Raleigh/Wake City-County
Bureau of Identification
Crime Laboratory Division

FORENSIC COMPUTER UNIT
TECHNICAL PROCEDURES MANUAL

Contents

All copies of this document are uncontrolled when printed

Chapter 1: Administration

1.1 Purpose

The purpose of the procedure is to establish procedures and guidelines for the collection and examination of digital devices by the CCBI Forensic Computer Unit.

1.2 Scope

The Forensic Computer Unit will provide thorough and professional digital examination services to the Wake County law enforcement community by qualified personnel.

1.3 Organization

The Forensic Computer Unit shall be a component of the CCBI Crime Laboratory Division and under the direction of the Crime Laboratory Division Deputy Director.

1.4 Forensic Examination Services

1.4.1 Personnel in the Forensic Computer Unit may conduct forensic examinations of computer systems, digital recording/storage devices, mobile/handheld devices, and digital storage media upon request by a law enforcement agency or District Attorney's Office typically served by CCBI.

1.4.2 Personnel in the Forensic Computer Unit may also conduct forensic examinations of the types of devices listed above in the following circumstances:

- Where the evidence items were seized by non-Wake County law enforcement agencies but the offense committed affects the citizens of Wake County;

- Where the North Carolina State Bureau of Investigation or the North Carolina State Crime Laboratory requests the Forensic Computer Examiner's assistance in an Internet Crimes Against Children Taskforce case; or

- Where exigent circumstance exist.

1.4.3 Personnel in the Forensic Computer Unit may also conduct forensic examinations of digital media or computer systems belonging to Wake County specifically in regards to investigations conducted by the CCBI Office of Professional Standards at the discretion of the Director.

1.5 Limitations on Forensic Examination Services

1.5.1 If personnel in the Forensic Computer Unit have determined that an investigator has turned a digital device on or done anything to make changes to original evidence, it will be at the discretion of the Crime Laboratory Division Deputy Director whether or not a forensic examination will be conducted by CCBI. If the Forensic Computer Unit proceeds with a forensic examination, any changes made to the evidence, known by CCBI staff, prior to the submission of such evidence shall be documented in the CCBI case record or CCBI report.

1.5.2 Any request to examine a forensic image or forensic duplicate/clone rather than the original evidence will be at the discretion of the Crime Laboratory Division Deputy Director. If the Forensic Computer Unit proceeds with a forensic examination, the party submitting the forensic image or forensic duplicate/clone must provide the Forensic Computer Unit with information regarding how and when the forensic image or forensic duplicate/clone was obtained.

1.5.3 Personnel in the Forensic Computer Unit generally will only provide full forensic examination, which includes making a forensic image (where applicable), analyzing that image, and producing a written report. Any requests for creation of forensic images or other such services shall be at the discretion of the CCBI Crime Laboratory Division Deputy Director.

1.6 Scope of Search and Plain View Searches

Personnel in the Forensic Computer Unit should be familiar with the scope of the search warrant before performing any forensic examination. If the examiner finds evidence of a separate crime in plain view during a forensic examination, the examiner should stop immediately. The examiner will print a copy of the evidence item located in plain view and provide a report and the printout of the evidence to the case investigator. The examiner should recommend to the case investigator to write a supplemental search warrant to cover the newly found evidence. Such a recommendation will be documented.

1.7 Services Other Than Forensic Examination

1.7.1 Upon Crime Laboratory Division Deputy Director approval, the Forensic Computer Unit may assist with the physical seizure of computer systems or networked computer systems that have been identified as or suspected of containing data relating to or constituting criminal offenses which are the subject of a criminal investigation. Preferably, the Forensic Computer Unit will conduct the subsequent requested evidence examination; however, the service described in this section is not contingent on CCBI's role in the examination.

1.7.2 Upon investigator or Crime Laboratory Division Deputy Director request, the Forensic Computer Unit may assist personnel in the preparation of search warrants relating to the seizure of computer systems and equipment. Any search warrants provided to or examined by the Forensic Computer Unit in regards to the requested examination that are believed by the Forensic Computer Unit to be insufficient or otherwise questionable should be brought to the CCBI Crime Laboratory Division Deputy Director prior to conducting the requested examination.

1.7.3 Upon CCBI Crime Laboratory Division Deputy Director approval, the Forensic Computer Unit will provide related training to CCBI employees, investigators, patrol officers, other law enforcement agencies, and other groups.

1.8 Ethics

The Forensic Computer Unit will operate under the ethical guidelines put forth by the International Association of Computer Investigative Specialists (IACIS) code of ethical conduct. This IACIS "Forensic Code of Ethical Conduct" states that examiners must:

- Maintain the highest level of objectivity in all forensic examinations and accurately present the facts involved.
- Thoroughly examine and analyze the evidence in a case.
- Conduct examinations based upon established, validated principles.
- Render opinions having a basis that is demonstratively reasonable.
- Not withhold any findings, whether inculpatory or exculpatory, that would cause the facts of a case to be misrepresented or distorted.
- Never misrepresent credentials, education, training, and experience or membership status.
- Advise and provide assistance to all qualified IACIS Forensic Examiners, regardless of agency affiliation.

1.9 Forensic Computer Examination Unit Case Records

The CCBI Evidence Technician shall be responsible for maintaining all records on active cases assigned to the Forensic Computer Unit. The Forensic Computer Unit may retain case records on cases in which evidence is actively being examined and will ensure that such case records are maintained securely during such possession.

Once all evidence has been relinquished to the requesting agency, the case record will be transferred by the CCBI Evidence Technician to Central Records for filing.

1.10 Cases Involving Child Pornography

During investigations where images depicting possible child pornography are discovered, CCBI employees shall comply with the following steps to ensure that there is no accidental distribution or unnecessary reproduction of the images.

1.10.1 The Forensic Computer Unit will securely store the original evidence. Upon completion of the examination, the original evidence will be returned to the investigating agency.

1.10.2 Any media, photographs, or any other item created or recovered by the Forensic Computer Unit as a result of an examination shall be documented, numbered, and packaged as evidence. Upon the completion of the requested examination, all resulting evidence will be transferred to the custody of the requestor. Such transfer shall be completed and documented in accordance with CCBI evidence policies.

1.10.3 If the Forensic Computer 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.

1.11 County Network and Internet Acceptable Use Policy

Routinely, the examiners in the Forensic Computer Unit are requested by law enforcement agencies and prosecuting attorneys to perform analysis on computers and other digital/multimedia devices to retrieve suspected child pornographic images. At times, it is necessary for the Forensic Computer Unit to access internet sites and download, print, or store information that may be considered to be in violation of the Wake County Network and Internet Acceptable Use Policy (effective date 01/20/01).

Once files on an evidence device are located, it may be necessary for the examiner to download proprietary software from the internet, using the information that is embedded in the data, to observe

and authenticate the images/video clips on the multimedia device. Without the proprietary software, the files cannot be viewed. The necessity to access, download, print, and store information from these sites is a function that is primarily required in the computer and forensic cell phone recovery sub disciplines.

1.12 Forensic Computer Unit Personnel

Forensic Computer Unit personnel that are not in a trainee status will have 25% of their completed case records technically reviewed by a competent technical reviewer prior to the publication of the report. The ~~reviewer~~ examiner may coordinate with the technical reviewer and will define the method of his/her choice for identifying case records to technically review; for example, every fourth case record. The reviewer will complete a Computer Forensics Unit Technical Review Coversheet, which will then be secured in the case record.

Forensic Computer Unit personnel that are in Phase III trainee status will have 100% of their completed case records technically reviewed by a competent technical reviewer.

All Forensic Computer Unit personnel who participate in casework activities will successfully complete at least one (1) internal or external proficiency test per calendar year per discipline.

1.13 Evidence Security

When an individual with evidence in his/her immediate custody leaves the work area during the workday for a short time (e.g. restroom break, meal break), the evidence in the work area must be secured by locking the work area door. When evidence is to be left unattended for an extended period (i.e. longer than a meal break), the evidence must be secured by returning it to the unit secure area for evidence storage. Computer Forensics evidence that is actively being processed on a password protected computer system may be left unattended for an extended period if the computer system is secured by a locked work area door.

1.14 References

CCBI Crime Laboratory Administrative Procedures Manual

CCBI Forensic Science Quality Manual

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, U.S. Department of Justice National Institute of Justice, April 2008, URL: www.ncjrs.gov/pdffiles1/nij/219941.pdf

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

IACIS Code of Ethics, URL: www.iacis.com/new_membership/code_of_ethics

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
May 1, 2013	2	Addition of Tech Review Coversheet (1.12)
7/14/14	3	Require technical review prior to the publication of the report. Update evidence security.
4/13/15	4	Update identification of case records for technical review

Chapter 2: Equipment Maintenance

2.1 Equipment Maintenance

2.1.1 All equipment is to be maintained in accordance with the manufacturer's specifications and recommendations as per operating and warranty manuals.

2.1.2 All maintenance is to be documented and retained in the unit maintenance log.

2.1.3 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. This documentation will be maintained in the unit maintenance log

2.2 Performance Checks and Verifications

2.2.1 The forensic computers should be maintained in proper working order. 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. This process is as follows:

2.2.2.1 A "control" media device ~~floppy disk~~ is inserted in the forensic machine and forensically imaged in the applicable forensic software each day before any examinations are carried out. ~~Since the control disk can be physically write-blocked, it is permissible to image the disk in either Windows or DOS.~~

2.2.2.2 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 ~~disk~~. 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.

2.2.2.3 The known MD5 hash value for the control ~~disk~~ media device and the hash value for the image of the control media device ~~disk~~ 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 Tool and Technique Validation

It is necessary to have tools and techniques that provide reliable results. Methods, procedures, and tools shall be validated before being used on evidence. Validation can be performed by third parties. Validation testing should be performed whenever new, revised, or reconfigured tools, techniques or procedures are introduced into the forensic process.

Testing of new technical procedures shall be accomplished using known data sets so that the outcome shall be known. Procedure validation shall be conducted using the standard workstations and software found in the laboratory. Where possible, the results of testing shall be documented in written form.

Formatted: Font: Italic

2.4 Prevention of Unauthorized Access

All forensic computers within the Forensic Computer Unit are password protected, and these passwords remain confidential within the Forensic Computer Unit. The master images of the operating system drives for all forensic machines shall be securely stored.

2.5 Laboratory Conditions

Other than standard laboratory conditions, no other factors influence quality of tests in the Forensic Computer Unit.

2.6 References

~~EnCase Forensic User Manual~~
FTK Forensic User Manual
FTK AccessData BootCamp

Various computer user manuals

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 2.2.2.2: Replace control "floppy disk" with control "media device". Delete "Since the control disk can be physically write blocked, it is permissible to image the disk in either Windows or DOS." Section 2.2.2.2: Replace control media "disk" with "device". Section 2.2.2.3: Replace control "disk" with control media device. Section 2.6: Removal of "Encase Forensic User Manual" and addition of "FTK Forensic User Manual" and "FTK AccessData Boot Camp"

All copies of this document are uncontrolled when printed

Chapter 3: Minimum Examination Standards

3.1 Purpose

This section describes an overview of the examination process.

3.2 Scope

This is information defining the structure of the examination process.

3.3 Examination Request

3.3.1 All forensic examinations must have a written request for service. Forensic Computer Unit personnel should communicate with the requestor to determine the focus and parameters of the forensic examination. The purpose of the request for services form is to collect information that is necessary for a successful analysis.

3.3.2 A request for forensic services will include:

3.3.2.1 The type of examination requested

Attention should be paid to whether the request requires examinations by other disciplines.

3.3.2.2 The necessary legal authority

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

3.3.2.3 Any known safety hazards (e.g., chemical, blood borne pathogens, etc.).

3.3.2.4 The identity of the party requesting the services and the date of the request.

3.4 Evidence Preservation

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 Forensic Computer Examiner should consult with forensic examiners in the appropriate disciplines.

3.5 Forensic Examination

At a minimum, an examination consists of the following:

3.5.1 Visual Inspection

The Forensic Computer Examiner will determine the type of evidence, its condition, and relevant information to conduct the forensic examination.

3.5.2 Forensic Duplication

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.

3.5.3 Media Examination

Examination of the media should be completed in a logical and systematic manner.

3.5.4 Evidence Return

Item(s) are returned to appropriate location.

3.6 Documentation

While documentation may vary, the following items may be included in the CCBI case record:

3.6.1 Request

The examination request for service form must be included.

