**Raleigh/Wake City-County**

**Bureau of Identification**

**Crime Laboratory Division**

**DIGITAL EVIDENCE UNIT**

**TECHNICAL PROCEDURES MANUAL**



**Contents**

[Chapter 1: Administration 6](#_Toc34150872)

[1.1 Purpose 6](#_Toc34150873)

[1.2 Scope 6](#_Toc34150874)

[1.3 Equipment 6](#_Toc34150875)

[1.4 Procedure 6](#_Toc34150876)

[1.5 Limitations 7](#_Toc34150877)

[1.6 Safety – N/A 7](#_Toc34150878)

[1.7 References – N/A 7](#_Toc34150879)

[Chapter 2: Equipment 9](#_Toc34150880)

[2.1 Purpose 9](#_Toc34150881)

[2.2 Scope 9](#_Toc34150882)

[2.3 Equipment 9](#_Toc34150883)

[2.4 Procedure 9](#_Toc34150884)

[2.5. Limitations – N/A 10](#_Toc34150885)

[2.6. Safety - N/A 10](#_Toc34150886)

[2.7 References – N/A 10](#_Toc34150887)

[Chapter 3: System Image Restoration 12](#_Toc34150888)

[3.1 Purpose 12](#_Toc34150889)

[3.2 Scope 12](#_Toc34150890)

[3.3 Equipment 12](#_Toc34150891)

[3.4 Procedure 12](#_Toc34150892)

[3.5 Limitations – N/A 12](#_Toc34150893)

[3.6 Safety - N/A 12](#_Toc34150894)

[3.7 References 12](#_Toc34150895)

[Chapter: 4 Target Media Preparation 14](#_Toc34150896)

[4.1 Purpose 14](#_Toc34150897)

[4.2 Scope 14](#_Toc34150898)

[4.3. Equipment 14](#_Toc34150899)

[4.4. Procedure 14](#_Toc34150900)

[4.5 Limitations – N/A 14](#_Toc34150901)

[4.6 Safety - N/A 14](#_Toc34150902)

[4.7 References 14](#_Toc34150903)

[Chapter 5: Write Protection 16](#_Toc34150904)

[5.1 Purpose 16](#_Toc34150905)

[5.2 Scope 16](#_Toc34150906)

[5.3. Equipment 16](#_Toc34150907)

[5.4 Procedure 16](#_Toc34150908)

[5.5 Limitations 16](#_Toc34150909)

[5.6 Safety - N/A 16](#_Toc34150910)

[5.7 References 16](#_Toc34150911)

[Chapter 6: Forensic Imaging 18](#_Toc34150912)

[6.1 Purpose 18](#_Toc34150913)

[6.2 Scope 18](#_Toc34150914)

[6.3. Equipment 18](#_Toc34150915)

[6.4 Procedure 18](#_Toc34150916)

[6.5 Limitations 18](#_Toc34150917)

[6.6 Safety - N/A 19](#_Toc34150918)

[6.7 References 19](#_Toc34150919)

[Chapter 7: Forensic Imaging Using Target Disk Mode 21](#_Toc34150920)

[7.1 Purpose 21](#_Toc34150921)

[7.2. Scope 21](#_Toc34150922)

[7.3. Equipment 21](#_Toc34150923)

[7.4 Procedure 21](#_Toc34150924)

[7.5. Limitations – N/A 21](#_Toc34150925)

[7.6 Safety - N/A 21](#_Toc34150926)

[7.7 References 22](#_Toc34150927)

[Chapter 8: Mobile Devices 24](#_Toc34150928)

[8.1 Purpose 24](#_Toc34150929)

[8.2 Scope 24](#_Toc34150930)

[8.3 Equipment 24](#_Toc34150931)

[8.4 Procedure 24](#_Toc34150932)

[8.5 Limitations 25](#_Toc34150933)

[8.6 Safety – N/A 26](#_Toc34150934)

[8.7 References 26](#_Toc34150935)

[Chapter 9: Minimum Standards 28](#_Toc34150936)

[9.1 Purpose 28](#_Toc34150937)

[9.2 Scope 28](#_Toc34150938)

[9.3 Equipment 28](#_Toc34150939)

[9.4 Procedure 28](#_Toc34150940)

[9.5 Safety – N/A 30](#_Toc34150941)

[9.6 Limitations 30](#_Toc34150942)

[9.7 References – N/A 30](#_Toc34150943)

