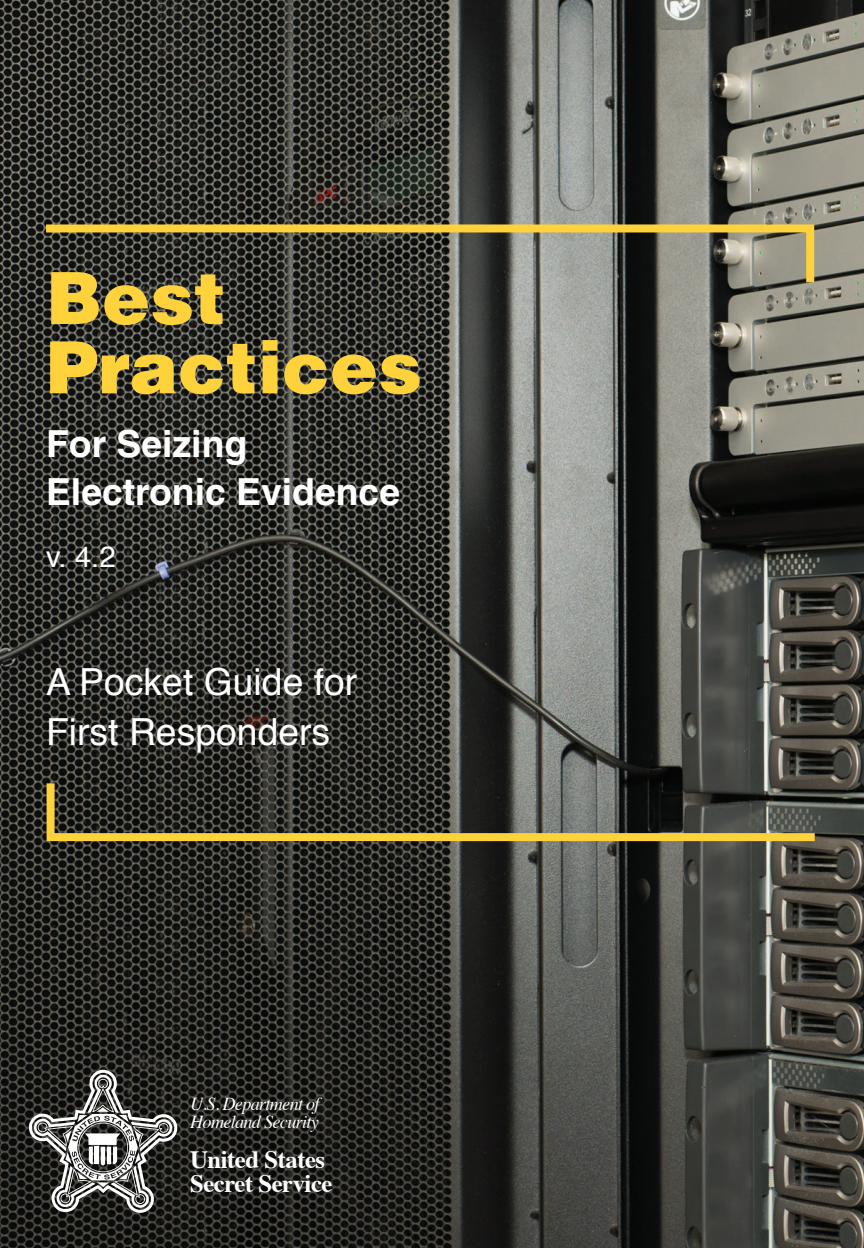


Best Practices

For Seizing Electronic Evidence

v. 4.2

A Pocket Guide for First Responders

U.S. Department of Homeland Security

United States Secret Service

TABLE OF CONTENTS

INTRODUCTION

This fourth edition of the Best Practices for Seizing Electronic Evidence was updated as a project of the United States Secret Service and participating law enforcement agencies. A working group of various law enforcement agencies was convened to identify common issues encountered in today's electronic crime scenes. Representatives from the following agencies contributed to the creation of this manual:

Hoover Police Department, Alabama
Los Angeles Police Department, California
Los Angeles County Sheriff's Department, California
Los Angeles County District Attorney's Office - Bureau of Investigations, California
Santa Monica Police Department, California
Beverly Hills Police Department, California
California Highway Patrol, California
United States Secret Service

For additional copies, please contact the local office of the United States Secret Service. The committee wishes to thank those departments and agencies who provided their personnel and resources in support of the publication of this guide.

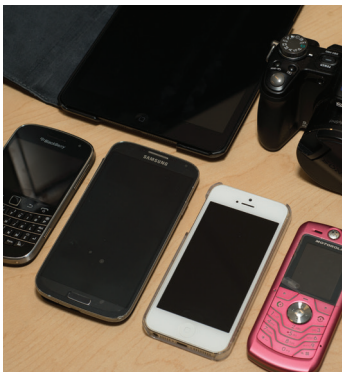
OFFICER SAFETY

The safety of the officer is paramount in the investigation of any crime. Always ensure that the appropriate personal protective equipment is used. Today, virtually every crime has an electronic component in terms of computers and electronic technology being used to facilitate the crime. Computers used in crimes may contain a host of evidence related to the crime being investigated, whether it is a conventional crime or a terrorist act. In light of this, law enforcement officers and investigators should not become complacent with individuals or their environment simply because the crime may involve a computer.

During the investigation of electronic crimes or the seizure of computers and electronic items, be aware that as in any other crime, unexpected changes to a subject's involvement in a case may occur resulting in unexpected individual and environmental threats to an officer's safety. For this reason, the first responder should immediately take all reasonable steps to ensure the safety of all persons, including fellow investigators and suspects at the crime scene.

After all safety procedures are followed, it is then the responder's responsibility to ensure the integrity of the crime scene and any potential evidence.

In today's society, people utilize various computers, electronic devices, and other electronic media in numerous aspects of their lives. Criminals also use these same devices in the facilitation of their unlawful activities. Current technology permits criminals to commit crimes internationally and remotely with near anonymity. Instant communication and electronic mail provides a venue for communication between criminals as well as victims. As such, computers and other electronic media can be used to commit crimes, store evidence of crimes, and provide information on suspects and victims. This field guide is designed to assist the patrol officer, detective, and investigator in recognizing how computers and electronic devices may be used as an instrument of a crime or as a storage device for evidence in a host of federal and state crimes. It will also assist these individuals in properly securing evidence and transporting it for examination at a later time by a Computer Forensic Examiner/Analyst. We recommend that the patrol officer, detective, and investigator consult and seek assistance from their agency's resources or other agencies that seize electronic media. This may include your local District Attorney, State Prosecutor, U.S. Attorney or Assistant United States Attorney.



This guide assumes that the patrol officer, detective or investigator is legally present at a crime scene or other location and has the legal authority to seize the computer, hardware, software or electronic media.

If you have a reason to believe that you are not legally present at the location or the individual (suspect or victim) does not have the legal ability to grant consent, then immediately contact the appropriate legal counsel in your jurisdiction.

PLAIN VIEW
The plain view exception to the warrant requirement only gives the legal authority to **SEIZE** a computer, hardware, software and electronic media, but does **NOT** give the legal authority to conduct a **SEARCH** of this same listed electronic media.

CONSENT
When obtaining consent, be certain that your document has language specific to both the seizure and the future forensic examination of the computer hardware, software, electronic media and data by a trained Computer Forensic Examiner/Analyst.

If your department or agency has a consent form relevant to computer or electronic media and its analysis by a Computer Forensic Examiner/Analyst, it should be used. If you do not have a form and are drafting a consent form, consult with your District Attorney, State Prosecutor, U.S. Attorney or Assistant United States Attorney for advice regarding proper language and documentation.

SEARCH WARRANT
Search warrants allow for the search and seizure of electronic evidence as predefined under the warrant. This method is the most preferred and is consistently met with the least resistance both at the scene and in a court of law. When drafting the search warrant, be certain that the document includes language specific to both the SEIZURE and SEARCH (forensic examination) of the computer hardware, software, electronic media, documentation, and user notes.

AUTHORITY FOR SEIZING EVIDENCE: CONSIDERATIONS

Role of the computer
The search warrant should state the computer's role in the crime and why it will contain evidence.

Nexus
Establish why you expect to find electronic evidence at the search location.

Specify evidence sought
Specifically describe the evidence you have probable cause to search for and any evidence of ownership of the computer.

Boiler plate language
Adapt all search language to the specific facts of your case. Avoid using boilerplate language.

Location of search
Is it practical or safe to conduct a search of the computers and electronic media on site? Consider the vast storage capacities of consumer hard disk drives that were only available commercially not too long ago. It is not uncommon for computer forensic examinations to take many hours, or in some cases days.

Non-Disclosure
May be necessary to protect informants or to prevent the disclosure of trade secrets/intellectual property.

Special Master
Special legal considerations should be given to investigations involving doctors, attorneys, spouses, publishers, clergy, etc.

CONSENT TO SEARCH ELECTRONIC MEDIA

The following is a general reference guideline for consent forms pertaining to computers and electronic media. Consult your District Attorney, U.S. Attorney or Assistant U.S. Attorney regarding consent language applicable to your jurisdiction.

I, _____, have been asked to give my consent to the search of my computer/electronic equipment. I have also been informed of my right to refuse to consent to such a search.

I hereby authorize _____ to conduct a complete search of all computer/electronic equipment located at _____ _____. These officers/agents (and any other person(s) designated to assist, including but not limited to computer forensic examiners/analysts) are authorized by me to take from the above location(s), any computers, including internal/external hard disk drives, compact discs (CDs), digital video discs (DVDs), USB drives, scanners, printers, other computer/electronic hardware or software and related manuals, and any other electronic storage devices, including but not limited to, cellular/mobile telephones and electronic pagers, and any other electronic equipment capable of storing, retrieving, and/or accessing data. I hereby consent to a complete search of those items by these personnel for any data or material that is contraband or evidence of any crime. I understand that this contraband or evidence may be used against me in a court of law. I give this written permission voluntarily. I have not been threatened, placed under duress or promised anything in exchange for my consent. I have read this form or it has been read to me and I understand it. I understand the _____ language and have been able to communicate with the agents/officers.

I understand that I may withdraw my consent at any time for any reason. I may also ask for a receipt for all things taken.

Signed: _____
Signature of Witnesses: _____
_____
Date and Time: _____

There are general principles to follow when responding to any crime scene in which computers and electronic technology may be involved. Several of those principles and considerations are as follows:

Whenever possible, it is best to have a trained Computer Forensic Examiner/Analyst collect electronic evidence.

Do you have a legal basis to seize the computer (plain view, search warrant, consent, etc.)?

If you have reason to believe that the computer is involved in the crime you are investigating, take immediate steps to preserve the evidence.

If the computer is OFF, leave it OFF. Do NOT power it on to begin searching through the computer.

If the computer is ON, and a properly trained Computer Forensic Examiner/Analyst is not available, go to the appropriate section in this guide on how to properly secure the computer and preserve evidence.

If you reasonably believe that the computer is destroying evidence, immediately shut down the computer by pulling the power cord from the back of the computer.

In all instances, document the location and state of the computer to include attached electronic media.

In all instances, take photographs of the computer, the location of the computer, and any electronic media attached. If the computer is on and the screen is blank, move the mouse or press the space bar (this will display the active image on the screen), then photograph the screen.

Do special legal considerations apply (doctor, attorney, clergy, psychiatrist, newspapers, publishers, etc.)?

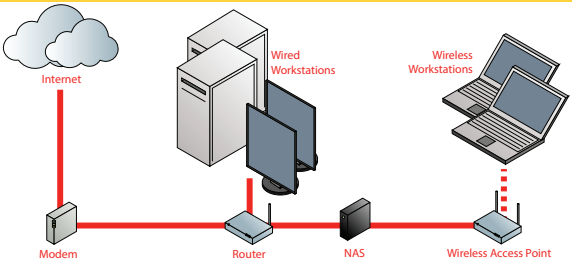
HOME PERSONAL COMPUTER OR LAPTOP COMPUTER

For proper evidence preservation, follow these procedures in order:

- Do not use the computer or attempt to search for evidence.
- Photograph the surrounding area prior to moving any evidence.
- Photograph the front and back of the computer and diagram/label cords and connected devices.
- If the computer is OFF, leave it OFF.
- If the computer is on and something is displayed on the monitor, photograph the screen.
- If the computer is on and the screen is blank, move the mouse or press the space bar (this will display the active image on the screen). After the image appears, photograph the screen.
- If the computer is on and a Computer Forensic Examiner/Analyst is available, consider conducting a volatile memory (RAM) acquisition to capture the data that may be lost when powered off.
- If the computer is on and networked (attached to a network device such as a router and/or modem) and a Computer Forensic Examiner/Analyst is available consider capturing the volatile network information (IP addresses, open ports, active network connections) and network logs if applicable.
- If networked, unplug the power to the network device(s), and record the MAC address(es) from the device(s).
- If a Computer Forensic Examiner/Analyst is unavailable, unplug the power cord from the back of computer.
- If the laptop computer does not shutdown when the power cord is removed, locate and remove the battery.
- The laptop computer battery is commonly located on the bottom and there is usually a button or switch that allows for the removal of the battery.*
- If the laptop computer battery cannot be removed (Apple MacBooks, etc.), shut down the computer as normal.*

**It is important to note that laptop computers often have wireless communication capabilities and could potentially be manipulated by the owner if it has power and the ability to receive a wireless signal. Consider using a faraday bag or similar to block communication to the laptop computer.*

- If the laptop computer battery is removed, do not return it to the battery compartment.
- Disconnect all cords and devices from the computer.
- Package components and transport/store as fragile cargo.
- Seize additional electronic storage media (see electronic storage media section).
- Keep all computers and electronic storage media away from magnets, radio transmitters (such as police radios - portable or vehicle based) and other potentially damaging elements.
- Collect instruction manuals, documentation, and notes (notes may contain passwords).
- Document all steps involved in the seizure of the computer and components.
- See section on important investigative questions.



As seen in this diagram, a home network is often comprised of a modem, router, desktop or laptop computers, and possibly network attached storage (NAS). The home network typically shares a single internet connection, such as DSL, cable, fiber-optic, or dial-up. A home network also allows multiple users to share information with other computers or devices on the network.

Special Consideration in Seizing Networked Devices

When confronting a home network, consideration should be given to collecting the volatile network information (IP addresses, open ports, active network connections, etc.) by a trained first responder or Computer Forensic Examiner/Analyst. The identification of open ports or connections to other computers may identify remote storage devices, applications used to facilitate the crime, or other persons involved in the crime. Remote storage devices or shared network drives may store additional electronic evidence. Active network connections may also indicate whether someone is exercising external control over the computer(s). If you are unable to collect this information, contact someone who is familiar with networks before disconnecting the network connection. To disconnect the computer(s) from the home network, disconnect the power source from the modem and router.

In many instances home networks are connected via wireless access points, which can be easily hidden. When conducting the search, first responders should locate the router, and trace all cables running from it to determine if they are connected to other network devices (such as a wireless access point) possibly hidden in other parts of the building. Most home network routers also serve as a wireless access point. Also consider wireless access points not physically at the target location, such as a neighbor's unsecured wireless network used by the suspect. Consider scanning for the presence of wireless access points and document the findings.

Increasingly, many home networks also serve as small offices or businesses. When confronting these types of home networks, you should contact a network specialist such as a Computer Forensic Examiner/Analyst and have him or her present or be readily available to provide assistance with seizing the computer and digital evidence.

NETWORK SERVER/BUSINESS NETWORK

Whenever possible, have a Computer Forensic Examiner/Analyst conduct a volatile memory (RAM) acquisition to capture the live data that may be lost when powered off. Unless the servers or computers on the business network are NOT able to be properly shut down and safely moved, the examination of network servers or business networks should ONLY be attempted by a Computer Forensic Examiner/Analyst.

DO NOT DISCONNECT THE POWER CORD

Pulling the plug could:

- Severely damage the system
- Disrupt legitimate business
- Create officer/investigator and department liability

When dealing with network or business servers, the first responder should determine who is responsible for maintaining the computer network. If possible, establish contact with the information technology (IT) personnel familiar with the system and direct him/her to gather the data the investigator believes is of evidentiary value.

ELECTRONIC STORAGE MEDIA

Electronic storage media is used to store data from electronic devices. Electronic storage media can take many forms to include: Internal and external hard disk drives (HDDs) and solid state drives (SSDs), USB thumb drives, CD's, DVD's, Blu-Ray discs, memory cards, and floppy disks (less common). These items vary in storage capacity and could contain a vast amount of data.

When seizing electronic storage media, collect the instruction manuals, documentation, and any notes. Remember to document all steps involved in the seizure of electronic storage media.

SPECIAL CONSIDERATIONS FOR FIRST RESPONDERS

Volatile Data

If a Computer Forensic Examiner/Analyst is available, consideration should be given to capturing volatile memory (RAM) on live computers to preserve the data that may be lost when powered off.

Encryption

If a Computer Forensic Examiner/Analyst is available, consideration should be given to checking if encryption is present on live computers found by first responders. Powering off computers using full disk encryption and/or individual file encryption could make the data extremely difficult or unlikely to be recovered. Consideration should be given to live imaging the computer(s) by a Computer Forensic Examiner/Analyst if encryption is present.

MOBILE PHONES, SMART PHONES, TABLETS, AND GPS UNITS (MOBILE DEVICES)

"Mobile Devices" such as tablets, mobile (cellular) phones, smart phones, and GPS units may store data directly to internal memory or may contain removable storage media.

The following section details the proper seizure and preservation of these devices and associated removable storage media. If possible, have a properly trained Mobile Device Examiner/Analyst conduct an immediate examination of the device. If a Mobile Device Examiner/Analyst is unavailable, follow these steps for each respective device.

