Massachusetts Digital Evidence Consortium

Digital Evidence Guide for First Responders

January 2013

A Note to the Reader

There are an unlimited number of legal and technical variables in any criminal investigation involving digital evidence that will determine the appropriate course of action in a particular case. This guide is intended to serve as a basic educational resource for law enforcement officers encountering digital evidence in criminal investigations. This guide does not and should not be interpreted as a policy or legal document. Law enforcement agents seizing digital evidence should contact their local prosecutor or agency counsel with requests for legal guidance. Within this guide you will find forms frequently used in the collection of digital evidence. These forms are designed for you to photocopy to letterhead for ease of use.

Additional Assistance

If you need further assistance in the seizure of digital evidence, or you are in an emergency situation requiring immediate assistance, please contact the **Massachusetts State Police Communications Center at (508) 820-2121** and ask for the on-call contact from the Digital Evidence and Multimedia Section. The Digital Evidence and Multimedia Section contact will offer triage assistance or coordinate a response through a law enforcement officer assigned to a digital evidence laboratory, district attorney's office, or law enforcement council in the jurisdiction.

To speak to a representative from a digital evidence laboratory in your jurisdiction, or to get access to additional cyber crime training materials, please visit the Office of the Attorney General's secure law enforcement training site at **www.maagocybercrime.org**.

Additional Digital Evidence First Responder Resources

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

National Institute of Justice:
Forensic Examination of Digital Evidence: A Guide for Law Enforcement
https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

National Institute of Justice:
Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition
https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

National Institute of Justice:
Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders
https://www.ncjrs.gov/pdffiles1/nij/227050.pdf

National Institute of Justice:
Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors
https://www.ncjrs.gov/pdffiles1/nij/211314.pdf

Department of Justice:
Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

Interview and Interrogation Questions for Crimes Involving Digital Evidence

Always obtain passwords and/or security codes for all pieces of digital evidence.

1. Where are the digital crime scenes? These crime scenes may include: (1) locations within the jurisdiction, like homes, where computers and other digital devices are located; (2) offices and business networks; and (3) third-party providers like internet or cellular service providers. The legal and technical considerations for digital evidence collection vary depending upon the type of crime scene.
2. Is there an ongoing risk of injury or loss to any person or property?
3. What is the motive for the offense? Determining motive will help the investigator locate essential witnesses and critical evidence.
4. What computers, mobile devices, digital media, or internet accounts do the victims, witnesses, and suspects use? How and where do these individuals access these systems and/or devices?
5. Is evidence of the crime also held by a third party internet, cellular, or remote computing service provider? If so, collection of the information may be subject to the provisions of federal and state statutes pertaining to law enforcement access to records and communications held by these providers. Preserve any records, communications, or subscriber information held by these providers using the freeze order in this Guide, then consult with legal counsel or your local prosecutor. To find appropriate law enforcement contacts at these companies, visit www.search.org/programs/hightech/isp/.

Interview and Interrogation Questions for Crimes Involving Digital Evidence

Alway obtain passwords and/or security codes for all pieces of digital evidence.

6. For computer systems, what is the name of each person who uses the computer? What are each users' account name(s), privileges, passwords, and usage habits?
7. For computer systems and mobile devices, what operating system is installed? What applications on the computer or mobile device relate to the current investigation?
8. Are there any data encryption, security, or backup applications installed on the device? What are the names of the applications, and passwords to bypass the security? Where is backup data saved? (ie. cloud account, removable media, computer system, etc.)
9. What internet-based (ie. social network, web, electronic mail, etc.) or cellular services or accounts do the witnesses and suspects in your case use? How are they accessed by the user? What are the user names and passwords? Does anyone else have access to or use these accounts?
10. Has the witness or suspect lost, lent out, allowed access to, or experienced problems with a device or computer that contains evidence? If the answer is yes, ask for a detailed explanation.