3.6.2 Chain of Custody

The chain of custody must include a description of the item and a documented history of each transfer.

3.6.3 Notes

3.6.3.1. Notes stemming from the examination shall include, at a minimum, the procedural steps of the examination, with a minimum of the start and end dates of the analysis. These steps should be written in sufficient detail to allow another Forensic Computer Examiner, competent in the same area of expertise, to be able to identify what has been done and to assess the findings independently.

3.6.3.2 Each page of notes must be marked with the unique CCBI case number and the Forensic Computer Examiner's initials or signature. Two-sided documents must contain the unique case identifier and Examiner's initials or signature on both sides.

3.6.3.3 If multiple Forensic Computer Examiners are working on the same case and producing combined notes, the initials of the Forensic Computer Examiner performing each procedural step shall be included.

3.7 Demonstrative Photographs

If the Forensic Computer Examiner takes digital photographs of evidence items in order to record their state at the time of evidence acceptance, those digital photographs will be uploaded to the CCBI Digital Crime Scene database. Digital photographs taken for the purpose of recording evidence will not be stored in the CCBI Digital Crime Scene database but will instead be tendered to the contributing agency.

3.8 Approved Software

The Forensic Computer Examiner may use any software necessary, in his/her discretion, to complete the forensic examination. This includes freeware, shareware, "trial-ware," and retail software. The Forensic Computer Examiner should document what software, including what version number, was used during the examination in his/her notes.

3.8.1 Purchasing and Receipt of Software.

The Unit Technical Leader will maintain a list of software that affects the quality of testing. Purchasing and receipt will comply with the Laboratory Administrative Procedure for Purchasing and Receipt of Consumables, Services, and Supplies, LAPM 07.

~~3.8~~ 3.9 References

CCBI Crime Laboratory Administrative Procedures Manual

CCBI Forensic Science Quality Manual

Best Practices for Seizing Electronic Evidence v3, United States Secret Service, October 2006, URL: http://www.forwardedge2.usss.gov/pdf/bestPractices.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

All copies of this document are uncontrolled when printed

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
May 1, 2013	2	Added section 3.7 “demonstrative photographs”, prior 3.7 became 3.8
April 13, 2015	3	Updated for compliance with LAPM07 and FSQM04

Chapter 4: Case Prioritization

4.1 Purpose and Scope

This policy discusses how digital evidence cases are received, triaged, prioritized, and assigned for forensic examination.

4.2 Case Prioritization

4.2.1 Once a digital evidence examination request for service is accepted, the Forensic Computer Examiner is responsible for prioritization. Generally, the Forensic Computer Examiner will prioritize examination requests based upon the facts known to him/her at the time of prioritization.

4.2.2 Digital evidence examination requests will be prioritized as follows:

1. Mobile devices (regardless of case type);
2. Homicides for which no arrest has been made;
3. Crimes against children for which no arrest has been made;
4. Homicides for which an arrest has been made;
5. Crimes against children for which an arrest has been made;
6. Suicide/Death investigations;
7. Felony assaults;
8. Felony drug crimes;
9. Felony financial crimes;
10. Other felonies.

4.2.3 Submitted cases will be worked on a first-come, first-served basis based upon the date that the examination request for service was received.

4.3 Exceptions and Modifications to Case Prioritization

4.3.1 Special circumstances (factors stated above or additional considerations) may add a cumulative value to the prioritization of cases. On a case-by-case basis, the Crime Laboratory Division Deputy Director may authorize an examination request be given priority outside of this policy.

4.3.2 If a requestor desires a "rush" examination requests, the appropriate form (Rush Request for Evidence Analysis, CCBI-101.1) must be filled out and forwarded to the appropriate personnel. No "rush" examination will begin until authorized by the appropriate Deputy Director. Any accepted "rush" examination cases may be given the highest examination priority at the discretion of the Crime Laboratory Division Deputy Director.

4.4 Triage

Casework may be triaged to identify primary evidentiary items for examination and eliminate items having no evidentiary interest to an investigation. Triage may involve several methods including, but not limited to: review of item locations within the scene; on-site preview; laboratory preview, etc.

4.5 Active Examination Time Period

The time period for active examination shall not be open-ended. Because active examinations may need to be suspended due to a "rush" examination, activity in the judicial system, or other events, it is understood that cases may remain open for a period of time. However, there is the expectation that once a case has been opened, examination will be completed.

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 5: System Image Restoration

5.1 Purpose

The purpose of this procedure is to restore workstation system drives used in forensic casework to a default state in order to ensure that no data overlap occurs between cases.

5.2 Scope

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

5.3 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

5.4 Definitions

- System drive – The hard drive that contains the operating system.
  System temporary file drive- The hard drive that contains the forensics software temporary files.
- System image – Factory default or user-created image of the drive that is used to restore the hard drive(s) on the forensic workstation.

~~**5.5 Limitations**~~

~~Failure to wipe the information from a previously used hard drive can lead to potential data overlap.~~

5.5~~6~~ Procedures

Each case should be examined inside of a separate baseline virtual machine image or after laying down a clean image of the forensic machine operating system drive and wiping the system temporary file drive. Examinations from different cases will not be comingled within one virtual machine or conducted using the same forensic machine operating system drive.

5.5~~6~~.1 If a previously created system image is available, skip to step 8.6.5.

5.5~~6~~.2 If no previously created system image is available, use the original system restoration disc(s) to perform a fresh installation of the operating system.

5.5~~6~~.3 Install necessary software and configure the new system.

5.6.4 Use a backup utility to create an image of the system.

5.6.5 Restore the system drive using the prepared system image.

5.7 References

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
January 2, 2014	2	Section 5.4: Addition of "System temporary file drive- The hard drive that contains the forensics software temporary files." Section 5.5: Deletion of "5.5 Limitations Failure to wipe the information from a previously used hard drive can lead to potential data overlap." Renumbering of remaining 5.6 to 5.5. Section 5.5: Addition of "and wiping the system temporary file drive" to the first sentence.

Chapter 6: Physical Inspection

6.1 Purpose

The purpose of this procedure is to properly catalogue and document the condition of digital evidence.

6.2 Scope

This procedure applies to all submitted digital evidence.

6.3. Equipment

- Tool kit (screw driver, etc.)
- Camera
- Permanent markers

6.4 Limitations

Some manufacturers of computers have mechanisms that alert the user the computer case has been opened.

6.5 Procedures

6.5.1 Where possible, bags sealed with evidence tape shall be opened so that the evidence tape and/or initials are not disturbed. Computer cases that are sealed with evidence tape should be opened in a manner that will only minimally disturb the previously applied seal. Any evidence tape sealing the case should be cut, not removed, to enable opening the case.

6.5.2 Assess the potential for a destructive device, biological contaminant, or hazardous material and take appropriate action.

6.5.3 Photograph evidence items if necessary.

6.5.4 Record the evidence item's individual characteristics such as media type, brand, size, and external markings.

6.5.5 If foreign substances such as dirt or dust may interfere with examination, the evidence item will require cleaning.

6.5.6 Label submitted evidence items in accordance with the CCBI Forensic Science Quality Manual and CCBI Crime Laboratory Administrative Procedures. The location of the labeling is to be determined by the examiner but should not interfere with additional examinations or damage the evidence.

6.5.7 If applicable, remove the cover from the case in order to locate and identify internal components; document serial/model numbers if necessary; and check power leads and cabling and document abnormalities.

6.5.8 Upon completion of the hardware examination, replace the cover and secure the case, if applicable.

6.6. References

CCBI Crime Laboratory Division Administrative Procedures

CCBI Forensic Science Quality Manual

User manuals for specific software and hardware

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 7: Write Protecting Media

7.1 Purpose

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

7.2 Scope

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

7.3 Equipment

7.3.1 Hardware

- Write protection firmware and/or hardware
- Internal or external hard drive
- Removable media (e.g., flash media, floppy disk, tapes)

7.3.2 Software

Write protection software utilities such as:

- Hard Disk Write Lock (HDL RCMP Tool)
- Forensic Boot CD
- Write Blocker XP/2K (ACESLE Tools)
- Unix/Linux command mount –r (Read only: all Unix/Linux recognized file systems)

7.4 Limitations

7.4.1 General

7.4.1.1 Write protection software may not protect against programs using direct access writes to media.

7.4.1.2 Write protection software in a network or RAID environment may not be applicable.

7.4.2 Specific

7.4.2.1 ~~Write Blocker XP~~: ~~Not recommended for use with USB floppy drives or USB CD/DVD writers.~~

~~7.4.2.2 Unix/Linux Command mount –r:~~ ~~Only effective for the file system(s) mounted as read only. This command will not provide protection at the device level. This command may not mount all file systems. This command may not provide full protection when mounting a journaled file system.~~

7.4.2.13 ~~3~~ IDE Jazz and Zip drives: None of the write protection hardware above has been verified to effectively write protect this type of media.

7.5 Procedures

7.5.1 Original evidence must be write-protected when possible. Built-in write protection mechanisms must be utilized whenever available to complement hardware and software write protection (ex. the "lock" switch on floppy disks and some flash drive adapters). If write protection is not possible, this must be documented.

7.5.2 It shall be the policy of the Forensic Computer Unit to make every effort possible to avoid working on original evidence. It is understood, however, that in rare circumstances original evidence may have to be examined due to hardware configurations or certain operating systems. If this must be done, the Forensic Computer Examiner will document actions taken during the examination to clarify any date/time changes.

7.5.3 Hard Disk Drives and Solid State Storage Devices

For hard disk drives and solid state storage devices (e.g. USB thumb drives, memory cards, or flash cards) the following two methods can be used together or separately:

7.5.3.1 Follow the manufacturer's instructions when using a hardware or firmware write-protect device.

7.5.3.2 Use the appropriate operating system or boot media when using software write protection. If write protection software was not started during the boot process, initiate write protection software prior to attaching the media.

7.5.4 For Iomega Zip and Jaz disks

Iomega Zip and Jaz disks utilize a proprietary software utility that changes a storage location on the media to indicate a write protected or "read only" state. Use the appropriate operating system version of Iomega Tools to make the disk read only. Whenever possible, use software write protection.

~~**7.5.5 CDs and DVDs**~~

~~CD-RW and DVD-RW discs should be read in CD-ROM and DVD-ROM drives. This will prevent changes from being made to the evidence.~~

7.6 References

User manuals for listed software and hardware.

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 7.4.2: Deletion of "7.4.2.1 Write Blocker XP: Not recommended for use with USB floppy drives or USB CD/DVD writers." and "7.4.2.2 Unix/Linux Command mount –r: Only effective for the file system(s) mounted as read only. This command will not provide protection at the device level. This command may not mount all file systems. This command may not provide full protection when mounting a journaled file system." Renumbering of remaining section 7.4.2.3 as section 7.4.2.1. Deletion of "7.5.5 CDs and DVDs. CD-RW and DVD-RW discs should be read in CD-ROM and DVD-ROM drives. This will prevent changes from being made to the evidence."

All copies of this document are uncontrolled when printed

Chapter 8: Wiping Media and Target Drive Preparation

8.1 Purpose

The purpose of this procedure is to overwrite all data on media, commonly known as "wiping." Wiping can be used to sanitize target media prior to the examination process and ensures that no data overlap occurs between cases.

8.2 Scope

This procedure applies to media authorized to be wiped.

8.3 Equipment

- Forensic workstation or other hardware wiping device
- Wiping software or wiping device
- Hard drive

8.4 Limitations

The target drive is a hard drive that receives data from the subject drive and is used for processing casework. The target drive is not evidence.

8.5 Procedure

8.5.1 Select a target hard drive that has sufficient storage capacity to hold the forensic image files and recovered files generated from the evidence hard drive.

8.5.2 ~~Label the target drive with case information including the CCBI case number, the CCBI item number, the date, and the examiner's initials.~~

8.5.2~~3~~ Connect the target hard drive to the forensic computer or hardware wiping device.

8.5.3~~4~~ Use wiping software or wiping device to overwrite all sectors of the hard drive.

8.5.4~~5~~ Partition and format the target drive and give it a volume name to ensure it will not be confused with other hard drives (e.g. Target, Forensic Image, etc.).

8.6 References

User manuals for wiping software and hardware.

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL:

www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Deletion of "8.5.2 Label the target drive with case information including the CCBI case number, the CCBI item number, the date, and the examiner's initials." Renumbered remaining sections 8.5.3, 8.5.4, and 8.5.5 as sections 8.5.2, 8.5.3, and 8.5.4.

