Best Practices for Seizing Electronic Evidence

Version 2.0

PRICEWATERHOUSECOOPERS

This second edition of the *Best Practices for Seizing Electronic Evidence* was updated as a project of the International Association of Chiefs of Police Advisory Committee for Police Investigative Operations, PricewaterhouseCoopers LLP, Technical Support Working Group, and the United States Secret Service. The Committee convened a working group of a variety of law enforcement and industry representatives to identify common issues encountered in today's crime scenes. Representatives from the following agencies developed this manual:

Baltimore County Police Department
Combating Terrorism Technology Support Office, Technical Support Working Group
Dallas County District Attorney's Office
Department of Defense Computer Forensic Laboratory
Illinois State Police
Lakewood, Colorado Police Department
Lubbock, Texas Police Department
Michigan State Police Department
Naval Criminal Investigative Service
New Jersey Division of Criminal Justice
PricewaterhouseCoopers LLP (Cybercrime Prevention & Response Practice)
Richardson, Texas Police Department
Rockland County New York District Attorney's Office
Saint Louis County Prosecutor's Office
San Bernardino County Sheriff's Office
United States Customs Service, Cyber-smuggling Center
United States Department of Justice Computer Crimes and Intellectual Property Section
United States Secret Service

For additional copies, please contact the local office of the United States Secret Service. If you have comments or suggestions for the content of the guide or feedback on its use, please send email to iacp_manual@usss.treas.gov.

The committee wishes to thank Intel Corporation for its financial support in the publication of this guide.

Officer Safety

Officer safety is paramount in the investigation of any crime. Although the image often perceived in crimes related to technology may not appear threatening, law enforcement investigators should not become complacent with individuals or their environment.

Although technology brings forth with it new types of crimes and eventual passage of related laws, it is often only a vehicle or tool the criminal element uses to assist in the commission of conventional crimes and terrorist acts. The misuse of technology affords suspects enhanced global access, intelligence/counter intelligence, anonymity, speed, distance and a means for deploying booby traps.

Law enforcement's sole purpose during an investigation is to provide for the unbiased, and thorough, gathering of facts. As this process may cause unexpected changes to a subject's involvement in a case, unexpected individual and environmental threats to officer safety may unmask themselves at any time in the investigation process and remind us that officer safety is the foremost component of any investigation.

Best Practices for Seizing Electronic Evidence

Purpose

To develop a basic understanding of key technical and legal factors regarding searching and seizing electronic storage devices and media.

Recognizing Potential Evidence

Computers and digital media are increasingly involved in unlawful activities. The computer may be contraband, fruits of the crime, a tool of the offense, or a storage container holding evidence of the offense. Investigation of any criminal activity may produce electronic evidence. Computers and related evidence range from the mainframe computer to the pocket-sized personal data assistant to the floppy diskette, CD or the smallest electronic chip device. Images, audio, text and other data on these media are easily altered or destroyed. It is imperative that law enforcement officers recognize, protect, seize and search such devices in accordance with applicable statutes, policies and best practices and guidelines.

Answers to the following questions will better determine the role of the computer in the crime:

- Is the computer contraband or fruits of a crime?
  - For example, was the computer software or hardware stolen?

- Is the computer system a tool of the offense?
  - For example, was the system actively used by the defendant to commit the offense? Were fake ID's or other counterfeit documents prepared using the computer, scanner, and color printer?

- Is the computer system only incidental to the offense, i.e., being used to store evidence of the offense?
  - For example, is a drug dealer maintaining his trafficking records in his computer?

- Is the computer system both instrumental to the offense and a storage device for evidence?
  - For example, did the computer hacker use the computer to attack other systems and also to store stolen credit card information?

Once the computer's role is understood, the following essential questions should be answered:

- Is there probable cause to seize hardware?

- Is there probable cause to seize software?

- Is there probable cause to seize data?

- Where will this search be conducted?
  - For example, is it practical to search the computer system on site or must the examination be conducted at a field office or lab?
  - If law enforcement officers remove the system from the premises to conduct the search, must they return the computer system or copies of the seized data to its owner/user before trial?
  - Considering the incredible storage capacities of computers, how will experts search this data in an efficient, timely manner?

- What basic police skills are vital?
  - Basic police skills, such as interviewing, are important. For example, most passwords are obtained through the questioning of encryption users. In an interview, consider asking what software package or application was used.

Preparing for the Search and/or Seizure

Using evidence obtained from a computer in a legal proceeding requires:

- Probable cause for issuance of a warrant or an exception to the warrant requirement.
  - Caution: If you encounter potential evidence that may be outside the scope of your existing warrant or legal authority, contact your agency's legal advisor or prosecutor, as an additional warrant may be necessary.

