**Raleigh/Wake City-County**

**Bureau of Identification**

**Crime Laboratory Division**

**DIGITAL EVIDENCE UNIT**

**TECHNICAL PROCEDURES MANUAL**



**Contents**

[Chapter 1: Administration 5](#_Toc529956432)

[1.1 Purpose 5](#_Toc529956433)

[1.2 Scope 5](#_Toc529956434)

[1.3 Forensic Examination Services 5](#_Toc529956435)

[1.4. Scope of Search and Plain View Searches 5](#_Toc529956436)

[1.5. Cases Involving Child Pornography 5](#_Toc529956437)

[1.6. Equipment, Materials and ReCrime Scene Investigators – N/A 6](#_Toc529956438)

[1.7. Limitations 6](#_Toc529956439)

[1.8. Safety - N/A 6](#_Toc529956440)

[Chapter 2: Equipment Maintenance 8](#_Toc529956441)

[2.1 All equipment is to be maintained. 8](#_Toc529956442)

[2.2 Performance Checks and Verifications 8](#_Toc529956443)

[2.3. Limitations – N/A 8](#_Toc529956444)

[2.4. Safety - N/A 8](#_Toc529956445)

[Chapter 3: System Image Restoration 11](#_Toc529956446)

[3.1 Purpose 11](#_Toc529956447)

[3.2 Scope 11](#_Toc529956448)

[3.3 Equipment 11](#_Toc529956449)

[3.4 Procedures 11](#_Toc529956450)

[3.5 Limitations – N/A 12](#_Toc529956451)

[3.6 Safety - N/A 12](#_Toc529956452)

[Chapter: 4 Technical Procedure for Target Drive Preparation 14](#_Toc529956453)

[4.1 Purpose 14](#_Toc529956454)

[4.2 Scope 14](#_Toc529956455)

[4.3. Equipment, Materials and ReCrime Scene Investigators 14](#_Toc529956456)

[4.4. Procedure 14](#_Toc529956457)

[4.5 Limitations – N/A 14](#_Toc529956458)

[4.6 Safety - N/A 14](#_Toc529956459)

[Chapter 5: Write Protecting Media 16](#_Toc529956460)

[5.1 Purpose 16](#_Toc529956461)

[5.2 Scope 16](#_Toc529956462)

[5.3. Hardware 16](#_Toc529956463)

[5.4 Procedures 16](#_Toc529956464)

[5.5 Limitations – N/A 16](#_Toc529956465)

[5. 6 Safety - N/A 16](#_Toc529956466)

[Chapter 6: Hard Drive Imaging Protocol 18](#_Toc529956467)

[6.1 Purpose 18](#_Toc529956468)

[6.2 Scope 18](#_Toc529956469)

[6.3. Equipment 18](#_Toc529956470)

[6.4 Limitation 18](#_Toc529956471)

[6.5 Procedures 18](#_Toc529956472)

[6.6 Safety - N/A 19](#_Toc529956473)

[Chapter 7: Imaging a Macintosh Operating system using Target Disk Mode. 21](#_Toc529956474)

[7.1 Purpose 21](#_Toc529956475)

[7.2. Scope 21](#_Toc529956476)

[7.3. Equipment 21](#_Toc529956477)

[7.4 Procedures 21](#_Toc529956478)

[7.5. Limitations – N/A 21](#_Toc529956479)

[7.6 Safety - N/A 21](#_Toc529956480)

[Chapter 8: Technical Procedure for Mobile Device Extraction 23](#_Toc529956481)

[8.1 Purpose 23](#_Toc529956482)

[8.2 Definitions – N/A 23](#_Toc529956483)

[8.3 Equipment, Materials and ReCrime Scene Investigators 23](#_Toc529956484)

[8.4 Procedures 23](#_Toc529956485)

[8.5 Limitations- 24](#_Toc529956486)

[8.6 Safety – N/A 25](#_Toc529956487)

[8.7 References 25](#_Toc529956488)

[Chapter 9: Minimum Examination Standards 27](#_Toc529956489)

[9.1 Purpose 27](#_Toc529956490)

[9.2 Scope 27](#_Toc529956491)

[9.3 Definitions - N/A 27](#_Toc529956492)

[9.4 Equipment, Materials and ReCrime Scene Investigators 27](#_Toc529956493)