Chapter 9: Hard Drive Removal and BIOS Check

9.1. Purpose

The purpose of this procedure is to remove the hard drives from computers submitted for examination while maintaining the integrity of the evidence.

9.2 Scope

This procedure describes the steps to be taken in removing hard drives from computers that are evidence in forensic computer examinations.

9.3 Equipment

- Tool kit (screw driver, etc.)
- Permanent markers

9.4 Limitations

9.4.1 Removing hard drives from some devices may not be an option.

9.4.2 On some older or proprietary BIOS/CMOS chips, a setup floppy disk provided by the manufacturer is needed to access the BIOS.

9.4.3 On some systems, accessing BIOS with the drives disconnected may change the boot sequence.

9.4.4 Access to BIOS/CMOS can be protected by a password. Some manufacturers can provide a master password.

9.4.5 Precautions should be used to guard against electrostatic discharges that could damage or destroy the evidence hard drive.

9.5 Procedure

9.5.1 Record the system information from the evidence computer.

9.5.2 If necessary to document connections, m~~M~~ark the power cords and data ribbons/connectors connecting the hard drive to the evidence computer to facilitate proper reassembly.

9.5.3 Remove the hard drive(s) from the evidence computer.

9.5.4 Label the hard drive(s) removed from the evidence computer with case information as provided in the CCBI Forensic Science Quality Manual and CCBI Crime Laboratory Division Administrative Procedures.

9.5.5 Document the drive information such as make, model, serial number, capacity, jumper settings, etc.

9.5.6 With all hard drives removed, boot the evidence computer into the BIOS and document relevant BIOS settings and the actual date and time.

9.6 References

CCBI Crime Laboratory Division Administrative Procedures

CCBI Forensic Science Quality Manual

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 9.5.2: Addition of "If necessary to document connections" to the first sentence.

Chapter 10: Hard Drive Imaging Protocol Using Windows

10.1 Purpose

The purpose of this procedure is to use a Microsoft Windows operating system to create a forensically sound image of evidence hard drives.

10.2 Scope

This is the procedure to be utilized in imaging hard drives submitted as evidence, using the Microsoft Windows operating system.

10.3. Equipment

- Forensic computer
- Prepared target drive
- Forensic imaging hardware or software

10.4 Limitation

There may be instances when an evidence hard drive cannot be forensically imaged despite exhausting all approved methods of imaging. In these instances, attempts to properly image the hard drive must be completely documented.

Due to a failing hard drive, disk bad sectors or SSD Drive a stable hash value may not be obtainable. Even when connected to a write block a Solid State Disk may change hash values when under power.

10.5 Procedures

10.5.1 Attach the evidence hard drive to the forensic computer using a hardware or firmware write-blocking device.

10.5.2 Attach or insert the target drive into the forensic workstation and boot the forensic computer into the Windows operating system.

10.5.3 Obtain a hash value of the evidence hard drive before imaging.

10.5.4 Obtain a forensic image of the evidence drive using imaging software and save the forensic image to the target drive.

~~**10.5.5** If using EnCase to obtain the forensic image:~~

~~**10.5.5.1** Image the evidence drive by choosing the "Acquire" button on the tool bar.~~

~~**10.5.5.2** On the Options screen, enter the case information that the program requests. This information will be used by the program in preparing the EnCase report.~~

~~**10.5.5.3** Check the box for "Generate image hash." EnCase uses this hash value to verify that the target drive contains a forensic image of the evidence hard drive.~~

~~**10.5.5.4** If the forensic image may be saved on CD, choose 640MB as the maximum desired evidence file size. Larger file sizes may be used if the forensic image files will be saved on DVDs or other storage media.~~

10.5.5~~6~~ 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.).

10.5.5~~6~~.1 In instances where the virus scan takes an excessive amount of time to complete, it is permissible to copy all of the logical files from the evidence drive to the target drive and run the virus scan on the copied files.

10.5.6~~7~~ Verify and document the integrity of the image file(s).

10.5.7~~8~~ Remove the evidence hard drive from the forensic workstation.

10.5.8~~9~~ ~~EnCase~~ Access Data Forensic Toolkit is the primary forensic tool used by CCBI. Situations may occur when other tools must be used. Based on training and experience, another imaging tool may be used.

10.6 References

~~EnCase Computer Forensics II Course Manual~~

~~EnCase Forensic User Manual~~
AccessData Forensic User Manual

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL:
www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Formatted: Font color: Red

All copies of this document are uncontrolled when printed

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
January 2, 2014	2	Section 10.4: Addition of "Due to a failing hard drive, disk bad sectors or SSD Drive a stable hash value may not be obtainable. Even when connected to a write block a Solid State Disk may change hash values when under power." Deletion of "**10.5.5** If using EnCase to obtain the forensic image: **10.5.5.1** Image the evidence drive by choosing the "Acquire" button on the tool bar. **10.5.5.2** On the Options screen, enter the case information that the program requests. This information will be used by the program in preparing the EnCase report. **10.5.5.3** Check the box for "Generate image hash." EnCase uses this hash value to verify that the target drive contains a forensic image of the evidence hard drive. **10.5.5.4** If the forensic image may be saved on CD, choose 640MB as the maximum desired evidence file size. Larger file sizes may be used if the forensic image files will be saved on DVDs or other storage media." Renumbered remaining 10.5.6, 10.5.6.1, 10.5.7, 10.5.8, and 10.5.9 to 10.5.5, 10.5.5.1, 10.5.6, 10.5.7, and 10.5.8. Section 10.5.8: Deletion of "EnCase" and addition of "AccessData Forensic Tool Kit" in the first sentence. Section 10.6: Deletion of "EnCase Computer Forensics II Course Manual" and "EnCase Forensic User Manual" and addition of "AccessData Forensic User Manual"

Formatted: Indent: Left: 0"

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: (Default) +Body (Calibri), Font color: Black

All copies of this document are uncontrolled when printed

All copies of this document are uncontrolled when printed

Chapter 11: Hard Drive Imaging Protocol Using Linux

11.1 Purpose

The purpose of this procedure is to use a Linux operating system to create a forensic image of evidence items without altering the data.

11.2 Scope

This procedure describes the steps to image digital evidence using Linux.

11.3 Equipment

- Forensic computer
- Prepared target drive
- Bootable Linux operating system
- Software for forensic imaging

11.4 Definitions

Forensically sound Linux operating system: A bootable Linux operating system that runs entirely in the computer's memory and has been specially modified to mount all devices connected to the system in a read-only state.

11.5 Limitations

The examiner must be aware of the Linux mounting process. Linux operating systems must be tested to ensure all devices are mounted in a read-only state before use.

11.6 Procedures

Obtaining a forensic image using a forensically sound Linux operating system can be done in two ways: with the Linux disc in the evidence computer itself and a target drive attached, or with the evidence drive attached to the forensic computer using Linux.

11.6.1 Using a Linux Boot Disc in an Evidence Computer

11.6.1.1 Boot the evidence computer into its BIOS setup program.

11.6.1.2 Set the boot order to allow the Linux media to load first.

11.6.1.3 Insert the forensically sound Linux operating system (CD/USB device, etc.) and boot the evidence computer.

11.6.2 Using a Linux Workstation

11.6.2.1 Boot the forensic computer into the Linux operating system.

11.6.2.2 Attach the evidence drive to the forensic workstation.

11.6.3 Image with Linux

11.6.3.1 Obtain a hash value of the evidence drive before imaging.

11.6.3.2 Attach a target drive and allow read and write permissions.

11.6.3.3 Image the evidence to the target drive using imaging software.

11.6.3.4 Remove the evidence drive.

11.6.3.5 Verify and document the integrity of the image file(s) by comparing the acquisition and verification hash values.

11.6 References

Linux Desk Reference, Second Edition, Scott Hawkins, August 2001, (no URL)

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL:
www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 12: Cable Acquisition Protocol

12.1 Purpose

The purpose of this procedure is to image evidence drives installed in the evidence computers in a situation where the hard drive is difficult or impossible to remove. This procedure provides for imaging these computers without making changes to the data on the evidence drive.

12.2. Scope

This procedure describes the steps to be taken in imaging computers using a null-modem parallel (laplink) cable or network crossover cable.

12.3 Equipment

- Forensic computer
- Network crossover cable or parallel (laplink) cable
- Prepared target drive
- Forensic imaging software

12.4 Limitations

12.4.1 Media that has sustained physical or mechanical damage and/or electronic failure may not successfully or completely image.

12.4.2 In order to use a network crossover cable, the evidence computer must be equipped with a network interface card, and the forensic boot disk must contain the DOS drivers for that network interface card.

12.4.3 Some laptop hard drive/motherboard combinations may have security devices which do not allow them to be accessed outside of the laptop computer. Image these computers using a cable acquisition procedure or by booting the laptop using a forensic operating system environment.

12.5 Procedures

12.5.1 This procedure requires the use of a forensic tool that can function in a DOS or Linux environment. Examples include, but are not limited to, EnCase, LinEn, Raptor, and SPADA.

12.5.2 Remove the power and data cables from the evidence hard drive or remove the evidence hard drive from the evidence computer entirely. Check the evidence computer's BIOS/CMOS settings to be sure that the evidence computer will boot from attached removable media devices, changing if necessary.

12.5.3 Disable any power-saving features in the evidence computer BIOS, as available.

12.5.4 Once the BIOS/CMOS settings have been checked and changed, as necessary, turn off the evidence computer and reconnect the evidence hard drive to the evidence computer.

12.5.5 Attach or install a prepared target drive in the forensic computer.

12.5.6 Set up the evidence computer in server mode by booting into DOS or Linux using a forensic tool that allows this (for example, EnCase boot floppy). Server mode enables the evidence computer to send data to a forensic computer in a forensically safe manner for imaging. Always set up the evidence computer in server mode first before setting up the forensic computer.

12.5.7 Connect the evidence computer and forensic computer using a network crossover cable between the network interface cards, or connect the laplink cable from the parallel port of the evidence computer to the parallel port of the forensic computer (running through the dongle if a parallel port dongle is required).

12.5.8 Once the evidence computer has booted, run the forensic utility on the evidence computer according to the tool's instructions.

12.5.8.1 If using EnCase in DOS, the evidence computer will display hard drive information on the screen, and the evidence drive will display as locked.

12.5.8.2 If using EnCase in DOS, choose "server mode" from the choices at the bottom of the screen.

12.5.8.3 If using EnCase in DOS, a window will be displayed showing "Server Mode" and the message "waiting to connect."

12.5.9 Set up the forensic computer in client mode by booting the forensic computer into DOS/Linux. Client mode is the DOS/Linux mode enables the forensic computer to receive data from an evidence computer in a forensically safe manner.

12.5.9.1 If using EnCase in DOS, the forensic computer will display "client mode" in the title bar.

12.5.10 Prior to imaging the evidence hard drive, use a hashing program to obtain the MD5 hash value of the evidence drive.

12.5.11 When imaging is complete, follow the prompts to terminate the server/client mode and power down the evidence computer.

12.6 References

EnCase Forensic User Manual

Chapter 13: DOS Hard Drive Imaging

13.1 Purpose

The purpose of this procedure is to use the Microsoft DOS operating system to create a forensic image of evidence hard drives without altering the data on the hard drive.

13.2 Scope

This procedure describes the steps to be taken in using the Microsoft DOS operating system to image hard drives that are evidence in forensic computer examinations.

13.3 Equipment

- Forensic computer
- Prepared target drive
- Forensic boot disk
- Forensic imaging software

13.4 Limitations

13.4.1 The DOS imaging procedure may be used to image a hard drive when hardware or firmware to write protect the hard drive is not used.

13.4.2 Locking the evidence drive ensures that the target drive cannot be accidentally copied onto the subject hard drive.

13.5 Procedures

13.5.1 Insert the evidence drive and the target drive into the forensic computer.

13.5.2 Boot the forensic computer into DOS using a forensic boot disk.

13.5.3 Using a hashing program to obtain an MD5 hash value of the evidence drive before imaging.

13.5.4 Image the evidence drive using a forensic imaging tool and following the imaging procedures in the product manual. If imaging in EnCase:

13.5.4.1 Ensure that the evidence drive is locked and unlock the target drive.

13.5.4.2 EnCase presents an option to compress the file. Compression may be used in order to require fewer CDs or DVDs to store the forensic image at the completion of the analysis.