[Chapter 10: Reporting Results 32](#_Toc34150944)

[10.1 Purpose 32](#_Toc34150945)

[10.2 Scope 32](#_Toc34150946)

[10.3 Equipment – N/A 32](#_Toc34150947)

[10.4 Procedure 32](#_Toc34150948)

[10.5 Limitations- N/A 33](#_Toc34150949)

[10.6 Safety -N/A 33](#_Toc34150950)

[10.7 References -N/A 33](#_Toc34150951)

[Chapter 11: Evidence Transport 35](#_Toc34150952)

[11.1 Purpose 35](#_Toc34150953)

[10.2 Scope 35](#_Toc34150954)

[10.3 Equipment 35](#_Toc34150955)

[10.4 Procedure 35](#_Toc34150956)

[10.5 Limitations- N/A 35](#_Toc34150957)

[10.6 Safety -N/A 35](#_Toc34150958)

[10.7 References -N/A 35](#_Toc34150959)

[Chapter 12: Glossary 37](#_Toc34150960)

[12.1 Purpose 37](#_Toc34150961)

[12.2 Scope 37](#_Toc34150962)

[12.3 Definitions 37](#_Toc34150963)

[Appendix A – Technical Field Assistance Report Template 41](#_Toc34150964)

# Chapter 1: Administration

## Purpose

The purpose of this procedure is to establish guidelines for the extraction and examination of data from computing devices and digital storage devices.

## Scope

All data extraction and examination services provided by the Digital Evidence Unit.

## Equipment

**1.3.1** All forensic software and hardware tools approved for use in forensic examinations will be listed on the Digital Evidence Unit Equipment List. The Digital Evidence Unit Equipment List will be updated as necessary by a Digital Evidence Technical Leader.

**1.3.2** Application software may be downloaded from a creditable source by a Digital Examiner and utilized during a forensic examination when necessary as part of a forensic examination. Digital Examiners will list in the case notes the source of all downloaded application software utilized as part of a forensic examination. Application software does not need to be validated.

## Procedure

**1.4.1** The Digital Evidence Services personnel in the Digital Evidence Unit may conduct forensic extractions or examinations of computer devices, digital recording/storage devices, mobile/handheld devices, and digital storage media.

**1.4.2** Digital Examiners will understand the scope of search warrants and ensure there is legal basis to examine, extract and collect data from all computing devices or digital storage devices before performing any forensic extraction or examination. If a Digital Examiner finds evidence of a crime outside the scope of the legal right to examine, extract or collect data, the examiner will stop the extraction or examination and inform the case investigator that further legal basis is necessary to cover the newly found evidence. Such a recommendation will be documented in the case notes.

**1.4.3** When images depicting possible child pornography are discovered, Digital Examiners will store and transfer the files using methods that avoid accidental distribution or unnecessary reproduction of the images.If a Digital Examiner deems appropriate, images of child pornography may be electronically duplicated for the purposes of sending them to the National Center for Missing and Exploited Children, the FBI Innocent Images program, Immigration and Customs Enforcement, or other similar entities. CCBI will not maintain any electronically duplicated images of child pornography.

**1.4.4** Technical Reviews will be performed on at least 25% of the cases submitted for digital evidence examination and extractions.

**1.4.5** The Technical Leader of the Digital Evidence Unit will ensure that the minimum requirement for Technical Review is being met by marking cases subjected to technical review in the Digital Evidence Unit Tracker Log.

## 1.5 Limitations

Not all forensic examination or extraction requests may be supported by the current CCBI forensic software or hardware tools.

## 1.6 Safety – N/A

## 1.7 References – N/A

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. Added grammatical corrections, and ‘extractions’ to technical reviews |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 2: Equipment

## 2.1 Purpose

The purpose of this procedure is to ensure the proper performance and reliability of the equipment used in the examination of digital evidence by the Digital Evidence Unit.

## 2.2 Scope

This procedure applies to equipment used for examinations of digital evidence which consists of forensic hardware and software.

## 2.3 Equipment

**2.3.1** All forensic hardware maintenance will be documented in the Digital Evidence Unit Maintenance Log. If repairs or modifications are performed, a performance check will be conducted before it is utilized for casework purposes. The Digital Evidence Unit Maintenance Log will be stored on the CCBI Network Shared Drive in the Digital Evidence folder.