[9.5 The necessary legal authority 27](#_Toc529956494)

[9.6 Procedure- 27](#_Toc529956495)

[9.7 Evidence Preservation 27](#_Toc529956496)

[9.8 Forensic Examination 27](#_Toc529956497)

[9.9 Visual Inspection 28](#_Toc529956498)

[9.10 Forensic Duplication 28](#_Toc529956499)

[9.11 Media Examination 28](#_Toc529956500)

[9.12 Notes 28](#_Toc529956501)

[9.13 Approved Software 28](#_Toc529956502)

[9.14 Inspection forms 28](#_Toc529956503)

[9.15 Limitations 29](#_Toc529956504)

[Chapter 10: Generating Results 31](#_Toc529956505)

[10.1 Purpose 31](#_Toc529956506)

[10.2 Scope 31](#_Toc529956507)

[10.3 Procedures 31](#_Toc529956508)

[Chapter 11: Evidence Transport 33](#_Toc529956509)

[11.1 Evidence Transport 33](#_Toc529956510)

[Chapter 12: Glossary for Computer Forensics 35](#_Toc529956511)

[12.1 Purpose – 35](#_Toc529956512)

[12.2 Scope 35](#_Toc529956513)

[12.3 Definitions 35](#_Toc529956514)

[Appendix A – Technical Field Assistance Report Template 39](#_Toc529956515)

#

# Chapter 1: Administration

## Purpose

The purpose of the procedure is to establish procedures and guidelines for the collection and examination of digital devices by the Digital Evidence Unit. The Digital Evidence Unit will provide thorough and professional digital examination services to the Wake County law enforcement community by qualified personnel.

## Scope

The Digital Evidence Unit will provide professional digital examination services to the Wake County law enforcement community by qualified personnel.

## 1.3 Forensic Examination Services

Personnel in the Digital Evidence Unit may conduct forensic examinations of computer systems, digital recording/storage devices, mobile/handheld devices, and digital storage media.

##  Scope of Search and Plain View Searches

Personnel in the Digital Evidence Unit will understand the scope of the search warrant before performing any forensic examination. If the examiner finds evidence of a crime, outside of that scope and in plain view during a forensic examination, the examiner should stop the examination. The examiner will recommend to the case investigator to write a supplemental search warrant to cover the newly found evidence. Such a recommendation will be documented.

##  Cases Involving Child Pornography

**1.5.1** During investigations where images depicting possible child pornography are discovered, CCBI employees shall store and transfer the files using methods that avoid the accidental distribution or unnecessary reproduction of the images.

**1.5.2** If the Digital Evidence 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 shall not maintain any electronically duplicated images used for this purpose.

##  Equipment, Materials and ReCrime Scene Investigators – N/A

## Limitations

Not all digital evidence items are supported by the current CCBI forensic examination software or hardware.

##  Safety - N/A

**References** – CCBI Crime Laboratory Administrative procedures manual.

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedure Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 2: Equipment Maintenance

## 2.1 All equipment is to be maintained.

**2.1.1** All maintenance is to be documented and retained in the unit maintenance log. In the event that repairs or modifications are performed on equipment, a performance check will be conducted before the system or any of its components are utilized for casework purposes. The Digital Evidence maintenance log will be stored on the CCBI Network Share, in the Digital Evidence folder.

## 2.2 Performance Checks and Verifications

**2.2.1** Performance checks are made by conducting a successful power on self test (POST) and successful loading of the operating system.

**2.2.2** The forensic computer must be verified each day that it is used to ensure that the computer hardware and software are functioning properly. The results will be noted in the Computer Forensics Unit Calibration Log stored in the digital evidence section.

**Procedures**

**2.2.3** A “control” media device is inserted in the forensic machine and forensically imaged in the applicable forensic software each day before any examinations are carried out.

**2.2.4** The forensic image is opened in the applicable forensic software to ensure that the MD5 hash value for the captured forensic image matches the known MD5 hash for the control media device. A notation is made as to whether the hash values match on the unit calibration log. In addition, a notation that the forensic computer was verified is made in the examiner’s case notes.

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

## 2.3. Limitations – N/A

## 2.4. Safety - N/A

**References – N/A**

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedure Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 3: System Image Restoration

## 3.1 Purpose

The purpose of this procedure is to restore the forensic workstation system drives used in forensic casework to a default state in order.