Regardless of the type of device encountered, a few universal steps should always be followed:

- Prevent the device from communicating to any network or receiving any wireless communications.
- Photograph the device and screen display (if possible).
- Label and collect all cables (to include power supply) and transport with the device.
- Keep the device charged.
- If keeping the device charged is not possible, examination by a Mobile Device Examiner/Analyst should be completed prior to battery discharge or data may be lost.
- Seize additional electronic storage media (memory cards, etc.).
- Document all steps involved in the seizure of the device and associated components.
- Secure and protect the device from tampering or damage.

Mobile Phones, Smart Phones, Tablets, and GPS Units.

Device is OFF:

- Do not power the device on. Look for any SIM card slots, if found, remove the SIM card. This prevents contact with the cellular network on a GSM (AT&T, T-Mobile, etc.) only device.*
- If possible, remove the battery.
- If possible, store the device in a Radio Frequency (RF) shielded enclosure (such as a Faraday bag or Ramsey Shielded Enclosure) to block connectivity to cellular, Wi-Fi, GPS, Bluetooth, or other wireless signals.*

** Even if the device is powered off, an alarm may cause the device to "wake up" and power back on.*

Device is ON:

- Locate and remove any SIM cards (if applicable), and place the device in "Airplane" mode (usually found in "Settings").
- If the device has an Apple iOS operating system (iPhone, iPad, etc.) and the screen is locked with a passcode, you should be able to place it in Airplane mode by vertically swiping the screen and selecting the icon of an airplane. This option is only available on newer iPhones and iPads with updated operating systems.
- If the Apple device is unlocked and the previously mentioned option is unavailable, place it in Airplane mode by navigating to Settings and toggle Airplane mode.
- If the device has an Android operating system, it can usually be placed in Airplane mode even with a passcode or pattern lock enabled by holding down the power button and then selecting Airplane mode when prompted.
- If the Android device is unlocked, you can usually find Airplane mode under Settings.
- If the Android device is unlocked, place the device in "USB Debugging Mode" and "Stay Awake Mode" prior to powering the device off. This is done in case the device has passcode or pattern lock protection enabled. With these two modes enabled, most vendor solutions can still image a locked Android device.
- Once the above suggestions are followed (if applicable), power down the device and remove the battery if possible.*
- If possible, store the device in a Radio Frequency (RF) shielded enclosure (such as a Faraday bag or Ramsey Shielded Enclosure) to block connectivity to cellular, Wi-Fi, GPS, Bluetooth, or other wireless signals.*

** Even if the device is powered off, an alarm may cause the device to "wake up" and power back on.*

Although it is not a "forensically sound practice," if the device is unlocked and suspected to be passcode/pattern lock protected (and the passcode/pattern lock is unavailable) or may be encrypted (Blackberry (RIM), etc.), the first responder should consider making a cursory manual search of the device ONLY if the first responder has the legal authority to search the device. As always, document the steps taken and take photographs of the screen.

SPECIAL CONSIDERATION IN SEIZING MOBILE DEVICES

As there are many schools of thought in which to seize a device (keep it powered, turn it off, turn it off and remove the battery, keep it powered while in a faraday bag, etc.) one practice should be adhered to always – BLOCK COMMUNICATION BETWEEN THE DEVICE AND ITS HOST NETWORK(S). This can be accomplished by removing power from the device and/or by shielding it from radio frequencies/ Bluetooth/802.11 signals, etc.

There are two reasons why shielding is vital. There are several ways a suspect or accomplice can alter or destroy evidence on a device when it is out of their physical control. When a device connects to its host network, several items on the device can change as a matter of normal functionality or worst case scenario, the device could be remotely wiped by the owner or someone with access to that functionality.

Products are readily available from vendors designed to block that communication flow.

For further information on the matter, please contact the U.S. Secret Service Cell Phone Forensic Facility or the nearest U.S. Secret Service office.

OTHER DEVICES

Consideration should be given to other electronic devices capable of storing, transmitting, and/or receiving data. These devices include but are not limited to:

- Video gaming consoles/systems such as Xbox, PlayStation (PS3, PS2, PSP), etc.
- In-vehicle “Infotainment” systems, GPS units, MP3 players, movie players, etc.
- Surveillance systems with recording devices such as a digital video recorder (DVR).

The following crimes may involve the use of a computer or other electronic media; listed below are the crimes and potential evidence which may be recovered.

