CONTACT INFORMATION

Morgantown Laboratory (DFU North)
Troops 1, 2 & 3
3040 University Avenue, Suite 3108
Morgantown, WV 26505
Office: 304-293-6400
Fax: 304-293-5137
dfumorgantown@wvsp.gov

Huntington Laboratory (DFU South)
Troops 4, 5, 6, 7
1401 Forensic Science Drive
Huntington, West Virginia 25701
Office: 304-691-8973 / 304-691-8974
dfuhuntington@wvsp.gov

Evidence is to be submitted based on your Troop location or services requested to the respective laboratory above.
Should you have any questions, please contact the Digital Forensics Unit.

Contents

Revision #	***Effective date***	***History***
0	*11/01/2005*	*Original Issue*
1	*09/08/2009*	*General review and update; conversion to ISO format*
2	*02/20/2011*	*Updated submission procedures*
3	*03/17/2011*	*Updated submission procedures*
4	*04/26/2011*	*Added contact information*
Rev 1 (Qualtrax)	*06/05/2022*	*Incorporation into WVSP Forensic Laboratory Management System; general update*

1. General Information

This manual has been written to provide law enforcement agencies investigating criminal matters within the State of West Virginia with a general guide for the collection, preservation, and submission of digital evidence. This manual is supplemental to the West Virginia State Police Forensic Laboratory Field Manual.

This manual is regularly revised to make it as up-to-date as possible, however it should be noted that the techniques, procedures, and capabilities contained herein may change as the field of digital forensics is evolving at a rapid rate. Law enforcement agencies are encouraged to keep regular contact with the WVSPFL Digital Forensics Unit.

1.1. Mission Statement

The mission of the West Virginia State Police Forensic Laboratory Digital Forensics Unit (DFU) is to conduct forensic examinations on electronic evidence for the purpose of criminal or administrative investigations, in direct support of requesting law enforcement officers and agencies located in the state of West Virginia. The DFU will further support and may assist with criminal and administrative investigations involving the technical aspects of any cybercrime related incident or technology facilitated crime.

1.2. Glossary

Allocated Space:	Space on a storage device that is storing active data.
Artifact:	Another term for evidence.
AXIOM:	Full featured forensic examination software developed by Magnet Forensics utilized by forensic examiners
Bit:	Unit of information that can be a 1 or a 0; how all digital media stores its data
Bluetooth:	Short range wireless technology used to exchange data between devices.
Byte:	8 bits.
CAM:	Digital Camera.

CD: Compact Disc. Form of optical storage media that typically has a maximum storage of 700 MB.

CDMA: Code Division Multiple Access. One of two radio networks used by wireless carriers.

Cellular: Networking technology that consists of mobile communication over an area comprised of transceivers (cell sites).

Cellebrite: Software used by forensic examiners to extract, process and review contents of mobile devices.

Cloud: Virtual storage or workplace located on the internet in multiple locations but seen as one.

Cookie: A file that is kept on a user’s system that is managed by the user’s web browser. Its main purpose is to keep track of the user and their preferences.

Cryptocurrency: Digital or virtual currency that does not rely on banks.

CT: Cell Phone / Smartphone.

CVIP: Child Victim Identification Program: identifies victims of sexual exploitation of children offenses.

Database: Large quantity of digital information that can be searched and/or manipulated.

Digital Case Report: The final results of a digital forensics examination in digital form and viewable in a web browser.

Digital Media: Any physical item capable of storing binary (digital) data.

DVD: Digital Video Disc.

DVR: Digital Video Recorder.

DVR Examiner: Software used by forensic examiners to extract, process and review contents of DVR’s.

Encrypted: Encryption is the method by which data is converted from a readable form to an encoded form.

Extraction: Three fundamental methods.
Logical-contains all current, active (non-deleted) files.

File System Contains all files from a logical and some deleted files.

Physical Contains all possible data current and deleted. Considered the most comprehensive extraction.

File Path: Location to where a file is in the file system. Example: c:\users\admin\documents\doc1.

File System: Structure of files and directories located on a storage device.

Forensic Image: An exact copy of all data contained within a device.

FTK: Forensic Tool Kit. Forensic examination software suite developed by AccessData.

FTK Imager: Forensic imaging program created by AccessData

GSM: Global System for Mobile Communications. One of two radio networks used by wireless carriers.