## 3.2 Scope

This procedure applies to personnel who prepare workstation system drives used in forensic computer examinations.

## 3.3 Equipment

* Forensic workstation
* Hard drive
* Software for creating and restoring system images
* Previously created system image (if available) or factory restore image on CD or DVD

## 3.4 Procedures

**3.4.1** A forensic workstation system image will be created for each desktop workstation used in casework. The baseline image will be checked for malware and verified to be working properly. The image for each workstation will be stored on the digital evidence NAS storage for system image restoration.

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

**3.4.3** If no previously created system image 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 a backup utility to create an image of the system.

**3.4.7** Restore the system drive using the prepared system image.

## 3.5 Limitations – N/A

## 3.6 Safety - N/A

**References –** Scientific Working Group on Digital Evidence Best Practices for Computer Forensics

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedure Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter: 4 Technical Procedure for Target Drive Preparation

## 4.1 Purpose

The purpose of this procedure is to wipe all data from Target drives used in forensic casework in order to ensure that no cross contamination occurs between cases.

## 4.2 Scope

This procedure describes the steps to be taken by personnel of the Digital Evidence Unit in preparing Target drives for use in forensic computer examinations.

## 4.3. Equipment, Materials and ReCrime Scene Investigators

* Forensic Computer or Forensic Tool
* Digital media
* Approved software or hardware device for wiping data

## 4.4. Procedure

**4.4.1** Select digital media to be used as target drive.

**4.4.2** Use an approved software or hardware device for wiping data to overwrite all data from the target drive.

**4.4.3** Format the target drive.

**4.4.4** Name the target drive so that it can be easily identified as such.

## 4.5 Limitations – N/A

## 4.6 Safety - N/A

**References –** Scientific Working Group on Digital Evidence Best Practices for Computer Forensics

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedure Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 5: Write Protecting Media

## 5.1 Purpose

The purpose of this procedure is to preserve the integrity of the evidence during examination by preventing alterations.

## 5.2 Scope

**5.2.1** This procedure applies, when possible, to all digital storage media and/or devices that have been submitted for examination.

## 5.3. Hardware

**5.3.1** Write protection firmware and/or hardware

**5.3.2** Internal or external hard drive

**5.3.3** Removable media

## 5.4 Procedures

**5.4.1** Original evidence will be write-protected when possible. Some digital evidence items require a two way communication to allow access to the digital contents.

**5.4.2** The Digital Evidence Unit is to avoid working on original evidence. It is understood, however, that original evidence may have to be examined due to hardware configurations or certain operating systems. If this must be done, the Digital Evidence Examiner will document actions taken during the examination. Under most circumstances it’s not possible to write protect a mobile device and successfully extract its contents.

## 5.5 Limitations – N/A

## 5. 6 Safety - N/A

**References –** Scientific Working Group on Digital Evidence Best Practices for Computer Forensics**,** Forensic Toolkit (FTK) User Guide.

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedure Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 6: Hard Drive Imaging Protocol

## 6.1 Purpose

The purpose of this procedure is to create a forensically sound image of evidence hard drives.

## 6.2 Scope

This is the procedure to be utilized in imaging hard drives submitted as evidence or during a field response.

**Definitions**

## 6.3. Equipment

* **Approved forensic software tool or hardware device for acquisition**
* **Forensic computer**
* **Write-Blocker**
* **Target drive**
* **Control media**

## 6.4 Limitation

Due to a failing hard drive, disk bad sectors or some SSD Drive’s, a stable hash value may not be repeatable from the device.

## 6.5 Procedures

**6.5.1** Attach the evidence hard drive to a hardware or firmware write-blocking device.

**6.5.2** Attach or insert the target drive into the forensic workstation and boot the forensic computer into the operating system. It may be necessary to attach the Target drive to the evidence computer when using a Linux boot disc or USB drive and exporting an evidence image.

**6.5.3** Obtain a forensic image of the evidence drive using forensic imaging software and save the forensic image to the target drive. Post verify the exported Hash value of the image matches the calculated hash during the imaging process.

**6.5.5** While the evidence hard drive is attached to the write-blocker, additional programs that require access to the physical disk may be run (e.g. anti-virus software, etc.).

