Digital Evidence: Search and Seizure

Introduction to Digital Evidence and the IWRCFL

Detective Sean Drew
Sandy City Police Department
Computer Forensic Examiner, IWRCFL
What is the IWRCFL?

- **Intermountain West Regional Computer Forensic Laboratory**
- **FBI sponsored single service forensic laboratory devoted to the examination of digital evidence in support of criminal, counterterrorism, and counterintelligence investigations.**
- A team of sworn and non-sworn law enforcement individuals trained in digital forensics to examine digital evidence and provide testimony of that evidence in a court of law.
- **ASCLD/Lab International Accreditation**
- A unique law enforcement partnership (Federal, State & Local LE Agencies) that promotes quality and strengthens digital forensics capacity.
16 RCFLs in the United States
Participating Agencies

- FBI (4 total)
  - Salt Lake City (3 full-time)
  - Montana (1)
- Utah State DPS (2)
  - 1 audio / video
- Utah Attorney General’s Office (1)
- Boise PD (1)
- Ada County Sheriff (1) (Idaho)

- Salt Lake City PD (1)
- Sandy PD (1)
- Davis County Sheriff (1)
- West Valley PD (1 full-time)
  - 1 associate
- Billings PD (1) (Montana)
The Problem

All law enforcement agencies continue to experience the exponential growth of the use of computers to commit crimes.

Computer Crimes include:

- Child Pornography
- Computer Intrusion-Hacking-theft
- Drug Trafficking
- Environmental Crime
- Financial - WCC-ID Theft, $ laundering
- Internet Fraud
- Terrorism-recruitment-financial support
The Challenges

Law enforcement officers need training in the proper procedures for seizing digital evidence. What do I do with the evidence?

Defense attorneys are beginning to challenge how computer-based evidence is collected and how long it takes law enforcement to image or examine evidence.

Attacking the Forensic process in court

The average imaging and analysis process takes approximately 20 hours for each hard drive associated with a case. Cases typically have multiple CPUs and hard drives in addition to other media.
Evidence Examined by the IWRCFL (fiscal year)
Increasing Capacity

• Today’s (2014) Average Computer Hard Drive
  • 1 terabytes = 800 million typed pages or 250,000 mp3 @ 4MB or 128 Full length DVDs @8GB
    • 1TB = 1024 GB
  • As of 8/2/2013, (Newegg.com)
    - 1 Terabyte hard drive = $70 ($56 as of 10/4/2011, $109 5/14/2012)
    - 2 TB = $80 as of 10/4/2011, $119 now
    - 3TB = $180 as of 10/4/2011, same price now
  • One Megabyte of printed material is about 500 typed pages
  • Two Gigabytes of printed material stacked would be the approximately the height of the Washington Monument 555 feet tall.
Criminal Uses of Digital Technology

- Devices such as computers may be the **target** of the crime (e.g. systems intrusion)

- Digital devices may be the **instrument** of the crime

- Electronics devices may be the **repository** of the evidence
What is Digital Evidence?

- Desktop Computers
- Laptop Computers
- Networked CPUs
- Floppy Diskettes
- CD / DVD
- Hard Drives- External and Internal
- Solid State drives
- Thumbdrive/Flash Memory/SD cards
- Digital watches
- Tapes
- PDAs
- Cell Phones
- Digital Cameras

*Some digital storage devices are as small as a dime!*
Computers as Targets of the Crime

Intrusions

- Theft of data
- Theft of service
- Damage to data
- Web defacement

Victims because:

- Agency/company target
- Easy target
  - Systems not patched
  - Weak security
Computers as 
Instruments of Crime

Examples to think about:

• Solicitation of Minors
• Harassment and Stalking
• Medical Fraud
• Credit Card Fraud
• Identity Theft / Fraud
• Counterfeiting

This list is by no means exhaustive
Computers as Repository of the Evidence

- Fraud and Embezzlement
- Child Pornography
- Narcotics
- Traditional Crimes
  - Such as homicide or burglary
- Think outside of the box with digital evidence in these cases
Criminal Uses of Digital Technology

Digital devices can help criminals avoid detection:

- **Anonymity**
  - Hiding their ID (Spoofing)
  - Anonymizing Websites
  - Proxy Servers

- **Data encryption**
  - Prevents law enforcement from finding digital evidence - temporarily

- **Key loggers**
- **Data Sniffers**
What about other activity?

- Possible relationship between criminal activity of all sorts and potential digital evidence.

- Domestic Violence
- Stalking
- Harassment
- Drug cases
Protecting evidence on a personal computer

- Unplug power to modem or router
- If computer is on, photograph the screen
- Look for icons indicating encryption
- If possible, have owner disable encryption software
- Label and photograph back of computer and all component wires
- Unplug power cord from back of tower
Protecting evidence on a laptop computer

- Turn off WiFi switch, and unplug modem or router
- Photograph the screen
- Look for encryption icons
- Laptop will run on battery after unplugging it – Keep the power cable!
ID Theft Tools

- Key Loggers
  - Hardware
  - Software
    - SpectraSoft
    - WebWatcher
    - MobiStealth
    - Squidoo

- IP Cameras
- Wireless
On Line Storage

- Access anywhere there is an internet connection.
- Relatively inexpensive
- Newer technology
- Hosted off site
Wireless Technology

• Secured or unsecured? WEP/WPA
Evidence Items that a mobile device examination can retrieve are:

- Missed phone calls
- Last dialed calls
- Received calls
- Phone book
- Text messages
- Graphic images
- Stored video

Sometimes...it depends
Protecting Data on a mobile device

- Put the device in airplane mode
- Turn off WiFi
- If possible, turn security features off
- Write down swipe code or password
- Secure device in a faraday bag or evidence canister
What information data records provide:

- Contact Lists
- Date and time of calls
- Phone number called
- Phone company
- Location of the cell site
- General location of calls made from personal cell phones
- SMS and MMS
- Photographs
- Videos
What do cell sites look like?

- Some are on buildings
- Some are actual towers
Obtaining Metadata from device

- Suspect’s phone seized during arrest
- Processed for information, including pictures
- Latitude and Longitude metadata from pictures on phones provided locations of other grows
Identifying Digital Evidence
Game Systems
Identifying Digital Evidence
Flash Drives
Access PC from anywhere

- Using the Remote software a user can log onto their computers from off-site locations.
  - User logs onto their work computer from home using the built in utility or a web browser application.
Wireless Concerns

• Investigator may want to have a Wifi Locator (most smartphones) to see if there are any wireless networks at the search location

• Remember there maybe other computers, or hard drives hidden
**Encryption**

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.

ciphertext - is encrypted text
Encryption Icons

XP style encrypt

Strong Encryption
Reference Materials

www.ncjrs.gov

www.rcfl.gov
Questions?

sdrew@sandy.utah.gov