## 2.4 Procedure

**2.4.1** Forensic workstations will be performance checked prior to initial use and then prior to each forensic examination or forensic extraction to ensure they are functioning properly.

**2.4.1.1** Performance checks of forensic workstations are performed by a successful power on self-test (POST), successful loading of the operating system, and hashing of control media.

**2.4.2** Forensic write blockers/bridges will be performance checked prior to initial use and then on an annual basis to ensure they are functioning properly.

.

**2.4.2.1** Control media will be inserted into the forensic workstation and a forensic image will be acquired using forensic software. The forensic image will be hashed using approved software and hardware.

**2.4.2.2** The known hash value for the control media and the acquisition hash and verification hash value for the forensic image of the control media must match. If the hash values do not match, the forensic computer must not be used for casework until the source of the error in the hash values has been identified and corrected.

**2.4.2.3** Forensic Examiners will ensure the status indicator of the write blocker indicates that it is in write blocking mode for each examination.

**2.4.3** Verification of forensic software will becompleted to the extent practical and will be based upon the designed function(s) and specifications of the software prior to being approved for use in forensic examinations.

**2.4.3.1** Verification of all aspects and functionality of forensic software is not required for commercial of-the-shelf (COTS) software being utilized within the designed range of use.

**2.4.3.2** Forensic software designed to acquire, view, process, parse, and/or analyze data as part of a forensic examination of digital evidence will be verified by using control media.

**2.4.3.3** At least one intended aspect or functionality of the forensic software will be verified. As an example, forensic software designed to acquire a data structure may be used to acquire and hash an image of controlled media. The acquired hash value will be compared to the hash value of the controlled media to verify the functionality.

**2.4.3.4** Performance verification does not need to be completed on operating systems or software customarily utilized for administrative tasks. (i.e. Microsoft Office Suite, Adobe Reader, etc.)

**2.4.4** Documentation of verification of forensic hardware, write blockers and forensic software will be recorded as follows:

**2.4.4.1** The initial performance check of forensic hardware and write blockers will be documented in S:\Crime Laboratory\Digital Evidence\Verification Documents.

**2.4.4.2** Performance checks of forensic hardware used in forensic examination will be documented in the Digital Evidence Unit Calibration Log, and a notation that the performance check was completed will be made in the case notes

**2.4.4.3** Verification of the forensic software will be documented on the Digital Evidence Unit Equipment List along with the control media utilized.

## 2.5. Limitations – N/A

## 2.6. Safety - N/A

## 2.7 References – N/A

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. Changed chapter title, added software to scope, added verification process of software. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 3: System Image Restoration

## 3.1 Purpose

The purpose of this procedure is to restore forensic workstations to a known state.

## 3.2 Scope

This procedure applies to forensic workstations used in the Digital Evidence Unit.

## Equipment

**3.3.1** Forensic workstation

**3.3.2** System media

**3.3.3** Forensic software for creating and restoring system images

**3.3.4** Vendor restore image on CD or DVD

## 3.4 Procedure

**3.4.1** Forensic workstation system media will be created for each forensic workstation used in casework. The system media will be checked for malware and verified to be working properly. The system media for each workstation will be stored on the Digital Evidence Network Attached Storage (NAS) system for image restoration.

**3.4.2** If previously created system media is available, skip to step **3.4.7.**

**3.4.3** If no previously created system media is available, use the original system restoration disc(s) to perform a fresh installation of the operating system.

**3.4.4** Install necessary software and configure the new system.

**3.4.5** Check the freshly installed operating system for malware and verify it to be working properly.

**3.4.6** Use forensic software create an image of the system and store the system image on the Digital Evidence Unit NAS.

**3.4.7** Use system media to restore forensic workstation system image.

## 3.5 Limitations – N/A

## 3.6 Safety - N/A

## **3.7 References**

*Scientific Working Group on Digital Evidence*

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter: 4 Target Media Preparation

## 4.1 Purpose

The purpose of this procedure is to describe how to prepare target media used in forensic casework.

## 4.2 Scope

This procedure applies to all target media used in casework and is intended to ensure that no cross contamination occurs between cases.

