Computer Forensics and Digital Evidence

James Phelps, Ph.D.
Angelo State University

james.phelps@angelo.edu
325-942-2167
Pre-Test

• So we can evaluate how well we do.
The Chinese utilize a large, well-organized network to facilitate collection of sensitive information and export-controlled technology from U.S. defense sources.
Why is Cybersecurity Important?

• Chinese authors emphasize defense as the top priority and indicate that Computer Network Defense (CND) must be the highest priority in peacetime; Chinese doctrine suggests that “tactical counteroffensives” would only be considered if an adversary’s operations could not be countered.

• How would they do this?
Visualizing a DDOS Attack

• [http://flowingdata.com/2013/05/30/ddos-attack-animation/](http://flowingdata.com/2013/05/30/ddos-attack-animation/)
Digital Evidence Collection Training for Law Enforcement

Intro
• A problem has been detected and windows has been shut down to prevent damage to your computer.
• MULTIPLE_IRP_COMPLETE_REQUESTS

• Collecting data for crash dump…
• Initializing disk for crash dump…
• Beginning dump of physical memory.
• Dumping physical memory to disk: 100
• Physical memory dump complete.
• Contact your system admin or technical support group for further assistance.
A Few Cyber Crimes

- Child Abuse/Exploitation
- Computer Intrusion (hacking)
- Counterfeiting
- Domestic Violence/threats, Extortion
- Stalking
- Gambling
- Identity Theft
- Narco-trafficking
- Fraud
- Prostitution
- Software Piracy
Electronic Evidence

- Computer Systems
- Storage Devices
- Handheld Devices
- Peripheral Devices
- Network Systems
Digital Evidence Collection Training for Law Enforcement

Sources
Digital Evidence Collection Training for Law Enforcement

For a 26 page booklet version of this publication go to

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ
NOV. 09

Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders

www.ojp.usdoj.gov/nij
Building a Course

- Digital Evidence Collection Training for Law Enforcement
- Kal Loper, Ph.D.

- Course Syllabus
Digital Evidence Collection Training for Law Enforcement
Presenter

Name: Dr. D. Kall Loper

Affiliation: International Data Forensics Solutions Center
Electronic Crimes Technology Center of Excellence
Southern Methodist University
“Big 4” Accounting Firm Investigations/CF

Experience: Computer crime and digital forensics since 1997
Breaks will be 10 minutes before the hour
Restrooms –
Please set cell phones to silent & feel free to take calls outside
This course provides digital evidence collection training. This material is not intended to supplant or supersede any prevailing laws or departmental policies.
Introductions

Name,

Agency,

Assignment,

Experience with electronic crime & digital evidence
Upon completion of this course, students will:

- Be able to properly identify, collect and preserve digital evidence
- Understand the value of digital evidence to an investigation
- Understand the importance of Digital Evidence Collection and Preservation Training
This training is funded through a cooperative agreement with the International Data Forensic Solution Center (IDFSC) and the National Institute of Justice, Office of Justice Programs, United States Department of Justice.
This training is based on the NIJ publication *Electronic Crime Scene Investigation: A Guide for First Responders, 2nd Edition*, updated by the ECPI.
Digital Evidence

- Information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.
Overview

- Computers & electronic devices are prevalent in every aspect of life
- Computers fit in a pocket in the form of Smartphones, PDAs & PocketPCs.
- Computers are present at almost every crime scene.
- Criminals use them to communicate and manage information—just like everyone else.
All criminal justice personnel at some point may be:

- Responsible for securing an electronic crime scene as well as identifying, collecting, preserving, securing, packaging, transporting and storing digital evidence.

- Law enforcement personnel at every level should understand that digital evidence is fragile and receive training in collecting and preserving the integrity of digital evidence.
Target Audience:

This course will provide Patrol Officers, Deputies, Patrol Supervisors, Detectives, Crime Scene Investigators, Digital Evidence Examiners & Analysts, Sheriffs, Chiefs, and Administrators with training on the proper collection and preservation of digital evidence.
Goals:

- Ensure that students understand and can identify:
  - Crimes and criminal activity committed or facilitated through the use of computer and cell phone technology
  - Devices and components that should be secured as evidence based on the nature of the investigation
  - The value of digital evidence to an investigation
Goals:

- Ensure that students understand and can identify:
  - Components & software that enable electronic devices to function as intended as well as alternate uses for components & software
  - The importance of power supplies, adapters, User Manuals and software CDs
Goals:

- Ensure that students understand and can identify:
  - The impact of digital evidence on investigations & prosecutions
  - The advantages of successful introduction of digital evidence in criminal proceedings
  - The consequences that improperly collected or improperly handled digital evidence can have on an investigation and prosecution
The Foremost Priority

- At every scene, **Officer safety** and the **safety of others** should be the primary consideration at all times.

- Potential hazards exist at every scene.
  - From persons or animals
  - Physical & environmental hazards
  - Electrical hazards
  - Biological, chemical or explosive hazards
  - Hazards that develop or arise at the scene
Questions?
Computer Systems
The devices as well as the information stored on them may constitute potential digital evidence you need to preserve.

Some of the devices may require internal or external power supplies to maintain the stored information.
Laptops
Computer Systems

PC

MAC
Computer Systems

Desktop Computers

- various shapes & sizes

Desktop PC

MAC Mini

iMac
Mini Computers / NetBooks

- Can be hand held & easily concealed
- May be located in small areas
  - Drawers, purse, coat pocket
Computer Systems

- May be partially disassembled but still operational
- Require careful handling to prevent damage and loss of Digital Evidence
- Condition should be thoroughly documented & photographed
Potential Evidence on Computer Systems

- Child pornography
- Financial records of fraudulent activities
- Email messages regarding criminal activities
- Chat logs and buddy lists of conspirators
- Internet history related to criminal activity
- Templates used to create forged documents
Storage Devices
Storage devices vary in size and the manner in which they store and retain data. Regardless of the size or type, these devices may be valuable to an investigation or prosecution.

Examples of storage devices

- hard drives
- removable media
- thumb drives
- memory cards
Hard Drives

- Data storage devices that consist of an external circuit board; external data and power connections; and internal magnetically charged glass, ceramic or metal platters that store data.

- Hard drives that are not connected or installed in a computer may be present.

- Loose hard drives should not be overlooked; they may contain valuable information.
Digital Evidence Collection Training for Law Enforcement

Storage Devices

Hard Drives

SCSI  IDE  SATA  IDE  2.5 inch

IDE 40-pin  2.5” IDE 44-pin
Storage Devices

Hard Drives

- Solid State Hard Drive with Serial ATA (SATA) connector
- 1.8” Hard Drive with Zero Insertion Force (ZIF) connector
External hard drives

- Hard drives can also be installed in an external case designed to increase the data storage capacity and provide users with the convenience of data portability. Generally, external hard drives require a power supply and a universal serial bus (USB), Firewire, Ethernet or wireless connection to a computer system.
External hard drives

- 3.5 inch External
- 2.5 inch External
- 3.5 inch External Wireless
- NAS (Network Attached Storage)
Removable Media

- Are cartridges and disk based data storage devices
  - Floppy Disks
  - Zip Disks
  - CDROMs
  - DVDs

- Typically used to store, archive/backup, transfer and transport data from one computer, location or device to another
  - Documents
  - Photographs
  - Software
  - Utilities
Removable Media

Optical Media / Optical Discs
Storage Devices

Thumb Drives

- Small, lightweight, removable data storage devices with USB connections.
- Also referred to as flash drives
- Easily concealed & transported
- Can be part of or disguised as common & unique items such as:
  - Wristwatches
  - Swiss Army Knife
  - Key Fob
Storage Devices

Common Thumb Drives
Other types of Thumb Drives

- USB Pen
- USB Watch
- USB Thumb Drive with Fingerprint Reader
Memory Cards

- Small data storage devices used with cameras, computers, cell phones, digital music players, personal digital assistants (PDAs), video game consoles, handheld and other electronic devices.
  - Smart Media (SM)
  - Secure Digital (SD)
  - Mini Secure Digital (MiniSD)
  - Micro Secure Digital (MicroSD)
  - CompactFlash (CF)
  - Memory Stick
Digital Evidence Collection Training for Law Enforcement

Storage Devices

Memory Cards

Images are not to scale
Memory Cards
Digital Evidence Collection Training for Law Enforcement

Storage Devices

Memory Cards

- SanDisk CompactFlash 2.0 GB
- SanDisk Memory Stick Pro
- SanDisk MicroSD 512 MB
- SanDisk MiniSD 1.0 GB
- SanDisk SDHC 4 GB

Intro
Storage Devices

Memory Cards
Handheld Devices

Portable data storage devices that provide communications, digital photography, navigation systems, entertainment, data storage and personal information management.
Handheld Devices – Cell Phones
Handheld Devices – Smart Phones
Hand Held Devices

Evidence that may be found on Thumb Drives, Memory Cards, & Hand Held Devices:

- Email messages
- Internet browsing history
- Internet chat logs
- Buddy lists
- Photographs
- Image files
- Databases
- Financial records
- Event logs
- Software applications
Digital Evidence Collection Training for Law Enforcement

Handheld Devices

It is important to note:

- Data or digital evidence may be lost if power to the handheld device is not maintained.
- Data or digital evidence on cell phones and smart phones can be overwritten and rendered unrecoverable while the device remains on and activated.
It is important to note:

- Software is available for various mobile & smart phones that can be activated remotely to render the device unusable and make the data it contains inaccessible if the phone is lost or stolen. The software can produce similar results if activated on a device seized as evidence by law enforcement.

- Precautions must be taken to prevent the loss of data on devices seized as evidence.
Peripheral Devices

Input and output components that can be connected to a computer to expand user access the computer’s functions
Peripheral Devices

- Keyboard / Mouse
- Microphone
- USB Hub
- Portable Web Cam
- Card Reader
- Soft Phone
- KVM Switch
Digital Evidence Collection Training for Law Enforcement

Peripheral Devices

- Credit Card Reader
- Printers, Fax Machines, Copiers, Multi-Function Centers (MFC)
- Modems
- Wireless Network Access Points
- USB Wireless Network Adapter
- Data Tape Drive
- Directional Antenna
- ZIP drive readers
Digital Evidence Collection Training for Law Enforcement

Peripheral Devices

- Biometric Reader
- Handheld scanner
- Communication Headset & Microphone
- Thumb drive copier
- GPS Receivers
Peripheral Devices

Potential Evidence:

- The devices themselves and the functions they perform may be of evidential value.
- The information stored on the device regarding its use may be of value
  - Incoming & outgoing phone & fax numbers
  - Recently scanned, faxed or printed documents
  - Information regarding the purpose or use of the device; credit card readers
- Peripheral devices can be sources of fingerprints, DNA & identifiers and should be handled in a manner to preserve that evidence
Other Sources of Digital Evidence

Items and devices may be present that function independently or connected to computers. These items may be digital evidence.
Other Sources of DE

- Video Cameras
- Digital Cameras
- Digital Video Recorders
- Monitoring & Surveillance Equipment
- Audio Recorders
- Satellite Receivers & Access Cards
Digital Evidence Collection Training for Law Enforcement

Other Sources of DE

Game Consoles

Chat Communicators

Reference Material

SIM Card Reader

Video Players

MP3 & Audio Players
Potential Evidence:

- The intended use of the device
  - What is was designed to do
- The actual use of the device
  - What is was being used / adapted for
- The device may contain data, settings, or other information of evidential value
Questions?
Investigative Tools & Equipment
In most cases, items or devices containing digital evidence can be collected using standard seizure tools & materials.

- Use caution when collecting, packaging, transporting or storing electronic devices to avoid altering, damaging, or destroying digital evidence.

- Avoid using any tools or materials that may produce or emit static electricity or a magnetic field which can damage or destroy the evidence.
If the complexity of the Electronic Crime Scene exceeds the expertise of the First Responder or other Law Enforcement personnel at the scene:

- Request assistance from law enforcement personnel with advanced training, experience and equipment in digital evidence collection.
If a computer, cell phone, electronic device or component is turned off when it is located, leave it off.

- Do not turn on a computer, cell phone, electronic device or component.
- Digital evidence collection procedures will be addressed in detail later.
Tools & Materials for Collecting Digital Evidence
Tools & Materials for Collecting DE

In addition to tools for processing crime scenes in general, First Responders should have the following items in their Digital Evidence Collection toolkit:

- Cameras (photo & video)
- Cardboard boxes
- Notepads
- Gloves
- Evidence inventory logs
- Evidence tape
- Paper evidence bags
- Evidence stickers / labels
- Crime scene tape
- Antistatic bags
- Permanent markers
- Nonmagnetic tools
First responders should also have Radio Frequency (RF) shielding material available collecting digital evidence.

- Cell phones use Radio Frequency signals to send & receive communications
- RF shielding material blocks the Radio Frequency connection between cell phone and the service provider signal
Faraday isolation bags, RF shielding material or aluminum foil can be used to wrap cell phones, smart phones and other mobile communication devices after they are seized as evidence.

- Wrapping the phones / devices in RF shielding material prevents the phones from receiving a call, text message or other communication signal that may alter the evidence.
It is important to remember:

- Applications designed to erase the data from a phone & render it unusable if it is lost or stolen are available.
- That technology can be activated if a phone is seized as evidence and remains connected to the service provider’s network.
- To maintain the integrity of the data on the phone, it is important to prevent a cell phone from accessing a network with RF shielding material.
It is important to remember:

- Some cell phones will boost power to acquire a signal when they are wrapped in RF shielding material.
- The battery may lose its charge faster than normal causing the phone to turn off.
- If a phone turns off, data may be lost.
Securing & Evaluating the Scene
Securing & Evaluating the Scene

Remember, Officer safety & the safety of everyone at the scene is the most important consideration.

- All actions and activities carried out at the scene should comply with departmental policy as well as federal, state & local laws.
- After securing the scene & all persons at the scene, visually identify all potential evidence & ensure that the integrity of all evidence is preserved.
- Digital evidence can be easily altered, deleted or destroyed.
- Digital evidence should be documented, photographed & secured as soon as possible.
When securing & evaluating the Electronic Crime Scene:

- Follow departmental policy for securing crime scenes
- Immediately secure all electronic devices, including personal & portable devices
- Ensure that no unauthorized person has access to any electronic devices at the crime scene
- Refuse offers of help or technical assistance from any unauthorized persons
- Remove all persons from the scene and the area from which evidence is to be collected
- Ensure that the condition and power state of any electronic device is not changed
Securing & Evaluating the Scene

Components & peripheral devices may contain latent evidence such as fingerprints, DNA or other physical evidence that should be preserved.

- Ensure that latent evidence is not compromised during documentation of the scene or evidence collection

- Ensure that latent evidence processing does not affect the integrity of the digital evidence
If a computer is powered “on” or the power state cannot be determined:

- **Look & listen** for indications that the computer or device is running,
  - **Listen** for fans running or drives spinning
  - **Look** to see if any Light Emitting Diodes (LEDs) are on

- **Check** the screen for indications that digital evidence destruction is taking place
  - **Look** for on-screen indication of data destruction such as: delete, format, remove, copy, move, cut, or wipe
Securing & Evaluating the Scene

Look for indications that the computer is being accessed from a remote computer or device:

- **Look** for signs of active or ongoing communication with other computers or users
  - Instant Messaging
  - Chat Rooms
- Take note of all cameras, web cameras (webcams) & determine if they are active
Developments in computer & communication technology can link conventional devices & services to each other, computer systems & the Internet.

- Digital evidence may also be found in:
  - telephone systems
  - digital video recorders
  - video & audio monitoring devices
  - household appliances
  - motor vehicles
  - Watercrafts - GPS
Preliminary Interviews
Preliminary Interviews

Separate & identify all adults at the scene and record their location at the time of entry onto the scene

- Do not allow anyone to access any computer or electronic device
Preliminary Interviews

Obtain and document:

- Users and account information for the computers & devices
- All computer & Internet user information
- All login names & user account names
- Purpose & uses of computers & devices
- All passwords
- Any automated applications in use
- Type of Internet access & Service Provider
- Any offsite data storage
- Installed software documentation
- All Email accounts
- Security provisions in use
- Web mail account information
- Data access restrictions in place
- All Instant Message screen names
- All destructive devices or software in use
- MySpace, Facebook or other Online social site information
- Any other information relevant to the investigation
Questions?
Documenting the Scene
Documenting the Scene

Documentation of a scene creates a record for the investigation and prosecution

- It is important to accurately record the:
  - Location of the scene
  - Scene itself
  - Location, state, power status & condition of computers, components, cell phones & electronic devices
  - Internet & network access

All of the digital evidence may not be in close proximity to the computer or other devices
Documenting the Scene

Thorough documentation may involve moving a computer or device to locate serial number or identifiers.

- Some documentation may be performed during the collection phase presented in Module 5.
- The location & position of the computer or electronic devices should be documented & photographed before it is moved.
- All actions should be documented in detail.
Documenting the Scene

Initial documentation

- video, photographs, notes or sketches
- all activity and processes on display screens should be fully documented

Documentation should include

- Location
- the type
- position of the computers, components, peripherals & electronic devices
- Powered on or not!!!!
Documenting the Scene

The scene may expand to multiple locations

- Document:
  - All connections
  - Network components
  - Wireless access points
Documenting the Scene

Network & wireless access points indicate Internet access and access to remote computers or devices that may not be at the initial scene

- Remote computers indicate that additional digital evidence may exist elsewhere
- Remote computers or devices can be used to run destructive processes in an attempt to destroy digital evidence
Circumstances may prevent the collection of all the digital evidence at a scene

- Prevailing laws, agency policies or other factors may prohibit the collection of some computer systems, components or devices and the information they contain, however these devices should be included in the documentation of the scene.
Questions?
Evidence Collection
Evidence Collection

Proper authority to search for & collect evidence must exist

- Plain View
- Consent
- Court Order
- Exigent circumstances

If in doubt

- Follow departmental guidelines
- Consult a supervisor
- Contact the prosecuting attorney
Evidence Collection

The integrity of the physical device as well as the data it contains must be preserved

- Some digital evidence requires special collection, packaging and transportation
- Data can be damaged or altered by common environmental factors
  - static electricity
  - electromagnetic fields
  - radio transmitters.
Evidence Collection

Cell phones, smart phones, and PDAs should be secured & prevented from transmitting or receiving a signal

- RF Shielding material should be used to prevent access to a service provider’s network
- Incoming calls or messages could alter and possibly destroy data on the phone
Collection Tools
Faraday Cloth
Collection Tools & Materials

Faraday Tent
Questions?
Computer System Assessment
Once the power state of the computer, component or device is determined, follow the steps that best match the situation

- Document the details of the situation and the steps you followed to collect the Digital Evidence
Examples of assessing the situation are listed on pages 22 to 27 of the “Guide for First Responders” and on pages 12 to 20 of the Flip Guide: “On-the-Scene Reference for First Responders”
Assess the Situation

**Situation 1:** The monitor is on. It displays a program, application, work product, picture, Email, or Internet site on the screen

**Step 1:** Photograph the screen & record the information displayed

**Step 2:** Proceed to “If the Computer is ON”
Assess the Situation

**Situation 2:** The monitor is on and a screensaver or picture is visible

**Step 1:** Move the mouse slightly WITHOUT depressing any buttons or rotating the wheel. Note any onscreen activity that causes the display to change to a login screen, work product or other visible display.

**Step 2:** Photograph the screen & record the information displayed.

**Step 3:** Proceed to “If the Computer is ON”
Situation 3: The monitor is on however the display is blank as if the monitor is off

Step 1: Move the mouse slightly WITHOUT depressing any buttons or rotating the wheel. Note any onscreen activity that causes the display to change to a login screen, work product or other visible display

Step 2: Photograph the screen & record the information displayed

Step 3: Proceed to “If the Computer is ON”
Situation 4a: The monitor is powered off
The display is blank

Step 1: If the monitor power is off, turn the monitor on. If the display changes from a blank screen to a login screen, work product or other visible display, document the change in the display.

Step 2: Photograph the screen & record the information displayed.

Step 3: Proceed to “If the Computer is ON”.
Situation 4b: The monitor is powered off
The display is blank

Step 1: If the monitor power switch is in the off position, turn the monitor on. The display does not change, it remains blank. Document that no change in the display occurs.

Step 2: Photograph the blank screen.

Step 3: Proceed to “If the Computer is “OFF”
**Situation 5:** The monitor is powered on. The display is blank

**Step 1:** Move the mouse slightly without pressing any buttons or rotating the wheel; wait for a response

**Step 2:** If there is no change on the display, confirm that the monitor has power, check the computer case for indications that the computer is on.

**Step 3:** If the screen is blank & there is no indication that the system is powered on, proceed to “If the Computer is OFF”
If the computer is OFF

Desktop, tower & minicomputer, follow these steps:

1. Document, photograph & sketch all wires, cables & devices connected to the computer
2. Label power supply cord & all cables, wires, & devices attached to the computer as well as the connection each cord, wire, cable, & device occupies on the computer
3. Photograph the labeled cords, cables, wires & devices & the corresponding connection
4. Remove & secure the power supply cord from the back of the computer & from the wall outlet, power strip or battery backup device
5. Disconnect & secure all cables, wires, & devices from the computer & document the device connected to the other end.
Seizing a Computer

If the computer is OFF

Desktop, tower & minicomputer, follow these steps:

6. Place tape over the floppy disk slot (if present)
7. Ensure the CD & DVD drive trays are retracted, note if the drive is empty, contains a disk or if it is unknown. Place tape over the drive tray
8. Place tape over the power switch
9. Document the make, model, serial number & any user applied identifiers
10. Log the computer, cords, cables, wires, devices & components as evidence according to departmental procedures
11. Package all evidence to prevent damage or alteration during transportation or storage
Seizing a Computer

If the computer is OFF

For laptop computers follow these steps:

1. Document, photograph & sketch all wires, cables & devices connected to the laptop
2. Label all wires, cables & devices connected to the laptop & the connection they occupy
3. Photograph the labeled wires, cables & devices & the connection they occupy
4. Remove & secure the power supply & all batteries
5. Disconnect & secure all cables, wires & devices from the laptop & document the device at the other end
Seizing a Computer

If the computer is OFF

For Laptop computers follow these steps:

6. Place tape over the floppy drive (if present)
7. Ensure the CD / DVD drives are retracted & note if they are empty, occupied or unknown. Place tape over drive
8. Place tape over the power switch
9. Document the make, model, serial numbers & user applied markings
10. Log the laptop, cables, wires & devices as evidence as per departmental procedures
11. Package all evidence to prevent damage during transportation or storage
Seizing a computer

If the computer is ON

- For practical purposes, removing the power supply from the back of the computer when seizing a computer is generally the safest option.

- If evidence of a crime is visible on screen, request assistance from personnel with experience in volatile data capture & preservation before pulling the plug.
Seizing a computer

If the computer is ON

In the following situations, immediate power disconnection IS recommended:

- Information or onscreen activity indicates that data is being deleted or overwritten
- Indication that a destructive process is being performed on the data storage devices
- The computer is running in a Microsoft® Windows® environment. Pulling the power from the back of the computer will preserve information about the last user account logged in, time of last login, most recently used documents, most recently used commands & other valuable information.
Seizing a computer

If the computer is ON

In the following situations, immediate power disconnection IS NOT recommended:

Information of apparent evidentiary value is in plain view onscreen. Seek assistance from personnel with experience & training in volatile data capture & preservation before proceeding.
Seizing a computer

If the computer is ON

If there are indications that any of the following are active or in use:

- Chat Rooms
- Open text documents
- Remote data storage is being accessed
- Open Instant Message windows
- Child Pornography
- Contraband
- Financial documents or transactions
- Obvious illegal activities

Request assistance from personnel with experience & training in volatile data capture and preservation
Seizing a computer

Servers, networked computers & mainframe computers:

- Secure the scene & request assistance from personnel who have experience & training in seizing large or complex computer systems. Technical assistance is available in your Guide for First Responders, Second Edition Books and Pocket Guides.
Labeling Digital Evidence
Labeling Digital Evidence

Each item of evidence seized should be clearly labeled and identified

- Components should only be disassembled to the extent necessary to secure & transport

- If disassembly or disconnection of components is necessary, clearly label each component and each connection to facilitate re-assembly

- If more than one computer system is seized, uniquely label the computer system to ensure the components and connections of each system are clearly identified
Perfect World:
Label the computer, all cables and corresponding connections

Real World:
Take digital images and document of all connections prior to removing them and only seize the computer itself.
Other Forms of Evidence
Other forms of Evidence

Look for:
- Pieces of paper with possible passwords
- Handwritten notes
- Blank pads of paper with impressions from prior writings
- Hardware & software manuals & instructions
- Calendars
- Literature & reference materials
- Text or graphic printed material from the computer that may be relevant to the investigation

These items should be documented and seized as evidence following departmental procedures.
Other Electronic & Peripheral Devices of Potential Evidential Value
Other Electronic & Peripheral Devices

The following devices may be, or contain digital evidence

- Audio recorders
- Answering machines
- Computer chips
- Pagers
- Cordless phones
- Scanners
- Caller ID units
- Fax Machine
- Hard drive duplicators

If these devices are seized, the power supplies, adapters & documentation for these devices should be seized as well.
Digital evidence and electronic devices should not be operated and the information they contain should not be accessed directly, except in emergent situations.

- If the circumstances warrant immediate access to the device and the information contained, all actions taken should be thoroughly documented.
- Data may be lost or damaged if a device is not properly handled or if the data is not properly accessed.
Other Electronic & Peripheral Devices

Special handling may be required to preserve the integrity of these devices.

- For more information or technical assistance, refer to your Guide for First Responders Second Edition Books, and the Pocket Guides.
Computer Networks and Computers in a Business Environment
Business environments

- complicated configurations
- multiple computers
- common server
- networked devices

- Securing a scene & collecting digital evidence in a business environment may pose challenges.

- Improperly shutting down a system may result in loss of data, loss of digital evidence and potential civil liability
Servers

- Rack Mounted
- Blade
- A PC can be used as a server

- Servers should only be seized by personnel trained in server seizure
Similar environments exist in residential locations, particularly when a business is operated from the home

- Such circumstances are beyond the scope of this course.
- For more assistance refer to your Guide for First Responders Second Edition Books, and your Pocket Guides.
Computer Networks

- Computer networks consist of two or more computers linked by data cables or wireless connections that are capable of sharing resources & data

- Often include:
  - Printers
  - Peripheral devices
  - Data routing devices
    - Hubs
    - Switches
    - Routers
Computer Networks
Computer Networks

Items that indicate a wireless network, additional computer systems, external hard drives or other data storage devices may be located at the scene.
Evidence that may be found on computer networks:

- Email messages
- Internet browsing history
- Internet chat logs
- Buddy lists
- Photographs
- Documents
- Image files
- Database files
- Financial records
- Event logs
- Software
Questions?
Packaging, Transportation & Storage of Digital Evidence
Digital evidence is fragile and sensitive to:
- extreme temperatures
- humidity
- physical shock
- static electricity
- magnetic fields

Take precautions when:
- documenting
- photographing
- packaging
- transporting
- storing
Packaging Procedures
All actions should be thoroughly documented

- identification,
- collection,
- packaging,
- transportation
- storage
When packing digital evidence for transport:

- Ensure that all Digital Evidence collected is properly labeled and logged.
- Digital Evidence may also contain latent, trace, or biological evidence, handle accordingly.
- Antistatic packaging is preferred
  - paper bags
  - Envelopes
  - cardboard boxes
  - antistatic containers
- Avoid plastic packaging
Packaging Procedures

Packing procedures

- Ensure that all Digital Evidence is packaged in a manner that will prevent it from being bent, scratched or otherwise damaged
- Label all containers used to package & store digital evidence clearly & properly
Packaging Procedures

Packing procedures

- Leave cell phones & smart phones in the power state in which they were found; (on or off)

- Use RF signal blocking material such as faraday isolation bags, radio frequency shielding material or aluminum foil
  - prevent calls or data messages from being sent or received by the seized devices.

- Collect all power supplies and adapters
Transportation Procedures
Transporting digital evidence

- Keep Digital Evidence away from magnetic fields
  - radio transmitters
  - speaker magnets
  - magnetic mount emergency lights

- Other potential hazards
  - vehicle seat heaters
  - vehicle carpet
  - trunk lining material
When transporting digital evidence:

- Avoid leaving digital evidence in a vehicle for a prolonged period
  - heat
  - cold
  - humidity
  - can damage or destroy digital evidence

- Protect from shock or vibration
- Maintain the chain of custody
Storage Procedures
Storage Procedures

Storing digital evidence:

- Inventory in accordance with agency policies
- Store in a secure, climate controlled environment
  - Avoid locations subject to extreme temperature or humidity
- Avoid
  - magnetic fields
  - Moisture
  - Dust
  - Vibration
- any elements that may damage or destroy it
Dates, times and system configuration settings may be lost due to prolonged storage

- batteries or power source that preserve this information may fail over time

Advise the evidence custodian and forensic examiner that the electronic devices are battery powered and require prompt attention to preserve the data.
Questions?
Electronic Crime & Digital Evidence Considerations by Crime Category
Evidence collection should focus on the crime and criminal activity under investigation

- some items are collected as evidence in every investigation
- items and devices unique to a crime category can be valuable
- know where to get information on evidence of relevance in each crime category
The following are examples of items that should be secured at Electronic Crime Scenes by crime category.

These are listed on pages 35 to 47 of the “Guide for First Responders” and on pages 23 to 36 of the Flip Guide: “On-the-Scene Reference for First Responders”
Potential Digital Evidence by Crimes:

- Child Abuse and/or Exploitation Cases
- Computer Intrusion
- Counterfeiting
- Death Investigations
- Domestic Violence, Threats, and Extortion
- E-mail Threats, Harassment, and/or Stalking
- Gambling
- Identity Theft
- Narcotics
- Online Fraud and/or Economic Fraud
- Prostitution
- Software Piracy
- Telecommunication Fraud
- Terrorism
E-Crime & DE Considerations

The following information should be submitted with the digital evidence to be examined:

- A Summary of the case facts
- Passwords for digital evidence
- Investigation point of contact
- Preliminary Reports, Court Orders, Consent forms & relevant documents
- Keyword lists & search criteria
- Suspected criminal activity
- Suspect information
Potential Digital Evidence in all cases!

- Computers
- External Data storage devices
- Removable media
- Cell Phones / Smart Phones
- Internet activity records
- Records of chat sessions
- Screen names & buddy lists
- Printed Email & notes
- Web cameras
- Microphones
- Information on Steganography
- User names & passwords
- Contact lists
Questions?
Post Test Evaluations
Get Out Early
Post Test

- So we can evaluate how well we did.