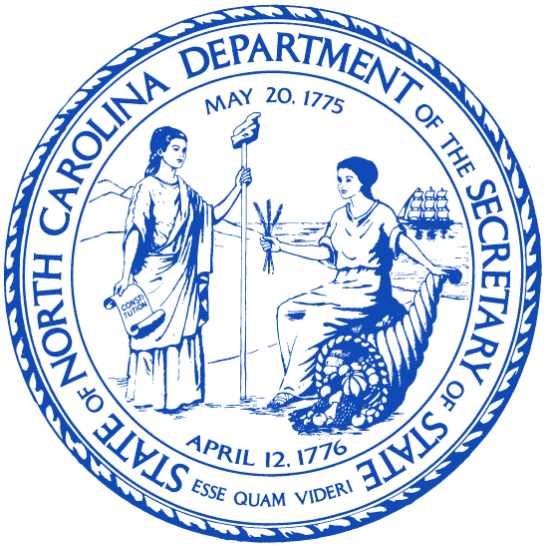

State of North Carolina

Department of the Secretary of State

Information Technology Division

Digital Forensics Laboratory

Standard Operating Procedure

SOP-Lab

Ashley L. Cappadonia

Digitally signed by Ashley L. Cappadonia
DN: cn=Ashley L. Cappadonia, o=NCSOS Digital Forensics Laboratory, ou, email=acappadonia@sosnc.gov, c=US
Date: 2019.03.01 13:15:17 -05'00'

Issued: March 1, 2019 **Reauthorization: SPruett & ACappadonia March 1, 2019** **Version: 1.0**

Table of Contents

Unit 01 - GLOSSARY OF COMMONLY ENCOUNTERED TERMS

Acquisition Control: Media with a known hash value and data set used for the purpose of verifying that the hardware and software appears to function correctly
Acquisition Hardware/Software: Hardware or software, such as write blockers but not the cables, that has direct access or connection to the media for the purposes of creating a forensic image.
BIOS: Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system.
Bit: The smallest discrete unit of data that a computer can handle
CD: Compact Disk or Compact Audio Disk.
CD-R: Compact Disk-Recordable. A disk to which data can be written, but not erased.
CD-ROM: Compact Disk-Read Only Memory. A laser-encoded optical memory storage medium.
CD-RW: Compact Disk-Rewritable. A disk to which data can be written and erased.
CMOS: Complementary Metal Oxide Semiconductor. Battery powered-backed memory found in PC's that stores and maintains the clock setting and system configuration information.
Compressed file: file that has been reduced in size through a compression algorithm to save disk space.
CRC (Cyclical Redundancy Checksum): An error detection method to verify the integrity of a block of data. The CRC is order sensitive. That is, the string "1234" and "4321" will produce the same checksum but not the same CRC. Most hard drives store one CRC for every sector (512 bytes). When a read error is generated from a disk, the CRC value of the sector does not match the value that is recomputed by the drive hardware after the sector is read.
Deleted File: A file that is marked for deletion by having the first character in the file changed. The file remains intact until new data overwrites the physical area where the deleted file is located.
Digital Evidence: Information stored or transmitted in binary form that may be relied upon in court.
DVD: Digital Versatile Disk. Similar in appearance to a compact disk, but it can store larger amounts of data.
Forensic Acquisition: The act of creating a forensic image of media while ensuring no changes to the media are made.
Forensic Image: A bit for bit copy of media which has a verifiable and reproducible hash value
Forensic Workstation: A machine designated for use in the Digital Evidence Section to analyze submitted evidence. This machine is not allowed to have access to a network or be accessed by a network outside the complete control of the analyst assigned to the Digital Evidence Section in order to ensure no co-mingling of data and evidence.

Gigabyte (GB): A unit of information storage equal to 1,073,741,824 bytes.
Hash Set: A listing of hash values of known files used for identification purposes only.
Kilobyte: A unit of information storage equal to 1,024 bytes.
MD5 Hash: The MD5 Hash is a 128-bit (16-byte) number that uniquely describes the contents of a file. The code to compute the MD5 was developed by RSA and is publicly available. The odds that two files with different contents have the same hash value are roughly two raised to the 128TH power. This is essentially a "digital fingerprint" of a file or an entire disk.
Major software upgrade: A release of software that is not merely a revision but which contains substantial changes. Traditionally, major releases are indicated by a change in the number to the left of the first period in the version number.
Minor software upgrade: A release of software that is a revision, and is not deemed by the manufacturer to contain substantial changes. Traditionally, minor releases are indicated by a change in the number to the right of the first period in the version number.
Mobile Device: A portable electronic device which allows a user to process, receive and/or send data without the need to maintain a wired connection
Optical Media: Data storage media in which the data is written and read by an optical device such as a laser
POST: A series of tests run by the computer at power-on.
Primary Analysis Hardware/Software: Hardware or software, such as standalone cell phone forensic tools, that has direct access or connection to the media but is not strictly used for the purpose of creating a forensic image.
RAM: Random Access Memory. Each computer has a certain amount of volatile read/write memory locations whose contents are lost when the power is turned off. The operating system, programs and drivers are all loaded into RAM at the same time
(SHA) Secure Hash Algorithm: SHA 1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard.
Stand-alone Computer: A computer not connected to a network or other computer.
Terabyte: A unit of information storage equal to 1,099,511,627,776 bytes.
Virus: A program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy programs or data on the hard disk. A Trojan is similar to a virus, except that it does not replicate itself.
Volatile Memory: computer memory that requires power to maintain the stored information