## 4.3. Equipment

 **4.3.1** Forensic software and hardware device capable of wiping target media

 **4.3.2** Target media

## 4.4. Procedure

**4.4.1** Select a media device to be used as target media.

**4.4.2** Use a forensic software and hardware to wipe and overwrite all data on the target media.

**4.4.3** Format the target media.

**4.4.4** Name the target media so that it can be identified.

**4.4.5** Check that the target media is wiped using forensic software and hardware.

## 4.5 Limitations – N/A

## 4.6 Safety - N/A

## 4.7 References

*Scientific Working Group on Digital Evidence*

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 5: Write Protection

## 5.1 Purpose

The purpose of this procedure is to ensure the integrity and prevent the alteration of digital evidence during forensic examination and extractions.

## 5.2 Scope

This procedure applies to all digital evidence.

## 5.3. Equipment

**5.3.1** Forensic software and hardware

## 5.4 Procedure

**5.4.1** Write-protect digital evidence and work with forensic images of digital evidence when possible.

**5.4.2** Connect write protection hardware or evoke write protection measures prior to starting a forensic examination or forensic extraction.

**5.4.3** When it is not possible to write protect digital evidence due to hardware configurations, operating system or other constraints and successfully image, examine or extract data, the digital evidence may be utilized to perform the forensic work requested.

**5.4.4** Digital Examiners will document in the case notes when a forensic image could not be utilized, and all the write protection methods that were attempted.

## **5.5** Limitations

It is not always possible to write protect all digital evidence. Under most circumstances it’s not possible to write protect mobile devices. Some digital evidence requires a two-way communication to allow access to the digital contents.

## 5.6 Safety - N/A

## 5.7 References

*Scientific Working Group on Digital Evidence*

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 6: Forensic Imaging

## 6.1 Purpose

The purpose of this procedure is to ensure digital evidence is imaged in a forensically sound manner.

## 6.2 Scope

This procedure applies to all digital evidence imaged for a forensic examination.

## 6.3. Equipment

**6.3.1** Forensic hardware and software

**6.3.2** Write protection software and/or hardware

**6.3.3** Target Media

## 6.4 Procedure

**6.4.1** Attach a target media into the Forensic Workstation and boot its operating system

or attach the target media to the evidence computer if using a Linux boot disc to export an evidence image.

**6.4.2** Connect write protection hardware or evoke write protection measures prior to starting a forensic examination of the computing device or digital storage device.

**6.4.3** Obtain a forensic image of the digital evidence using forensic software and save the forensic image to the target media.

**6.4.4** Obtain an acquisition hash value of the forensic image and a verification hash value of the forensic image.

**6.4.5** While the evidence hard drive is attached to the write protection, additional application software that requires access to the digital evidence may be run (e.g. anti-virus software, etc.).

## 6.5 Limitations

A stable hash value may not be able to be obtained for a failing hard drive, media devices with bad disk sectors and some SSD Drives.

## 6.6 Safety - N/A

## 6.7 References

*Scientific Working Group on Digital Evidence*

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 7: Forensic Imaging Using Target Disk Mode

## 7.1 Purpose

The purpose of this procedure is to ensure a Macintosh computer is imaged in a forensically sound manner using Target disk mode without removing the internal drive.

## 7.2. Scope

This procedure applies to computers running the Macintosh operating system.

## 7.3. Equipment

**7.3.1** Forensic workstation

**7.3.2** Target media

**7.3.3** Transfer cable supported by the evidence computer.

## 7.4 Procedure

**7.4.1** Attach a target media into the forensic workstation and boot the operating system.

**7.4.2** Connect a transfer cable to a write blocker and then to the Macintosh computer to be imaged. Boot the computer into Target Disk Mode.

**7.4.3** Obtain a forensic image of the digital evidence using forensic software and save the forensic image to the target media.

**7.4.4** Obtain an acquisition hash value of the forensic image and a verification hash value of the forensic image.

**7.4.5** Remove the digital evidence from the forensic workstation.

## 7.5. Limitations – N/A

## 7.6 Safety - N/A

## 7.7 References

How To: Forensically Sound Mac Acquisition in Target Mode, SANS Computer Forensics and Incident Response, February 2011, URL: <http://computer-forensics.sans.org/blog/2011/02/02/forensically-sound-mac-acquisition-target-mode>

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 8: Mobile Devices

## 8.1 Purpose

This procedure establishes a systematic process for data extraction from mobile devices.

## 8.2 Scope

This procedure applies to all mobile computing devices submitted for forensic extractions and examinations.