~~**13.5.4.3** When presented a MD5 hash option, choose "YES." EnCase uses this hash to verify that the target drive is an exact forensic image of the evidence hard drive.~~

~~**13.5.4.4** EnCase offers the ability to password protect the forensic image. Do not password-protect the forensic image.~~

~~**13.5.4.5** The maximum desired evidence file size should be set to 640MM if the forensic image is to be saved to CDs. Larger file sizes may be used if the image files will be written to DVDs or other storage media.~~

~~**13.5.4.6** After verifying that the forensic image has been successfully completed, remove the evidence hard drive from the forensic computer.~~

~~**13.6 References**~~

~~EnCase Forensic User Manual~~

~~User manuals for forensic software~~

Chapter ~~14~~14: Imaging a Macintosh Computer

~~14~~14.1. Purpose

The purpose of this procedure is to properly create a forensic image of a device running the Apple Macintosh operating system without altering the data. This procedure covers imaging of Macs when the hard drive can be removed as well as in situations when the hard drive cannot be removed.

~~14~~14.2. Scope

This procedure applies to Macintosh computers.

~~14~~14.3. Equipment

- Forensic computer
- Prepared target drive
- Forensically sound, bootable CD for Power PC-based Macintosh hardware
- Forensically sound, bootable CD for Intel-based Macintosh hardware

~~14~~14.4 Definitions

~~14~~14.4.1 **FireWire Target Disk Mode** – FireWire Target Disk Mode allows a Mac system to act as if the entire computer were an external FireWire 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 Mac system during the boot process.

~~14~~14.4.2 Forensically sound, bootable CD for Power PC Macintosh hardware – A forensically sound, bootable CD for Power PC Macintosh hardware is a Linux operating system variant on a CD that has been specially constructed for forensic examination of live Macintosh systems that have the Power PC processor chips. The CD is forensically sound due to the fact that all media on the system is placed in read-only mode.

~~14~~14.4.3 Forensically sound, bootable CD for Intel-based Macintosh hardware – A forensically sound, bootable CD for Intel-based Macintosh hardware is a Linux operating system variant on a CD that has been specially constructed for forensic examination of live Macintosh systems that have the Intel processor chips. The CD is forensically sound due to the fact that all media on the system is placed in read-only mode.

~~14~~14.4.4 fstab – fstab is a configuration file that contains information for all of the partitions and storage devices in a Linux-based computer. fstab contains information concerning how and where the partitions and storage devices in a Linux-based system should be mounted.

~~14~~14.4.5 HFS – Hierarchical File System (HFS) is a file system developed by Apple for use in computers running Mac OS. HFS is also referred to as Mac OS Standard.

~~14~~14.4.6 HFS+ – HFS Plus or HFS+ is a file system developed by Apple to replace their Hierarchical File System (HFS) as the primary file system used in Macintosh computers (or other systems running Mac OS). HFS Plus is an improved version of HFS, supporting much larger files (block addresses are 32-bit length instead of 16-bit) and using Unicode for naming the file items. HFS Plus also uses a full 32-bit allocation mapping table, rather than HFS's 16 bits. HFS Plus is also referred to as Mac OS Extended.

~~14~~14.5 Limitations

~~14~~14.5.1 Macintosh Computers

~~14~~14.5.1.1 Plug in a power cable to any MacBook or other Macintosh laptop to be imaged. Do not allow a laptop to run on battery power during an acquisition if the appropriate AC power cord is available.

~~14~~14.5.1.1 If an Intel-based Macintosh in dual boot firewire mode is attached to a Windows system, the Windows partition, if present, will be mounted.

~~14~~14.5.1.2 If an open firmware password is enabled, it will not be able to be accessed while the HDD is connected to that computer.

~~14~~14.5.1.3 An Intel-based Macintosh does not have open firmware; the only way to determine if there is a boot password is to boot with the "option" key depressed.

~~14~~14.5.1.4 If using another Mac as the examination platform, the examiner must turn off Disk Arbitration; otherwise there may be inadvertent writes to the evidence Mac system.

~~14~~14.5.2 Linux Boot CD

A Linux Boot CD will only work with an Intel-based Macintosh.

~~14~~14.5.3 Windows Computers

Do not use a Microsoft Windows operating system to image a live Macintosh system. Microsoft operating systems "touch" drives during the boot sequence and hence modify the data of the evidence computer.

~~14~~14.6 Procedures

Macintosh computers that have an open firmware password enabled will prevent booting with external media and target disk mode from working properly. The examiner must then remove the hard drive for imaging or be able to obtain or defeat the open-firmware password on the evidence computer.

~~14~~14.6.1 Booting using external media

If using external media with OS X, disable auto-mounting or disk arbitration.

~~14~~14.6.1.1 Verify that computer is powered off.

~~14~~14.6.1.2 Insert a boot disc in the evidence computer. Attach the target drive to the evidence computer to store the forensic image.

~~14~~14.6.1.3 While holding down the appropriate key(s), boot the evidence computer.

~~14~~12.6.1.4 Observe the bootable external media device and display screen carefully to make sure that the system is accessing the boot media. If there are no indications that the computer is accessing the boot media, turn off power to the evidence computer immediately.

~~14~~14.6.1.5 When the forensically sound Linux environment has fully loaded, open up a terminal session.

~~14~~14.6.1.6 Navigate to the /etc directory.

~~14~~14.6.1.7 Edit the fstab file using "vi" or another text editor. Navigate to the entry in the fstab file that corresponds to the HFS partition on the evidence computer's hard drive and change the partition type from "hfs" to "hfsplus."

~~14~~14.6.1.9 Save the changes to the fstab file and close the terminal session. The changes to the fstab file allow the forensically sound Linux environment to properly read the file system on newer Macintosh systems while remaining in a read-only state. Because this file remains in the active memory of the computer it remains forensically sound and does not "touch" the suspect computer.

~~14~~14.6.1.9 If using the GUI, click once on the Mac hard drive icon to mount the drive. Repeat this process for the target drive to mount the target drive. If using the command line, mount both the subject drive and the target drive.

~~14~~14.6.1.10 Use a hashing program to obtain the MD5 hash value of the subject drive before imaging.

~~14~~14.6.1.11 Image the subject drive to the target drive.

~~14~~14.6.1.11.1 If the examiner desires to analyze the data from the evidence computer in the native (Mac) format, then the image file must be saved in raw/DD format as a single file.

~~14~~14.6.1.12 Verify the forensic image was successfully completed.

~~14~~14.6.1.13 Shut down the evidence computer and disconnect the Firewire cable.

~~14~~14.6.2 Target Disk Mode

~~14~~14.6.2.1 Boot the evidence computer while holding down the "Option" key until the selection dialog is presented. If the evidence computer presents a lock icon and a password dialog box (Figure 1), there is a firmware password in place, and the subject drive cannot be imaged without the password. If icons for bootable partitions are visible, then there is no firmware password, and the subject drive may be imaged.

Figure 1

~~14~~14.6.2.2 If no firmware password is installed, reboot the evidence computer while holding down the "T" key until a FireWire logo is displayed (Figure 2). Selecting this boot option will place the evidence computer into Target Disk mode.

Figure 2

~~141~~4.6.2.3 Attach the evidence computer to the forensic computer via a Firewire connection.

~~141~~4.6.2.4 Boot the forensic computer into a forensically sound operating system environment.

~~141~~4.6.2.4.1 If the forensic computer is running a Windows operating system, the forensic computer must be booted with a forensically sound Linux boot CD.

~~141~~4.6.2.4.2 If the forensic compute is running a Mac operating system, the evidence computer must be mounted in read-only mode. Disk Arbitration must be turned off in the forensic computer.

~~141~~4.6.2.5 Use a hashing program to obtain the MD5 hash value of the subject drive before imaging.

~~141~~4.6.2.6 Make a forensic image of the evidence computer onto the target drive. A single disk image file (raw or DD format) must be used to view Mac data natively.

~~141~~4.6.2.7 Verify the forensic image was successfully completed.

~~141~~4.6.2.8 Shut down the evidence and forensic computers and disconnect the Firewire cable.

~~141~~4.6.3 Removing HDD from the evidence computer

~~141~~4.6.3.1 Remove the subject hard drive from the evidence computer and obtain a forensic image.

~~141~~4.6.3.2 If the examiner desires to analyze the data from the evidence computer in the native (Mac) format, then the image file must be saved in raw/DD format as a single file.

~~141~~4.7 References

Acquisition, The Apple Examiner, URL: www.appleexaminer.com/MacsAndOS/Img_Pwds/Acquisition/acquisition.html

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

Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit, Ryan Kubasiak, December 2008, (no URL)

Macintosh Imaging Tools and Techniques or How to Image Macs Without Macs, Nicole Donnelly, October 2007, URL: www.techsec.com/pdf/Monday/Techno%20Forensics%2020071029%20NDonnelly%20Macintosh%20Imaging.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 1515: Previewing a Macintosh Computer

1515.1 Purpose

The purpose of this procedure is to use the HELIX Linux operating system to preview evidence hard drives without altering the data on the hard drive.

1515.2 Scope

This procedure describes the steps to be taken to use the HELIX Linux operating system to preview evidence computers running the Apple Macintosh operating system.

1515.3 Equipment

- Forensic computer
- FireWire (IEEE 1394) cable
- HELIX CD
- Prepared target drive (as needed)

1515.4 Definitions

1515.4.1 FireWire Target Mode – FireWire Target Mode allows an Apple Macintosh system to act as if the entire computer were an external FireWire 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.

1515.4.2 HELIX – HELIX is a Linux operating system variant that was specially constructed for forensic examination of live systems due to the fact that all media on the system is placed in read-only mode.

1515.4.3 fstab – fstab is a configuration file that contains information for all of the partitions and storage devices in a Linux-based computer including how and where the partitions and storage devices should be mounted.

1515.4.4 HFS - Hierarchical File System (HFS) is a file system developed by Apple for use in computers running the Apple Macintosh OS. HFS is also referred to as Apple Macintosh OS Standard. HFS+ - HFS Plus or HFS+ is a file system developed by Apple to replace their Hierarchical File System (HFS) as the primary file system used in Apple Macintosh computers (or other systems running Apple Macintosh OS). HFS Plus is an improved version of HFS, supporting much larger files (block addresses are 32-bit length instead of 16-bit) and using Unicode for naming the file items. HFS Plus also uses a full 32-bit allocation mapping table, rather than HFS's 16 bits. HFS Plus is also referred to as Apple Macintosh OS Extended.

1515.5 Limitations

1515.5.1 Macintosh Computers

~~15~~15.5.1.1 Plug in a power cable to any MacBook or other Macintosh laptop to be previewed. Do not allow a laptop to run on battery power during a preview or acquisition if the appropriate AC power cord is available.

~~15~~15.5.1.2 If using another Mac as the examination platform, the examiner must turn off Disk Arbitration; otherwise there may be inadvertent writes to the evidence Mac system.

~~15~~15.5.2 Windows Computers

Do not use a Microsoft Windows operating system to preview a live Macintosh system. Microsoft operating systems "touch" drives during the boot sequence and hence modify the data of the evidence computer.

~~15~~15.6 Procedure

~~15~~15.6.1 With both systems powered off, connect the forensic computer to the evidence computer using a FireWire cable.

~~15~~15.6.2 Boot the evidence computer and place in FireWire Target Mode by pressing the "T" key until a screen with a FireWire logo appears.

~~15~~15.6.2.1 Boot the evidence computer into FireWire Target mode as this mode engages at the firmware level before the operating system is booted.

~~15~~15.6.3 Boot the forensic computer into the HELIX environment.

~~15~~15.6.4 When the HELIX environment has fully loaded, open a terminal session.

~~15~~15.6.5 Navigate to the /etc directory.

~~15~~15.6.6 Edit the fstab file. Navigate to the entry in the fstab file that corresponds to the HFS partition on the subject drive and change the partition type from "hfs" to "hfsplus."

~~15~~15.6.7 If there is a need to copy data off the suspect drive during the preview, the target drive must be mounted as read/write in the fstab file by changing the "ro" characteristic (Read-Only) to "rw" (Read-Write).

~~15~~15.6.7.1 The changes to the fstab file allow the HELIX environment to read the file system on newer Apple Macintosh systems while remaining in a read-only state.

~~15~~15.6.8 Close the terminal session.