Computer Fraud Investigations:

- Account data from online auctions
- Accounting software and files
- Address books
- Calendar
- Chat Logs
- Customer information
- Credit card data
- Databases
- Digital camera software
- E-mail, notes and letters
- Financial and asset records

Child Abuse and Pornography Investigations:

- Chat logs
- Digital camera software
- E-mails, notes and letters
- Games
- Graphic editing and viewing software which classify images
- Images
- Internet activity logs
- Movie files
- User created directory and file names

Network Intrusion Investigations:

- Address books
- Configuration files
- E-mails, notes and letters
- Executable programs
- Internet activity logs usernames and passwords
- Malware
- Cache information
- Internet protocol address
- Website history
- Internet chat logs
- Source code
- Registry information
- Random Access Memory (RAM)
- Network connections

Homicide Investigations:

- Address books
- E-mails, notes and letters
- Financial asset records
- Internet activity logs
- Legal documents and wills
- Medical records
- Telephone records
- Diaries
- Maps
- Photos of victim/suspect
- Trophy photos

Domestic Violence Investigations:

- Address books
- Diaries
- E-mails, notes and letters
- Financial asset records
- Telephone records

Financial Fraud and Counterfeiting Investigations:

- Address books
- Calendar
- Currency images
- Check and money order images
- Customer information
- Databases
- E-mails, notes and letters
- False identification
- Financial asset records
- Images of signatures
- Internet activity logs
- On-line banking software
- Counterfeit currency images
- Bank logs
- Credit card numbers

E-Mail Threats, Harassment and Stalking Investigations:

- Address books
- Diaries
- E-mails, notes and letters
- Financial asset records
- Images
- Internet activity logs
- Legal documents
- Telephone records
- Victim background research
- Maps to victim locations

Narcotics Investigations:

- Address books
- Calendar
- Databases
- Drug recipes
- E-mails, notes and letters
- False ID
- Financial asset records
- Internet activity logs
- Prescription form images

Software Piracy Investigations:

- Chat logs
- Torrents
- Video and audio files
- E-mails, notes and letters
- Image files of software certificates
- Internet activity logs which classify copyrighted software
- Software serial numbers
- File sharing web sites
- Contains copyrighted media
- Software cracking utilities
- User created directories and file names

Telecommunication Fraud Investigations:

- Cloning software
- Customer database records
- Electronic serial numbers
- Mobile identification numbers
- E-mails, notes, and letters
- Financial asset records
- Internet activity logs

Identity Theft Investigations:

- *Hardware and Software Tools*
- Backdrops
- Credit card reader / writer
- Embosser
- Scanner software

- *Internet Activity Related to ID Theft*
- E-mail and forum postings
- Deleted documents
- On-line orders
- On-line trading information
- Internet activity logs

- *Identification Templates*
- Birth certificates
- Check cashing cards
- Digital photo images
- Driver's licenses
- Electronic signatures
- Counterfeit vehicle registrations
- Counterfeit insurance documents
- Social security cards

- *Negotiable Instruments*
- Business checks
- Cashier's checks
- Credit card numbers
- Counterfeit court documents
- Counterfeit gift certificates
- Counterfeit loan documents
- Counterfeit sales receipts
- Money orders
- Personal checks

PURPOSE: This section provides assistance to the patrol officer, detective or investigator in identifying particular types of electronic crimes as well as providing general questions which should be asked during the initial phases of the investigation.

In conjunction with these investigative questions, the following information should be provided to assist in the forensic examination of the computers, mobile devices, or other electronic evidence:

- Case Summary - investigative reports, witness statements
- Key Word List - names, locations, identities, IP addresses, website names/ addresses, etc.
- True Names/Nicknames - all true names/nicknames used by suspect(s) or victim(s)
- Photographs - photographs of the suspect(s)
- Passwords - all passwords used by suspect(s) or victim(s)
- Points of Contact - name of investigator making request
- Supporting Documents - consent form, search warrant, etc.
- Type of Crime - provide specific information
- Evidence Handling - DNA or fingerprint sensitive?

General Investigative Questions that may be asked regarding a crime involving computers and electronic evidence are as follows:

- When and where was the computer obtained? Was it new or used?
- Who has access to the computer hardware and software?
- Where is the computer's electronic storage media (CD's, DVD's, thumb drives, etc.) stored?
- Whose fingerprints might be found on the computers and/or electronic media?
- If other people have access to the computer, hardware or software, can they access everything on the computer or only certain files, folders or programs?
- How many people use the computer? Who are they?
- What is the level of computer experience of each computer user?
- What times of the day do the individual users have access to the computer?
- What programs are used by each computer user?
- Does the computer require a user name and password? What are they?
- Is there any software that requires a username or password?
- How does the computer have access to the internet (DSL, Cable, Fiber-Optic, Dial-Up, etc.)?
- Does the victim or suspect have an e-mail account? Who is the service provider (Yahoo, Gmail, Hotmail, etc.)?
- Which e-mail client (program) does the suspect or victim use?
- If e-mails are involved in the case, ask the victim and suspect for their e-mail addresses.

