Concurrent Session VI: 6.03 Digital Evidence Handling: Chain of Custody

September 26, 2006

2:45pm-3:45pm

Jody S. Hawkins, ISO, Children's Medical Center Dallas

Definitions

- Electronic Discovery – (also called e-discovery or ediscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network. Court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery.
- Chain of Custody – The "chain of custody" is a concept in jurisprudence which applies to the handling of evidence and its integrity.
  - "Chain of custody" also refers to the document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.
  - Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

Important Information

- This presentation will cover investigative procedures dealing with electronic files contained on a single hard drive
- These procedures would need to be followed for each separate hard drive containing digital evidence

What We Will Cover

- Securing Electronic Data
- Establishing a Chain of Custody
- Best Evidence vs. Working Copies
- Securing Electronic Evidence
- Transfer of Electronic Evidence
- Storage of Electronic Evidence
- Affidavit of Electronic Evidence

Securing Electronic Data

- Copy entire hard disk
  - Best to use Forensic Tools
  - Must perform md5 or similar hash on all copies
    - There are tools available that can copy multiple disks at 3gig/minute while performing an md5 checksum of the entire disk
  - Very detailed information should be maintained
    - Workstation, Server, Smart Phone?
    - Make, Model, Serial Number?
    - Physical and Virtual Location?
    - MAC Address?

Establishing a Chain of Custody

- Field notes are invaluable
  - Date and Time references
  - Thorough, legible, notes describing all actions
- Secure one copy of data to be a “best evidence” copy
  - Never use the best evidence copy to perform digital forensic examination
  - Always annotate all actions pertaining to the best evidence copy
    - Transfer of custodianship
    - Checksum copy made for forensic analysis
    - Location change
- Formal reports should not cause conflicts with the chain of custody
  - Accurate timelines
  - Same make, model, serial, etc. annotated in both reports

Best Evidence vs. Working Copies

- There is only one “best evidence” copy of the data
- Always use the best evidence copy to make working copies
  - Working copies should be checksum validated against best evidence copy that has been checksum validated against original data
  - Never make a working copy from a working copy
- You can have as many working copies as needed
  - All should be validated from the best evidence copy

Securing Electronic Evidence

- Working from the “working copy”
  - Forensic analysis software is extremely useful
  - Computer Cop’s Forensic Examiner and EnCase’s EnCase Forensic are both good tools
    - Fill out all pertinent information prior to performing the analysis
    - Both tools give you exceptional ways to secure evidence while performing md5 checksum verification on the files you commit to evidence
      - These checksums can then be verified to the original verification performed on the original data
  - Document every action performed and keep exceptional notes
- The evidence obtained can be kept separately; however, these evidence files are simply “pointers” to the best evidence copy and, thus, the original data

Transfer of Electronic Evidence

- Once you have your evidence files documented, you should treat these with the same care as the best evidence copy of your seized data
  - The discovered, separated, and validated evidence files can be maintained separately from the best evidence copy, but an inventory of the evidence files should be kept with the best evidence copy
  - Since the evidence files are ultimately maintained on the best evidence copy, you can establish a single chain of custody for the best evidence copy and all evidence files or you may wish establish separate chains of custody for each evidence item. This will depend on the individual case
- For all transfers of custodianship of any item (best evidence copy, evidence files) you should have a form or receipt that shows the transfer and you must keep all transfers documented
  - If it is discovered that someone had the data in their possession that is not documented in the chain of custody then is can be argued that that data can no longer be trusted

Storage of Electronic Evidence

- Since the best evidence copy contains all the digital evidence, we will talk about these items as one. If you have separate copies of each piece of digital evidence then I would store them the same
- Anti-Static pouches/bags
  - Hard Drives are shipped in Anti-Static bags so if you keep these bags then you will not need to purchase more
    - If you need to purchase, they run around $53.00 per 1000
    - You may wish to purchase bags due to labeling, etc.; however, this is merely for storage purposes
- Sometimes data and digital evidence may sit for several months or years before needing to be used
  - Exceptional documentation is a must

Affidavit of Electronic Evidence

- I would suggest completing an affidavit of the evidence as quickly as possible
  - Everything is fresh in your mind
  - All notes and documentation is organized
- If the evidence is ever needed you should pull the original affidavit from the case file, review your affidavit, and then have the affidavit notarized
- A lot of times well documented descriptions of evidence files accompanied by copies of the evidence files (even hard copies) along with your affidavit swearing that all evidence files are accurate is enough in a court of law
  - You may not be asked to produce the original “best evidence” copy as long as everything is documented
  - You can make a checksum verified copy for legal to review

Questions?