## 8.3 Equipment

**8.3.1** Forensic software or hardware tool for data extraction

**8.3.2** Forensic workstation

**8.3.3** Target media

**8.3.4** Cables / connectors

**8.3.5** Isolation equipment

**8.3.6** SIM card adapter

## 8.4 Procedure

**8.4.1** Determine if the device is supported by available forensic software or hardware tools.

**8.4.2** Place the device into airplane mode if the device is received in a power “On” state or in isolation before powering the device “On” and immediately into airplane mode once powered “On”.

**8.4.3** Remove the SIM card if the device is in a power “Off” state.

**8.4.4** Determine if the device is locked (PIN, passcode, pattern lock, fingerprint lock, etc.) and forensic software or hardware tools support a password bypass.

**8.4.3** Determine if the device contains removable media (e.g. a micro SD card) that requires removal from the device for extraction or imaging purposes and remove it from the device prior to beginning an extract or examination. Removable media may be left in the mobile device during extraction or examination.

**8.4.5** Refer to support documentation for specific forensic tools to determine if a physical, file system, and / or logical extraction of the mobile device is supported by the forensic software and hardware tool.

**8.4.6** Conduct an acquisition of the removable media onto target media using a forensic hardware or software tool. Forensic software and hardware may be used to clone a SIM card if necessary, to access mobile device data. If the forensic tool requires removable media, it is permissible to insert wiped media or cloned media into the device for data extraction.

**8.4.7** Extract data from the mobile device data onto a target media using a forensic software or hardware tool. Refer to the mobile device tool support documentation for the appropriate procedural steps, cable connections, and settings for the device. Data extractions can require utilization of Bluetooth to obtain an extraction from the device. If Bluetooth is required, it is permissible to pair the mobile device with the forensic tool through a Bluetooth connection. Some data extractions may require removable media to be inserted into the device if the removable media slot is empty.

**8.4.8** Create a raw data file and / or forensic software report for the forensic extraction.

**8.4.9** Examine the extracted data using forensic software or hardware if a forensic examination is necessary.

**8.4.10** If a mobile device is not supported by available software or hardware tools, a manual examination of the device may be performed.

**8.4.11** In the event that the mobile device has internal or external damage, the Digital Examiner will determine the appropriate procedure for extraction and examination.

## 8.5 Limitations

**8.5.1** Not all mobile devices are supported by available software or hardware tools.

**8.5.2** Mobile devices powered on for extraction can result in the alteration of evidence or may allow a remote wipe signal to reach the device.

**8.5.3** The inability to utilize isolation equipment can result in the alteration of evidence.

**8.5.4** Insertion of a target media or cloned media into a mobile device can result in the alteration of evidence.

**8.5.5** Mobile devices can be set to lock or wipe after a set number of failed passcode unlock attempts. The unknown number of passcode unlock attempts taken prior to submission to the CCBI Laboratory can impact the ability to extract data from a mobile device.

**8.5.6** Removal of SIM cards or SD cards can result in accidental device button activation.

**8.5.7** The level of extraction will depend on the support for the device.

## 8.6 Safety – N/A

## 8.7 References

*Scientific Working Group on Digital Evidence*

*National Institute of Standards and Technology Guidelines on Mobile Device Forensics*

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 9: Minimum Standards

## 9.1 Purpose

The purpose of this procedure is to outline minimum standards for conducting and documenting forensic examinations and forensic extractions in the Digital Evidence Unit.

## 9.2 Scope

This procedure applies to work conducted in the Digital Evidence Unit by CCBI Crime Laboratory personnel.

## 9.3 Equipment

**9.3.1** Digital Examiners may use any forensic software or hardware he or she deems necessary to complete forensic examinations and forensic extractions.

## 9.4 Procedure

**9.4.1** Digital Examiners will document in the case file if the work performed is a forensic examination or forensic extraction.

**9.4.2** Digital Examiners will document in the laboratory case file the legal right to examine, extract and collect data from digital evidence. Digital Examiners will place search warrants, court orders and any other legal document granting legal right to examine, extract and collect data from digital evidence in the administrative documents of the case file.

**9.4.3** Digital Examiners will list an inventory of all of digital evidence forensically examined or forensically extracted in the case file.

**9.4.4** Digital Examiners will document the following information in the case notes about digital evidence when possible and available:

**9.4.4.1** Manufacturer

**9.4.4.2** Make

**9.4.4.3** Model number

**9.4.4.4** Serial number

**9.4.4.5** Storage size or capacity

**9.4.5** Photographs taken of digital evidence will be stored in the Digital Crime Scene (DCS) database. The DCS call id will be noted in the case notes.