**6.5.7** Remove the evidence hard drive from the forensic workstation.

## 6.6 Safety - N/A

**References –** Scientific Working Group on Digital Evidence Best Practices for Computer Forensics, Forensic Toolkit (FTK) User Guide.

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedure Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 7: Imaging a Macintosh Operating system using Target Disk Mode.

## 7.1 Purpose

**7.1.1** The purpose of this procedure is to forensically image a Macintosh computer without removing the internal hard drive by using Target disk mode.

## 7.2. Scope

This procedure applies to computers running the Macintosh operating system.

## 7.3. Equipment

* Forensic computer
* Prepared target drive
* Transfer cable supported by the evidence computer.

## 7.4 Procedures

**7.2.1** Connect the proper cable to the write blocker and then to the Macintosh computer to be imaged.

**7.2.2** Boot the computer into Target Disk Mode. Use a forensic imaging software export and evidence image to the Target drive on the forensic workstation. Post verify the exported Hash value of the image matches the calculated hash during the imaging process.

## 7.5. Limitations – N/A

## 7.6 Safety - N/A

**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** |
| 1/24/18 | 1 | New Technical Procedure Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 8: Technical Procedure for Mobile Device Extraction

## 8.1 Purpose

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

## 8.2 Definitions – N/A

## 8.3 Equipment, Materials and ReCrime Scene Investigators

* Approved mobile device tools for data extraction (software or hardware)
* Forensic computer
* Target drive
* Set of cables and connectors
* Isolation equipment
* SIM card adapter

## 8.4 Procedures

**8.4.1** This procedure describes the steps to be taken by personnel of the CCBI Crime Laboratory in extracting data from mobile devices.

**8.4.2** Determine if a Physical, File System, or Logical extraction of the mobile device is supported by approved mobile device tools. Refer to the support documentation for each tool to determine support for individual devices. The level of extraction will depend on the support for the device.

**8.4.3** Determine if the device contains a SIM card or removable media such as a micro SD card. All SIM cards and removable media shall be physically taken out of the device if possible prior to beginning the examination.

**8.4.4** A mobile device tool can be used to clone the SIM card onto an access SIM card for Insertion into the mobile device.

**8.4.5** To ensure proper isolation once powered on, place the device into airplane mode or flight mode if possible. Disable Wi-Fi and Bluetooth connections.

**8.4.6** Determine if the device is locked (PIN, passcode, pattern lock, fingerprint lock, etc.) and whether or not approved mobile device tools support a password bypass.

**8.4.7** Conduct an acquisition of the removable media using an approved software or hardware tool before returning it to the mobile device. After acquisition is complete, insert the removable media back into the mobile device. Extract mobile device data onto a target drive using an approved mobile device tool. Refer to the mobile device tool support documentation for the appropriate procedural steps, cable connections, and settings for the device. Document the methods used to extract data from the device.

**8.4.8** Create a raw data file and or report for the data extraction in an approved digital

forensic tool.

**8.4.9** Copy the raw data file and or report to digital media to return to the submitting

agency.

## 8.5 Limitations-

**8.5.1** Mobile devices present unique challenges due to numerous models of devices, proprietary software, rapid changes in technology, passcodes, and encryption. Not all mobile devices are supported by forensic tools. In the event that the mobile device is not supported by forensic tools, a Digital Evidence Examiner may conduct a manual examination of the device. This shall be documented in the case notes.

**8.5.2** Mobile devices are powered on for extraction. Not utilizing isolation may result in the alteration of evidence or may allow a remote wipe signal to reach the device.

**8.5.3** Some extractions may require the Digital Evidence Examiner to utilize Bluetooth to obtain an extraction from the device. In the event that the forensic tool requires a Bluetooth extraction, it is permissible to pair the mobile device with the forensic tool through a Bluetooth connection.

**8.5.4** Some extractions may require removable media to be inserted into the device if the removable media slot is empty. In the event that the forensic tool requires removable media, it is permissible to insert forensic media (wiped and formatted) into the device for extraction

**8.5.5** In the event that the mobile device has internal or external damage, the Digital Evidence Examiner may determine the appropriate procedure for examination based on training and experience.

**8.5.6** Always proceed with caution when attempting passcodes on a mobile device. Some devices are set to lock or wipe after a set number of failed attempts. It is also unknown how many passcode attempts may have already taken place before the device was submitted to the Laboratory.