Unit 02 – ABBREVIATIONS USED IN CASE FILES

AGP	Advanced Graphics Port
BD BRD	Blu-Ray Disc
BIOS	Basic Input/Output System
C or c/	Containing
C # or Case #	Case Number
CD, CDR (CD-R), CD-ROM	Compact Disc, Compact Disc-Recordable or Recordable Compact Disc, Compact Disc Read Only Memory
CMOS	Complementary Metal Oxide Semiconductor
CF	Compact Flash Card
Cont. or cont.#	Container Number
CPU	Central Processing Unit
DAT	Digital Audio Tape
DL	Double Layer
DOPV	Data of Potential Value
DVD, DVDR (DVD-R), DVD-ROM, DVD-RW	Digital Versatile Disc – Recordable or Recordable Digital Versatile Disc, Digital Versatile Disc Read Only Memory
EFS	Encrypting File System
Ex. Or Ex#.	Exhibit Number
EXTDOS	Extended DOS Partition
FAT, FAT16, FAT32	File Allocation Table, File Allocation Table that uses 16 bit values, File Allocation Table that uses 32 bit values, New Technology File System
FFD	File Folder Disc
FTK	Forensic Tool Kit – forensic software used in the analysis of data
FWS	Forensic Workstation
GB, gbytes	Gigabyte, Gigabytes
HD, HDD	Hard Disk Drive, Hard Disk Drive
HFS	Hierarchical File System
I/O	Input/Output
IM	Instant Messaging
IDE	Integrated Drive Electronics
ISA	Industry Standard Architecture
KB	Kilobyte
LT	Laptop
MB, Mbytes	Megabyte, Megabytes
MHZ	Megahertz
MMS	Multimedia Messaging Service

MSD	Micro Secure Digital Card
NA	Not Applicable
NC SOS	North Carolina Department of Secretary of State
NF	None Found
NIC	Network Interface Card
NR	None Recorded
NS	Not Suitable
NTFS	New Technology File System
NV	No Value
OB	On Board
OS	Operating System
P2P	Peer to Peer
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PDS	Paraben Device Seizure
Pot.	Potential
PRIDOS	Primary DOS Partition
RAM	Random Access Memory
RAID	Redundant Array of Inexpensive (or Independent) Disk
ROM	Read Only Memory
SATA	Serial Advanced Technology Attachment
SMS	Short Message Service
S/N or SN	Serial Number
SD	Secure Digital Card
SCSI	Small Computer System Interface
SDHC or HCSD	Secure Digital High Capacity
SIM	Subscriber Identity Module
Sub or sub#	Submission Number
SYS	System
TB	Terabyte
USB	Universal Serial Bus
W or w/	With
WIN95, WIN98, WINME, WIN2000, WINXP, W2K	Windows 95, Windows 98, Windows Millennium, Windows 2000, Windows XP
ZIF (Socket)	Zero Insertion Force

Unit 03 – HARDWARE AND SOFTWARE/QUALITY ASSURANCE
1.0 PURPOSE:

The purpose of this procedure is to document the maintenance of the acquisition and primary analysis software and hardware that is used on a regular basis in the analysis of digital evidence and its quality assurance documentation. This procedure only refers to the software and hardware that has direct connection/access to the original evidence media as acquisition and primary analysis software.

2.0 MATERIALS:

2.1 Forensic workstation
2.2 Logbook
2.3 Forensic software and hardware
2.4 Acquisition control

3.0 PROCEDURES:

3.1 Forensic Workstations

3.1.1 A logbook should be kept on each forensic workstation. Each logbook will include an identifier for the workstation. This identifier will be the name used in the analyst notes.
3.1.2 All activities of the workstation must be documented in the logbook.
3.1.2.1 If the motherboard of a forensic workstation is changed, it shall be documented in the logbook along with the date of change and the analyst initials.
3.1.2.2 All POST results must be documented in the logbook with the analyst initials and date of activity.
3.1.2.3 All acquisition controls used in casework shall be documented in the logbooks and in the case notes.
3.1.2.4 All casework activity shall be documented in the logbook to include date, analyst initials and case number.
3.1.2.5 If maintenance is performed on a forensic workstation, a notation of when the workstation is taken out of service shall be documented in the logbook. Once the maintenance has been completed and prior to the workstation be placed into service, the workstation shall be tested by use of acquisition control media to show that the issues have been resolved
3.1.2.6 Upgrades to acquisition software and primary analysis software shall be documented on the machine receiving the upgrade.
3.1.2.7 Anytime the OS of the forensic workstation is changed or reinstalled, it shall be documented in the logbook of the workstation.

3.2 Acquisition and Primary Analysis Hardware

3.2.1 All primary analysis hardware, such as write blockers, shall have unique identifiers associated with the devices. This hardware shall be documented in a logbook and in the case notes.
3.2.2 All new acquisition and primary analysis hardware shall be tested prior for use in casework by the analyst in the Digital Forensic Laboratory.
3.2.3 After the validation/performance test has been completed and documented in the logbook, the hardware will be approved for use in casework by the Lab Manager.
3.2.4 Acquisition and primary analysis hardware testing data and results will be maintained by the lab Manager.
3.2.5 If at any time, the critical software/hardware has or appears to have an issue that may adversely impact the integrity or examination of evidence; it shall be pulled from service. It shall remain out of service until the issue is resolved or determined not to be valid.
3.2.6 If the hardware has been repaired, it shall be tested prior to use in casework.
3.2.7 The approved list shall be maintained and shall include the hardware name.

3.3 Acquisition and Primary Analysis Software

3.3.1 All new acquisition and primary analysis software shall be tested prior for use in casework by the lab analyst.
3.3.2 After the validation/performance test has been completed, it will be documented by the Lab Manager for approval for use in casework.
3.3.3 Acquisition and primary analysis software testing data and results will be maintained.

3.3.4 Acquisition and Primary Analysis Software Upgrades
3.3.4.1 Major upgrades to acquisition and primary analysis software shall be tested by the lab analyst prior to use in casework.
3.3.5 Analysts are not required to immediately upgrade the acquisition and primary analysis software at the time it is approved for use. Instead, they should complete the case in the version they started the case. Upon completion of the case and at the earliest possible date, the analyst shall upgrade the software to the latest approved version.
3.3.6 All acquisition and primary analysis software shall be identified by title and version in the case notes.
3.3.7 If at any time the acquisition and primary analysis software has or appears to have an issue that may adversely impact the integrity or examination of evidence, it shall be pulled from service. It shall remain out of service until the issue is resolved or determined not to be valid.
3.3.8 The approved list of analysis software shall be maintained and shall include software name, date of approval and version number

3.4 Validation shall include testing to ensure the data cannot be accessed from outside sources. This will prevent unauthorized access to computer systems used for examining electronic data.

4.0 LITERATURE REFERENCES:

None

Unit 04 – ASSISTING WITH SEARCH WARRANTS

1.0 PURPOSE:

This procedure is intended to provide an overview of how to assist investigators on-site when they serve the search warrant. There may be circumstances where strict adherence to this procedure is not practical or possible. Analysts will utilize their experience and training to determine the best course of action and will thoroughly document all steps taken and tools used. Hardware, software, tools and techniques used will be approved and tested prior to use and the analyst will be familiar with their proper use.

2.0 MATERIALS:

2.1 Notebook/pads.
2.2 Pens (writing and labeling).
2.3 Digital camera.
2.4 Labels (for marking cables).
2.5 Laptop and write blocking device
2.6 Forensic Hardware and software
2.7 Plastic bags, evidence tape, bubble wrap
2.8 Ample storage media including optical media, thumb drives and hard drives
2.9 Paint cans with tight fitting lids

3.0 PROCEDURES:

3.1 When assisting with the serving of the search warrant, the analyst shall wait until the investigators have secured the scene before entering the premises.
3.2 Unless the search warrant indicates otherwise, digital items should be seized and brought to the laboratory for analysis.
3.3 If the scene consists of a business type network or a server, it may be necessary to contact the system administrator for assistance. Keep in mind that the system administrator may not be available or he/she may refuse to cooperate.

3.4 If applicable, disconnect any external network connections (including wireless) to prevent remote access to the devices on scene.
3.5 For each computer you encounter document non-peripheral cable connections prior to disconnecting any devices. This is particularly important when networks or servers are involved.
3.6 If a computer is powered on, you should determine what type of system it is, photographically document the monitor and all open programs, the encryption status of the drive(s), and whether or not collection of volatile data is possible.

3.6.1 Document all the following steps including date/time, case number (if available), initials, tools/techniques used including version number, results and disposition of results/work product.
3.6.2 When possible, use an approved forensic tool, collect the volatile data including system memory
3.6.3 Using a tested and approved on-scene triage tool, gather system information including hard drive encryption status. If the results indicate that the hard drive is or may be encrypted, live acquisition may be necessary. See 3.10 for basic instructions.

3.6.4 Place collected data from the triage software and the volatile data collection on optical media or a USB drive and collect that item to be submitted to the laboratory as evidence.
3.6.5 After all data has been collected from the powered-on system; the system will be shut down for seizure. If the system is a Windows machine remove the power cord from the back of the computer. If it is a Macintosh or Linux system, use the proper shut down sequence. If the system is a laptop, remove the battery.

3.7 If other digital devices are seized, try to locate power cords, power adapters, etc. to include in the submission to the laboratory. Devices should be powered off, and batteries should be removed from mobile devices if possible.
3.8 Any on scene analysis or imaging should be conducted in compliance with the standard operating procedures as outlined in this procedure manual. Any analysis or imaging completed shall be thoroughly documented to include date/time, case number (if available), initials, tools/techniques used including version number, results, and disposition of results/work product.

3.9 Only approved software and hardware shall be used to forensically image or preview data at the scene. The integrity of the data shall remain intact.
3.10 If a live imaging job is required due to encryption or other circumstances, the following guidelines shall apply:
3.10.1 Only approved software/tools shall be used.
3.10.2 Images shall be saved to a wiped external hard drive which will be submitted to the laboratory as evidence.
3.10.3 Use of control procedures shall not apply.
3.11 All collected data, to include media containing triage data/reports, memory dumps, forensic images, and digital photographs, shall be collected as evidence and submitted to the laboratory. Handwritten notes will be maintained by the analyst and included in the laboratory case file if applicable.

3.12 All items to be submitted to the laboratory shall be packaged per the Evidence Submission Manual guidelines.

3.13 Evidence collected from a crime scene by laboratory personnel shall be protected from loss, cross-transfer, contamination and or deleterious chance, whether in a sealed or unsealed container, during transportation to and evidence facility.
3.13.1 Evidence shall be labeled and recorded with the appropriate case number and item number as it is collected and documentation shall accompany the evidence to the storage facility.
3.13.2 Evidence shall be packaged and entered into the evidence storage facility as soon as practical.

4.0 LITERATURE REFERENCES:

Mandia, Kevin and Chris Prosise. *Incident Response.* Berkeley, California: Osborn/McGraw-Hill, 2001.
National Institute of Justice. *Electronic Crime Scene Investigation. A Guide For First Responders.* Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.
U.S. Department of Justice, Computer Crime and Intellectual Property Section. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington, D.C.: U.S. Department of Justice, Computer Crime and Intellectual Property Section, 2001.

Unit 05 – EVIDENCE HANDLING
1.0 PURPOSE:

The purpose of this procedure is to establish reasonable steps to ensure the preservation of the integrity of the evidence and best practices when certain evidence is submitted for analysis.

2.0 MATERIALS:

2.1 Proper packaging materials
2.1.1 Anti-static bags
2.1.2 Anti-static bubble packaging
2.1.3 Foam rubber padding
2.1.4 Storage media

3.0 PROCEDURES:

3.1 Submitted Media: With the exception of cables, power adapters and batteries, only non-evidentiary parts will be used to make a non-functional piece of evidence operational.