**9.4.6** Digital Examiners will list all software and hardware tools used to conduct forensic examinations and forensic extractions in the case file.

**9.4.6** Digital Examiners will perform the following if possible, to ensure digital evidence is unaltered during forensic examinations and forensic extractions:

**9.4.6.1** Document the result of performance checks.

**9.4.6.2** Obtain and document in the case file acquisition, verification, and post examination hash values.

**9.4.6.3** Document any forensic imaging acquisition errors.

**9.4.6.4** When hash values and acquisition errors are stored on derivative media as part of forensic software reports or reporting features, Digital Examiners will document in the case notes the location (i.e. the evidence item number) where the information can be found and the results of hash value comparisons in the case notes.

**9.4.7** Forensic examinations will be conducted using a forensic image of digital evidence when possible. Digital Examiners will document in the case notes the reason(s) and or cause(s) a forensic examination was conducted directly on digital evidence or when digital evidence has been subjected to potential alteration during a forensic examination or forensic extraction.

**9.4.8** Digital Examiners will document recovered evidence, results and conclusions of forensic examinations in the case file. Recovered digital evidence, raw data files, digital reports or reporting features created from forensic software or hardware tools which are necessary to support forensic examinations and conclusions or that result from forensic extractions will be placed on derivative media.

**9.4.9** Digital Examiners will label derivative media as an item of evidence and document in the case notes the contents of derivative media (i.e., digital evidence, raw data files, and digital reports located on the derivative item of evidence).

**9.4.10** Derivative media will be returned to the submitting agency of the digital evidence.

**9.4.11** Digital Examiners will use the following forms to document forensic examinations and extractions:

 **9.4.11.1** Physical Examination and Forensic Extraction (CCBI-136)

 **9.4.11.2** CCBI Additional Notes Form (CCBI-111)

**9.4.12** Digital Examiners will consult with Forensic Examiners in the appropriate disciplines to ensure that evidence will not be lost when other forensic examinations have been requested.

## 9.5 Safety – N/A

## 9.6 Limitations

**9.6.1** Manufacturer,make, model, serial number, and memory and storage capacity may not always be readily available.

**9.6.2** In some instances it may not be possible to write protect digital evidence.

**9.6.3** Errors may occur during forensic image acquisition; however, acquisition errors do not preclude examination of a forensic image.

## 9.7 References – N/A

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 10: Reporting Results

## 10.1 Purpose

This procedure establishes the guidelines for reporting of results of forensic examinations and forensic extractions.

## 10.2 Scope

This procedure applies to forensic examinations and forensic extractions conducted by the Digital Evidence Unit.

## 10.3 Equipment – N/A

## 10.4 Procedure

**10.4.1** All forensic extractions will be reported using the Technical Field Assistance Report Template in Appendix A.

 **10.4.1.1** Wording in **black** is required.

**10.4.1.2** Wording in **green** is optional and will be completed as necessary to accurately complete the forensic extraction report.

**10.4.1.3** Wording in ***italic gray***is instructional and will be completed by the Examiner in conformance with the instruction(s).

**10.4.2** All forensic examinations will be reported using the CCBI Laboratory General Report Format template located in the CCBI Report Writing Manual. The following information shall be added to the General Report Format template, when applicable:

**10.4.2.1** The **“**Items Submitted” section will be completed in accordance with the General Report Format template instructions.

**10.4.2.2** The “Type Examination Requested” section will be listed as “Digital Evidence Analysis”.

**10.4.2.3** The “Results and Conclusions” section will contain the following when applicable to the forensic examination:

**10.4.2.3.1** A statement describing the information, digital data, and evidence recovered pursuant the legal scope(s) the forensic examination.

**10.4.2.3.2** A statement identifying the derivative evidence by item number which contains digital reports or reporting features created from forensic software or hardware tools which are necessary to support forensic examinations results and conclusions.

**10.4.2.3.3** A statement identifying by item number derivative evidence resulting from the forensic examination.

**10.4.2.3.4** The laboratory report will contain the following statement if any of the items of evidence examined contain images of child sexual exploitation: *“Digital media examined in this case contains images of child sexual exploitation.”*

**10.4.2.3.5** A statement identifying the software and its version number used.

**10.4.2.4** The “Disposition” section will contain the following statement when applicable to the forensic examination: “*The following evidence was returned to the submitting agency: <insert the CCBI evidence item numbers returned to the submitting agency >.*

**10.4.3** Digital Examiners may modify or add statements to a laboratory report as necessary to clarify a laboratory report.

## 10.5 Limitations- N/A

## 10.6 Safety -N/A

## 10.7 References -N/A

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. Added reporting requirement of software and version. |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 11: Equipment and Evidence Transport

## 11.1 Purpose

This procedure establishes the guidelines for transporting the equipment used in digital evidence examinations and digital evidence to and from the Crime Laboratory. These guidelines are intended ensure to proper functioning and prevent damage to equipment during transport.

## 11.2 Scope

This procedure applies to CCBI Digital Examiners transporting digital evidence equipment and digital evidence.

## 11.3 Equipment

 **11.3.1** Isolation container (i.e., Faraday Container)

## 11.4 Procedure

**11.4.1** Place equipment and digital evidence on the floor of the vehicle to minimize the potential for damage and movement. Do not place equipment or digital evidence in the trunk of a vehicle.

**11.4.2** Protect equipment and digital evidence from electromagnetic energy (i.e., magnets, radio transmitters, etc...) where possible.

**11.4.3** When appropriate, an isolation container can be used to prevent unintended loss of, or remote access to digital evidence.

## 11.5 Limitations- N/A

## 11.6 Safety -N/A

## 11.7 References -N/A

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 12: Glossary

## 12.1 Purpose

The purpose of this glossary in to define and clarify the meaning of terms used by the Digital Evidence Unit.

## 12.2 Scope

The glossary pertains to Digital Evidence Unit notes, reports, technical procedures, and the training program.

## 12.3 Definitions

* **Application Software –** operating system(s) and software program(s) designed to help the user of a computing device perform a specific task.
* **Child Pornography**- media containing images depicting the sexual acts or lascivious exhibitions of genitals or pubic areas of a minor.
* **Clone -** a bit by bit duplication of evidence media that is readily modifiable.
* **Control Media** – digital media with a known hash value or a known discrete data structure used for quality control purposes.
* **Derivative Media –** wiped media used to store recovered digital evidence, raw data files, digital reports or reporting features created from forensic software or hardware tools used by a Digital Evidence Examiner during a forensic examination or forensic extraction.
* **Digital Evidence** – Any computing device, digital storage device, digital file or electronic file containing evidence of a crime.
* **Evidence Media** –any source digital storage device that is forensically examined or from which data is forensically extracted.
* **File System Extraction** – A method of extraction that includes the file system and user data of the device and may contain deleted data from databases in the file system.
* **Forensic Examination** – an extraction of data from a computing device or digital storage device and analysis by a forensic examiner of the data resulting in conclusions or interpretations about the data.
* **Forensic Extraction** – an extraction of data from a digital computing device or digital storage device.
* **Forensic Image** – a duplication of Evidence Media in a compressed format that is not readily modifiable.
* **Forensic Software and Hardware** – forensic software and hardware devices listed on the Digital Evidence Equipment List which are approved for use in forensic examinations and extractions performed by the Digital Evidence Unit.
* **Forensic Workstation-** A computer system designated for forensic examinations and forensic extractions.
* **Format** - to prepare a storage medium with a file system for reading and writing by an operating system.
* **Hash Value** – An alphanumeric value that uniquely represents a set of data.
	+ **Acquisitions hash** – a hash value obtained during acquisition of a forensic image.
	+ **Verification hash** – a hash value obtained after acquisition of a forensic image.
	+ **Post hash** – a hash value obtained after a completion of a forensic examination.
* **Isolation** –prevention of connection of a computing device to a digital network, WI-FI, telecommunication or radio network.
* **Logical extraction** – A method of extraction that includes user data available through the device’s Application Program Interface but does not include deleted data or unallocated space.
* **Manual Examination**- A method of manual manipulation of a devices file system while recording video and/or photographing evidentiary items.
* **Mobile Devices** - portable devices that have embedded system architecture, processing capability, on–board memory, and or telecommunication capabilities (e.g., cell phones, tablets, and smartphones).
* **Pattern Lock** – A type of security lock set by the user to prevent access to the device that involves drawing a pattern to unlock the device.
* **Physical Extraction** – A method of extraction that includes a bit-by-bit image of the flash memory of a device that contains system and user data to include deleted data, hidden data, and unallocated space.
* **PIN** – The **P**ersonal **I**dentification **N**umber that may be enabled on computing devices or media device to control access to the device
* **Power On Self-Test (POST)** – A series of diagnostic tests that are performed when a computer
* **Raw Data Files** - digital files and images created during or associated with a forensic examination or forensic extraction which are necessary to re-examine, review, and recreate result conclusions
* **SIM Card** – The Subscriber Identity Module (SIM) card used in computing devices to connect to a telecommunications carrier network (i.e., AT&T, Verizon, Sprint, etc.).
* **System Media** – A storage device containing a known image of a Forensic Workstation which is used for a new or clean installation of the operating system and application software of a Forensic Workstation.
* **Target Disk Mode** – Target Disk Mode allows an Apple Macintosh system to act as if the entire computer were an external hard drive for another system. This mode works at the firmware level before the operating system is engaged and booted. It is entered by holding down the “T” key on the Apple Macintosh system during the boot process.
* **Target Media** – wiped media to which information or data from a forensic examination or forensic extraction will be written.
* **Wiped Media** –any digital storage device devoid of any data such that all bits in the device are set to a known common value.

