



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

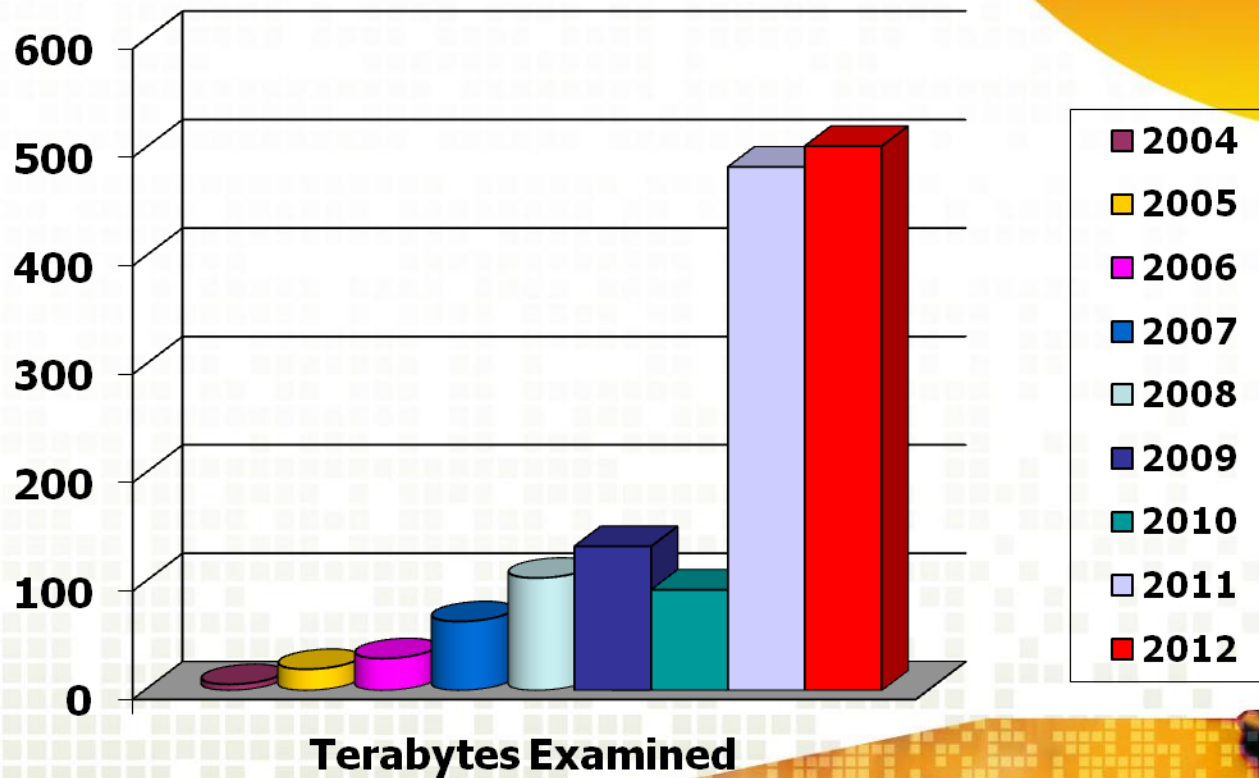
Law enforcement officers need training in the proper procedures for seizing digital evidence. What do I do with the evidence?

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)

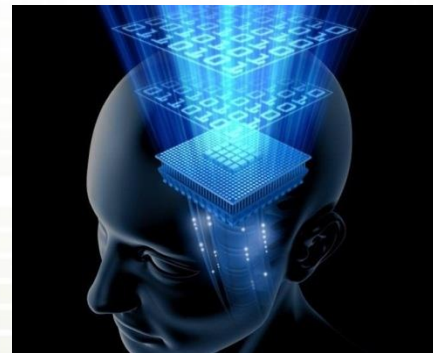


Increasing Capacity

- 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.

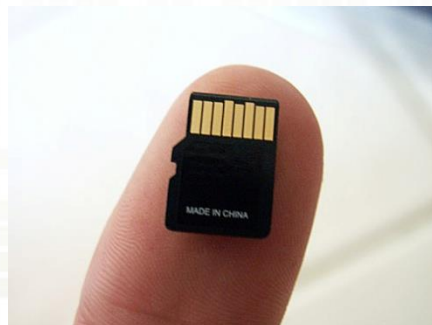
Criminal Uses of Digital Technology

- 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

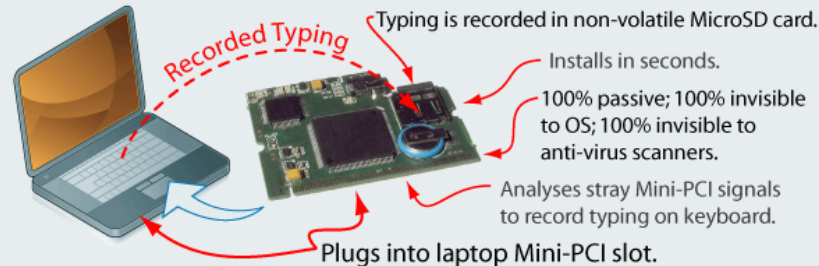
- SpectraSoft
 - WebWatcher
 - MobiStealth
 - Squidoo

- IP Cameras

- Wireless



Record typing on a laptop keyboard



On Line Storage

2009 Online Storage Services Product Comparisons

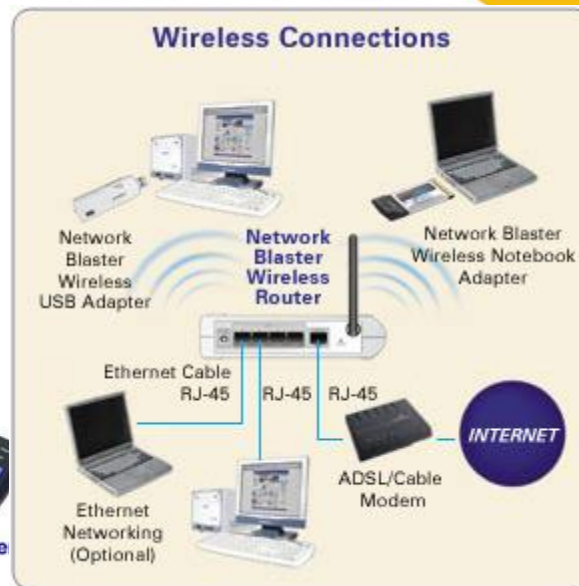
Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Services	Box.net	iCloud	Dropbox	Google Drive	OneDrive	Amazon Drive	Microsoft OneDrive	Dropbox	Google Drive	Amazon Drive
Monthly Fee for at Least 5 GB of Space	\$7.95	\$4.95	\$4.95	\$4.95	\$4.95	\$4.95	\$5.99	\$6.99	\$9.95	\$9.95
Overall Rating	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Features	Search Access	Mobile Access	Private File Sharing	Public File Sharing	Scheduled Backup	File Versioning	One and Done	Sub-Accounts	Offline File Access	Security
SSL Encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Storage Space/Price Month	1 GB	Free	Free	Free	Free	\$0.12	Free	\$0.12	Free	Free
5 GB	\$7.95						\$6.99	\$11.40	\$9.95	
15 GB	\$19.95						\$17.99	\$19.95	\$19.95	
25 GB							\$17.99	\$19.95	\$19.95	
50 GB		\$6.95					\$17.99	\$19.95	\$19.95	
100 GB		\$13.95					\$17.99	\$19.95	\$19.95	
200 GB							\$17.99	\$19.95	\$19.95	
250 GB		\$13.95					\$17.99	\$19.95	\$19.95	
300 GB							\$17.99	\$19.95	\$19.95	
500 GB		\$19.95					\$17.99	\$19.95	\$19.95	
750 GB		\$19.95					\$17.99	\$19.95	\$19.95	
1,000 GB		\$19.95					\$17.99	\$19.95	\$19.95	

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

Wireless Technology

- Secured or unsecured? WEP/WPA

From Computer Desktop Encyclopedia
Reproduced with permission.
© 2004 Cisco Systems, Inc.



Cell Phone Forensics

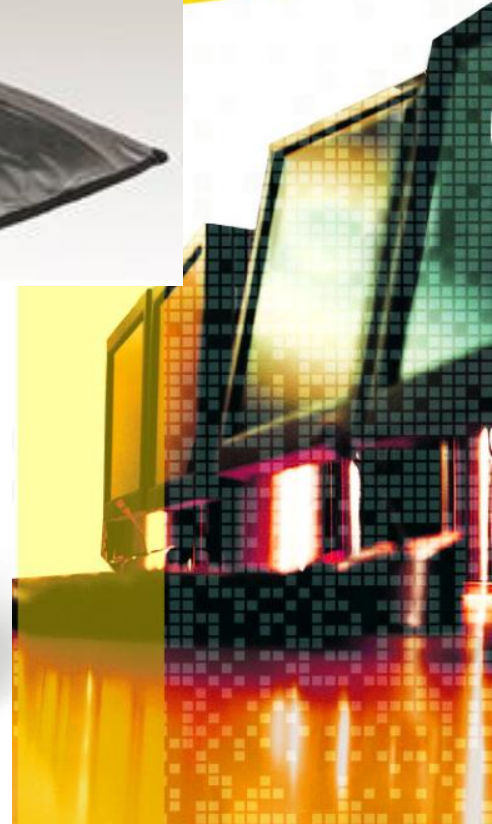
- Evidence Items that a mobile device examination can retrieve are:

- 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**



A collage of three images. The top-left image is a map of Salt Lake City, Utah, showing the downtown area. Key landmarks include the Capitol Hill, Salt Lake City City Hall, and the Salt Lake Area Chamber of Commerce. The map includes street names like 1st Ave, E South Temple, and E 400 S. The bottom-left image is a close-up of a modern building's glass facade, reflecting the surrounding environment. The right image is a close-up of a person's face, partially obscured by a grid pattern, with a bright light source visible in the background.

-
- The map displays a grid of streets in Salt Lake City, Utah. Major streets shown include N 400 W, N 200 W, N 100 S, W 400 S, W 200 S, W 100 S, W 600 S, W 700 S, W 800 S, W 900 S, W 1000 S, W 1100 S, W 1200 S, W 1300 S, W 1400 S, W 1500 S, W 1600 S, W 1700 S, W 1800 S, W 1900 S, W 2000 S, W 2100 S, W 2200 S, W 2300 S, W 2400 S, W 2500 S, W 2600 S, W 2700 S, W 2800 S, W 2900 S, W 3000 S, W 3100 S, W 3200 S, W 3300 S, W 3400 S, W 3500 S, W 3600 S, W 3700 S, W 3800 S, W 3900 S, W 4000 S, W 4100 S, W 4200 S, W 4300 S, W 4400 S, W 4500 S, W 4600 S, W 4700 S, W 4800 S, W 4900 S, W 5000 S, W 5100 S, W 5200 S, W 5300 S, W 5400 S, W 5500 S, W 5600 S, W 5700 S, W 5800 S, W 5900 S, W 6000 S, W 6100 S, W 6200 S, W 6300 S, W 6400 S, W 6500 S, W 6600 S, W 6700 S, W 6800 S, W 6900 S, W 7000 S, W 7100 S, W 7200 S, W 7300 S, W 7400 S, W 7500 S, W 7600 S, W 7700 S, W 7800 S, W 7900 S, W 8000 S, W 8100 S, W 8200 S, W 8300 S, W 8400 S, W 8500 S, W 8600 S, W 8700 S, W 8800 S, W 8900 S, W 9000 S, W 9100 S, W 9200 S, W 9300 S, W 9400 S, W 9500 S, W 9600 S, W 9700 S, W 9800 S, W 9900 S, W 10000 S, W 10100 S, W 10200 S, W 10300 S, W 10400 S, W 10500 S, W 10600 S, W 10700 S, W 10800 S, W 10900 S, W 11000 S, W 11100 S, W 11200 S, W 11300 S, W 11400 S, W 11500 S, W 11600 S, W 11700 S, W 11800 S, W 11900 S, W 12000 S, W 12100 S, W 12200 S, W 12300 S, W 12400 S, W 12500 S, W 12600 S, W 12700 S, W 12800 S, W 12900 S, W 13000 S, W 13100 S, W 13200 S, W 13300 S, W 13400 S, W 13500 S, W 13600 S, W 13700 S, W 13800 S, W 13900 S, W 14000 S, W 14100 S, W 14200 S, W 14300 S, W 14400 S, W 14500 S, W 14600 S, W 14700 S, W 14800 S, W 14900 S, W 15000 S, W 15100 S, W 15200 S, W 15300 S, W 15400 S, W 15500 S, W 15600 S, W 15700 S, W 15800 S, W 15900 S, W 16000 S, W 16100 S, W 16200 S, W 16300 S, W 16400 S, W 16500 S, W 16600 S, W 16700 S, W 16800 S, W 16900 S, W 17000 S, W 17100 S, W 17200 S, W 17300 S, W 17400 S, W 17500 S, W 17600 S, W 17700 S, W 17800 S, W 17900 S, W 18000 S, W 18100 S, W 18200 S, W 18300 S, W 18400 S, W 18500 S, W 18600 S, W 18700 S, W 18800 S, W 18900 S, W 19000 S, W 19100 S, W 19200 S, W 19300 S, W 19400 S, W 19500 S, W 19600 S, W 19700 S, W 19800 S, W 19900 S, W 20000 S, W 20100 S, W 20200 S, W 20300 S, W 20400 S, W 20500 S, W 20600 S, W 20700 S, W 20800 S, W 20900 S, W 21000 S, W 21100 S, W 21200 S, W 21300 S, W 21400 S, W 21500 S, W 21600 S, W 21700 S, W 21800 S, W 21900 S, W 22000 S, W 22100 S, W 22200 S, W 22300 S, W 22400 S, W 22500 S, W 22600 S, W 22700 S, W 22800 S, W 22900 S, W 23000 S, W 23100 S, W 23200 S, W 23300 S, W 23400 S, W 23500 S, W 23600 S, W 23700 S, W 23800 S, W 23900 S, W 24000 S, W 24100 S, W 24200 S, W 24300 S, W 24400 S, W 24500 S, W 24600 S, W 24700 S, W 24800 S, W 24900 S, W 25000 S, W 25100 S, W 25200 S, W 25300 S, W 25400 S, W 25500 S, W 25600 S, W 25700 S, W 25800 S, W 25900 S, W 26000 S, W 26100 S, W 26200 S, W 26300 S, W 26400 S, W 26500 S, W 26600 S, W 26700 S, W 26800 S, W 26900 S, W 27000 S, W 27100 S, W 27200 S, W 27300 S, W 27400 S, W 27500 S, W 27600 S, W 27700 S, W 27800 S, W 27900 S, W 28000 S, W 28100 S, W 28200 S, W 28300 S, W 28400 S, W 28500 S, W 28600 S, W 28700 S, W 28800 S, W 28900 S, W 29000 S, W 29100 S, W 29200 S, W 29300 S, W 29400 S, W 29500 S, W 29600 S, W 29700 S, W 29800 S, W 29900 S, W 30000 S, W 30100 S, W 30200 S, W 30300 S, W 30400 S, W 30500 S, W 30600 S, W 30700 S, W 30800 S, W 30900 S, W 31000 S, W 31100 S, W 31200 S, W 31300 S, W 31400 S, W 31500 S, W 31600 S, W 31700 S, W 31800 S, W 31900 S, W 32000 S, W 32100 S, W 32200 S, W 32300 S, W 32400 S, W 32500 S, W 32600 S, W 32700 S, W 32800 S, W 32900 S, W 33000 S, W 33100 S, W 33200 S, W 33300 S, W 33400 S, W 33500 S, W 33600 S, W 33700 S, W 33800 S, W 33900 S, W 34000 S, W 34100 S, W 34200 S, W 34300 S, W 34400 S, W 34500 S, W 34600 S, W 34700 S, W 34800 S, W 34900 S, W 35000 S, W 35100 S, W 35200 S, W 35300 S, W 35400 S, W 35500 S, W 35600 S, W 35700 S, W 35800 S, W 35900 S, W 36000 S, W 36100 S, W 36200 S, W 36300 S, W 36400 S, W 36500 S, W 36600 S, W 36700 S, W 36800 S, W 36900 S, W 37000 S, W 37100 S, W 37200 S, W 37300 S, W 37400 S, W 37500 S, W 37600 S, W 37700 S, W 37800 S, W 37900 S, W 38000 S, W 38100 S, W 38200 S, W 38300 S, W 38400 S, W 38500 S, W 38600 S, W 38700 S, W 38800 S, W 38900 S, W 39000 S, W 39100 S, W 39200 S, W 39300 S, W 39400 S, W 39500 S, W 39600 S, W 39700 S, W 39800 S, W 39900 S, W 40000 S, W 40100 S, W 40200 S, W 40300 S, W 40400 S, W 40500 S, W 40600 S, W 40700 S, W 40800 S, W 40900 S, W 41000 S, W 41100 S, W 41200 S, W 41300 S, W 41400 S, W 41500 S, W 41600 S, W 41700 S, W 41800 S, W 41900 S, W 42000 S, W 42100 S, W 42200 S, W 42300 S, W 42400 S, W 42500 S, W 42600 S, W 42700 S, W 42800 S, W 42900 S, W 43000 S, W 43100 S, W 43200 S, W 43300 S, W 43400 S, W 43500 S, W 43600 S, W 43700 S, W 43800 S, W 43900 S, W 44000 S, W 44100 S, W 44200 S, W 44300 S, W 44400 S, W 44500 S, W 44600 S, W 44700 S, W 44800 S, W 44900 S, W 45000 S, W 45100 S, W 45200 S, W 4

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



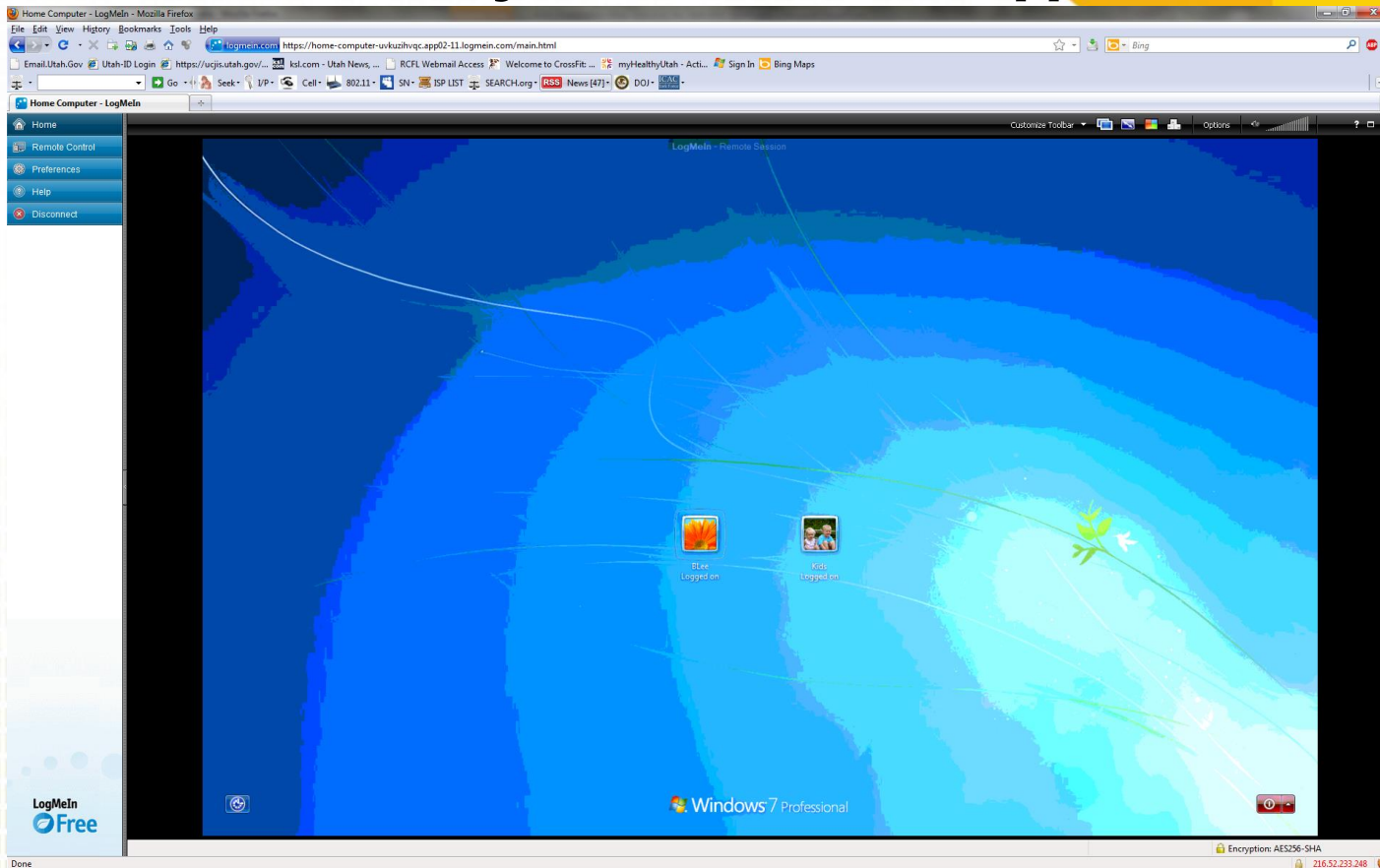
Identifying Digital Evidence

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

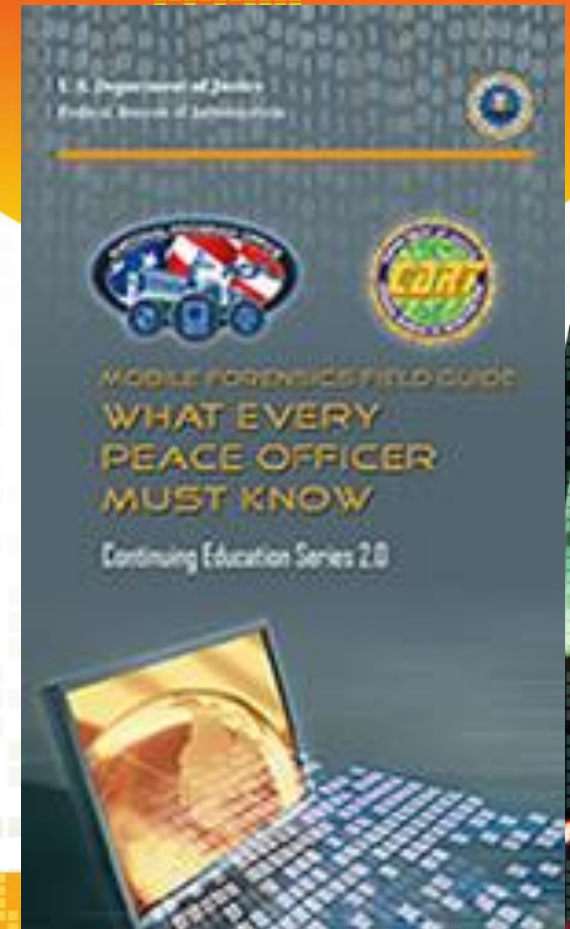
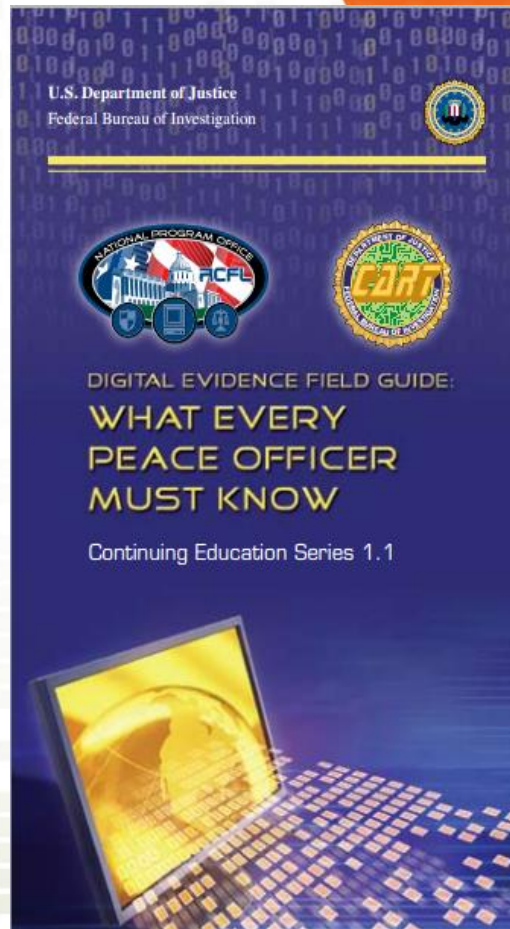
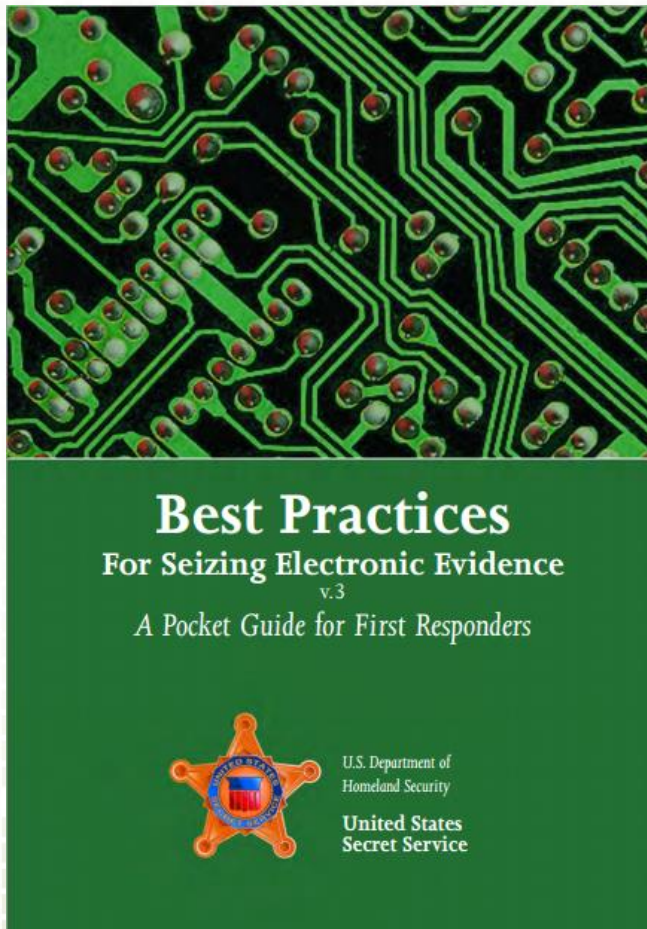
XP style encrypt



Strong Encryption



Reference Materials



www.ncjrs.gov

www.rcfl.gov

Questions?

sdrew@sandy.utah.gov