## 8.6 Safety – N/A

## 8.7 References

* Scientific Working Group on Digital Evidence Best Practices for Mobile Phone Forensics
* National Institute of Standards and Technology Guidelines on Mobile Device Forensics
* Cellebrite UFED User Manual
* XRY User Manual

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedures Manual |
| 11/15/18 | 2 | Modified 8.4.8 to create a raw data file or report; and using an approved digital forensic toolModified 8.4.9 to copy the raw data file and or report |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 9: Minimum Examination Standards

## 9.1 Purpose

**9.1.1** This section describes an overview of the examination process.

## 9.2 Scope

This document applies to CCBI Crime Laboratory personnel who generate results for computer forensic casework.

## 9.3 Definitions - N/A

## 9.4 Equipment, Materials and ReCrime Scene Investigators

* Forensic Tower
* Target Hard drive
* Forensic Software

## 9.5 The necessary legal authority

**9.5.1** All computer systems and/or digital media submitted to the Digital Evidence Unit for analysis will be accompanied by a copy of the search warrant, court order, or consent to search form authorizing the search.

## 9.6 Procedure-

## 9.7 Evidence Preservation

**9.7.1** Digital evidence submitted for examination must be maintained in such a way that the integrity of the data is preserved. Evidence must be handled in a manner preventing cross contamination. If other forensic processing will be conducted, the Digital Evidence Examiner should consult with forensic examiners in the appropriate disciplines.

## 9.8 Forensic Examination

**9.8.1** At a minimum, an examination consists of the following:

## 9.9 Visual Inspection

**9.9.1** The Digital Evidence Examiner will determine the type of evidence, its condition, and relevant information to conduct the forensic examination. Photographs may be used to document the evidence condition.

## 9.10 Forensic Duplication

**9.10.1** Conducting a forensic examination on the original evidence media should be avoided if possible. Forensic examinations should be conducted on forensic duplicates/clones or forensic image files.

## 9.11 Media Examination

**9.11.1** Examination of the media will be completed in a logical and systematic manner.

## 9.12 Notes

**9.12.1** Notes stemming from the examination shall include:

* Forensic software programs used during the examination.
* The start and end dates of the analysis.
* Evidence Item numbers in the case and description.
* CCBI case number.
* Imaging or file extraction process used by the examiner.
* Forensic Software version.

## 9.13 Approved Software

The Digital Evidence Examiner may use any software necessary, in his/her discretion, to complete the forensic examination. The Digital Evidence Examiner will document what software that was used during the examination in his/her notes.

## 9.14 Inspection forms

**9.14.1** The forensic examiner will fill out the digital evidence inspection form that pertains to the type of evidence being examined.

**9.14.2** The digital evidence inspection forms are stored on the CCBI forms database.

## 9.15 Limitations

 Media of appropriate size may be used to copy recovered files and forensic image(s).

***References***

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedures Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 10: Generating Results

## 10.1 Purpose

The purpose of this procedure is to provide guidelines for generating case results.

## 10.2 Scope

This policy applies to personnel who generate results for computer forensic casework.

## 10.3 Procedures

**10.3.1** At the conclusion of the forensic examination, copy the forensic image to a prepared media item with enough storage space to accept the image. The image will be returned to the submitting agency, as will the original evidence.

**10.3.2** Copy files recovered in the case and associated work product to a prepared media item. Any media item that has apparent pornographic images of children copied on it as part of the examination will be labeled as follows: “This media may contain contraband and is intended for use by law enforcement in an official criminal investigation. Dissemination of this material may result in a criminal violation.”

**10.3.3** The raw forensic working files generating during the examination will be placed on a prepared media item noted as the forensic working files for release to the submitting agency.

**10.3.4** The digital reports created during the examination will be placed on a prepared media item and noted as the digital evidence reports for release to the submitting agency.

**10.3.5** If data analysis is performed, a written laboratory report will be completed on the CCBI report template. The type of Examination Requested will be “Digital Evidence Analysis”.

**10.3.6** If only data extraction is performed, a written Technical Field Assistance report will be completed. The Technical Field Assistance report template in Appendix A will be used for documenting digital data extractions.