3.1.1 Hard Drives
3.1.1.1 Stand-alone hard drives that are submitted for analysis should be placed in protective packaging such as anti-static bags and boxes or anti-static bubble wrap prior to return.
3.1.1.2 Hard drives that are removed from computer systems in the laboratory will be handled carefully and not be subjected to adverse environmental conditions.
3.1.1.3 Hard drives should not be placed in or left in situations whereby accidental contact with them would cause damage to the hard drive or loss of digital information.
3.1.2 Computer Systems:
3.1.2.1 Generally, the computer will have to be partly disassembled to gain access to the hard drive. Care should be taken to avoid damage to the computer components during disassembly.
3.1.2.2 Ensure that all items removed from the computer during disassembly (screws, cables, hard drives, etc.) are replaced when the analysis is completed. The computer should be returned to the Evidence Room in such a manner as to prevent damage to the computer after the analysis is completed.
3.1.2.3 Electrostatic discharges may destroy internal components of the computer system. Care should be taken to ensure that the analyst is grounded when working with computer systems.
3.1.2.4 When/if the computer is on, care must be taken to avoid electrical shocks.

3.1.3 CD-R's, DVD-R's, and other media:

3.1.3.1 Prior to analysis of these types of digital media, the evidence should not be placed in or left in situations whereby accidental contact with them would cause damage to the media or loss of digital information.
3.1.3.2 The media that was submitted as evidence may be placed within the appropriate protective containers.
3.1.3.3 In the event a PDA is submitted for analysis, the power to the device needs to be maintained either through batteries or power cable to ensure that no data is lost.

3.2 Digital Evidence Section Generated Media
3.2.1 Archival Data Media:

3.2.1.1 After evidence has been imaged, an archive of the image will be created. The archives may be placed on a hard drive or optical media. Steps outlined in section 3.2.4 of this procedure shall be followed prior to the release of the archival data media. A secondary copy may be placed on other media such as hard drives per the request of the submitting agency.
3.2.1.2 After creating appropriate sub-item(s) in LIMS, it will be packaged and labeled following existing evidence handling policies and procedures.
3.2.1.3 Optical media that is placed within the sub-item will be placed into protective plastic sleeves or cases prior to being returned.

3.2.2 Recovered Data Media

3.2.2.1 After data has been extracted from the image files of the exhibits, the data will be placed on the following media. If the total amount of the recovered data is greater than 160 gigabytes the data may be placed on a hard drive. Steps outlined in section 3.2.4 of this procedure shall be followed prior to the release of the data. If the total amount of the archive(s) is less than 160 gigabytes in size, then it shall be placed on media that is unalterable. A secondary copy may be placed on other media such as hard drives per the request of the submitting agency.
3.2.2.2 After creating appropriate sub-item(s) in LIMS, it will be packaged and labeled following existing evidence handling policies and procedures.
3.2.2.3 Optical media that is placed within the sub item will be placed into protective plastic sleeves or cases prior to being returned.

3.2.3 File Copy Media:

3.2.3.1 The file copy media will be media that is unalterable. This media will be maintained in the file folder in accordance with existing case file retention policy.
3.2.3.2 This CD-R or DVD-R is considered a work copy and therefore is not entered into LIMS. It shall contain items such as complete file listings and other EnCase Reports to support findings and conclusions in lieu of printing those reports.

3.2.3.3 CD-R's or DVD-R's will be placed into protective sleeves or cases.

3.2.4 Data Storage on Alterable Media

3.2.4.1 Media shall be wiped and formatted prior to use.
3.2.4.2 Data placed on media that can be altered shall be documented in such a way that the integrity of the data can be validated. Each file that does not already contain a hash value established shall be hashed to provide a means to validate that the data cannot be altered without detection.
3.2.4.3 After the establishment that all files have a hash value, a complete file listing of all items placed on the hard drive shall be generated. This listing shall at a minimum contain the following data (file name, file path, hash value, associated dates and sizes). This listing shall be maintained in the file folder.

3.2.4.4 Agency-supplied media, upon which the archive or recovered data is placed, shall not be received in the lab as an additional piece of evidence. Once the data or archive has been placed on this media for return to the agency, it will be entered into the LIMS system as a sub-item and be tracked as evidence at that time.

4.0 LITERATURE REFERENCES:

NCSOS Evidence Submission Manual

Unit 06 – PERFORMANCE CHECK OF FORENSIC WORKSTATIONS

1.0 PURPOSE:

The purpose of this procedure is to establish protocol on performance check of forensic workstations.

3.0 PROCEDURES:

3.1 The performance check of the forensic workstation will be performed by the system's POST (Power On Self Test).
3.2 A successful POST of the forensic workstation must be noted in the logbook.
3.3 If the workstation continually is unable to boot correctly then repairs should be made and a notification entered in the logbook.

4.0 LITERATURE REFERENCES:

SWGDE "Best Practices" 2004

Unit 07 – USE OF CONTROL

1.0 PURPOSE:

The purpose of this procedure is to establish protocol on using a control for forensic acquisition of evidence.

2.0 MATERIALS:

2.1 A forensic workstation
2.2 Appropriate forensic software and hardware.
2.3 Acquisition Control
2.4 Write blocking device

3.0 PROCEDURES:

3.1 Creation of the Acquisition Control

3.1.1 An acquisition control is media with a known hash value that is used to ensure the integrity of the hardware and software prior to the creation of a forensic image.
3.1.2 An Acquisition control may be created by an assigned analyst in the Digital Forensics Laboratory provided that the media used for the control has a documented hash value that has been verified by at least two (2) different approved software products.
3.1.3 The acquisition control media shall be given a unique identifier.
3.1.4 The hash value must be maintained with the acquisition control media.
3.1.5 The type of media, the unique identifier assigned to the media, and the hash value of the media shall be documented and maintained by the Quality Manager.

3.2 Use of the Acquisition Control

3.2.1 This procedure will be used as a performance check and standard control when acquiring any piece of evidence.
3.2.2 For purposes of this procedure, a successful POST of the computer along with the subsequent loading of the operating system will be considered as a performance check. This will be noted in the workstation logbook.

