

5.3 Standards and Controls - All forensic computers and forensic tools shall be functioning properly before beginning a computer forensic examination. Control media with a known hash value is used to ensure the proper functioning of acquisition tools for forensic computers and forensic tools.

5.4 Calibrations – N/A

5.5 Maintenance – N/A

5.6 Sampling - N/A

5.7 Calculations - N/A

5.8 Uncertainty of Measurement - N/A

6.0 Limitations – N/A

7.0 Safety – N/A

8.0 References

-
- Scientific Working Group on Digital Evidence, *SWGDE Model Standard Operating Procedures for Computer Forensics*, 2012, Version 3.0.
- Approved Software and Hardware List for Digital Evidence
- Scientific Working Group of Digital Evidence, *SWGDE Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics*, 2024, Version 2.1

9.0 Records - N/A

10.0 Attachments - N/A

Revision History		
Effective Date	Version Number	Reason
08/02/2024	6	Header – updated issuing authority 3.0 - Deleted definitions 5.1.1.3 - updated the language of the control media used 5.2.3 – Added language for the use of a writeblocker verification tool 5.2.6 – updated where the notation shall be documented 8.0 – updated references