~~15~~15.6.9 On the HELIX desktop, click once on the subject drive icon to mount the drive. Repeat this process for the target drive (if used) to mount the target drive.

~~15~~15.6.10 Preview the evidence computer system using the tools of choice.

~~15~~15.6.11 At the completion of the preview, power down the evidence computer and disconnect the FireWire cable between the two systems.

~~15~~15.7 References

Acquisition, The Apple Examiner, URL: www.appleexaminer.com/MacsAndOS/Img_Pwds/Acquisition/acquisition.html

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

Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit, Ryan Kubasiak, December 2008, (no URL)

Macintosh Imaging Tools and Techniques or How to Image Macs Without Macs, Nicole Donnelly, October 2007, URL: www.techsec.com/pdf/Monday/Techno%20Forensics%2020071029%20NDonnelly%20Macintosh%20Imaging.pdf

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

All copies of this document are uncontrolled when printed

Chapter 1~~6~~16: Examining Handheld/Mobile Devices

~~16~~16.1 Purpose

This procedure may be used for examinations of handheld/mobile devices to extract and/or recover data that may have value as evidence in criminal investigations. The purpose of these procedures is to establish a basic methodology for personnel conducting examinations of Handheld/Mobile Devices.

~~16~~16.2 Scope

This document applies to the forensic examination/data extraction of handheld/mobile devices, which may include mobile phones, personal digital assistants (PDAs), and Global Positioning System (GPS) devices.

~~16~~16.3 Equipment

- Forensic computer
- Forensic analysis software
- RF shielding
- Hardware extraction devices
- Hardware/software write-blockers
- SIM card reader
- Appropriate charging cables and universal battery charging kit
- Data cables or cradles
- Manufacturer & 3rd party software
- Blank and/or sterile media (HD/CD/DVD or other removable devices)
- Camera and/or camcorder

~~16~~16.4 Limitations

~~16~~16.4.1 Mobile phones present a unique challenge to examiners due to rapid changes in technology. There are numerous models of mobile phones in use today. New families of mobile phones are typically manufactured every three (3) to six (6) months. Many of these phones use closed operating systems and proprietary interfaces making it difficult for the forensic extraction of digital evidence.

~~16~~16.4.2 Cables – Data Cables are often unique to a particular device. Frequently cables are specific to the forensic tool to be used. Data cables often have a wide variety of connection, which results in a large number of cables being required for forensics analysis of mobile phones.

~~16~~16.4.3 COM Ports – Some tools may require the use of specific ports. Operating systems may not release control of ports after use.

All copies of this document are uncontrolled when printed

~~16~~**16.4.4 Condition of the Evidence** – Commercially available tools may not provide solutions to deal with physically damaged mobile phones.

~~16~~**16.4.4 Destruction of Data** – There are methods to destroy data locally and remotely on a mobile phone.

~~16~~**16.4.5 Drivers** – Conflicts may occur due to: existing operating system drivers; proprietary drivers; driver version inconsistencies; and vendor specific drivers. Ability to find proper drivers may be difficult. Drivers may be included with the tool or downloaded from a web site. Drivers may compete for control for the same resource if more than one forensic product is loaded on the analysis machine.

~~16~~**16.4.6 Dynamic Nature of the Data** – Data on active (powered-on) mobile phones is constantly changing. There are no conventional write-blocking methods for mobile phones.

~~16~~**16.4.7 Encryption** – Data may be stored in an encrypted state preventing analysis.

~~16~~**16.4.8 Field analysis** – First responders should be aware of the risks associated with triaging mobile phones. Triaging mobile phones is not considered a full examination. The device should be protected for further examination.

~~16~~**16.4.9 Hash Values** – Individual data objects (e.g., graphics, audio, video files) will often maintain consistency between the forensic workstation and the hash value reported by the mobile phone application. Due to the volatility of mobile phone operating systems, overall case file hashes of system files will typically not be consistent due to file system optimization.

~~16~~**16.4.10 Incoming and Outgoing Signals** – Attempts should be made to block incoming and outgoing signals of a mobile phone. Common methods include Radio Frequency (RF) blocking container or jamming appliances. Blocking RF signals will drain the battery, may be expensive, are not always successful and may result in the alteration of mobile phone data.

~~16~~**16.4.11 Industry Standards** – Manufacturers and carriers lack standardized methods of storing data (e.g., closed operating systems, proprietary data connections).

~~16~~**16.4.12 Loss of Power** – Many mobile phones may lose data or initiate additional security measures once discharged or shut down.

~~16~~**16.4.13 Memory Cards** – Processing these cards inside the device pose risks (e.g., not obtaining all data including the deleted data, altering date/time stamps, etc.).

~~16~~**16.4.14 Passwords** – Authentication mechanisms can restrict access to a device and/or data. Traditional password cracking methods can lead to permanent inaccessibility or destruction of data. There are different methods to protect a device (e.g., Personal Identification Number (PIN), Phone Unlock Key (PUK), and handset protection).

~~16~~**16.4.15 Subscriber Identity Module (SIM) Cards** – Lack of or removal of a SIM may prevent the examiner from accessing data stored on the internal memory of a handset. Inserting a SIM from another phone may cause the loss of mobile phone data.

~~16~~**16.4.16 Unallocated Data / Deleted Data** – Many mobile phone forensic tools may only provide the logical acquisition of data. Deleted data may only be recoverable from a physical acquisition.

~~16~~16.5 Data Acquisition

~~16~~16.5.1 Levels of Analysis

The level of analysis is dependent on the request and the specifics of the investigation. Higher levels of analysis require a more comprehensive examination, additional skills, and may not be applicable or possible for every device or situation. The levels are as follows:

~~16~~**16.5.1.1** Manual – A process that involves the manual operation of the keypad and handset display to document data present in the mobile phone's internal memory.

~~16~~**16.5.1.2** Logical – A process that extracts a portion of the file system.

~~16~~**16.5.1.3** File System—A process that provides access to the file system.

~~16~~**16.5.1.4** Physical (non-invasive)—A process that provides physical acquisition of a device's data without requiring opening the case of the device.

~~16~~**16.5.6.5** Physical (invasive)—A process that provides physical acquisition of a device's data requiring disassembly of a device providing access to the circuit board (e.g. JTAG). At this time, CCBI cannot provide this level of analysis.

~~16~~**16.5.1.6** Chip-Off – A process that involves the removal and reading of a memory chip to conduct analysis. At this time, CCBI cannot provide this level of analysis.

~~16~~**16.6.1.7** MicroRead – A process that involves the use of a high-power microscope to provide a physical view of memory cells. At this time, CCBI cannot provide this level of analysis.

~~16~~16.5.2 Procedures

~~16~~**16.5.2.1** If possible, determine make and model of the mobile/handheld device and acquire the user manual. ~~Research the user manual before removing the battery and/or powering on the mobile/handheld device to ensure proper handling so as to reduce the possibility of data alteration.~~

If appropriate cabling is available, charge the device when required to prevent memory loss.

~~16~~**16.5.2.2** Remove any media storage, such as a memory card, and process separately. ~~If the mobile/handheld device has a SIM card, process it separately.~~

~~16~~**16.5.2.3** Protect the mobile/handheld device from external signals and/or other inadvertent access by placing it in Faraday bag (or other RF-blocking device) before powering on. If "Airplane Mode" is available, engage it immediately after turning the device on. Turn any wireless communication features off if the option is available to the examiner.

~~16~~**16.5.2.4** Identify the software and /or hardware that support data extraction from the mobile/handheld device and follow the data extraction methods as outlined by the manufacturer.

~~16~~**16.5.2.4.1** If the mobile/handheld device is supported by a hardware extraction device, the only preparation necessary is a wiped USB device, such as a thumb drive, used to store extracted data.

~~16~~**16.5.2.4.2** If the mobile/handheld device is supported by computer software

~~16~~16.6 References

Cellebrite UFED User Manual

Best Practices for GPS Examinations v1.0, Scientific Working Group on Digital Evidence, June 2012, URL: www.swgde.org/documents/Current%20Documents/2012-06-04%20SWGDE%20Best%20Practices%20for%20GPS%20Devices%20v1.0

Best Practices for Mobile Phone Examinations v2.0, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Released%20For%20Public%20Comment/2012-09-13%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20v2.0

Guidelines on Cell Phone Forensics, National Institute of Standards and Technology, May 2007, URL: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

Hashing Techniques for Mobile Device Forensics, Shira Danker, Rick Ayers, and Richard P. Mislan, June 2009, www.nist.gov/customcf/get_pdf.cfm?pub_id=901361

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 16.5.2: Deletion of "Research the user manual before removing the battery and/or powering on the mobile/handheld device to ensure proper handling so as to reduce the possibility of data alteration." Section 16.5.2.2: Deletion of "If the mobile/handheld device has a SIM card, process it separately."

Chapter 1717: Evidence Search Protocol

1717.1 Purpose

The purpose of this procedure is to provide a systematic means of searching digital evidence in order find the data sought by the search authorization.

1717.2 Scope

This policy describes the steps taken in searching submitted computer evidence.

1717.3 Equipment

- Forensic computer
- Forensic software

1717.4 Limitations

Results may vary between different utilities due to the different methods and algorithms being applied.

1717.5 Procedures

1717.5.1 Read the search authorization (e.g., search warrant or consent) to ensure the scope of search is authorized by the document. Install the forensic computer's operating system drive and the target drive into the forensic computer.

1717.5.2 Boot the forensic tower from the operating system drive.

1717.5.3 Examine the forensic image of the evidence drive for the presence of any hidden or deleted partitions. ~~If any hidden or deleted partitions are noted, these partitions shall be recovered if appropriate and possible.~~

1717.5.4 Examine the forensic image of the evidence drive for the presence of any deleted files. Any deleted evidentiary files shall be recovered where possible.

1717.5.5 Examine the forensic image of the evidence drive for the presence of any deleted folders of evidentiary value. Any deleted evidentiary folders shall be recovered where possible.

~~**17.5.6** If using EnCase, run a file mounter EnScript to mount relevant types of zipped or compressed files so that the files contained inside can be examined. Mounted files should be saved as Logical Evidence Files and added to the EnCase case.~~

~~17~~**17.5.**6~~7~~ Run a signature analysis against all files in the case prior to the examination of these files. The signature analysis checks the file header information to ensure that the files have not been identified with an incorrect file extension.

~~17~~**17.5.**7~~8~~ Search procedures may include some of, but are not limited to, the following, depending on the type of the case and scope of the search authority.

~~17~~**17.5.**8~~7~~**.1** Recover data

~~17~~**17.5.**7~~8~~**.1.1** Recover and/or bypass passwords and encryption
~~17~~**17.5.**7~~8~~**.1.2** Carve data from unallocated space, unused space, or file slack
~~17~~**17.5.**7~~8~~**.1.3** Extract Internet history

~~17~~**17.5.**7~~8~~**.2** Conduct searches

~~17~~**17.5.**7~~8~~**.2.1** Conduct keyword, text string, and/or regular expression searches
~~17~~**17.5.**7~~8~~**.2.2** Use hash databases to include or exclude known data
~~17~~**17.5.**7~~8~~**.2.3** Detect malware programs or artifacts
~~17~~**17.5.**7~~8~~**.2.4** Detect evidence of system compromise
~~17~~**17.5.**7~~8~~**.2.5** Detect counter/anti-forensic programs or artifacts

~~17~~**17.5.**7~~8~~**.3** Identify and Analyze

~~17~~**17.5.**7~~8~~**.3.1** Conduct registry analysis
~~17~~**17.5.**7~~8~~**.3.2** Identify user accounts
~~17~~**17.5.**7~~8~~**.3.3** Analyze communications (email, chat messages, instant/private messaging, newsgroups)
~~17~~**17.5.**7~~8~~**.3.4** Analyze document files (text files, spreadsheets, databases, presentations)
~~17~~**17.5.**7~~8~~**.3.5** Analyze picture files and multimedia files
~~17~~**17.5.**7~~8~~**.3.6** Analyze program files
~~17~~**17.5.**7~~8~~**.3.7** Analyze internet history
~~17~~**17.5.**7~~8~~**.3.8** Conduct timeline analysis

~~17~~**17.5.**8~~9~~ **Suspect Image Restoration**

At times it may be necessary to view the evidence computer in a bootable state, just as the suspect would have viewed it at the time it was in use. There are a number of methods to achieve this:

~~17~~**17.5.**8~~9~~**.1** Clone the evidence hard drive onto a forensically prepared hard drive of similar storage capacity using forensic software or hardware. The cloned drive can then be inserted into the evidence computer and used to boot the evidence computer. Determine the hash value of the cloned drive and compare it to the hash value of the subject drive for verification, if possible.

