Deviation Request Form (DRF)

Directions: The Initiator will complete Sections A through C. Additional continuation pages can be included if necessary.

Initiator	Alexa Scala	**Date**	1/31/2022

A. Requested deviation applies to (Technical Procedure – include specific section):

Technical Procedure for Computer Performance Verification

B. Requested deviation:

Section 5.2.6, replace with "A notation shall be made in the Forensic Scientist's case notes."

C. Necessity for the deviation:

A notation does not have to be made within the FA system because it is documented in the examiner's case notes.

D. Technical review and Authorization (to be completed by the Quality Manager and/or Technical Leader)
Comments(to include merits and impacts):

No comments.

Approved	☑	Yes	☐	No	Duration	1 Year
Signature	Matthew A. Wood Digitally signed by Matthew A. Wood DN: C=US, OU=Digital Evidence, O=North Carolina State Crime Laboratory, CN=Matthew A. Wood, E=mawood@ncdoj.gov Reason: I am the author of this document Location: your signing location here Date: 2022.01.31 09:55:08-05'00' Foxit PhantomPDF Version: 10.1.6				Date	1/31/2022

E. Quality Assurance Authorization (to be completed by the Quality Manager, Forensic Scientist Manager or designee)

Acceptable within general QA guidelines and good laboratory practice?	☑	Yes	☐	No
Significant negative impact to Crime Laboratory Quality System?	☐	Yes	☑	No

Restrictions/limitations:

Effective 02/01/2022

☑	Authorized	☐	Rejected	Signature	Timothy G. Suggs Digitally signed by Timothy G. Suggs DN: cn=Timothy G. Suggs, o=North Carolina State Crime Laboratory, ou=Quality Manager, email=tsuggs@ncdoj.gov, c=US Date: 2022.01.31 13:24:44 -05'00'	Date	01/31/2022

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

- **Control Media –** A standard piece of media with a known hash value.
- **Control Image – A forensic image of a known piece of media.**
- **Hash Value –** An alphanumeric value that uniquely represents a set of data.
- **Power-On Self Test (POST) –** A series of diagnostic tests that are performed when a computer powers on and determines proper functioning of the hardware components.
- **Forensic Tool** – Forensic software tool or standalone hardware device utilized to conduct acquisitions in casework.
- **System Image –** Backup of the system drive that contains a clean install of the operating system (OS).

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 Control Image.

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 (see the Technical Procedure for System Image Restoration).

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 The Control Media with a known hash shall be acquired prior to acquiring an item of evidence in a case. The Control Media shall be acquired each day that items of evidence are acquired and for each forensic software tool or hardware device being utilized. 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.

5.2.4 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 log within the FA system for the applicable forensic computer or tool. In addition, 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

- Technical Procedure for System Image Restoration
- 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

9.0 Records - N/A

10.0 Attachments - N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
10/31/2013	2	Added issuing authority to header
08/29/2014	3	Added control thumb drive to 5.1, 5.4, and 6.1 Removed sentence regarding 3.5" floppy disk imaged in Windows or DOS from 5.1
11/07/2016	4	Throughout document: changed procedure from daily occurrence to prior to beginning a computer forensic examination; changed control disk to control media; removed references to tower and VM and changed to forensic computers and forensic tools 3.0 – removed definition for VM and added new definitions 4.0 – added to equipment list 5.1 – changed and moved to 5.2; added new statements for 5.1 to include system restoration and POST 5.2 – changed statement to Control media; changed MD5 hash to hash value 5.4 – edited Standard and Control to reflect updated procedure 6.0 – Incorporated into section 5.0 8.0 – updated References
01/05/2018	5	Document-wide – adjusted to the headers to reflect the Digital Evidence Section 1.0 - added language to indicate this procedure shall be used to verify software and hardware tools prior to use in casework. 2.0 – adjusted the scope to personnel in the Digital Evidence Section. 3.0 – added definition for "Control Image." 4.0 – adjusted language to reflect the usage of software/hardware from the Approved Software and Hardware List for Digital Evidence; added Control Image to the list. 5.0 – added subsections 5.1 and 5.2; added existing language to subsection 5.2; deleted old 5.1. 8.0 – corrected citation formatting for SWGDE document; added "Approved Software and Hardware List for Digital Evidence."