3.2.3 An device that is of a similar nature and interface must be, at a minimum, hashed either logically or physically prior to the acquisition of the evidence item on the calendar day of the beginning of the acquisition. The hash value must match a known value to be considered a valid control. Upon successful verification, a report depicting the validation of the hash value shall be stored in the case file.
3.2.4 If multiple items of the same type are to be acquired, then a single control hash once a day will suffice. Each different type of item/interface shall require its own acquisition control hash.

3.2.5 If it is not practical or possible to hash a device of similar nature and/or interface then another device (as similar as possible) may be hashed and the circumstances documented in the case notes. The hash value must match a known value to be considered a valid control. Upon successful verification, a report depicting the validation of the hash value shall be stored in the case file.
3.2.6 A notation in the case file must be made as to whether the acquisition control hashed with the appropriate value and the date(s) the control was hashed. Additionally, a notation will be made in the appropriate logbook indicating that the hash was successful.
3.2.7 If the acquisition control hashes with a value other than the known value, then another acquisition control of a similar nature will be used to determine if the original control has failed or if the computer has developed a hardware/software problem.
3.2.8 No analytical work will be conducted on the computer until the source of the problem has been determined and corrected.

4.0 LITERATURE REFERENCES:
None

Unit 08 – GATHERING SYSTEM INFORMATION

1.0 PURPOSE:

The purpose of this procedure is to provide general guidelines to obtaining the system information from computer systems.

2.0 MATERIALS:

2.1 Appropriate tools to disassemble a PC.
2.2 Appropriate compatible input/output devices and power cords.
2.3 Forensic Boot disk, CD/DVD or other forensic tools

3.0 PROCEDURES:

3.1 Physical description:
3.1.1 Document the make, model and serial number of the computer if available.
3.1.2 Access the computer and document the make, model, serial number, and size of the hard drive(s) if the drive is marked with this information. Record the jumper settings and cabling information, if applicable.
3.1.3 Document any missing parts or physical damage to the computer system.

3.2 CMOS settings
3.2.1 With the hard drive(s) disconnected, boot the computer and access the date/time settings via the BIOS settings or other means. RAID systems may require the hard drives be present to preserve the RAID configuration. The manufacturer may be contacted for guidance.
3.2.2 Record the date/time settings.

3.3 Partition Information
3.3.1 Utilizing a forensic boot disk, forensic boot CD/DVD, and/or other approved software, record the partition information of the hard drive(s).

4.0 LITERATURE REFERENCES:

National Institute of Justice. *Electronic Crime Scene Investigation. A Guide For First Responders.* Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736. U.S. Department of Justice, Computer Crime and Intellectual Property Section. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington, D.C.: U.S. Department of Justice, Computer Crime and Intellectual Property Section, 2001.
White, Ron. *How Computers Work. Millennium Edition.* Indianapolis, IN: QUE, A Division of Macmillan Computer Publishing, 1999.

Unit 09 – ACQUIRING MEDIA

1.0 PURPOSE:

The purpose of this procedure is to establish best practices for creating forensic images

2.0 MATERIALS:

2.1 A forensically sound workstation
2.2 Extra hard drives.
2.3 Acquisition software
2.4 Acquisition control of similar nature
2.5 Hardware or software write blocker

3.0 PROCEDURES:

3.1 Write-protect media. Document the method of write blocking used in the case notes and logbook of the forensic workstation or the write blocker. When write blocking is not possible or necessary, the circumstances shall be documented in the case file.
3.2 Follow the “Use of Control” procedure
3.3 Acquire using appropriate approved software and/or hardware. Refer to the manual for the appropriate method for using the software and/or hardware. The acquisition software and version along with the forensic workstation used to acquire the media shall be documented in the case notes.
3.4 If systemic read errors are noticed during acquisition, then the control shall be rehashed following the “Use of Control” procedure to ensure the cables and devices are working correctly.
3.5 Upon completion of the acquisition, the submitted media shall be placed in the original containers and protected from damage or loss of digital information.
3.6 Any deviation from this shall be fully documented and maintained in the case file.

4.0 LITERATURE REFERENCES:

EnCase Forensic Version 6.13 Manual. Guidance Software Pasadena, CA 2009
AccessData Forensic Tool Kit Manual, AccessData, UT 2005
AccessData Forensic Tool Kit Manual version 1.80, AccessData, UT 2008
AccessData Forensic Tool Kit Manual, version 2.0, AccessData, UT 2008
Manuals and FAQs for Devices

Unit 10 – MOBILE DEVICE ANALYSIS

1.0 PURPOSE:

Mobile devices may contain, but are not limited to, data such as text messages, phone numbers audio files and graphic files.
Due in large part to the various protocols used on mobile devices by the various manufacturers, a variety of tools and techniques should exist in order to analyze these devices. Tools shall be constantly updated as new devices with new protocols are released, or as research determines that more data may be extracted for certain models.

2.0 MATERIALS:

2.1 Approved forensic hardware/software to include necessary cables
2.2 Device to block the transmission and reception of data for mobile devices

3.0 PROCEDURES:

3.1 Stop the reception and transmission of data by use of a transmission blocking barrier or device setting, if applicable.
3.2 Ensure that a sufficient power supply is present for acquisition.
3.3 Gather all proprietary cables and cradles (if necessary).
3.4 Physically remove any removable media cards from the mobile device and analyze as defined in the “Acquiring Media” procedure.
3.5 If the mobile device contains a SIM card, remove the card and analyze it first.
3.6 Determine the appropriate software/hardware. Once the service request has been met, further analysis may be terminated.
3.7 Analyze the device using appropriate approved software and/or hardware. Refer to the manual for the appropriate method for using the software and/or hardware.
3.8 Some tools may require additional steps in order to thoroughly analyze a mobile device. These steps may include loading a software “agent,” particular key presses, or gaining root access to the device as long as these steps are performed as directed by the tool and are reversible they are permitted.
3.8.1 If the tool/mobile device allows you to install the software on a removable media card (such as a micro SD card), then a freshly wiped “lab use only” media card may be placed in the mobile device for this purpose. This media card is not considered evidence and will be removed from the device after analysis and remain in the Digital Lab for future use.
3.8.2 If the tool/mobile device does not allow you to install the software on a removable media card, then a note in the file that the software was installed by the tool will suffice.

4.0 LITERATURE REFERENCES:

National Institute of Justice. *Electronic Crime Scene Investigation. A Guide for First Responders.* Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.

Unit 11 – DIGITAL CAMERA EXAMINATIONS

1.0 PURPOSE:

The purpose of this procedure is to establish best practices when examining digital cameras. The method used for recovery of data of possible evidentiary value from digital cameras depends on the manufacturer, make and model of the camera. The data may be stored in a non-removable internal data storage unit or one of numerous removable internal data storage cards. Manuals should be used if available to determine how to access the internal data storage in the digital camera. A search of the Internet may provide an electronic copy of the manual and any necessary software if not available from the investigator.

2.0 MATERIALS:

2.1 A forensic workstation
2.2 Appropriate forensic software and hardware.
2.3 Bit stream imaging software
2.4 Cables for connecting camera to forensic computer
2.5 Batteries or power supply for camera
2.6 Software/hardware write blockers

3.0 PROCEDURES:

3.1 If the camera has a removable storage media, refer to the “Acquiring Media” procedure.
3.2 If the camera has batteries or is rechargeable, ensure that power is maintained to the device.
3.3 Follow the “Use of Control” procedure if using bit stream imaging software to acquire the data.
3.4 Use the appropriate write blocker (hardware or software).
3.5 Attach the camera to the forensic computer using the appropriate cables.
3.6 If the internal memory is visible to your forensic tool, acquire a forensic image of the stored internal data. If this is not possible, then use the appropriate software to access the internal memory. Document the procedure and software used to access the internal memory.
3.7 Record the date and time found on camera, if available.

4.0 LITERATURE REFERENCES:

EnCase Forensic Version 6.13 Manual. Guidance Software, Pasadena, CA 2009
White, Ron. *How Computers Work. Millennium Edition.* Indianapolis, IN: QUE, A Division of Macmillan Computer Publishing, 1999.

Unit 12 – EXAMINATION DOCUMENTATION

1.0 PURPOSE:

The purpose of this procedure is to document the contents of case file notes and the responsibilities of the case analyst.

2.0 MATERIALS:

2.1 Materials for documentation of exam

3.0 PROCEDURES:

3.1 Control

The use of an acquisition control shall be documented in the case notes as outlined in the "Use of Control" Procedure.

3.2 Acquisition
All methods of write blocking shall be documented. All hardware write blockers used in casework shall be documented with a unique identifier in the case notes. All critical software used shall be documented by name and version in the case notes. The name and version of the acquisition software, the workstation used to acquire the data, and the start date of acquisition of the submitted media shall be included in the case notes.

3.3 System Information
The system information from the submitted item(s) shall be documented in the case notes as outlined in the "Gathering System and Hardware Information" procedure.
3.4 Exam

3.4.1 During examination, all software names and versions used to extract data shall be noted in the case notes so that each process may be replicated at a later date. A report that displays the results of the acquisition and verification hashing functions shall be created to ensure that the forensic image completely verified with no errors. This report shall be placed in the case file either in physical or electronic form.

3.4.2 The process to recover deleted files and folders and their structure shall be performed and documented in the case notes, if applicable.

3.4.3 A signature and hash analysis shall be performed on all files and documented. Approved hash sets may be used to identify notable files and the particular hash set shall be documented in the case notes. The results of the hash analysis shall be documented in the case notes. If the hash sets are used for detecting specific files or for the purpose of

excluding known system files in the review process, then the hash sets shall be documented in the case notes.
3.4.4 When a keyword search is performed for specific terms related to the case, the date of the search shall be documented in the case notes. A listing of the terms with the summary results shall be documented in physical or electronic form in the case notes. All search term settings, to include inactive settings and the keywords themselves, shall be documented in the case notes in physical or electronic form.

3.4.5 If data from the forensic image file is extracted, it will be documented in the case notes. A file listing of all files extracted and placed on media for review by the agency shall be created and placed on the case file media.

3.4.6 If a virus scan is performed, it shall be documented in the case notes. The specific antivirus program to include version and virus definitions with revision, and summary of results must be documented in the case notes.

3.4.7 Automated searches, such as Enscripts, and the settings used to parse and process the forensic image file for the purpose of locating data that may be of potential value will be documented in the case file. Textual content of all generated reports shall be recorded on the case file media. The results shall be clearly noted and understood as to whether data was found, data was found and of no value or no data was found.

3.4.8 The time zone settings shall be noted in the case file for all items analyzed with forensic acquisition software.

3.5 Lab Generated Media
The date the forensic image was archived with the number and type of media it was placed on will be documented in the case notes. If an automated disc archiving system is utilized, any administrative documentation generated will be included in the case file. The date the recovered media is generated with the number and type of media it was placed on will be documented in the case notes.

Unit 13 – LABORATORY REPORTS

1.0 PURPOSE:

The purpose of this procedure is to document items to be included in the laboratory reports for the Digital Evidence Discipline. Each report shall be accurate, clear, unambiguous and objective, and in accordance with any specific instructions in the test methods.

2.0 MATERIALS:

None

3.0 PROCEDURES:

3.1 In the [EVIDENCE] section of the report, each item should have a description to include the make and model of the item. In addition, each hard drive should include the size of each submitted hard drive.

3.2 In the [RESULTS] section of the report, each item analyzed should have a brief description of the type of analysis performed on that item. If data of value was extracted, it should be noted where that data resides (i.e. which disc). The explanation for the abbreviations for CD-R and DVD-R are not required.

3.3 The CMOS date and time information shall be recorded in the [RESULTS} section to reflect the date and time registered on the computer and the actual date and time this information was recorded. If no date and time was obtained from the computer system, then a notation such as “Unable to obtain CMOS settings,” must be included in the report.