~~17~~**17.5.~~8~~9.2** Restore the evidence hard drive onto a forensically prepared drive that has similar storage capabilities as the suspect drive. This restored drive can then be inserted into the evidence computer and used to boot the evidence computer. ~~Determine the hash value of the restored drive and compare it to the hash value of the subject drive for verification, if possible.~~

~~17~~**17.5.~~8~~9.3** Utilize virtual imaging technology to spawn a virtual computer using the forensic image of the suspect's computer as the basis for the virtual machine. This will allow the examiner to examine the suspect's computer in a virtual environment that simulates the suspect's computer in its native state.

~~17~~**17.5.~~8~~9.4** Mount a forensic clone of the suspect drive or forensic image files as a virtual drive on the forensic machine using forensic software. Run Virtual Machine software and attach the virtual drive to the virtual machine. Boot a virtual image of the computer in the virtual machine software.

~~17~~**17.5.~~8~~9.5** ~~Use Live View to C~~create a virtual machine using a DD or E01 image of the subject hard drive. Save the virtual machine to the forensic computer and boot the virtual machine in virtualization software.

~~17~~17.6 References

EnCase Forensic User Manual

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 17.5.3: Deletion of "If any hidden or deleted partitions are noted, these partitions shall be recovered if appropriate and possible." Section 17.5.4: Addition of deleted "evidentiary" files. Deletion of "**17.5.6** If using EnCase, run a file mounter EnScript to mount relevant types of zipped or compressed files so that the files contained inside can be examined. Mounted files should be saved as Logical Evidence Files and added to the EnCase case." Renumbering of remaining 15.5.7 and 15.5.8 as 15.5.6 and 15.5.7. Section 17.5.8.2: Deletion of "Determine the hash value of the restored drive and compare it to the hash value of the subject drive for verification, if possible." Section 17.5.8.5: Deletion of "Use LiveView to" at beginning of first sentence. Addition of "or E01" to first sentence.

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: (Default) +Body (Calibri), Font color: Black

Chapter 1818: Macintosh Native Examination

1818.1 Purpose

The purpose of this procedure is to examine data methodically from a device running the Apple Macintosh OS X or iOS operating systems by means of a forensic examination platform running the Apple OS X operating system.

1818.2 Scope

This procedure applies to all personnel who examine data from devices running the Apple Macintosh OS X or iOS operating systems submitted as evidence.

1818.3 Equipment

- Macintosh computer specifically designated for use in Mac forensics analysis
- Prepared target drive containing a RAW or DD image of the suspect device

1818.4 Definitions

1818.4.1 OSX – The OS Ten (X) operating system for Apple computers, originally built off of the BSD UNIX kernel, which has been ported to work on Intel processors.

1818.4.2 iOS – The operating system for Apple devices (iPods, iPads, iPod Touches, iPhones, etc.).

1818.4.3 Finder – An application in the Apple OS X operating system that allows access to the files and folders on a given computer (similar to Windows Explorer on the Windows platform).

1818.4.4 File Vault - An application on versions of OS X that allow the user to encrypt the contents of their Home folder. File Vault uses AES-128 encryption.

1818.4.5 Home Folder – A folder in the Apple OS X directory structure in which all user data for a given user account is stored.

1818.4.6 Shadow File – A mounted file that is attached to, but not part of, a locked forensic image file. The mounted shadow file can then be indexed by Spotlight to find relevant data.

1818.4.7 Spotlight – An application in the Apple OS X operating system that indexes the contents of files and allows for subsequent searching of the index.

1818.4.8 iTunes - An application in the Apple OS X operating system that is used to "sync" and transfer data to and from devices running the iOS operating system.

1818.5 Limitations

~~18~~18.5.1 Great care must be taken when selecting the forensic image file during the locking process. Double-clicking on a forensic image file before the file has been locked will mount the image file read-write in the operating system and will change data on the forensic image file.

~~18~~18.5.2 The Apple OS X operating system has options to securely delete files, rendering them impossible to recover. Furthermore, due to the optimization routines on OS X file systems, it is possible that previously deleted files might not be recoverable because they have been overwritten by other data.

~~18~~18.5.3 File Vault utilizes an AES-128 encryption scheme and is therefore virtually impossible to decrypt by means of brute-force.

~~18~~18.5.4 Some iPhones are password protected and cannot be backed up to any account except the one under which it was registered. Furthermore, most iPhones are set to erase all of its data if the incorrect password is entered more than ten times.

~~18~~18.5.5 Any iPhone (beyond version 2) can be remotely wiped by the user. Measures must be taken to prevent the iPhone from receiving RF signals whenever powered on.

~~18~~18.5.6 A sync of an iPhone may, or may not, give the examiner access to voicemails and emails. A sync of an iPhone will not provide a copy of unallocated space for examination.

~~18~~18.5.7 Due to the ease with which an iPod can be modified during the syncing process, it is recommended that any iPod be connected to a forensic USB bridge device before being connected to a computer.

~~18~~18.6 Procedures

~~18~~18.6.1 If the suspect device is a computer running the Mac OSX Operating System:

~~18~~18.6.1.1 Attach the target drive to the forensic Mac computer.

~~18~~18.6.1.2 In Finder, locate the subject drive's forensic image file on the target drive. Be careful not to mount the forensic image file before it has been locked (see limitations section above). Right-click or press 'Command + I' to open the "Get Info" dialog box in Finder. Select the "locked" radio button to lock the forensic image into read-only mode.

~~18~~18.6.1.3 Mount the locked forensic image by double-clicking on the forensic image file.

~~18~~18.6.1.4 If File Vault is enabled:

~~18~~18.6.1.4.1 Create dictionaries for use in the decryption process.

~~18~~**18.6.1.4.2** Utilize the created dictionaries in concerted decryption attacks against the File Vaulted directory(s) using password cracking applications.

~~18~~**18.6.1.4.3** If the decryption efforts are successful, copy the File Vaulted Home directory to the target drive and decrypt it. Then, mount the unlocked Home directory for further examination.

~~18~~**18.6.1.5** Create a shadow file for the locked forensic image file. Mount the shadow file and index it for use in Spotlight.

~~18~~**18.6.1.6** Create a new user account for use in examining the suspect data. Enable "fast user switching" in the process.

~~18~~**18.6.1.7** Copy all relevant user data from the locked forensic image into the newly created forensic examination user account.

~~18~~**18.6.1.8** Log into the newly created forensic examination user account.

~~18~~**18.6.1.9** Utilize the native OS X applications on the forensic Mac computer to examine the data in the newly created forensic examination user account.

~~18~~**18.6.1.10** Using the native OS X applications, create report artifacts by means of the built-in "print to PDF" and screenshot capabilities.

~~18~~**18.6.2** If the suspect device is running the Mac iOS Operating System:

~~18~~**18.6.2.1** Create a new user account for use in examining the suspect data. Enable "fast user switching" in the process.

~~18~~**18.6.2.2** Using the newly created forensic examination user account, open the iTunes application. Set the option to prevent automatic syncing with the computer by selecting: iTunes → Preferences → and check the "Prevent iPods, iPhones, and iPads from syncing automatically" option.

~~18~~**18.6.2.3** Connect the device to the forensic Mac computer (see limitations section above).

~~18~~**18.6.2.4** Take a screenshot of the Summary tab of the iTunes application to record information concerning the device.

~~18~~**18.6.2.5** Right-click on the root of the device's entry (on the left side of the screen) and select "Back-Up" from the menu. This will copy the contents of the device (see limitations section above) to the directory ~/Library/Application Support/MobileSync/Backup/(GUID for the device).

~~18~~18.6.2.6 Upon successful completion of the backup process, remove the device from the forensic Mac computer.

~~18~~18.6.2.7 Examine the contents of the device's backup files for data of relevance.

~~18~~18.7 References

Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit, Ryan Kubasiak, December 2008, (no URL)

Macintosh Forensics: A Guide for the Forensically Sound Examination of a Macintosh Computer, Ryan R. Kubasiak, May 2007, URL: www.appleexaminer.com/Downloads/MacForensics.pdf

Processing iPhone / iPod Touch Backup Files on a Computer, Selena Ley, URL: http://www.appleexaminer.com/iPhoneiPad/iPhoneBackup/iPhoneBackup.html

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 1~~9~~19: Generating Results

~~19~~19.1 Purpose

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

~~19~~19.2 Scope

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

~~19~~19.3 Equipment

- Forensic computer
- Blank or forensically prepared media

~~19~~19.4 Limitations

CD-RW and DVD-RW discs may not be used to store recovered files because data on the discs may be altered.

~~19~~19.5 Procedures

~~19~~19.5.1 At the conclusion of the forensic examination, copy the forensic image onto a set of CDs ~~or~~ DVDs, Blue-ray or hard disks. These discs will be returned to the submitting agency, as will the original evidence.

> **~~19~~19.5.1.1** In the event that the forensic image or recovered files are of excessive size, ~~the CCBI Crime Laboratory Division Deputy Director may authorize~~ the storage of such data on media other than optical media is authorized.

~~19~~19.5.2 Copy files recovered in the case and associated work product to CDs or DVDs. Any CD or DVD 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."

~~19~~19.5.3 Any media, photographs, or any other item created or recovered by the Forensic Computer Unit as a result of an examination shall be documented, numbered, and packaged as evidence. Upon the completion of the requested examination, all resulting evidence will be transferred to the custody of the authority requesting the initial examination. Such transfer shall be completed and documented in accordance with CCBI evidence policies.

~~19~~19.5.4 When creating a CD or DVD, all sessions shall be finalized.

~~19~~**19.5.5** A laboratory report shall be created in OSSI. Reports issued by the Forensic Computer Examiner must address the requestor's needs and contain the following items:

~~19~~**19.5.5.1** A title;

~~19~~**19.5.5.2** The name and address of CCBI and/or the location where the examination/analysis was completed if other than the laboratory;

~~19~~**19.5.5.3** A unique CCBI case number;

~~19~~**19.5.5.4** Page numbers;

~~19~~**19.5.5.5** The name, address, and the submitting customer agency case number;

~~19~~**19.5.5.6** The date the evidence was received;

~~19~~**19.5.5.7** A written description, including the CCBI unique item number(s) assigned, the condition of the item(s), and unambiguous identification of the item(s) tested (including all items submitted and not examined);

~~19~~**19.5.5.8** The test results will include the following when appropriate for the interpretation of the test results:

~~19~~**19.5.5.8.1** Units of measurements
~~19~~**19.5.5.8.2** Changes to standard test methods;
~~19~~**19.5.5.8.3** Opinions and interpretations;
~~19~~**19.5.5.8.4** Qualified and clearly communicated associations if associations are made;
~~19~~**19.5.5.8.5** Eliminations made as a result of comparative examinations; and
~~19~~**19.5.5.8.6** Reasons when no definitive conclusion can be reached.

~~19~~**19.5.5.9** The author's official title with a signature or equivalent identification; and

~~19~~**19.5.5.10** A confidentiality statement signifying the end of the report.

~~19~~**19.5.6** The target drive used to temporarily store the forensic image and files recovered in the case may be wiped and reused in further casework examinations.

~~19~~**19.5.7** CCBI shall not retain any copies, electronic duplications, or any other reproductions of any evidence generated by a forensic computer examination.

~~19~~**19.6 References**

CCBI Crime Laboratory Division Administrative Procedures

All copies of this document are uncontrolled when printed

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 19.5.1.1: Deletion of "the CCBI Crime Laboratory Division Deputy Director ay authorize" and addition of "is authorized".

Chapter 2020: Technical Field Assistance, Evidence Preservation

2020.1. Purpose

The purpose of this procedure is to secure digital evidence located at a non-laboratory location to preserve its integrity for further forensic processing.

2020.2. Scope

This policy describes procedures to follow when providing digital forensics assistance at non-laboratory locations.

2020.3. Equipment

A digital forensics field response kit may contain, but is not limited to, the following:

- Digital camera
- Sterilized removable media
- Forensic computer or laptop
- Hardware write-blocking devices
- Forensically sound boot disks
- Mobile device acquisition tools
- Tool kit (screw drivers, etc.)
- Evidence packaging materials

2020.4. Definitions

2020.4.1 Mobile devices – Portable devices that have digital storage and network connectivity such as cellular telephones, PDAs, GPS devices, mp3 players, iPods, iPads, etc.