GB: Gigabyte. 1024 megabytes equals 1GB

Hardware Write-Blocker: Physical hardware device used to prevent data being written to digital media. Allows for read only access to ensure evidence integrity.

Hash: A Hash is a unique hexadecimal value that identifies a particular string of data, such as a file, forensic image or any other folder.

HD: Hard Drive.

HEX: Base 16 where it uses a combination of numbers that range from 0-9 and letters A-F.

Hyperlink: Graphic or text that links to another file.

ICAC: Internet Crimes Against Children. A national taskforce that investigates child abuse and exploitation online.

ICCID: Integrated Circuit Chip Identifier. A serial number on a SIM card.

IEF: Internet Evidence Finder. Forensic examination software developed by Magnet Forensics.

IMEI: International Mobile Equipment Identity. A unique number used to identify mobile devices.

IMSI: International Mobile Subscriber Identity. A unique number that allows access to a cellular network.

IOT: Internet of Things device. Any device, hardware, or gadget used to digitally record, detect, measure, transmit and / or receive data to a computer or network device. Examples: webcam, digital home appliances, Alexa, Google Nest, Ring and home automation devices.

IP: Internet Protocol. A unique address that identifies a device on the internet.

ISP: Internet Service Provider: A company that provides individuals wireless or wired connection to the Internet. (i.e. AT&T, U.S. Cellular, Comcast, Frontier, Google, Facebook, etc.).

KB: Kilobyte. 1024 bytes equals 1 KB.

MAC: Medium Access Control. A unique hexadecimal physical address that is given to a device connected to a network.

MD: Mobile Device. Example: Tablet computers, MP3 players, electronic game systems, Drones, digital watches, etc.

MB: Megabyte. 1024 kilobytes equals 1 MB.

MEID: Mobile Equipment Identifier. A globally unique identification number used by CDMA carriers.

Modem: Hardware that connects a device or router to a network.

NCMEC: National Center for Missing and Exploited Children. The organization that handles cases for missing/exploited children.

Network: Collection of digital devices that are interconnected and can share data with each other.

NFC: Near Field Communication. Examples are Apple Pay and Google Wallet.

Operating System: Software that is installed on a storage device that runs programs. An example would be Windows/macOS or iOS/Android for mobile devices.

Passcode: A value used to secure or encrypt data using numbers, letters or movements on the screen.

Peer to Peer: Multiple computers connected together without the use of a server.

Plug-In: Software that enhances a program's capabilities. An example of this is Adobe Flash.

RAM: Random Access Memory. Short-term storage that stores data while the computer is powered on. When the power is cut the data stored will be lost.

RM: Removable Media. Any storage media easily removed from a device. Example: Thumb-drives and media cards.

Serial Number: A unique value that can have a combination of letters and numbers that identifies a device.

Server: A computer connected to a network of other workstations called clients.

SIM: Subscriber Identity Module. Small removable card that is used to gain access to a cellular network.

Social Media: Websites that allow groups of people to share information or communicate with each other.

Software Write-Blocker: Software used to prevent data being written to digital media. Allows for read only access to ensure evidence integrity.

TB: Terabyte. 1024 GB equals 1TB.

Unallocated Space: Space on a drive that is not storing active data. It may contain data that was deleted from a user.

URL: Uniform Resource Locator. Address to locations on a network.

UTC: Coordinated Universal Time. A standard used to set all time zones around the world.

WiFi: A device that transmits a signal that allows wireless connections to the internet or other devices.

1.3. Scope of Examination

1.3.1. The Digital Forensics Unit provides services for forensic examination and retrieval of digital evidence from a variety of digital media sources. This includes, but is not limited to, computers, hard drives, cellular devices, tablet devices, USB thumb drives, flash cards, DVRs, digital camera memory, and more.

1.3.2. The focus of the examination will depend on the criminal offense of the case. For example, the examination of a drug case will often be focused on communication about drugs in the chats and photos/videos of any drugs in the media. The examination of a child pornography case will mainly be focused on suspect photos or videos.

1.4. General Procedures

1.4.1 Handling digital evidence at the crime scene normally consists of the following steps:

- Recognition and identification of the evidence.
- Collection and preservation of the evidence.
  - Documentation of the crime scene.
- Packaging, transportation, storage, and submission of the evidence.