Frequently Seized Devices - Smartphones and Other Mobile Devices

BlackBerry Bold

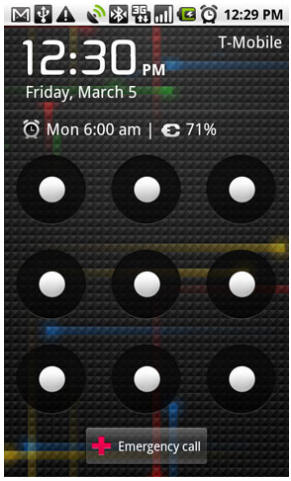
Step 1 - Document the device and all collection procedures and information

- Photograph
- Video
- Sketch
- Notes
- Chain of custody

Step 2 - Determine if the device is on or off

- Look for lights
- Listen for sounds
- Feel for vibrations or heat

NOTE - Many mobile devices save power by turning off screens after a specified amount of time. Despite the screen status, the device is likely still active. Ask if the device is currently powered on. Where legal, pressing the power button quickly will activate the screen.



Android unlock screen

Apple iPhone 5

Step 3 - If the device is off, **do not turn it on**

- Collect and package (**see Step 5**)
- Ask for password/pass pattern
- Transport (**see Step 6**)

Step 4 - If the device is on, proceed with caution

Samsung Galaxy Nexus

WARNING - The two most significant challenges for officers seizing mobile devices are: (1) isolating the device from cellular and Wi-Fi networks; and (2) obtaining security passwords or pass patterns for the device so the evidence can be examined forensically. Always ask if there is any security feature enabled on the phone. These can include passwords (simple or complex), security/wiping apps, pass patterns, or biometrics (facial scan). Document (see the attached consent form for guidance) and confirm the password or pass pattern.


Faraday Bag

Step 5 - Collection and Package

WARNING - You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from smartphones and mobile devices. Work with crime scene technicians or trained forensic personnel to preserve such evidence without disturbing the integrity of the data on the device. Be sure to advise forensic examiners in advance of submission of the possible existence of hazardous material on the device.

- Secure data and power cables
- Consider collecting computers that may contain device backups
- Package the device so it will not be physically damaged or deformed
- Package the device in evidence bags or boxes

Step 6 - Transport

- Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible
- Protect from temperature extremes and moisture

Frequently Seized Devices – Laptop and Desktop Computer Systems

Step 1 - Document the System

- Photograph
- Video
- Sketch
- Notes
- Chain of custody

Step 2 - Determine if the system is on or off

- Apply the "Look, Listen, and Feel" test
- Look for flashing lights, listen for sounds, and feel for heat or vibrations

Step 3 - If the system is off, do not turn it on

- Disassemble (see Step 5)
- Transport (see Step 6)

Step 4 – If the system is on, proceed with **CAUTION**

- Do not type, click the mouse, or explore files or directories without advanced training or expert consultation

- Ask about passwords and/or encyption of the system
- Observe the screen, and look for any running programs that indicate access to internet-based accounts, open files, encryption, or the presence of files or data of potential evidentiary value
- If you see anything on the screen that concerns you or needs to be preserved, consult with an expert (if you don't know who to contact, call the number on the inside cover of this manual)
- Photograph the screen
- Once you are prepared to power down the system, pull the plug from the back of the computer system
- Remove the battery from a laptop system

Step 5 – Disassemble and package the system

WARNING – You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from computer systems, digital devices, and electronic media. Work with crime scene service technicians or trained forensic personnel to preserve such evidence without disturbing the integrity of the digital media.

- Photograph the system from all perspectives
- Clearly mark evidence and document chain of custody, location, and other important details about the seized item(s)
- Disconnect and secure cables
- Check media ports and cd/dvd trays for the presence of removable media
- Package the system, and peripheral devices, for transport using laptop bags (if applicable), boxes, or evidence bags

Step 6 – Transport

- Protect from temperature extremes and moisture
- Do not place evidence in the cruiser's trunk
- Protect from electro-static discharge
- Package evidence so it will not be physically damaged or deformed
- Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as practicable

Other Commonly Seized Devices That May Store Digital Evidence

There are many other storage media and technical devices that may process and store digital evidence. Examples of these devices include media cards (ie. secure digital, SIM, flash, memory sticks), thumb drives, optical media (ie. CD, DVD, and Blu-ray), digital cameras, MP3 players, iPods, servers, surveillance systems, gaming stations (ie. Xbox, PlayStation, Wii), and GPS devices.

MicroSD Card


Blu-ray Disc

Each of these devices is capable of holding significant digital evidence that will help your case. And each is handled in a separate way. Seizure of these items should be performed with special care. Consider working with an experienced digital evidence analyst to collect these items.