2020.4.2 Removable media – Digital storage media such as: CDs, DVDs, Zip disks, Jazz disks, floppy disks, external hard drives, memory cards, USB drives, SIM cards, etc.

2020.5. Limitations

2020.5.1 Networked Computers

2020.5.1.1 Unplugging a suspect computer from a network may cause data loss and could potentially damage other computers on the network.

2020.5.1.2 Computer networks can be technically complex and may prevent collection of evidence in a timely manner. If the system administrator is a suspect in the case, assistance should be sought from personnel knowledgeable in the network's operation.

~~20~~20.5.2 Non-networked Computers

~~20~~20.5.2.1 If evidence may be destroyed or manipulated during the crime scene search or while securing the computer, the computer should be forcibly shut down.

~~**20**18.**5.2.2** Powering down a suspect's computer forcibly may cause data loss and could potentially damage the operating system.~~

~~20~~20.5.3 Removable Media

~~20~~20.5.3.1 Most removable media is very small, often hard to locate, and often overlooked.

~~20~~20.5.3.2 Removable media may be obfuscated to thwart detection.

~~20~~20.5.3.3 Some removable media is susceptible to immediate physical destruction.

~~20~~20.5.4 Handheld Digital Devices

~~20~~20.5.4.1 Active devices are susceptible to data destruction due to network communication.

~~20~~20.5.4.2 Mobile devices may lose data or initiate additional security measures once discharged or shut down.

~~20~~20.5.4.3 Blocking RF signals may drain the battery, may be expensive, are not always successful, and may result in the alteration of data.

~~20~~20.5.4.4 Some components and devices are susceptible to immediate physical destruction and should be physically secured.

~~20~~20.5.4.5 A device may be protected with a password, PIN, token or other authentication mechanism.

~~20~~20.6. Search and Seizure Procedures

During investigations, only CCBI employees who have been trained in computer forensics shall seize computers, digital devices, or digital media, unless other circumstances exist requiring other CCBI personnel to seize said devices or media. Whenever possible, seizures should be done by the Forensic Computer Examiner.

These procedures should be adapted as necessary based upon the situation.

~~20~~20.6.1 General

~~20~~20.6.1.1 Ensure the safety of all individuals at the scene.

~~20~~20.6.1.2 Protect the integrity of evidence.

~~20~~20.6.1.3 Evaluate the scene and formulate a search plan.

~~20~~20.6.1.4 Identify potential evidence.

~~20~~20.6.1.5 All potential evidence should be secured, documented, and/or photographed.

~~20~~20.6.1.6 Any item to be removed from the scene should be properly packaged and secured.

~~20~~20.6.2 Computers

~~20~~20.6.2.1 Ensure that the suspect is removed from the computer and power supply and is not allowed access to them. If the computer to be searched is on a network, ensure that all computers on the network are secured and that no one is allowed access to these computers until the crime scene search is completed.

~~20~~20.6.2.2 The scene should be searched to determine if any wireless networks or networking devices exist.

~~20~~20.6.2.3 If the evidence computer or device is connected to an internal network:

~~20~~20.6.2.3.1 Assistance should be sought from the system administrator in isolating the computer or device from the network, presuming the administrator is not a suspect in the case. ***Note:*** *If the system administrator is a suspect in the case, assistance should be sought from personnel knowledgeable in the network's operation.*

~~20~~20.6.2.3.2 Once it is determined that no networking information needs to be collected, i~~I~~solate and remove the evidence computer or device from the network immediately.

~~20~~20.6.2.4 Document the location and condition of all computers and/or digital devices.

~~20~~20.6.2.4.1 If the computer is turned off, do NOT switch it on.

~~20~~20.6.2.5 Document any open files or programs on the computer.

~~20~~20.6.2.5.1 If at any point while securing the computer, CCBI personnel believes that digital evidence may be being destroyed on a desktop or tower computer, the power cable should immediately be pulled from the back of the computer, not from the wall outlet. If the computer is a laptop, the battery should be removed in addition to the power cable being pulled from the back of the computer.

~~20~~20.6.2.5.2 Indications of possible digital data destruction include, but are not limited to, the following situations: data deletion program running; disk wipe program running;

Windows Add or Remove Programs dialog box open or application running; or Windows Disk Defragmenter dialog box open or application running.

~~20~~**20.6.2.5.3** If there is no indication of active destruction of digital evidence, allow any print devices to complete printing.

~~20~~**20.6.2.6** The Forensic Computer Examiner may choose to capture live memory. (*see* Live Capture Technical Procedure *infra*)

~~20~~**20.6.2.7** Shutdown procedures

~~20~~**20.6.2.7.1** Pull the plug from the back of the computer, not from the outlet. When necessary, normal shutdown procedures should be utilized.

~~20~~**20.6.2.7.2** For laptops, unplug any power cable from the back of the computer, push the power button until the system shuts off, and then remove the battery.

~~20~~**20.6.2.7.3** Do not unplug an Uninterruptable Power Supply (UPS) backup unit to cut power to a computer. The battery in the UPS could power the computer long enough to complete any destructive processes.

~~20~~**20.6.2.8** Document all connections to the computer. Photograph or document in notes the hardware connections to the computer, including mouse, keyboard, phone cable, network cable, external data storage drives, print devices, scanners, other peripheral devices, etc.

~~20~~**20.6.2.9** Search the area around the computer(s) and wider crime scene for passwords, account numbers, login names, user IDs, or other pertinent information that may be written down. Also search for diaries or notebooks with notations that may be related to this type of information.

~~20~~20.6.3 Removable Media

~~20~~**20.6.3.1** Document the location and condition of all removable media.

~~20~~**20.6.3.2** Remove any connected external media (e.g. external drives, flash cards, or thumb drives) after the computer has been powered down. Do not remove any CDs or DVDs contained in the computer's optical drive(s).

~~20~~20.6.4 Handheld Digital Devices

~~20~~**20.6.4.1** Document the location and condition of all handheld digital devices including onscreen data.

~~20~~**20.6.4.2** Power off the device in the appropriate manner and, if possible, physically remove the battery from the device.

~~20~~20.6.4.3 Search the scene for removable media, passwords, or other pertinent information.

~~20~~20.7. Evidence Packaging Procedures

~~20~~20.7.1 General

~~20~~20.7.1.1 The power cable should be seized and packaged with the seized device.

~~20~~20.7.1.2 The seizure of keyboards, mice, monitors, and peripheral devices that do not store data (e.g. print devices, scanners, speakers, webcams, modems) is left to the discretion of the CCBI Field Agent or Forensic Computer Examiner. However, documentation of the presence of these devices is recommended in the event that their later seizure becomes necessary. This documentation should include identifying characteristics for the item such as product name or serial number.

~~20~~20.7.2 Computers

~~20~~20.7.2.1 The computer should be packaged in its entirety in a paper bag, paper box, or paper wrapping.

~~20~~20.7.2.2 If this is not possible, packaging or evidence tape should be placed across each drive slot in such a way that media can neither be removed nor added without breaking the tape. In addition, packaging or evidence tape should be placed across the power cable receptacle on the computer. Finally, packaging or evidence tape should be placed across the computer case in such a way that it cannot be opened without breaking the tape (e.g. taping the locking rings together, taping the removable case cover shut, etc.).

~~20~~20.7.2.3 If the computer is packaged in a box, do not pack it in Styrofoam peanuts or shredded paper. Crumpled paper makes a good padding.

~~20~~20.7.2.4 If the computer has been contaminated with body fluids or other hazardous material, mark the outer packaging appropriately.

~~20~~20.7.3 Mobile Devices

~~20~~20.7.3.1 Document the mobile device's screen.

~~20~~20.7.3.2 Turn the mobile device off and remove its battery. The device, its battery, and its power cable should be packaged together in a paper bag, paper envelope, paper box, or paper wrapping.

~~20~~20.7.3.3 If a device is left on, the device must be shielded from radio frequencies by placing it in Faraday cloth, several wraps of heavy duty aluminum foil, or in a sealed arson can. Seal the arson

can with packaging or evidence tape. Alert the Computer Forensic Examiner as soon as possible that a powered-on device is awaiting examination.

~~20~~20.7.4.4 If the device has been contaminated with body fluids or other hazardous material, mark the outer packaging appropriately.

~~20~~20.7.4 Removable Storage Media

~~20~~20.7.4.1 Count and package similar storage media (e.g. floppy disks, CDs and DVDs, ZIP disks, etc.) and itemize by type on the evidence inventory form.

~~20~~20.7.4.2 Media removed from digital devices at the time of seizure should be listed separately on the evidence inventory form and clearly marked as having been removed from the digital device.

~~20~~20.7.4.3 Do not use a ballpoint or gel pen when marking removable storage media as damage to data can occur. Use felt markers only (such as Sharpies).

~~20~~20.7.4.4 Media should be packaged in paper envelopes, paper bags, or paper wrapping. If possible, optical media such as CDs and DVDs should be placed in sleeves or cases to protect against damage while in evidence.

~~20~~20.8. 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.

~~20~~20.9. References

CCBI Crime Laboratory Division Administrative Procedures

Best Practices for Mobile Phone Examinations v1, Scientific Working Group on Digital Evidence, January 2012, URL: www.swgde.org/documents/Released%20For%20Public%20Comment/2012-01-15%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20v1.1

Best Practices for Seizing Electronic Evidence v3, United States Secret Service, October 2006, URL: http://www.forwardedge2.usss.gov/pdf/bestPractices.pdf

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, U.S. Department of Justice National Institute of Justice, April 2008, URL: www.ncjrs.gov/pdffiles1/nij/219941.pdf

Guidelines on Cell Phone Forensics, NIST Special Publication 800-101, May 2007, URL: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Deletion of "20.5.2.2 Powering down a suspect's computer forcibly may cause data loss and could potentially damage the operating system. Section 20.6.2.3.2: Addition of "Once it is determined that no networking information needs to be collected," to first sentence.

Formatted: Indent: Left: 0", Space After: 10 pt, Add space between paragraphs of the same style, Line spacing: Multiple 1.15 li, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Calibri, Font color: Auto

Formatted: Font: Not Bold

Formatted: Font: Not Bold

All copies of this document are uncontrolled when printed

Chapter 2121: Technical Field Assistance, Live Memory Acquisition

2121.1 Purpose

The purpose of this procedure is to describe the steps to acquire data stored in Random Access Memory (RAM) located at a non-laboratory location to preserve its integrity for further forensic processing.

2121.2 Scope

This procedure shall be followed when the acquisition of RAM is desired.

2121.3 Equipment

- Removable media (USB thumb drive or USB hard drive)
- Memory acquisition software for the target operating system
- Memory acquisition software user manual or documentation

2121.4 Limitations

2121.4.1 Inserting USB drives will change the configuration files of the operating system of the subject computer.

2121.4.2 Running a computer program will cause a portion of RAM to be overwritten. Sacrificing a small portion of RAM by running a memory-capturing tool may potentially yield several gigabytes of data stored in RAM that would not otherwise be recoverable.

2121.4.3 Due to the dynamic nature of RAM, authentication of acquired memory is not possible.

2121.5 Procedure

2121.5.1 Determine amount of RAM in the subject computer.

2121.5.2 Wipe and format removable media larger than the amount of RAM in the subject computer.

2121.5.3 Copy memory acquisition software to the removable media.

2121.5.4 Insert the prepared removable media into the subject computer and run the memory acquisition software in accordance with the software's user documentation.

2121.5.5 Safely eject the USB drive from the subject computer.

2121.6 References

Capturing a Running Computer System: What Every Digital Forensics & Cyber Professional Should Know, Federal Bureau of Investigation Regional Computer Forensic Laboratory Continuing Education Series, October 2010, (no URL)

Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, National Consortium for Justice Information and Statistics, 2006, URL: www.search.org/files/pdf/CollectEvidenceRunComputer.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 2222: Technical Field Assistance, Preview and Imaging

2222.1 Purpose

The purpose of this procedure is to describe the steps for forensically previewing and forensically imaging computers and digital media on-scene.

2222.2 Scope

This procedure shall be followed when forensically previewing and forensically imaging computers and digital media on-scene.