- Does the victim or suspect remotely access their computer (can they get into their computer when away from the office or home)?
- Do any of the users use online or remote storage? Online backup?
- Have any programs been used to "clean" the computer?
- Does the computer contain encryption software or hard drive wiping utilities?
- Is the computer always on?

Electronic Crime Specific Questions target specific offenses and are as follows:

Identity Theft/Financial Crimes:

Victim Questions:
- Are you aware of any unusual activity on any of your accounts?
- What accounts have been compromised?
- Have you provided any personal information to any organization or individual?
- For what purpose was that information provided?
- Have you recently completed any credit applications or loan documents?
- Do you maintain any of your personal information on your computer?
- Have any bills or other financial statements not regularly arrived via mail?
- Have you checked your credit reports?

Suspect/Target Questions:
- Where is your computer software (DVDs, CDs, thumb drives, etc.)?
- Does the computer contain any software for making checks or other financial documents?
- Does the computer contain any software to manipulate photographs?
- Does the computer contain any scanned or manipulated identification?
- Was the computer used to conduct any on-line purchases?
- Does the computer have any type of encryption software installed?

Internet Crimes Against Children (ICAC):

Victim Questions:
- Has the victim been online in any chat rooms?
- Does the victim use the internet, e-mail or chat from any other computers? If so, at what locations?
- Did the victim provide any information to anyone online regarding their true name, age and location?
- What is the victim's e-mail address or online chat room name?
- Who is on the victim's "buddy list" in chat rooms?
- Does the victim save/archive chat room logs?
- What type of chat/email client does the victim use?
- What were the specific sexual acts observed in the images or the electronic communications?
- Has the victim received any pictures or gifts from the suspect?

Suspect/Target Questions:

- Where are all of the suspect's computers?
- Does the suspect remotely store data (external hard drive, online storage, etc.)?
- What is the suspect's online identity or chat room name?
- Has the suspect electronically communicated with any person?
- How does the suspect communicate with other persons? (chat, emails, etc.)
- Has the suspect viewed any child pornography using the computer? If so, how did the suspect obtain the child pornography?
- Did the suspect send child pornography to any other person in the suspect's state or in another state?
- Did the suspect realize that they were viewing images of children as opposed to computer generated images of children?
- Does the computer have any type of encryption software installed?

Intrusions/Hacking: (Network Questions)

Home Networks

- Can you physically trace all of the network cables back to their respective computers?
- Can each computer be associated to an individual user?
- Is the network connected to the Internet?
- How is the network connected to the Internet (DSL, Cable, Fiber-Optic, etc.)?
- Where is the modem/router located? Is it currently connected?
- Who is the Internet service provider (ISP)?
- Is there more than one computer that can connect to the Internet?
- Is there any wireless networking in place?
- Do the computers have any type of encryption software installed?

Business Networks

- Who first observed the illegal activity?
- Obtain the type of illegal activity and contact information for all witnesses.
- Identify the network administrator and obtain contact information. (The network administrator should not be contacted by the first responder).
- Are any employees/former employees considered to be a suspect?
- Is there a printed diagram of the network available?
- Are computer logs being maintained?
- Can the computer logs be immediately secured for further investigation?
- Have any other law enforcement agencies been contacted?

Crimes Involving E-Mails:

Victim Questions:

- Identify victim e-mail addresses and Internet service provider (ISP) information.
- Identify all usernames and e-mail accounts used by the victim.
- Obtain any printed copies of e-mails that the victim has received. Do not turn on the computer to print e-mails.

Suspect/Target Questions:
- Identify suspect e-mail addresses and internet service provider (ISP) information.
- Identify all usernames and e-mail accounts used by the suspect.
- Obtain all passwords and associated software/usernames used by the suspect.
- Identify any type of encryption used.

Instant Messaging/Internet Chat Crimes

Victim Questions:
- Ask if the victim had logging or archiving activated during chat sessions.
- Identify the victim's online screen name and e-mail addresses.
- Obtain copies of any material the victim has already printed.
- What type of software/chat client is used by the victim?

Suspect/Target Questions:
- Identify the suspect's online screen name and e-mail addresses.
- Obtain all passwords and associated software/usernames used by the suspect.

BACKUP: A copy of information from a computer.

BOOT: To load the first piece of software to start a computer.

BYTE: A unit of data generally consisting of 8 bits.