Step 1 - Document the device and all collection procedures and information

- Photograph
- Video
- Sketch
- Notes
- Chain of custody


Sony PlayStation 3

Step 2 - For items that have power, determine if the device is on or off

- Look for lights
- Listen for sounds
- Feel for vibrations or heat


USB drive

Step 3 - Ask if there are any security features enabled on the device including passwords or encrypted file protection.

Step 4 - If the device is off, **do not turn it on**

- Collect and package (**see Step 6**)
- Transport (**see Step 7**)

Step 5 - While assessing, collecting, packaging, and transporting, follow these device-specific rules

- Only trained personnel should collect data from a server. If you don't know what you are doing, stop and call an expert. Be careful when asking for the assistance of information technology or other personnel on-site

Garmin GPS

- **GPS devices**, **MP3 players**, and **digital cameras** should be turned off to secure data. Be sure to ask for any passwords or security features
- If available, paper evidence bags, or static-free evidence bags, are best for the storage of media
- Media contained in binders or carriers should remain in the container
- Be careful not to scratch optical media during seizure.
- Gaming stations should be seized in the same manner as computers

WARNING - Collecting evidence from surveillance systems can be difficult. Time is of the essence as digital surveillance systems often have proprietary software and hardware needs for playback. Speak to your prosecutor or agency legal counsel when making a decision about the seizure of a digital surveillance system as opposed to footage or segments of video extracted from the system. Also, be sure to get the company and installer name and contact information for the person that installed or maintains the system.

Step 6 - Collection and Package

- Follow chain-of-custody procedures
- Secure data and power cables
- Label the evidence container(s), <u>not</u> the device(s)
- Package the device so it will not be physically damaged or deformed
- Package the device in evidence bags or boxes


Microsoft Xbox 360

Step 7 - Transport

- Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as practicable
- Protect from temperature extremes and moisture

DEMAND FOR THE PRESERVATION OF RECORDS PURSUANT TO 18 U.S.C. § 2703(f)

ATTENTION: KEEPER OF RECORDS
PROVIDER: _____
DATE: _____
FAX: _____

Dear Sir or Madam:

Please be advised that this agency is conducting an official criminal investigation that involves the below listed account. We are in the process of reviewing the investigation to obtain a search warrant, grand jury subpoena, or other applicable court order to obtain information believed to be in your possession. As I am sure you are aware, 18 U.S.C. § 2703(f), titled "Requirement to Preserve Evidence," provides:

"(1) In general - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewed request by the governmental entity."

As such, we are requesting that your office take steps to immediately preserve any and all information in your custody related to the account below, including but not limited to, subscriber information, transactional records, service history, payment records, login and logout records, and account content for the user or subscriber:

_____

Because this is a criminal investigation, we are requesting that neither you nor your office disclose the fact or the existence of our request, the investigation, and/or any compliance or action made with respect thereto. I thank you in advance for your attention to this matter. Should you have any question, please do not hesitate to contact me using the contact information below.

Sincerely yours,

_____

Contact Name: _____

Agency: _____

Phone: _____

Email: _____

I, _____, (DOB ____ / ____ / ____), hereby authorize _____ _____, an officer with the _____, or any other law enforcement officer or digital evidence analyst working with the aforementioned officer, to take custody of, copy, and analyze the items detailed below for evidence. I understand that copies of the contents of the items, including all files and data, may be created and retained for analysis. I also understand that the analysis of the copies of the media may continue even after the items designated for analysis are returned. I provide my consent to this analysis freely, willingly, and voluntarily, and with the knowledge that I have the right to refuse to consent. I provide my consent without fear, threat, coercion, or promise of any kind.

Make	Model	Serial Number	Owner/User(s)

Notes

Computer/Device Security	
Password Type (Device, Acct, Etc.): _____	Pass Pattern (Use Arrows for Direction)
Password Type (Device, Acct, Etc.): _____	

Printed Name	Signature
Witness 1 Name	Signature
Witness 2 Name	Signature

Members of the MDEC Executive Board represent the following agencies

Officer Safety Is Top Priority

Do…

Make sure you are lawfully present and have appropriate legal authority to conduct the search.

Secure the scene.

Make sketches and/or take photos.

Consult technical experts as needed.

Use seizure form if collecting digital evidence.

Do Not…

Turn on computers or other digital devices.

Touch a computer if it is 'on' unless you are properly trained.

Allow anyone access to computers or other digital devices.