1.4.2 Visitors

Due to the sensitive nature of the work performed by the Digital Forensic Unit, visitors are restricted from bringing electronic devices into the Unit. These devices should remain in your vehicle or in a secure area outside of the Unit. Also, visitation for the purposes of viewing sensitive images/content is restricted to 30 min (or 600 images) whichever comes first. Should you need additional time, another 30-minute visit can be scheduled for a later date. **When time is of the essence due to the provisions of a court order, the Digital Forensics Unit will make every effort to accommodate the viewing party.** These provisions are enacted to ensure confidentiality and respect the sensitive nature of the evidence in possession of the Digital Forensics Unit.

A log shall be maintained to document all visitors.

2. Recognition and Identification of Digital Evidence

2.1. Identifying and recognizing potential digital evidence is essential in any criminal investigation. Digital storage media can take many forms from the obvious thumb-drive to the most irrelevant looking item. Searching for and locating digital media has its challenges because it can be in many from a MicroSD media card to a large multi-drive NAS (Network Attached Storage) system.

2.2. Keep in mind that USB storage drives can be in the form of any imaginable object. Covert USB drives and devices are quite common and easily purchased.

2.3. When seizing any digital device that has internet or other network services, a Preservation Order should be immediately sent to ensure the provider retains the potentially evidentiary account information and data. A sample Preservation Order is depicted in the Appendix section of this manual.

3. Collection and Handling of Digital Evidence

3.1. Mobile Devices

3.1.1. The most common device encountered is a cell phone, almost every person has one, if not multiple. The following procedure can be used for cell phones and tablets.

3.1.2. Procedures:

- Keep the mobile device **TURNED ON**. The likelihood of tools retrieving the passcode are much higher if the device has not been turned off. Protect the device from the internet and plug in the mobile device to keep it charged.
- It is important to keep mobile devices from connecting to its cellular network and from having the ability to receive/send signals. A remote signal can be sent to a mobile device to wipe the device of any and all data. The device can be protected through the following ways:
- A faraday isolation bag should be used if one is available.
- **ALWAYS** ask the owner of the device for a passcode for the device.
- Place the device in airplane mode.
- Remove the SIM card from the device.

  - In most newer devices, you can use the end of a paperclip to insert into the hole on the side or top of the phone to remove the SIM tray.
  - In older devices where the back of the phone can be removed, remove the back panel, and remove the SIM from its slot.
    - If you have to remove the battery, do not remove the SIM.
- If you cannot place the device in airplane mode or remove the SIM, or do not have a faraday bag, you can wrap the device in several layers of aluminum foil and place it in an unused metal paint can to shield the device from any potential signals.
- Determine the birthdate and SSN, and any other available personal information (spouse's name, anniversary dates, favorite color, etc.) of the owner for the lab to use as possible passcodes.
- Obtain a preservation order and search warrant for applications used by the owner that log out after a certain amount of time. For example, Snapchat usually only keeps data for 30 days.

3.2. Desktop Computer

3.2.1. **CAUTION:** Multiple computers may indicate a computer network. Likewise, computers located at businesses are often networked. In these situations, specialized knowledge about the system is required to effectively recover evidence and reduce your potential for civil liability. *When a computer network is encountered, contact a digital forensics analyst.*

3.2.2. Simply unplugging a suspect computer from a network can cause encryption, data loss, and damage the network. However, if at any point while securing the computer the analyst believes that evidence may be destroyed, the power cord should be pulled from the back of the computer.

3.2.3. Any running computer related to a priority investigation should be considered for immediate on-~~-~~site forensic preview and RAM dump.

3.2.4. Procedures:

- Remove the subject from the computer and do not allow the subject access to it. After securing the scene, **read all steps below before taking** any action (or evidentiary data may be altered).
- Observe the monitor and determine if it is on, off, or in sleep mode. Then decide which of the following situations applies and follow the steps for that situation.

Situation A: Monitor is on and work product and/or desktop is visible.

- Photograph screen and record information displayed.
- Proceed to Situation C.

Situation B: Monitor is on and screen is blank (sleep mode) or screen saver (picture) is visible.

- Move the mouse slightly (without pushing buttons). The screen should change and show work product or request a password.
- If mouse movement does not cause a change in the screen, DO NOT touch any keys or move the mouse.
- Photograph the screen and record the information displayed.
- Proceed to Situation C.

Situation C: Monitor is off.