KILOBYTE (KB): A Kilobyte is 1024 bytes.

MEGABYTE (MB): A Megabyte is 1024 Kilobytes.

GIGABYTE (GB): A Gigabyte is 1024 Megabytes.

TERABYTE (TB): A Terabyte is 1024 Gigabytes.

PETABYTE (PB): A Petabyte is 1024 Terabytes.

CD-R: Compact disc to which data can be written to but not erased.

CD-RW: Compact disc to which data can be written and erased.

CPU: Central processing unit. It is the "brain" that performs arithmetic, logic, and control functions.

DDOS: Distributed denial of service. An assault on a network that floods it with so many additional requests that regular traffic is slowed or completely interrupted.

DVD: Digital versatile disc or digital video disc. Similar in appearance to a compact disc, but can store larger amounts of data (typically a minimum of 4.7GB of data per single layer).

BLU-RAY: Optical disc storage medium. Designed to replace the DVD format with up to 25GB per single layer and 50GB per dual layered disk.

ENCRYPTION: The process of scrambling or encoding information in an effort to guarantee that only the intended user (or recipient in the case of communications) can read/view the information.

FIREWALL: A firewall allows or blocks traffic into and out of a network or computer. A firewall is a method for keeping computers secure from intruders.

HARD DISK DRIVE (HDD): Hard disk drives are found inside a computer and in portable external enclosures . They can store large amounts of data and contain internal moving parts. Popular types of hard disk drive interfaces are SATA, PATA (IDE) and SCSI.

HARDWARE: The physical parts of a computer that can be picked up.

ISP: Internet service provider. A company that sells access to the Internet via telephone line, cable line, or fiber-optic to your home or office.

MEMORY: The electronic holding place for instructions and data that a computer's microprocessor can reach quickly.

MODEM: A device that connects a computer to a data transmission line.

MONITOR: A device on which the computer displays visual information.

NETWORK ATTACHED STORAGE DEVICE (NAS): Storage device such as an external hard drive attached to a network, usually for shared data storage.

OPERATING SYSTEM: This software is usually loaded into the computer's memory upon powering the machine on. It is a prerequisite for the operation of any other software.

PIRATE SOFTWARE: Software that has been illegally copied.

RAM: Random Access Memory. The computer's volatile (short-term memory) that can be lost when the computer is turned off/powered-down.

REMOVABLE STORAGE MEDIA: Memory cards, USB thumb drives, CDs, DVDs and Blu-rays discs that store data and can be easily removed.

REMOVABLE MEDIA CARDS: data storage media which are more commonly found in other digital devices such as mobile phones, cameras, PDAs and music players.

ROUTER: A network device that connects two or more networks (example: personal home network to ISP network).

SOLID STATE DRIVES (SSD): Solid state drives are found inside a computer and in portable external enclosures. They can store large amounts of data and contain NO moving parts.

USB STORAGE DEVICES: Small storage devices accessed using a computer's USB ports. They store large volumes of data files. They are easily removed, transported and concealed. They are about the size of a car key or highlighter pen.

WRITE-BLOCKERS: Hardware or software that blocks data from being written to electronic storage media (HDDs, USB storage devices, etc.). These are used when accessing or copying (imaging) electronic storage media to maintain the integrity of the original piece of electronic storage media.

WARDRIVING: Driving around an area with a laptop and a wireless network adapter in order to locate unsecured wireless networks.

WIRELESS NETWORK CARD: An expansion card present in a computer that allows a wireless connection between that computer and other devices on a computer network. The card communicates by radio signals to other devices present on the network.

PREVENTION

- Never give out any of the following information to unknown sources:

Date/Place of Birth	**Social Security Number**
Credit Card Number	**Mother's Maiden Name**
Address	**Phone Number**

- Review credit reports at least once a year.

- Ensure secure online transactions by locating the closed lock icon at the bottom right side of your web browser before disclosing personal information.

- Unless absolutely necessary, do not store any financial information on a computer.

- Prior to discarding a computer, destroy all information contained on the hard drive. A wiping utility is necessary, as formatting will not safely destroy data.

- Use strong passwords and do not allow programs to save passwords.

- Use virus protection software and firewalls to prevent the loss of personal information from your computer or the introduction of malware.

RESPONSE

- Contact bank or credit card issuer to report fraud.

- Place a fraud alert with the following credit agencies:

Equifax - 800-525-6285
Experian - 888-397-3742
TransUnion - 800-680-7289

- File an identity theft complaint with your local police department and the Federal Trade Commission (FTC) at 877-382-4357.


UNITED STATES
SECRET SERVICE