2222.3 Equipment

- Forensic computer
- Linux boot media with preview/imaging software (Helix, Knoppix, etc.)
- Windows preview/imaging software (FTK Imager, EnCase, etc.)
- Hardware write blocker for various hard drive interfaces (EIDE, SATA, SCSI, etc.)
- Wiped and formatted "target" hard drive if imaging using evidence files (.E01 files)
- Wiped "target" hard drive if imaging using a RAW data dump (forensic clone of drive)

2222.4 Limitations

2222.4.1 Failure to control the boot order of the computer may result in unintentional writes to the subject computer's hard drive.

2222.4.2 Laptop drives may require special hard drive interface adapters.

2222.4.3 Hard drive removal from a computer may not be easily accomplished.

2222.4.4 The quantity of data and the time to process digital media can be limiting factors.

2222.5 Procedure

2222.5.1 General

2222.5.1.1 It shall be the policy of the Forensic Computer Unit to make every effort possible to avoid working on original evidence. It is understood, however, that in rare circumstances original evidence may have to be examined due to hardware configurations or certain operating systems. If this must be done, the Forensic Computer Examiner will document actions taken during the examination to clarify any date/time changes.

~~22~~22.5.1.2 Forensic imaging performed in the field will be performed in a forensically sound manner using a laptop computer; media storage such as an external hard drive; software, firmware, or hardware write blocker; and forensic software.

~~22~~22.5.2 Linux forensic preview

~~22~~22.5.2.1 Ensure the boot order of the subject computer is set to boot to the Linux media.

~~22~~22.5.2.2 Boot the subject computer to the Linux media and preview the computer's hard drive for evidence related to the case.

~~22~~22.5.2.3 Document the findings of the preview.

~~22~~22.5.3 Linux forensic imaging

~~22~~22.5.3.1 Ensure the boot order of the subject computer is set to boot to the Linux media.

~~22~~22.5.3.2 Boot the subject computer to the Linux CD.

~~22~~22.5.3.3 Image the computer's hard drive to the target drive.

~~22~~22.5.3.4 Verify and document the integrity of the image file(s) by comparing the acquisition and verification hash values.

~~22~~22.5.4 Windows forensic preview

~~22~~22.5.4.1 Remove the hard drive from the subject computer.

~~22~~22.5.4.2 Attach the subject hard drive to the appropriate hardware write blocker.

~~22~~22.5.4.3 Attach the write blocker to the forensic computer.

~~22~~22.5.4.4 If the computer's hard drive cannot be removed, ~~a crossover cable~~Windows FE acquisition method may be utilized.

~~22~~22.5.4.5 Boot the forensic computer and run the Windows preview/imaging software.

~~22~~22.5.4.6 Preview the subject computer's hard drive for evidence related to the case.

~~22~~22.5.4.7 Document the findings of the preview.

~~22~~22.5.5 Windows forensic imaging

~~22~~22.5.5.1 Remove the hard drive from the subject computer.

~~22~~22.5.5.2 Attach the subject hard drive to the appropriate hardware write blocker.

~~22~~22.5.5.3 Attach the write blocker to the forensic computer.

~~22~~22.5.5.4 If the computer's hard drive cannot be removed, a ~~crossover cable~~ Windows FE acquisition method may be utilized.

~~22~~22.5.5.5 Boot the forensic computer and run the Windows preview/imaging software.

~~22~~22.5.5.6 Image the subject computer's hard drive to the destination drive.

~~22~~22.5.5.7 Verify and document the integrity of the image file(s) by comparing the acquisition and verification hash values.

~~22~~22.6 References

Capturing a Running Computer System: What Every Digital Forensics & Cyber Professional Should Know, Federal Bureau of Investigation Regional Computer Forensic Laboratory Continuing Education Series, October 2010, (no URL)

Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, National Consortium for Justice Information and Statistics, 2006, URL: www.search.org/files/pdf/CollectEvidenceRunComputer.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 22.5.4.4: Deletion of "a crossover cable" and addition of "Windows FE" Section 22.5.5.4: Deletion of "a crossover cable" and addition of "Windows FE"

Chapter 2323: Technical Field Assistance, Mobile Device Collection

2323.1 Purpose

The purpose of this procedure is to describe the steps to collect mobile devices.

2323.2 Scope

This procedure shall be followed when collecting mobile devices on-scene.

2323.3 Equipment

- RF shielding device (e.g. Faraday bag, Faraday cloth, aluminum foil, arson can, etc.)
- Shielded power cable for mobile device

2323.4 Limitations

2323.4.1 Placing a mobile device in an RF shield may cause the mobile device to increase its transmit power in a search for a cell tower signal.

2323.4.2 Removing power from a mobile device may prevent the extraction of data from the device without the PIN or pass code.

2323.5 Procedure

2323.5.1 Physically secure the mobile device.

2323.5.2 Solicit information from mobile phone user to determine the phone number, pass codes, pattern locks, or PINs.

2323.5.3 If the phone is unable to be processed immediately, turn off phone and remove the battery. Package the battery with the mobile phone.

2323.5.4 The risks of turning off the mobile phone include possibly locking the phone by password or PIN. Exigency may dictate that the mobile phone remains on for immediate processing. If the mobile phone must be left on, isolate it from its network while maintaining power. This can be accomplished in the following ways:

2323.5.4.1 Contain the mobile phone in a radio frequency shielding material such as Faraday cloth, multiple wraps of heavy duty aluminum foil, or an arson can with sealed lid.

2323.5.4.2 Place the phone in “Airplane Mode” via the handset.

~~23~~**23.5.4.3** Disable Wi-Fi, Bluetooth, RF~~D~~ID, and IrDA communications via the handset where applicable.

~~23~~**23.5.5** Submit the mobile device for examination as quickly as possible.

~~23~~**23.6 References**

Best Practices for Mobile Phone Examinations v2, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Released%20For%20Public%20Comment/2012-09-13%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20v2.0

Guidelines on Cell Phone Forensics, NIST Special Publication 800-101, May 2007, URL: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

Model SOP for Computer Forensics v3, Scientific Working Group on Digital Evidence, September 2012, URL: www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3

All copies of this document are uncontrolled when printed

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Section 21.5.4.3: Deletion of "RDID" and addition of "RFID".

Chapter 2424: Abbreviations

@: at
+: and
Δ: defendant
00:00:00:00: hours, minutes, seconds, hundredths of seconds
1°: first degree
2°: second degree
3°: third degree

ABC: Board of Alcoholic Control
AC: alternating current
acct: account
ADA: assistant district attorney
admin: administration
AES: Advanced Encryption Standard
APD: Apex Police Department
ASCII: American Standard Code for Information Interchange
ATA: Advanced Technology Attachment

B&W: black and white
BIOS: Basic Input Output System

Cap: captain
CAPTCHA: Completely Automated Public Turing Test to Tell Computers and Humans Apart
CCBI: Raleigh/Wake City-County Bureau of Identification
CCE: Certified Computer Examiner
CD: compact disc
CDFS: compact disc file system
CDMA: Code Division Multiple Access
CD-R: recordable compact disc
CD-ROM: compact disc read only memory
CD-RW: rewritable compact disc
CF: compact flash
CFCE: Certified Forensic Computer Examiner
CGI: computer generated imagery
CHS: cylinder-head-sector
CMOS: complementary metal-oxide semiconductor
codec: coder/decoder
config: configuration
cont: continued
Corp: corporal
CP: child pornography
CPD: Cary Police Department

CPU: central processing unit

DA: district attorney
DB: database
DC: direct current
DCO: disk configuration overlay
DD: double density
Dep: deputy
Det: detective
dig: digital
DOS: Disk Operating System
DRM: digital rights management
DVD: digital video disc
DVD-R: recordable digital video disc
DVD-ROM: digital video disc read only memory
DVD-RW: rewritable digital video disc
DVI: digital visual interface
DVR: digital video recorder

ECPA: Electronic Communications Privacy Act
EFS: Encrypting File System

FAQ: frequently asked questions
FAT: File Allocation Table
FDD: floppy disc drive
fed: federal
FTP: file transfer protocol
FVPD: Fuquay Varina Police Department

GB: gigabyte
GHz: gigahertz
GMT: Greenwich Mean Time
GPD: Garner Police Department
GPS: global positioning system
GSM: Global System for Mobile Communications
GUI: graphical user interface
GUID: globally unique identifier

HD DVD: high definition digital video disc
HD: high density
HDD: hard disk drive
HDMI: high definition multimedia interface
HFS: Hierarchical File System
HKCU: HKEY_Current_User

HKLM: HKEY_Local_Machine
HPA: host protected area
HPFS: High Performance File System
hr(s): hour(s)
HSPD: Holly Springs Police Department
HTML: hypertext markup language
HTTP: hypertext transfer protocol
HTTPS: secure hypertext transfer protocol
HW: hardware
Hz: hertz

I/O: input/output
ICAC: Internet Crimes Against Children
ID: (n) identifier, identity; (v) identify
IDE: Integrated Drive Electronics
iDEN: Integrated Digital Enhanced Network
IE: Internet Explorer
IM: instant messaging
IMAP: Internet Message Access Protocol
IMEI: International Mobile Equipment Identity
IMSI: International Mobile Subscriber Identity
Inv: investigator
IP: internet protocol
IRC: internet relay chat
ISO: International Standards Organization

KB: kilobyte
KHz: kilohertz
KPD: Knightdale Police Department
KVM: keyboard, video, mouse

L: left
LBA: logical block addressing
LCD: liquid crystal display
LED: light emitting diode
LM: left message
Lt: lieutenant

MAC: media access control
Maj: major
MB: megabyte
MBR: master boot record
MD: message digest
MHz: megahertz

MIME: Multipurpose Internet Mail Extensions
min(s): minute(s)
MMS: multimedia messaging service
mobo: motherboard
MPD: Morrisville Police Department
MSISDN: Mobile Subscriber Integrated Services Digital Network

N/A: not applicable
NAS: network attached storage
NCGS: North Carolina General Assembly
NCPD: NC State Police Department
NIC: network interface card
NTFS: New Technology File System

OEM: original equipment manufacturer
Off: officer
OLE: object linking and embedding
OS: operating system

P2P: peer to peer
PCI: peripheral component interconnect
PCMCIA: Personal Computer Memory Card International Association
PDA: personal digital assistant
PIN: personal identification number
POP: Post Office Protocol
POP3: Post Office Protocol v3
POST: power on self test
PS/2: Personal System/2
PSU: power supply unit
PUK: PIN-unblocking key
PW: password

QA: quality assurance

Ⓡ: right
R/W: read/write
RAID: redundant array of independent disks
RAM: random access memory
RDP: remote desktop protocol
RDU: Raleigh-Durham International Airport Police Department
RE: regarding
rev: revised
ROM: read only memory
RPD: Raleigh Police Department

RSS: rich site summary
RVPD: Rolesville Police Department

S/N: serial number
SAM: Security Account Manager
SAN: storage area network
SATA: Serial Advanced Technology Attachment
SBI: State Bureau of Investigation
SCERS: Seized Computer Evidence Recovery Specialist
SCSI: Small Computer System Interface
SD: secure digital
sec(s): second(s)
SFTP: secure file transfer protocol
Sgt: sergeant
SHA: secure hash algorithm
SHP: State Highway Patrol
SID: security identifier
SIM: subscriber identity module
SMS: short message service
SMTP: simple mail transfer protocol
SOP: standard operating procedure
SP: service pack
SQL: Structured Query Language
SSD: solid state drive
SSID: service set identifier
Supp: supplement
SW: software
SWGDE: Scientific Working Group on Digital Evidence

TB: terabyte
temp: temporary
TPM: trusted platform module

UAC: user account control
UDF: Universal Disk Format
unk: unknown
UPC: universal product code
UPS: uninterruptible power supply
URL: universal resource locator
USB: universal serial bus
UTC: Coordinated Universal Time

v: version
V: victim

VGA: video graphics array
VHD: virtual hard drive
VM: virtual machine
VOIP: voice over internet protocol
VPN: virtual private network

WCSO: Wake County Sheriff's Office
WEP: Wired Equivalent Privacy
WFPD: Wake Forest Police Department
Windwos Fe: Windows Forensic Edition
WPA: Wi-Fi Protected Access
WPD: Wendell Police Department

XML: extensible markup language

ZIF: zero insertion force
ZPD: Zebulon Police Department

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
February 2, 2014	2	Addition of "Windows Fe: Windows Forensic Edition"