- Make a note of "off" status.
  - Turn the monitor on, then determine if the monitor status is as described in either S**ituation A** or **B** above and follow those steps.

- If the computer is networked, ensure that no one is allowed access to any of the computers until the computer of interest can be isolated from the network.
  - Assistance should be sought from the system administrator in isolating the computer from the network, providing the administrator is not a subject in the investigation.
  - If the system administrator is the suspect, assistance should be sought from personnel knowledgeable in the network's operation.
- Be sure all computers involved in the search are secured and no one is allowed access to them. Important data can be quickly damaged or destroyed.
- Document the condition of the computers with photographs and notes. This documentation should include any documents that are open and other information that may appear on the monitor such as the time given on the clock and running applications seen in the Task Bar.
- Shut down the computer by pulling the plug from the back of the computer, not the wall outlet, unless it's running a RAID array or is using FDE (Full Disk Encryption).
- Check for outside connectivity (e.g., telephone modem, cable, ISDN, DSL). If a telephone connection is present, attempt to identify the telephone number.
- Record make, model, and serial numbers.
- Photograph and diagram the connections of the computer and the corresponding cables.

- Label all connectors and cable ends (including connections to peripheral devices) to allow for exact reassembly. Label unused connection ports as "unused." Identify laptop computer docking stations to identify other storage media.
- Record and log all evidence.
- Search the scene for removable media.
- Search the area around the computer for any passwords, account numbers, or other pertinent information which may have been written down.

If further assistance is needed, document existing conditions and call a Digital Forensics Unit analyst.

3.3 Laptop Computer

3.3.1. Laptops incorporate a computer, monitor, keyboard and mouse into a single portable unit.

3.3.2. Laptops differ from other computers in that they can be powered by electricity or battery source. Therefore, they require the removal of the battery in addition to standalone power-down procedures.

3.3.3. Procedures:

- Power down the laptop and remove the battery.
- If possible, remove the hard drive from the computer. If not, submit the entire laptop to the DFU.

3.4. Removable Storage Devices

3.4.1. Removable media devices used to store data that do not lose the information when the power is removed from the card. Removable media can store thousands of images and videos in a very small package. Removable media can be used in a variety of devices including computers, digital cameras, and mobile devices.

3.4.2 Examples: USB thumb drives, memory cards, CDs, DVDs, SD cards

3.4.3. Procedures:

- Search the scene for hidden or disguised removable media

3.5. Global Positioning Systems (GPS)

3.5.1. Global Positioning Systems may provide information on previous travel via destination information, way points, and routes. Some automatically store the previous destinations and include travel logs. Limited data can be obtained.

3.5.2. Procedures:

- Remove the SIM card if the device contains one
- Submit the entire device to the DFU

3.6. Internet of Things (IoT)

3.6.1. Any device, hardware, or gadget used to digitally record, detect, measure, transmit and / or receive data to a computer or network device.

3.6.2. Examples: webcam, digital home appliances, Alexa, Google Nest, Ring, and home automation device

3.6.3. Procedures:

- Determine the account information associated with the device
- Obtain a Preservation Order and a search warrant on the associated account

3.7. Smart Watches

3.7.1. A watch able to connect to a cellular device. They are able to store data associated with health, location, travel and more.

3.7.2. Examples: Apple watch, Samsung Galaxy watch, Fitbit

3.7.3. Currently the DFU does not have the capabilities to extract data from a smart watch but may gain the capability in the near future.

3.8. Cryptocurrency

3.8.1. Digital or virtual currency that is secured by cryptography. Cryptocurrency does not have a central issuing or regulating authority, so it does not rely on banks. This allows anyone anywhere to send and receive payments around the world. There are many different types of cryptocurrency including Bitcoin and Ethereum.

3.8.2. Cryptocurrency Wallet: An application that stores different types of cryptocurrencies.
These can be located on mobile devices or external drives. All have muti-factor authentication.

3.8.3. Seed Words: Typically 12 or 24 randomly selected, unique words in a particular order used to recover a wallet if the password is forgotten.

3.8.4. Procedures:

- Search the scene for a possible seed word list.
- Contact the digital forensic unit in your area.