3.4 If automated data searches or scripts are initiated and successfully completed to recover data and information, then the results shall be included in the report.

a. If keyword searches are performed, a search summary shall be generated. This summary will be mentioned in the report. The search summary shall include the listing of the keyword and the number of matches the search made. If the keyword search was negative, it shall also be included in the report. This listing may be supplied to the agency in an electronic format on the disc containing the recovered data. Any text fragments that are exported shall be mentioned in the report.

b. If a virus scan has been performed on an item, then the results of that scan shall be noted in the report. The Antivirus program performing the scan, as well as the version of the virus definitions used, shall be identified in the case notes.

c. Any hash library used in the identification of certain files of possible interest shall be documented in the report.

d. If a search for email and/or internet activity has been performed, then the results of the search shall be noted in the report.
e. Other scripts and searches performed, such as digital camera searches, unallocated searches, or initialize case scripts, shall be noted in the report.

3.5 In the [REMARKS] section of the report, any forensic archives or products created should be noted and the type of media upon which they reside.

3.6 The Recovered Data Disc(s) Outline will be included in the Laboratory Report. This document will accurately describe the content and layout of the recovered data media.

3.7 A copy of the report shall be included with the recovered data disc(s).

3.8 A comment stating that further examination by the contributing agency should be performed shall be placed in the [REMARKS] section of the report.

3.9 The time zone settings utilized for all items analyzed with forensic acquisition software shall be documented in the [RESULTS] section of the report.

4.0 Any abbreviations or symbols specific to the laboratory that are recorded for an examination must be clearly defined by the laboratory

Unit 14 – TECHNICAL AND ADMINISTRATIVE REVIEW

1.0 PURPOSE:

This procedure provides a method for the review of all cases in the Digital Forensics Laboratory to ensure the documentation within the files complies with the North Carolina Department of Secretary of State Administrative Procedures Manual (DFLAPM) and Digital Forensics Laboratory Standard Operating Procedure (SOP).

2.0 MATERIALS:

2.1 Case file
2.2 Technical Review Worksheet
2.3 Laboratory Network computer with access to LIMS

3.0 PROCEDURES:

3.1 **Technical Review.** Technical review will be conducted by any qualified member on 50% of cases per calendar year. The reviewer is responsible for ensuring that the technical review is complete. Once the review is complete, the review will sign off on the technical review. Each case file submitted for technical review will be checked to ensure consistency with all SOPs, accurate conclusions, reporting procedures and evidence handling policies and procedures All file folder media will be reviewed. Each file will be checked, at a minimum, for the following:
3.1.1 All service requests, whether from the Case Tracking Form (CTF), Electronic Evidence Submission Checklist, or other communication with the contributing agency, have been addressed or completed by the examination.

3.1.2 Communications in case notes accurately reflect any deviation from the original service request.
3.1.3 Controls are appropriate for the evidence being analyzed, and approved critical hardware and software are used during the analysis.
3.1.4 Notes are complete and legible. Any applicable worksheet documentation is present and complete.
3.1.5 Notes accurately reflect each examination procedure and the software version used to complete each exam.
3.1.6 Notes are consistent and reflect analyses performed in compliance with SOPs.
3.1.7 All results are consistent with the examination procedures used.
3.1.8 Reported conclusions are consistent with the results as recorded in the notes and as outlined by the appropriate procedures.
3.1.9 All examinations conducted have been reported, and documentation of examinations that produced positive results will be included in the Results section of the report.

3.1.10 Any discrepancies between the submittal forms and the analyst's notes will be reported.
3.1.11 Any deviations or exceptions to the SOP have been documented and placed within the case file.

3.1.12 Any discrepancies found during the Technical Review shall be thoroughly documented on the report of the Technical Review and shall be initialed by the analyst performing the Technical Review. The examiner shall respond to the discrepancies by way of correcting the report according to procedure for Laboratory Reports, Case Record Contents, Management and Retention and if necessary, by performing the necessary testing to conform to the requirements and resubmit the case to the technical reviewer. All supplemental reports shall be maintained in the case record.

3.2 **Administrative Review.** Administrative review will be conducted by the Deputy Secretary-IT or other approved employee of the IT team. The reviewer is responsible for ensuring that the administrative review is complete. Once the review is complete, the reviewer will initial and date the bottom of the case report or the administrative review checklist included in the case records. Each case file submitted for administrative review will be checked to ensure consistency with laboratory policy and editorial correctness to include the following:

3.2.1 All documentation is securely attached within the file.
3.2.2 All administrative pages contain the unique laboratory case identifier. All examination documentation contains the unique laboratory case identifier and the examiner's handwritten initials. Two-sided documents are marked on both sides. Additionally, examination documentation must contain the initials of all individuals involved in the examination.
3.2.3 Examination documentation contains either the examination date or, at a minimum, the start and end dates of the analysis.
3.2.4 Examination notes must be legible and contain no obliterations. Any corrections are made with a single strikeout and initialed. All interlineations will be addressed according to the Laboratory Case Record Contents, Management and Retention Laboratory Administrative Procedure.
3.2.5 Review the chain of custody documentation and evidence disposition.
3.2.6 The report will follow the standard format per the Laboratory Reports Administrative Procedure.
3.2.7 The correct header information appears on all pages. Subsequent pages will contain the page number of total number of pages, the Digital Forensics Laboratory case number and submission number(s).
3.2.8 The name of the reporting member and his/her current title.
3.2.9 The report is free of grammatical and spelling errors.

3.2.10 All reported evidence is consistent with the Administrative Procedures requirements regarding numbering and description. If there is a need to change evidence numbering, documentation must exist to clarify the change.

Unit 15 – LABORATORY CONDITIONS

The lab environment shall facilitate correct performance of equipment and ensure that correct results are obtained through examinations performed in the lab.

Responsibilities

The Lab Manager/examiner shall ensure that the equipment is properly stored for use in examinations of evidence.

Equipment use and storage

The computers shall be stored on safe shelving, desks, or out of the walkway on the floor. They should be plugged into functional back up power supplies that are connected to electrical outlets located nearby so no cords are crossing the walkway.

Lighting

The correct and sufficient lighting shall be available in the laboratory to ensure the correct results are obtained in examinations of digital evidence. Any malfunctions in lighting shall be reported to the facility maintenance for repair.

Temperature

The temperature control is located in the laboratory room and can be adjusted by the Lab Manager if it is determined the lab temperature is insufficient for the correct operation of the lab equipment. The evidence room shall be maintained at a temperature that allows for evidence to be stored without condensation or other damage from temperature or humidity related issues.

Lab Coats and Gloves

Lab coats and protective gloves shall be available to protect the examiner from environmental factors that are temperature related or health/safety related. These can be worn at the examiners discretion.

Tear Down Table

The lab provides a tear down table for use by the examiner to ensure adequate space and tools for disassembling any evidence for imaging purposes and investigation. Evidence shall be kept separate to ensure no cross contamination of evidence occurs.

Static electricity

Anti-static mats are located in the evidence room and shall be placed in front of the storage shelving to ensure static electricity does not damage the evidence. The examiner shall take appropriate steps to ensure they have rid themselves of static prior to an examination (ie: touching metal before they touch the evidence).

Documentation

If any equipment is found to be damaged due to environmental factors, the occurrence shall be documented and the equipment shall be tested to ensure correct operation or taken out of service and replaced/repaired. The Lab Manager shall maintain documentation of this.

Housekeeping

The NC Department of Secretary of State has contracted general housekeeping for the main building. These contractors will be responsible for the trash that is set outside of the lab door daily. The lab manager shall have access to the vacuum and disinfecting cleaner and will be responsible for cleaning the most often handled surfaces weekly. This includes desktops, keyboards, phones, and door handles.

Unit 16 – LABORATORY SECURITY, HEALTH AND SAFETY PLAN

Security

Due to the volatile nature of digital evidence, the media submitted into the lab must be kept safe from damage and cross-contamination. This policy details the requirements of the physical security of the Digital Forensics Laboratory.

Personnel Responsibilities

The Lab Manager shall ensure the security and safety of the Lab and the Lab evidence room. Every effort must be made to maintain security, preserve evidence integrity, and ensure there are no unauthorized visitors in the lab.

Security and Access

All personnel directly involved with the Lab shall be assigned a key and given the security code that will allow them access to the Digital Forensics Laboratory. The key will operate the door lock and the security code shall disarm the security panel located outside the door. The alarm will be activated when leaving the lab or anytime the lab is unoccupied. These doors shall remain closed at all times. Alarmed sensors and cameras monitor the access point to the laboratory. The access door to the evidence room located outside of the lab requires a separate key and security code that has been assigned to designated evidence custodians. Accountability of all the lab keys and the provided security code is documented and their distribution is limited to those individuals designated by the Laboratory Director to have access. During vacant hours, the laboratory and evidence room have separate active alarm systems monitored by State Capital Police.

Visitors

Any visitors to the lab will sign into the lab on the sign-in sheet by the door. All visitors will be escorted into the lab by lab personnel. Visitors will remain with lab personnel at all times. At no time shall anyone other than lab personnel or the assigned evidence custodians be allowed into the evidence room.

In the event of an emergency requiring an evacuation, all Digital Forensics Laboratory employees shall safely evacuate the building while ensuring the integrity of the Lab facility as much as possible.

Fire Alarm and Evacuation Plan

In the event of a fire alarm activation for the building, all Lab personnel shall immediately

secure any evidence within the lab or evidence room and evacuate. The lab and evidence room doors will be closed and the alarms activated prior to leaving if possible.

In the event of a fire within the Lab facility, fire extinguishers are located in the South end corner of the building by the Custodian Closet and by the Southwest exit in the hallway. Lab personnel may attempt to extinguish small fires themselves if they feel it is safe to do so. If the fire is too large or too dangerous, Lab personnel should immediately dial 9-1-1, notify the Emergency Response Coordinator or a safety team member, pull the nearest fire alarm and evacuate.

Emergency Response/Evacuation Plan

All of this is in direct line with the Emergency Response/Evacuation Plan for the Secretary of State Office Building (Rev. Jan, 2012). A copy of this document will be retained with the Policy Manual/Quality Assurance Manual. Lab personnel should be familiar with the assigned safety personnel and evacuation routes.

It is important that personnel can work in an area that is free from hazards or safety issues. Safety is a top priority of the NC Department of Secretary of State and all personnel are considered safety officers with the duty to report safety issues and take action if unsafe conditions are found. This policy describes the health and safety program for the NC Department of Secretary of State Digital Forensics Laboratory.

Health and Safety Manager

The Digital Forensics Laboratory Manager shall assume the responsibility of the Health and SafetyManager.

Safety Inspections

The NC Department of Secretary of State Facility Maintenance will conduct routine inspections of the facility to ensure compliance with all required statutes, ordinances, and regulations. A copy of the findings will be provided and maintained by the Digital Forensics Laboratory Manager.

Safety Committee

The parent organization of the Digital Forensics Laboratory is the NC Department of Secretary of State. The Secretary has assigned Facility Maintenance Supervisor to lead the Department Safety Committee.

Safety Equipment

The facility is equipped with numerous fire extinguishers, the two closest to the Digital Forensics Laboratory are in the South end corner of the building and next to the Southwest exit in the middle of the building. Digital Forensics Laboratory employees should be familiar with their location and operation.

First Aid kits are located near the Server Room in the middle of the building. Lab employees shall know where these are at and should be able to access them at any time.

The Lab provided latex gloves to all employees for use with evidence that may be dirty, contaminated with bodily fluids or preserved for latent prints. Personnel should use latex gloves anytime they feel it is necessary. In addition, a hand sanitizing station is located outside the lab in the main hallway.

All phones have the ability to dial 9-1-1 in the event of an emergency.

Agency Requirements

Since the Lab is part of the NC Department of Secretary of State, it is the parent organization's responsibility to ensure that the employees are complying with their health and safety requirements.