- Appropriate collection techniques to avoid altering or destroying evidence.

- Forensic examination of the system completed by trained personnel in a timely manner with expert testimony available at trial.

Consent Search vs. Search Warrant

The *Search Warrant* allows for the search, seizure and examination of electronic evidence as predefined under the warrant. This method is most preferred and consistently is met with the least resistance at the scene and in the courts.

A *Consent Search* and/or *Seizure* allows the individual giving consent an opportunity to withdraw consent at any time during the search & seizure. Continued consent is typically difficult to ensure if the examination process is conducted at a later date and another location. It would be advisable to contact the prosecutor when executing consent searches for computers for this reason.

Search Warrants

Search Warrants for electronic storage devices typically focus on two primary sources of information:

- Electronic Storage Device Search Warrant
  - Search and seizure of hardware, software, documentation, user notes and storage media
  - Examination/search and seizure of data

- Service Provider Search Warrant
  - Service records, billing records, subscriber information, etc.
  - Request information via appropriate search warrant, subpoena or court order from the following:
    - ✔ Gas Utility Service Provider
    - ✔ Water Utility Service Provider
    - ✔ Electric Utility Service Provider
    - ✔ Cable Service Provider
    - ✔ Satellite Service Provider
    - ✔ Internet Service Provider
    - ✔ Electronic Data Storage Provider
    - ✔ Telephone Service Provider
    - ✔ Wireless/Cellular Service Provider
    - ✔ Pager Service Provider
    - ✔ Financial Institution/Credit Card Issuer
  - Obtain identification information for further investigative purposes

Issues of Concern:

Night Service	Officer safety, destruction of evidence, suspects(s) online or using hardware, access to employees, location and information.
No-knock	Officer safety and destruction of evidence.
Non-Disclosure	Jeopardy of investigation, trade secrets, and informants(s) protection.
Off-site Search	Field, law enforcement facility, off-site location government or civilian
Examination	Recovery by and/or examination by sworn and non-sworn personnel.
Duplicate Data	Authority to duplicate images/copies of data from electronic devices and/or storage media by sworn or non-sworn personnel.
Record Scene	Authorization to photograph and/or video tape the location, property and persons by investigative personnel, sworn or non-sworn who are authorized to assist in the search warrant.
Special Master	Special legal considerations involving: doctors, attorneys, spouses, publishers, etc.
Security Access	Ability to gain access to security devices, passwords, encryption and other security/access control measures. May become necessary for the court to impose an "Order to Compel" requiring the involved party to provide law enforcement the necessary means to gain access.

Conducting the Search and/or Seizure

Once the computer's role is understood and legal requirements are fulfilled:

Secure the Scene

- Officer safety is paramount
- Preserve area for potential fingerprints
- Immediately restrict access to computer(s) and attached peripherals
  - There are many methods to access computers remotely

Secure The Computer as Evidence

- If computer is "OFF," **Do Not Turn "On"**

- If computer is "ON"
  - Stand-alone computer (non-network)
  - Consult computer forensic specialist

- **If Specialist is Not Available**
  - Photograph screen, then disconnect all power sources; unplug from the back of the computer
  - Interrupting power from the back of the computer will defeat an uninterruptible power supply (UPS)
  - Laptops often have battery power supplies, if the laptop does not shutdown when the power cord is removed, locate and remove the battery pack. The battery is commonly placed on the bottom, and there is usually a button or switch that allows for the removal of the battery. Once the battery is removed, do not return it to or store it in the laptop. Removing the battery will prevent accidental start-up of the laptop
  - Place evidence tape over each drive slot
  - Photograph/diagram and label back of computer components with existing connections
  - Label all connector/cable ends to allow reassembly as needed.
  - If transporting is required, package components and transport/store components as fragile cargo
  - Keep away from magnets, radio transmitters and other potentially damaging elements
  - Collect all peripheral devices, cables, keyboards, and monitors
  - Collect instruction manuals, documentation, and notes
  - User notes may contain passwords

Networked or Business Computers

Consult a Computer Specialist for Further Assistance

- Secure the scene do not let anyone touch except personnel trained to handle network systems
- Pulling the plug could:
  - Severely damage the system
  - Disrupt legitimate business
  - Create officer and department liability

Other Electronic Storage Devices

Electronic devices may contain viable evidence associated with criminal activity. Unless an emergency exists, do not access the device. Should it be necessary to access the device, note all actions associated with the manipulation of the device in order to document the chain of custody and protect the integrity of the evidence.

Wireless Telephones

Awareness: Wireless telephones provide users with mobile communications using various protocols and formats (e.g. CDMA, TDMA, GSM, etc.) in various frequencies (e.g. 900MHz, 1.2 GHz, etc.).

- Potential Evidence Contained in Wireless Devices
  - Numbers called
  - Names and addresses
  - Caller ID for incoming calls
  - Other information contained in the memory of wireless telephones
    - Phone/pager numbers
    - Names and addresses
    - PIN numbers
    - Voice mail access numbers
    - Voice mail password
    - Debit card numbers
    - Calling card numbers
    - Email/Internet access information
    - Service Provider Information
    - On screen image may contain other valuable information
    - The wireless telephone may also serve as a Personal Data Assistant (PDA) – see PDA
    - Increasingly, wireless telephones can be used to complete financial and retail transactions

- On/Off Rule
  - If the device is "ON," **Do NOT Turn "OFF"**
    - Turning it "OFF" could activate lockout feature

- Write down all information on display (photograph if possible)
- Power down prior to transport (take any power supply cords present)

- If the device is "OFF," **Leave It "OFF"**
  - Turning it on could alter evidence on device (same as computers)
  - Upon seizure, deliver device to an expert as soon as possible or contact local service provider
  - The service provider can be identified through the phone number at www.fonefinder.net
  - Make every effort to locate any instruction manuals pertaining to device along with power cords and other related devices.
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage, e.g. cold, dampness.
  - Anticipate a compulsory process (e.g. subpoena, etc) for the service provider to supply additional information.

Cordless Telephones

Awareness: Cordless telephones provide users with freedom of movement with the wireless handheld transmitter/receiver as long as the user remains within the range of the telephone base station. The base station serves as the connection between the wireless device and the physical wire connection for telephone service.

- Potential Evidence Contained in Cordless Devices
  - Numbers called
  - Numbers stored for speed dial
  - Caller ID for incoming calls
  - Other information in the memory of cordless telephones
    - Phone/pager numbers
    - Names and addresses
    - PIN numbers
    - Voice mail access number
    - Voice mail password
    - Debit card numbers
    - Calling card numbers
    - On-screen image may contain valuable information

- On/Off Rule
  - If the device is "ON," **Do NOT Turn "OFF"**
    - Turning it "OFF" could activate a lockout feature.
    - Write down all information on display (photograph if possible)
    - Power down prior to transport (take any power supply cord present)
  - If the device is "OFF," **Leave It "OFF"**
    - Turning it "ON" could alter evidence (same as computers)
    - Upon seizure deliver device to an expert as soon as possible.
    - Delays in conducting the examination may result in loss of stored information if power supply becomes insufficient through battery or internal power supply
    - Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices

- Take appropriate care in handling and storage e.g. heat, cold, dampness
- Home systems are becoming network connected

Answering Machines

Awareness: Answering machines provide users with a means to capture messages from callers unable to reach the device owner or operator. These devices store messages on tape or in digital memory.

- Potential Evidence Contained in Answering Machines
  - Incoming and outgoing messages
  - Some double as a phone
  - Home systems are becoming network connected
  - Numbers called
  - Numbers stored for speed dial
  - Caller ID for incoming calls
  - Other information in the memory of cordless telephones
    - Phone/pager numbers
    - Names and addresses
    - PIN numbers
    - Voice mail access number
    - Voice mail password
    - Debit card numbers
    - Calling card numbers
    - On-screen image may contain valuable information

- On/Off Rule
  - If the device is "ON," **Do NOT Turn "OFF"**
    - Turning it "OFF" could activate a lockout feature.
    - Beware remote access; disconnect this device from telephone line as soon as possible. An incoming call could delete needed information.
    - Write down all information on display (photograph if possible)
    - If possible, use a tape recorder to record saved messages.
    - Power down prior to transport (take any power supply cord present)
  - If the device is "OFF," **Leave It "OFF"**
    - Turning it "ON" could alter evidence (same as computers)
    - Upon seizure deliver device to an expert as soon as possible.
    - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply
    - Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices
    - Take appropriate care in handling and storage e.g. heat, cold, dampness

Caller ID Devices

Awareness: Caller identification devices collect caller information. Often these devices display incoming calls and record established numbers of recent incoming call records.

- Potential Evidence Contained on Caller ID Device
  - May contain telephone and subscriber information from incoming telephone calls
  - Date and time of incoming calls

- On/Off Rule
  - If the device is "ON," **Do NOT Turn "OFF"**
    - Interruption of the power supply to device may cause loss of data if not protected by internal battery back up.
    - Document all stored data prior to seizure or loss of data may occur.
    - All manuals should be seized with equipment; if possible, along with power cords and other related devices.

Electronic Paging Devices

Awareness: Some pagers have evolved into two-way messaging systems; a nationwide and worldwide method of communication. The pagers that provide such features receive wireless information, and transmit information as well.

- Potential Evidence Contained in Paging Devices
  - Numeric Pagers receives only numeric digits (can be used to communicate numbers and code)
  - Alpha Numeric Pagers (receives numbers and letters and carry full text)
  - Voice Pagers (can transmit voice communications (sometimes in addition to alpha numeric))
  - 2-Way Pagers (containing incoming and outgoing messages)
  - Best Practices
    - Once pager is no longer in proximity to suspect – turn it off. Be aware, continued access to electronic communications over pager without proper authorization can be construed as unlawful interception of electronic communications; consult your prosecutor for details in your area.
  - Search of stored contents of pager
    - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply.
    - Take appropriate care in the handling and storage e.g. cold dampness.
    - May also require service provider search warrant to obtain additional information.
    - Turn it off.
    - Change Batteries

Facsimile Machines

Awareness: Facsimile machines provide the user with the ability to transmit documents via phone line from one point to another.

- Fax machines can contain:
  - Speed dial list
  - Stored faxes (incoming and outgoing)
  - Fax transmission logs (incoming and outgoing)
  - Header line
  - Clock setting

- Best Practices – Fax Machines
  - If fax machine is found "OFF," **Leave "OFF"**
  - If fax machine is found "ON"
    - Powering down may cause loss of last number dialed and/or stored faxes - see manufacturers manual if possible prior to power down.
    - Record saved data prior to powering off.
    - Photograph

- Other Considerations
  - Record telephone line number fax is plugged into
  - Record network line number fax is plugged into
  - Header line should be the same as the phone line; user sets header line
  - Some fax machines are also copiers, scanners, and printers.
  - All manuals should be seized with equipment, if possible

Smart Cards & Magnetic Stripe Cards

Awareness: Smart and magnetic stripe cards serve many functions, but possess similar characteristics. Both cards interface with a reader device capable of interpreting information stored on the magnetic stripe or computer chip embedded in the plastic card. The most familiar application of these technologies is the credit card. These technologies lend themselves to many additional applications because they are capable of storing any kind of information. These applications include, but are not limited to; driver's licenses, hotel room keys, passports, benefit cards, and security door passes. These technologies can also exist on a card together. (Uses: Point of Sale Transactions, ATM Capabilities)

Smart Cards: There are two basic types of smart cards. The first is memory card which is merely a digital storage device capable of holding large stores of information. The second

type is a microprocessor card which is basically a small computer capable of completing a number of calculations. The functionality provided in these cards allow for more robust security in protecting embedded information. The card readers for these cards can also be contact or proximity based. (uses: Direct exchange of value between card holders, exchange value over the internet, storing data or files similar to a computer, wireless telephones. satellite service devices)

Magnetic Stripe Cards: The magnetic stripe can be identified as a black or brown strip that runs across a card. Account or user information can be stored on numerous tracks on each magnetic stripe. To accurately read the information, magnetic stripe readers must include the capability to read the various tracks. This technology can also be used in a paper or disposable format such as metro passes or parking passes.

- Circumstances Raising Suspicion Concerning Smart & Magnetic Stripe Cards
  - Numerous cards, (different names or same issuing vendor)
  - Signs of tampering (cards are found in the presence of computer or other electronic devices)

- Questions to Ask When Encountering Smart & Magnetic Cards
  - Who is the card issued to (the valid cardholder)?
  - Who issued the card?
  - What are the uses of the card?
  - Why does the person have numerous cards?
  - Is there a device or computer present that can alter the card?

- Best Practices
  - Photograph of the card
  - Label and identify characteristics
  - Detect possible alteration or tampering during examination
  - Identify who possessed the card and exactly where it was found (separation from genuine identification and cards may help establish intent)

ID Card Printers

Awareness: These devices offer users the ability to print graphics and information onto a plastic card.

- ID card printer can contain stored data

- Best Practices
  - If ID card printer is found "ON," powering down may cause loss of stored data.

- Other Considerations
  - Check to see if it is network connected, stand alone, or portable
  - All manuals should be seized with equipment if possible, along with power cords and other related devices.
  - Can be used to provide counterfeit false identification

Scanners

Awareness: Scanners allow for the creation of a computer image of documents, papers, or items placed on the scanner bed.

- Scanners can contain stored data

- Best Practices
  - If scanner is found "ON," powering down may cause loss of stored data.

- Other Considerations
  - Check to see if it is network connected, stand alone, or portable
  - Some scanners are also copiers, printers, and facsimile machines.
  - All manuals should be seized with equipment, if possible along with power cords and other related devices

Printers

Awareness: Printers allow for the hard copy creation of items generated by computers. There are many printer technologies including laser, ink jet, thermal dye, and dot matrix.

- Printers can contain stored data

- Best Practices
  - If printer is found "ON," powering down may cause loss of stored data.

- Other Considerations
  - Check to see if it is network connected, stand alone, or portable
  - Record telephone line number printer is plugged into
  - Record network line number printer is plugged into
  - Some printers are also copiers, scanners, and facsimile machines.
  - All manuals should be seized with equipment if possible, along with power cords and other related devices.

Copiers

Awareness: Copiers allow for the duplication of items placed on the copying surface.

- Copy machines can contain:
  - Speed dial lists
  - Stored copies (incoming and outgoing)
  - Data files (Complete images or documents from computers in a network environment
  - Copy transmission logs (incoming and outgoing)
  - Header line
  - Clock setting

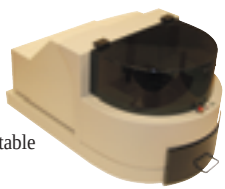
- Best Practices
  - If copy machine is found "ON", powering down may cause loss of last number dialed and/or stored copies

- Other Considerations
  - Check to see if it is network connected, stand alone, or portable
  - Record telephone line number printer is plugged into
  - Record network line number printer is plugged into
  - Some copiers are also printer, scanners, and facsimile machines.
  - All manuals should be seized with equipment if possible, along with power cords and other related devices.

Compact Disk Duplicators and Labellers

Awareness: Duplicators allow for the mass creation of compact disks. When used inappropriately these devices are typically used to commit violations of copyright law.

- Compact disk duplicators and labellers can contain:
  - Stored Data



- Best Practices
  - If duplicator/labeller is found "ON," powering down may cause loss of stored data.

- Other Considerations
  - Check to see if it is network connected, stand alone, or portable
  - All manuals should be seized with equipment; if possible along with power cords and other related devices.
  - Some networked copiers contain proprietary hard drives that store images

Digital Cameras/Video/Audio

Awareness: Video and audio media can be recorded as analog or digital information. Many different formats of media are available within both areas. Devices may be stand alone, networked, personal, home entertainment or business, e.g. text, still images, graphics, date/time, author, system used, etc. Some devices may have basic personal computing functions or may be a computer device itself. Devices are found as Portable and Fixed Devices, but can be easily moved. Devices may store data directly to internal memory and/or removable media. *See storage media for further information on media.*

- If the device is "OFF," **Do NOT Turn "ON"**

- If the device is "ON"
  - Consult a specialist

- If a specialist is not available:
  - Secure recorded media
    - Identify and secure recorded media as soon as possible
    - If recorded media needs to be reviewed immediately, **DO NOT PAUSE** tape media unless absolutely necessary. Pausing taped media, both video and audio, causes irreversible wear (damage) to the tape resulting in poor image/audible quality
    - Immediately secure **RECORD TABS** on the media to prevent accidental overwrite (recording)
  - Securing device
    - Photograph device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical
    - Place evidence tape over areas of access e.g. drive slots and media slots
    - Photograph/diagram and label back of components with existing connections
    - Label all connector/cable ends to allow reassembly as needed
    - If transport is required, package components and transport/store components as fragile cargo
    - Delays in conducting the examination may result in loss of information, if power supply becomes insufficient through battery or internal power supply
    - Take appropriate care in the handling and storage e.g. cold, dampness

- Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices

Electronic Game Devices

Awareness: These devices now provide users with greater functionality and are increasingly more comparable with a computer.

- Electronic gaming devices can contain:
  - Stored data – text, images, audio, video, etc.
  - Internet access information
  - Email
  - Basic personal computing functions
- Devices may be stand alone or Networked via Internet or wireless communication
- If the device is "OFF," **Do NOT Turn "ON"**
- If the device is "ON"
  - Consult a specialist
- If a specialist is not available:
  - Photograph device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical
  - Place evidence tape over areas of access e.g. drive slots and media slots
  - Photograph/diagram and label back of components with existing connections
  - Label all connector/cable ends to allow reassembly as needed
  - If transport is required, package components and transport/store components as fragile cargo
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply
  - Take appropriate care in the handling and storage e.g. cold, dampness
  - Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices

Home Electronic Devices

Awareness: Home electronic devices provide users with a greater degree of interaction with the device. The devices range from interactive television guides to smart kitchen appliances; such as, a microwave that stores messages for other family members, or a kitchen refrigerator that keeps track of food in its inventory when food items are used.

- Home electronic devices can contain:
  - Stored data – text, images, audio, video, etc.
  - Internet access information
  - Email
  - Telephone capabilities
  - Basic personal computing functions
  - Devices may be stand alone or networked within a home or an off-sight location

- If the device is "OFF," **Do Not Turn "ON"**

- If the device is "ON"
  - Consult a specialist

- If a specialist is not available:
  - Photograph device (screen/display).
  - If the device has a readily discernable audio playback feature, play back and record with a tape recorder
  - Disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical
  - Place evidence tape over areas of access e.g. drive slots and media slots
  - Photograph/diagram and label back of components with existing connections
  - Label all connector/cable ends to allow reassembly as needed
  - If transport is required, package components and transport/store components as fragile cargo
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply
  - Take appropriate care in the handling and storage e.g. cold, dampness
  - Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices
  - Care should be given to the ability of these systems to be remotely accessed. These systems are typically operated through a service provider. Data may not be stored on the system
  - May require a service provider search warrant to obtain additional information

Global Positioning System

- Awareness
  - Global Positioning systems provide users with the ability to locate their position on the Earth's surface by measuring signals transmitted by satellites. These devices assist with navigation and can integrate maps to help users travel from one point to another.
- Global positioning system can contain:
  - Stored data – text, images/maps
  - Internet access information
  - 2-Way radio capabilities
  - Telephone capabilities
  - Routes, marked locations
  - Timelines

- If the device is "OFF," **Do Not Turn "ON"**

- If the device is "ON"
  - Consult a specialist

- If a specialist is not available:
  - Photograph device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical
  - Place evidence tape over areas of access e.g. drive slots and media slots
  - Photograph/diagram and label back of components with existing connections
  - Label all connector/cable ends to allow reassembly as needed
  - If transport is required, package components and transport/store components as fragile cargo
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply
  - Can be portable or fixed device
  - Take appropriate care in the handling and storage e.g. cold, dampness
  - Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices
  - Care should be given to the ability of these systems to be remotely accessed. These systems are typically operated through a Service Provider. Data may not be stored on the system
  - GPS can be found as an integrated part of other portable devices. Some have been listed within this reference guide e.g. Palm devices, mini notebooks, notebook PC's, and digital cameras, etc.

Personal Data Assistants/Hand Held Computers

Awareness: Personal data assistants provide users with much of the functionality of full size personal computers, but are small in size.

- Palm devices/PDA's can contain:
  - Stored data – text, images, audio, video, etc.
  - Internet information
  - Email
  - Directories
  - Basic personal computing functions
  - Devices may be stand alone or networked within a home or an off-sight location
  - Devices typically range from interactive television guides to kitchen appliances

- If the device is "OFF," **Do Not Turn "ON"**

- If the device is "ON"
  - Consult a specialist

- If a specialist is not available:
  - Photograph device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical
  - Place evidence tape over areas of access e.g. drive slots and media slots
  - Photograph/diagram and label back of components with existing connections
  - Label all connector/cable ends to allow reassembly as needed
  - If transport is required, package components and transport/store components as fragile cargo
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply
  - Keep away from magnets, radio transmitters, and otherwise hostile environments including hot, cold and dirty conditions
  - Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices
  - Care should be given to the ability of these systems to be remotely accessed. These systems are typically operated through a Service Provider. Data may not be stored on the system
  - May require a Service Provider Search Warrant to obtain additional information

Security Systems

Awareness: These systems are installed as protective measures and are often positioned in strategic locations and can prove to be valuable information for an investigation.

- Security systems can contain:
  - Stored data – text, images, audio, video, etc.
  - Time stamp information
  - Device may be stand-Aalone or networked via the internet or a private network
  - Consult security personnel responsible for supporting system. If not available, contact specialist
  - If specialist is not available:
  - Immediately secure recorded data e.g. videotape media to prevent media from accidentally being overwritten
  - It is critical to obtain as much detailed system information as possible:
    - Make/model
    - PC based system
    - Video based system
    - Number of cameras
    - Type of cameras
    - Location of system
    - Location of cameras
    - Recording media
    - Media stored/archived
  - Photograph/diagram system and cameras if allowed

- Systems are found as portable-wireless and as fixed systems
- Computer based systems will require the same handling guidelines as covered under computers

Vehicle Computer Devices

Awareness: Vehicle computer devices provide users with many computer features within their vehicle.

- Vehicle computer devices can contain:
  - Stored data – text, images, maps, audio, etc.
  - Internet access information
  - Telephone capabilities
  - Routes, marked locations
  - Timelines
  - Email
- If the device is "OFF" **Do Not Turn "ON"**
- If the device is "ON"
  - Consult a specialist
- If a specialist is not available:
  - Photograph device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical. Most systems are built into the vehicle's interior, integrated into the dash or console areas making it impractical to remove the unit. Actual data may be stored elsewhere in the vehicle
  - Place evidence tape over areas of access e.g. drive slots and media slots
  - Photograph/diagram and label back of components with existing connections
  - Label all connector/cable ends to allow reassembly as needed
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply
  - Can be portable or fixed device
  - Take appropriate care in the handling and storage e.g. cold dampness, etc.
  - Make every effort to locate any instruction manuals pertaining to the device, along with power cords and other related devices
- Care should be given to the ability of these systems to be remotely accessed
- These systems may be integrated with many systems to include: communication, navigation, security, safety, entertainment, personal computing, internet, digital audio and imaging into networked environments supported at the home, work place, public services, and portable devices.
- May also require a Service Provider Search Warrant to obtain additional information

Storage Media

Storage Media is used to store data from an electronic device. Some devices have fixed storage space located within the device. This form of storage requires a means of interfacing to another source to transfer the data when necessary. Many devices of today have capabilities for both fixed (internal) storage/memory and the ability to also store data solely or simultaneously to removable storage media. Removable media is used to transfer and store data.

Some of these media types come in many variations and there are numerous other types currently in use that are not as prevalent and even more are being introduced into the market on a regular basis. Although there are some standards, the following list is some of the more common and well-established media types found in the consumer and commercial market-place.

- ✔ Floppy disk
- ✔ MD (Mini Disc)
- ✔ Jaz
- ✔ Flash memory card
- ✔ External hard drive
- ✔ DLT tape
- ✔ HiFD (High Density Floppy Disk)
- ✔ CD (Compact Disk)
- ✔ LS-120 (Super Disk)
- ✔ Click
- ✔ Smart media
- ✔ Micro-drive
- ✔ DAT (digital audio tape)
- ✔ DVD (Digital Video Disk)
- ✔ Zip
- ✔ Memory stick
- ✔ Removable hard drive
- ✔ Magneto optical drive
- ✔ DLT tape

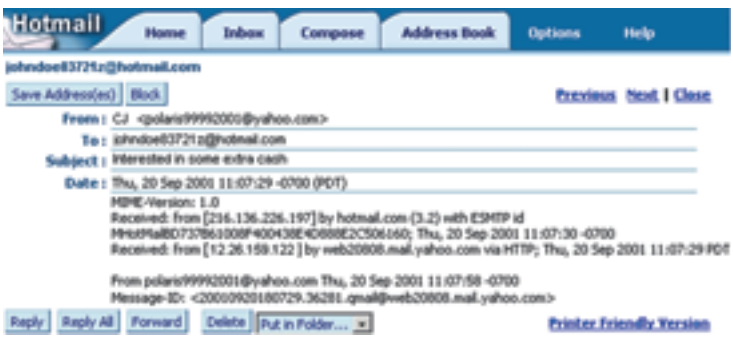
Skimmers / Parasites and other Criminal Technology

- Skimmers & parasites
  - Potential evidence
    - Stolen credit card number
    - Victim identification information
    - CVC and CVV numbers for compromised cards
- On/off rule
  - Do not attempt to remove batteries, or change batteries
  - Do not handle buttons or switches – some of these device are equipment with panic features to destroy potential evidence
  - Information about these devices can be found at www.elibrary.usss.treas.gov.
  - This device should be examined quickly to prevent loss of evidentiary material
- Criminal technology
  - Criminal devices are often homemade devices that may be somewhat fragile. These devices are developed for the sole purpose of carrying out various fraud schemes
  - On/off rule
    - Do not attempt to remove batteries, or change batteries
    - Do not handle buttons or switches – some of these device are equipment with panic features to destroy potential evidence
  - This device should be examined quickly to prevent loss of evidentiary material

Tracing an Internet Email

- When an Internet email message is sent, the user typically controls only the recipient lines(s) (To:, Cc:, and Bcc:) and the Subject: line.
- Mail software adds the rest of the header information as it is processed.
- Typically, only the From:, To:, Subject:, and Date: lines are displayed. The setting to view the full or extended header information is usually found in the Options or Preferences menu of the e-mail software.
- The full or extended email header will contain information useful in tracing the message back to the source. Internet Protocol (IP) addresses and assigned message id numbers along with the time and date stamps are integral in tracing the origin of a message, verifying the information in the From: line is correct or authenticating the transmission information for the message.
- Header information will vary depending on the type of mail system used and mail servers used to process the messages.

Email header:



In this example, the From: line suggests the sender is polaris99992001@yahoo.com. The "polaris99992001" is the name of the mailbox located at the "Yahoo" mail server location. The To: line indicates the recipient is johndoe83721z@hotmail.com. The Date: line indicates the date and time the message was submitted to a Yahoo mail server. Date and time stamps are only as reliable as the clock setting on the computers that process the message.

The extended header information is usually read from bottom to top. The Message ID is a unique number assigned to the email as it is processed by a server and may be useful in determining if the mail is a forgery by comparing the ID with logs retained by the server that issued the ID. The next line states the message is from polaris99992001@yahoo.com. The lines beginning with Received: in the extended email header are created as the message traverses mail servers. Information in the Received: lines varies depending on the mail server and software processing the message. The first Received: line in this example states- Received: from [12.26.159.122] by web20808.mail.yahoo.com via HTTP and is data/time stamped. This first Received: line can be valuable in this case to identify what computer or network was involved in transmitting the

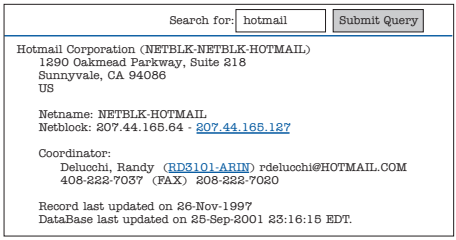
message to yahoo.com for processing. The next Received: line states – Received: from [216.136.226.197] by hotmail.com and contains an ID number and date/time stamp from the Hotmail mail server. The IP address, domain name, or server name can usually be associated with the following:

Numerous services provide a web Whois interface to research IP address information such as the American Registry for Internet Numbers (www.arin.net). An Internet search for nslookup will also provide several web interfaces to research the server names.

A Whois lookup on 12.26.159.122 reveals the IP address is associated with AT&T (ISP) and PricewaterhouseCoopers (customer). Contact information can be obtained by clicking on the links. Overall, this example indicates a computer located on the PricewaterhouseCoopers' network caused a message to be sent through the AT&T ISP network to a Yahoo email server which finally processed the message to a user's mailbox on the Hotmail email server.

In addition to looking up an IP address to identify a network/contact for investigation, an investigator can also look up a domain name using similar tools. For example, by visiting the same site www.arin.net, a user can type in the name of a domain, i.e. Hotmail and receive the contact/technical information necessary to further the investigation.

The contact listed may not be the best person to handle calls concerning a subpoena, court order or search warrant. But it provides a lead to identify the appropriate person. An additional resource is Infobin.org (www.infobin.org), which contains contact information relevant to an investigator for most of the ISP's.



ISP's and email service providers store data useful in identifying the sender of the email, such as subscriber information, billing information, and connection logs, which contain the IP addresses and date/time stamps used to connect to the ISP. The IP address may reveal the sender's ISP or employer, as in this example, the sender is using the service from work. In some cases, if the sender is using a modem and phone line, an Internet backbone company can use the connection information, provided by the ISP or e-mail service provider, to obtain the Automatic Number Identification (telephone number) of the phone line used to dial into the ISP.

There are many resources on the web that discuss email headers, including http://help.mindspring.com/docs/006/emailheaders/ and http://www.stopspam.org/email/headers/headers.html.

Things to Remember

- Officer safety and public safety
- Preservation of evidence (paper bags)
- Keep everyone away from the devices and/or storage media.
- Identify potential evidence/electronic devices and/or media.
- Is a search warrant needed for the search and seizure of the device and/or media including potential data from the device and/or media?
- Who owns the device or media?
- Who has control/possession of the device and/or media?
- Do exigent circumstances exist e.g. **OFFICER SAFETY, PUBLIC SAFETY, DESTRUCTION OF EVIDENCE, ESPIONAGE, DISRUPTION OF VITAL SERVICES, etc?**
- Does special legal information considerations apply, e.g. **DOCTOR, ATTORNEY, CLERGY, PSYCHIATRIST, PUBLISHER, etc?**
- Ability for remote access to devices.
- Off-site data storage.
- Recovery of software, power cords/adapters, peripheral devices, etc. used to support the seized devices and/or media.
- Recovery of passwords, encryption keys, physical keys, and other security access control devices and/or measures used maybe located at the scene or collected through interviews.
- Determination of suspect, victim, or witness knowledge, e.g. system, hardware, software, devices, Internet, Email, chat rooms, person or located target, etc.
- Determine suspect(s) access and control of areas and devices.
- Do not turn power on if already off.
- Do not try to access devices or data unless you are qualified to access the device. If required in an emergency situation, provide written and, if possible, photo documentation of what was done and why.