3.9. Peripheral Equipment

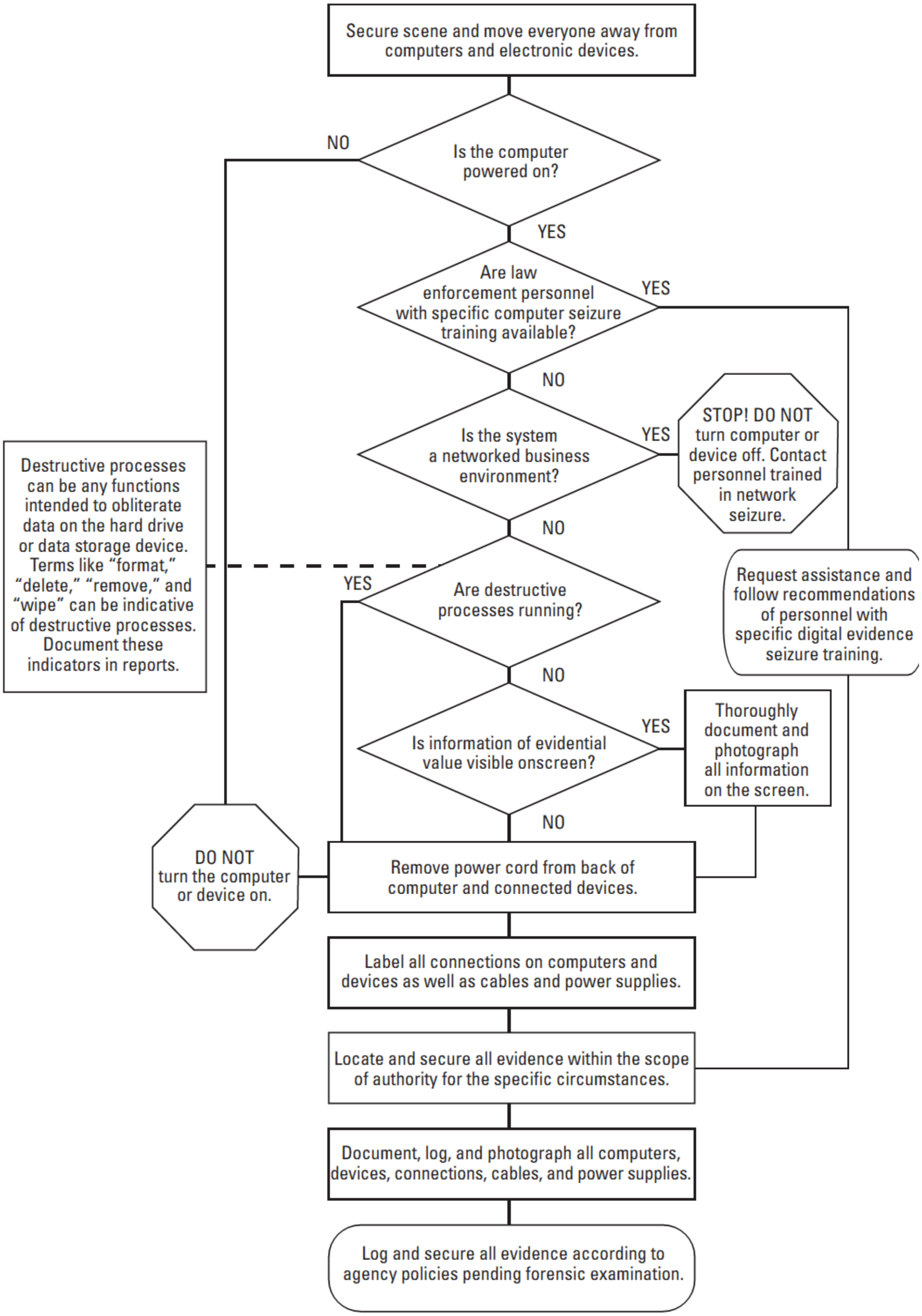
3.9.1. The following electronics **do not** need to be collected, as they do not have the ability to store data and do not have evidentiary value:

- Printers, scanners, monitors, keyboards, computer mice, fax machines, copiers

3.9.2. The following equipment may store data, but is encrypted and unable to be extracted, therefore has no evidentiary value:

- Gaming systems such as the Nintendo switch, PlayStation, Xbox

Collecting Digital Evidence Flow Chart


Secure scene and move everyone away from computers and electronic devices.
Is the computer powered on?
NO
YES
Are law enforcement personnel with specific computer seizure training available?
YES
NO
Is the system a networked business environment?
YES
STOP! DO NOT turn computer or device off. Contact personnel trained in network seizure.
NO
Destructive processes can be any functions intended to obliterate data on the hard drive or data storage device. Terms like “format,” “delete,” “remove,” and “wipe” can be indicative of destructive processes. Document these indicators in reports.
Are destructive processes running?
YES
Request assistance and follow recommendations of personnel with specific digital evidence seizure training.
NO
Is information of evidential value visible onscreen?
YES
Thoroughly document and photograph all information on the screen.
NO
DO NOT turn the computer or device on.
Remove power cord from back of computer and connected devices.
Label all connections on computers and devices as well as cables and power supplies.
Locate and secure all evidence within the scope of authority for the specific circumstances.
Document, log, and photograph all computers, devices, connections, cables, and power supplies.
Log and secure all evidence according to agency policies pending forensic examination.

4. Packaging, Transportation, Storage and Submission

4.1. Principle

Actions taken should not add, modify, or destroy data stored on a computer or other media. Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, and magnetic sources. Therefore, special precautions should be taken when packaging, transporting, and storing electronic evidence. To maintain chain of custody of electronic evidence, document its packaging, transportation, and storage.

4.2. Packaging of Evidence

4.2.1 Procedures:

- Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packaging.
- Pay special attention to latent or trace evidence and take actions to preserve it.
- Pack magnetic media in antistatic packaging (paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags.
- Avoid folding, bending, or scratching computer media such as diskettes, CD ROMs, and tapes.
- Ensure that all containers used to hold evidence are properly labeled.

4.2.2. If multiple computer systems are collected, label each system so that it can be reassembled as found (e.g., System A–mouse, keyboard, monitor, main base unit; System B–mouse, keyboard, monitor, main base unit).

4.3. Transportation of Evidence

4.3.1. Procedures:

- Keep electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.

- Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers may be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt.
- Maintain the chain of custody on all evidence transported.

4.4. Storage of Evidence

4.4.1. Procedures:

- Ensure that evidence is inventoried in accordance with department policies.

- Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants.

4.4.2. Be aware that evidence such as dates, times, systems configurations, and third-party applications, such as SnapChat, may be lost as a result of prolonged storage or when the device powers off. DFU analysts should be informed if a device powered by batteries needs immediate attention.

4.5. Submission of Evidence

4.5.1 Procedures**:**

- Complete a Forensic Laboratory Case Submission Form, WVSP-53.

- Remove all internal hard drives from the computer. DFU Laboratory will not accept complete desktop computers unless special circumstances exist such as the system running a RAID array and / or encryption. The hard drive(s) need to be removed from the desktop computer before submission. Laptops will be accepted.

- Mobile phones should be placed in airplane mode if possible. The SIM card can be removed to isolate the device from the cellular networks. **Always** ask the owner of the device for a passcode for the device. The DFU has the capability to bypass security measures; however, this does not guarantee access to the device.
- List, on a separate sheet of paper, a brief description of the case, evidence sought, and a list of keyword search terms relative to the case if appropriate. Names, aliases, dates of birth, social security numbers, screen names, e-mail addresses, and any other pertinent information should be included. Providing this

information will limit the amount of research time by the analyst prior to data acquisition.

- Package all digital/electronic media securely to prevent the media from moving around during transit.

4.5.2. Digital evidence should be submitted in a timely manner with consideration of the amount of time a digital acquisition, examination takes. A quicker examination may be conducted if sufficient supplemental information regarding images used for identification, suspect information, and possible passwords are provided when submitted.

4.5.3. Evidence presenting a biohazard or potential drug exposure should be identified with the appropriate label and noted on the Case Submission Form.

4.5.4. If you should need guidance in removing hard drives from a desktop or laptop computer, contact a digital forensics analyst.

4.6. Disposition of Evidence

Most evidence will be returned via certified U.S. Mail. Large or multiple items must be picked up from the laboratory if too awkward to mail.

This manual was developed by the West Virginia State Police Forensic Laboratory for use by the Digital Forensics Unit and will serve to inform employees and customers of the guidelines and measures used by the DFU to produce a quality product. In the event of a conflict or discrepancy between this manual and the West Virginia State Police Operational Policy and Procedures Manual or the WVSPFL Quality Assurance and Procedures Manual, the Operational and Procedures Manual and/or Quality Assurance and Procedures Manual will take precedence in resolving all issues; otherwise, the guidelines, regulations and procedures contained within this manual are to be followed until such time as they are amended or rescinded.

Appendix A

Sample cell phone search warrant language (Property To Be Seized): (Example)

“Included further for seizure and subsequent forensic analysis are any electronic communications devices designed for use on any cellular and / or other wireless networks, otherwise known as smartphones, cellular telephones, and tablet computers. Also included is any digital and / or electronic device(s) contained within any of the digital device items described in this application and search warrant. These items may include any and all SIM cards (Subscriber Identity Modules), digital media cards, embedded memory chips contained within the digital devices, or other digital storage media used with the above-described electronic devices. It should be further known that some forensic techniques to acquire the data contained within a smartphone, cell phone, or any digital device may require disassembly, soldering, and the application of heat to remove components and / or memory chips. These techniques can render a digital device inoperable and may effectively destroy the device. All non-invasive and non-damaging method would be attempted first.”

ISP Preservation Order

1. Consider doing a preservation request to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Many cellular communication carriers maintain records for only a very short period of time and have different data retention policies. This requests that can be used as a directive to third-party providers to preserve records and not disclose the investigation to the suspect. This is an important tool to use to prevent third-party providers from writing over or deleting data you need while you obtain a warrant. No laws govern how long a third-party provider must retain log or other information. Many deal with such a large volume of data that they routinely overwrite it every few days.

2. Make contact with the cellular service provider to ascertain the type and nature of records kept and any special terms or definitions that that carrier uses to describe those records.

(Example)

Facebook
Attention: Legal Department
156 University Avenue
Palo Alto, California 94301

VIA FACSIMILE: (650) 644-3229

RE: Request for Preservation of Records and Other Evidence.

To Whom It May Concern:

My agency and I are conducting a criminal investigation into a felony committed in the state of West Virginia pursuant to Title 18, United States Code Section 2703(f), this letter is a formal request for the preservation of all records and other evidence in your possession regarding the following social networking user account pending further legal process:

URL to Facebook Profile:
Facebook User ID / Group ID:
Displayed Name:
Displayed Hometown:
Displayed Email Addresses:
Displayed High School:

You are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession, including records stored on backup media, in a form that includes the complete record.
You are also requested not to disclose the existence of this request to the subscriber or any other person, or terminate service to the accounts described below, other than as necessary to comply with this request.

If compliance with this request may result in a permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me as soon as possible and before taking any such actions.

This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.

This preservation request applies to the following records and evidence:

A. All stored electronic communications and other files reflecting final or draft communications to, from, or within the requested account.

B. All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the requested account including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identity, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form; and

C. All connection logs and records of user activity for the requested account, including:

Connection date and time;
Disconnect date and time;
Method of connection (e.g., telnet, ftp, http);
Type of connection (e.g., dial-up modem, cable, DSL, T1);
Data transfer volume;
User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
Telephone caller identification records; and
Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.

D. Any other records and other evidence relating to the requested account. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through the requested account, whether such records or other evidence are in electronic or other form.

E. Specifically requested to preserved the following feed comment link information found at:

Thank you for your cooperation in this matter, if you have any questions, please feel free to contact me at the above listed telephone numbers or by e-mail at Robert.j.boggs@wvsp.gov

Sincerely,

Appendix B
When Describing Information Needed from Internet Service Provider for Cell Phone Triangulation

(Example)

Phone make/model and serial number, IMEI, ICCID:

Dates specifically requested are XXXX to XXXX.

Request all usage records including, but not limited to, amount of cellular data transferred to and from the device, IP connection logs including dates, times, and duration. Also request specific dates and times of the cellular data transfers.

-Devices used – ICCID and IMEI numbers and activation date(s) and retailer details.
-In-coming and out-going call detail records.
-In-coming and out-going cell tower records.
-Any data communications or access.
-Cell tower location, type (Lucent or Nortel), sector layout, and possible ranges.
-Beginning and terminating cell sites.
-Tower sector azimuths (center of sector) and beam widths (widths / degree of sector)
-Any cloud storage services and access to contents.
-In-coming and out-going text messages (SMS/MMS).
-Legend information – a definition of terms, codes, and abbreviations (explanation of cell tower layout and records).