**10.4 Technical Reviews**

**10.4.1** Technical Reviews will be performed on at least 25% of the cases submitted for digital forensic examination.

**10.4.2** 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.

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedures Manual |
| 8/31/18 | 2 | Added 10.4 Technical Reviews Section |
| 11/15/18 | 3 | Clarified 10.3.5 for laboratory reports to be completed if data analysis is performed. Added 10.3.6 to allow for the completion of TFA reports for data extractions. Referenced Appendix A as the TFA report template to be used for digital extractions.  |
|  |  |  |
|  |  |  |

# Chapter 11: Evidence Transport

## 11.1 Evidence Transport

Place seized device(s) and/or media on the floor of the vehicle, not on the seat, to minimize the potential for damage. Do not place the seized device(s) and/or media near magnets or radio transmitters or in the trunk of a vehicle.

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | New Technical Procedures Manual |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Chapter 12: Glossary for Computer Forensics

## 12.1 Purpose –

This procedure contains the specific definitions of the terms and abbreviations used in the computer forensics technical procedures.

## 12.2 Scope

These definitions are to be used to explain any terms within the computer forensics technical procedures and reports.

## 12.3 Definitions

* **AXIOM** – A forensic program from Magnet Forensics.
* **Clone** - The process of performing a sector-by-sector copy operation from the suspect drive to the destination drive. The number of sectors copied is determined by the size of the suspect drive.
* **Compression** - A method of storing files resulting in great savings in disk storage space. Compressed blocks are checked for validity in the same way as uncompressed blocks.
* **Control Media** – A standard piece of media with a known hash value.
* **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 workstation-** A computer system with components designed to conduct forensic examinations of digital media.
* **Format** - DOS command used to prepare a storage medium (hard drive, floppy disk) for reading and writing. Format does not erase data on the disk. It checks for bad sectors and resets the internal address tables (FAT).
* **FTK**- Forensic Tool Kit. A forensic processing program by AccessData.
* **Hash Value** – An alphanumeric value that uniquely represents a set of data.
* **Image drive** - Same as the target drive.
* **Isolation** – Method to ensure that the device cannot connect to a network during examination.
* **Logical file size** - The exact size of a file in bytes and is the number represented in the properties for a file. This is different than physical file size.
* **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.
* **MD5** - A 128-bit value that uniquely describes the contents of a file. This is the standard hash code used in forensics.
* **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 Personal Identification Number that may be enabled on devices or SIM cards to
* **Power-On Self Test (POST)** – A series of diagnostic tests that are performed when a computer
* **PUK** – The Personal Unlock Key is a code needed to unlock a SIM card after unsuccessful PIN attempts. A PUK code is generally only available from the network provider.
* **SIM card** – The Subscriber Identity Module card used in some devices that allows the device to connect to a carrier network (AT&T, Verizon, Sprint, etc.).
* **SIM card Adapter** – A device used to connect the various types of SIM cards (micro or nano) to the forensic tool for extraction.
* **Suspect drive** - The drive (or drives) that are removed from a subject’s computer, or in the possession of a subject, that will be imaged for later analysis. This drive is never analyzed; rather is copied so the analysis can be conducted on the forensic image.
* **System drive** - The forensic hard drive used to boot the forensic tower. This is the drive which contains the forensic search tools.
* **System Image** – Backup of the system drive that contains a clean install of the operating system (OS).
* **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 drive** - The drive to which information from the suspect drive is being written.
* **Virtual Machine (VM)** – A software emulation of a computer that executes programs like a real machine.
* **Wipe** – a procedure for sanitizing a defined area of digital media by overwriting each byte with a known value.
* **Child pornography**- is pornography that exploits children for sexual stimulation. It may be produced with the direct involvement or sexual assault of a child (also known as child sexual abuse images). Abuse of the child occurs during the sexual acts or lascivious exhibitions of genitals or pubic areas which are recorded in the production of child pornography.

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 1/24/18 | 1 | 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**

**Agency Case #:**

**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 Collected**

*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 and Conclusion**

The CCBI Crime Laboratory returned the device(s) described in this report to the submitting agency. *This statement may be modified as necessary.*

M. Brookreson, **certifications** *Insert professional certification(s) and educational degree(s).*

Forensic 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\*\*\***

|  |
| --- |
| **Revision History** |
| **Effective Date** | **Version Number** | **Reason** |
| 11/15/18 | 1 | New Appendix A – TFA report template |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |