Digital Forensics

An Overview of Digital Forensics…Emerging Trends and New Technologies
What is Digital Forensics?

- The recovery, preservation and analysis of electronic media found on a variety of digital devices in support of an ongoing Administrative, Civil or Criminal Investigation.

- Is unique and ever changing from the type of evidence to the methodologies used in any given investigation.
  - Digital Forensics Traditional Process Model
  - Cyber Forensics Field Triage Process Model (CFFTPM)

- Is a multifaceted field that typically involves a task-force approach to the entire investigation.
Various Types of Digital Media

- Desktop Computers
- Multi-use Printers
- iPhones
- Servers
- SD Card
- Android Devices
- CCTV
- USB Flash Drive
- Digital Camera
- GPS
- Laptops
Unusual Digital Media
Considerations for Search and Seizure

- **Search Warrant or Knock & Talk?**
  - Have you gathered enough Intelligence for Probable Cause?
  - Or is this merely a fishing expedition?

- **How will you draft a valid search warrant?**
  - Be careful of go-by’s.

- **What seized information could be privileged?**
  - Remember the scope of the investigation.

- **Is information belonging to 3rd parties privileged?**
  - Doctor-Patient, Clergy-Parishioner, Attorney-Client

- **On-sight Triage or Collect the Evidence and Analyze back in the Lab?**
Search and Seizure (cont.)

Wording of warrant and affidavit:

- Data and the media on which it is stored
- Computer hardware and related peripherals to allow us to read the data, if necessary
- Computer software to allow us to read the information and data
- Instruction manuals to allow us to learn about the particular equipment and programs
Laying the Ground Work

- Intelligence is crucial in every case.
  - Know your Target and their level of Computer Expertise.
- What kind of computer system are you supposed to search and seize?
  - Desktops, Laptops, Servers, Removable Media
- What Operating System is being used?
  - Windows, Mac, Unix, Linux, Proprietary
- How do you find out?
  - External Surveillance
  - Internal Surveillance
Case Prep

- What is the role of the electronic media in the case?
- Instrumentality of the offense?
  - Used to produce child pornography
  - Used to create fake Ids
  - Used in gambling operation
  - Used for Health Care Fraud
- Contraband?
  - illegal software
  - computer itself stolen
- Repository of evidence?
  - Electronic file cabinet
- Purchased with proceeds of a crime?
Case Prep (cont.)

- Email? Read/UnRead? How do you address this?

- Do you want to take the peripherals? Printers? Scanners? Media Card Readers? External Hard Drives?

- What Type of Network is it if any? Wired? Wireless?

- What do you intend to do with the computers once you secure them?
Search Prep

- **Forensic Laptop**
  - To include, write blockers, “Clean” external drive for on-site imaging or Triage.
- **Labels**
- **Felt tip marking pens**
- **Blank tags, both sticker and tie tags** for labeling all property.
- **Scissors**
- **Rubber Bands**
- **Rubber gloves**
- **Large and small boxes**
- **Packing material (anti-static bubble wrap if possible)**
- **Evidence bags**
- **Masking Tape**

- **Evidence Tape**
- **Digital Camera**
- **Property Receipt/Release Forms**
- **Inventory Log**
- **Backup Hardware - such as external drives, SCSI and IDE Hard Drives, Optical disk or tape backup.**
- **Printer cables.**
- **Gender changers, null modem cable for serial connections.**
- **Portable printer and computer, including paper, and labels (if used for evidence tagging).**
- **Surge protector, extra power cables, and extension cords.**

**Murphy's Law:**

“*Remember if you don’t bring it, you will end up needing it at the scene.*”
Digital Forensics Traditional Process Model

- Adapted from (cf. Carrier & Spafford, 2003; Beebe & Clarke, 2004; Reith, Carr, & Gunsch, 2002; Rogers, 2006; Stephenson, 2003)
- This method is labor intensive and time consuming.
- A true forensic image of the data on some system to be analyzed in a lab environment.
- Typically not used in a time sensitive investigation.
- Provides a more in-depth analysis of the data.

Where the Fun Begins:

The Search

- Secure the suspect
- Secure the electronic media
- Check the electronic media to see if they are connected to a network or phone line. Photograph connections on rear of computers, network connections at HUBS and any other connections you may need to reconnect
- Photograph (or video) the digital media & its surroundings
- Photograph the display screen and connections on front and back of tower or digital media
- Disconnect printers and all other peripherals. If printing, let finish
  - Remember some printers have hard drives. Print Spool Files can be invaluable.
The Search (cont.)

- Place evidence tape over drives
- Search area around digital media for passwords, notes, user names, etc.
- Seize other disks, CDs, external drives, manuals
- If the computer (s) you are seizing are on, turn them off by pulling the power cord from the rear of the computer. *(This is for Windows computers ONLY, Linux or servers will lose a great deal of data with this method)*
- Remember data you do not collect from the electronic media may not be available later
  - External/Internet Storage (I-drive, X-drive)
  - IRC connections and dialogue in place on arrival
  - Data held in RAM
Adapted from (Rogers, Goldman, Mislan, Wedge and Debrota, 2006)

“Computer Forensics Field Triage Process Model”

This method is completed at the scene

A preview of the User accounts and Browser history in a forensically sound manner.

Typically used in a time sensitive investigation.

Provides a quick scope specific analysis of the data.

There are legal considerations for each approach:

- Seizure and removal
- 4th Amendment issues
- Does the warrant provide for on-site examination?
Point to Ponder

- Other types of evidence.
- Would you give this a second thought?
- Would consider seizing?
- A USB Flash Drive key (like the one to the right) can hold up to 2 Gigabytes of data.
  - That’s:
    - 20,000 pictures
    - 400 mp3 songs
    - 100 videos
Typical Digital Crime Scene
Atypical Server Room
Electronic Evidence

- Electronic evidence is information and data of investigative value based on the scope of your investigation that is stored on or transmitted by an electronic device.
  - Often latent in the same sense as fingerprints or DNA.
  - Can transcend borders with ease and speed.
  - It is fragile and can be easily altered, damaged, or destroyed.
  - Can be time sensitive.
Forensic Analysis

- What happens once computer is seized?
- Hard drive or other storage is “imaged” or copied, usually to another hard drive
- Examinations are done on imaged drive or disk
- Using software such as Encase or FTK Ultimate Toolkit, the equipment is analyzed and searched depending on the type of case
- Erased folders and files are recovered and documented.
- The file structure of the hard drive is documented
- What are the most common places to find evidence?
Where is the Evidence?

Top ten locations for evidence:

1) Internet History files
   bookmarks
   search requests
2) Temp. Internet Files
   cache
      By default most of the internet browsers maintain a folder structure under the user account in temporary internet files. Normally, when an Internet web site is initially accessed, the web page data is downloaded into a cache folder.
   cookies
      A “cookie” is information stored on your computer by a web site.
      Helps that web site “recognize” later
      Typically it will record your preferences
      Each “web page request” is new
Top Ten Areas (cont.)

3) Slack/Unallocated Space
4) Buddy lists, personal profiles, chat room records, P2P other saved “areas”
5) News groups / club lists / postings
6) Settings, folder structure, file names
7) File Storage Dates
8) Software / Hardware added
   - Shows that the user is more than a novice. (i.e. Quickbooks, or some sort of database for record keeping.)
9) File sharing ability
   - Are there Network drives, Wireless, Clouds.
10) E-mail
## Freeware Tools of the Trade

### Computer Forensics Tools
- VLC – video player
- Handy Snap – screen capture
- Printkey2000 – screen capture
- FTK Imager 3.0 – imaging, mount, previewing
- Magic disc – .iso disc image mounting software.
- P2 eXplorer – drive mounting
- Skype log parser – analyze Skype logs files.
- VmWare – mount images as virtual machines
- WriteBlockerXP – software write block of the USB ports.

### Mobile Forensics Tools
- BitPIM – CDMA cell phone software.
- ART – Scroll Analysis software
- Blackberry Desktop Software
- ABC Amber Blackberry Converter
- Flash & Backup – Motorola iden phones
- EasyGPS – way-points and route mapping utility.
- GPSBabel – another GPS mapping utility.
- Phone Image Carver
- FTK 1.81.6 – 5000 objects without a dongle license.

### Triage Forensics (Live CD) Tools
- Bart-PE
- Helix
- Raptor
- Encase boot disk
- Backtrack4
- Deft Linux
- WinFe
Emerging Trends

- “Sexting”
- Human Trafficking via the web
  - Backpage
  - Craigslist
- Peer-to-Peer (P2P)
  - Limewire
  - Frostwire
- Gaming Systems (P2P)
  - Nintendo Wii
  - PlayStation 3
  - Xbox 360°
New Technologies

- Clouds
  - Off-site management of data.
- 4G Cellular technology
- Virtual Machines
  - VMware
  - VirtualBox
- Key loggers
Contact Information

Special Agent Joel F. Wade
Tennessee Bureau of Investigation
Technical Services Unit
901 R.S. Gass Blvd.  3rd Floor
Nashville, TN 37216
joel.wade@tn.gov
615.744.4259 (office)
615.739.1653 (mobile)