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix A – Technical Field Assistance Report Template

**Raleigh/Wake City-County Bureau of Identification**

**Crime Laboratory Division**

**3301 Hammond Road**

**Raleigh, North Carolina 27603**

**\*\*Requestor\*\***

**(Insert Name of Requesting Official)**

**Insert Requesting Agency Name**

**Insert Requesting Agency Street Address**

**Insert Requesting Agency City, State, Zip**

**Submitting Agency Case #:**

**Type of Case:**

**Submitted By:**

**Date Submitted:**

**Date Requested:**

**Subject: Subject Name**

**Victim: Name of Victim** *Insert* **(deceased)** *if applicable*

===================================================================

**CCBI Laboratory Technical Field Assistance Report**

**===================================================================**

**Type of Crime**

**Offense:** *Insert Offense Type*

**Warrant / Consent:** This device was accessed pursuant to

*Provide a description of the legal right to access the device (i.e., search warrant, consent form or the implied consent of the deceased victim). If legal right is pursuant to a deceased victim, ensure the submitting agency has denoted the victim as deceased on the Laboratory Request for Examination Form.*

**Technical Field Assistance**

The CCBI Crime Laboratory received the device(s) described in this report for the purpose of

*Choose the applicable option(s) from the following:*

*(a)* **a passcode-unlock**

**and**

*(b)* **data extraction.**

*Choose the applicable option(s) from the following:*

*(a)* **A passcode recovery application has been loaded onto the device. The device must be kept powered “On” until passcode recovery is complete. Once complete, the passcode will be displayed on the device screen. MAKE RECORD OF THE PASSCODE. Once the passcode is recovered, the device may be powered “Off”, and the application will be removed from the device. The passcode may be used to access the device at any time.**

*(b)* **The passcode for this device is** “*insert the passcode extracted from the device”***.**

*(c)* **Data was extracted from the device and stored on a digital media device provided by** *insert CCBI or submitting agency name.*

*(d)* **The device was unable to be accessed.**

**Physical Evidence**

*Choose the applicable option(s) from the following:*

*(a)* CCBI Item # *Insert CCBI item number.* **(Agency Item #)** *Insert agency item number if available***.** -*Insert a description of the device. Include available information specific for the device (i.e., manufacturer make, model, model#, serial#, FCC ID, etc.)***.**

*(b)* **CCBI Item *#*** *Insert the CCBI sub-Item number(s) for the digital media device(s) containing the data extracted from the parent device(s).**Provide a description of the type of data extracted from the parent device and a description of the device to which the extracted data was stored (e.g., a DVD containing a data extracted from CCBI Item # 1).*

**Disposition**

The following evidence was returned to the submitting agency:*Insert the CCBI evidence item numbers returned to the submitting agency. A disposition statement addressing all evidence received and derived during the extraction is required. The disposition statement may be modified to the extent necessary to clarify the disposition of evidence.*

*Insert examiner name*, **certifications** *Insert professional certification(s) and educational degree(s).*

Digital Evidence Examiner

**\*\*\* Confidential: This is an official file of the City-County Bureau of Identification. This report is to be used and distributed only in connection with an official criminal investigation and shall not be reproduced, except in its entirety, without written approval of the Director. End of Laboratory Technical Field Assistance Report\*\*\***

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 9/8/2020 | 1 | Released new technical procedures manual. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |