

First Responder

Collection and preservation of evidence

Norman PAN, cisa, pdcf
Doctor A Security Systems (HK) Ltd.
2004-01-08
Email: npan@drasecurity.com

- Something (not everything) **NEED TO KNOW** about
 - Collection and preservation of **DIGITAL EVIDENCE**
 - The need to be well prepared
- Discussion in cases, and Q&A
- Not for
 - Legal discussion
 - Technical Examination
 - ❖ You will see one later on
 - How to write a report
 - Recommending products
 - Training for First Responder, not to mention Computer Forensic

- Is computer forensic related to computers only?
- NO, besides computers, it also related to collection of papers, something about photography...

- Time: a Hot Summer afternoon
- A friend called in, the front page of the company's web site was defaced
- The web server - a Windows 2000 server
- Boot into Windows, check some files
- Shutdown the server, unplug the harddisk
- Evidence was put in a briefcase, put into luggage cabin rear side of a car.
- Plug the harddisk into his computer and use antivirus software to check the HD, identified some worms, and removed it.



Very limited of time, usually in hours!

Examination

Report

Collection

1. Collection

2. Examination

3. Analysis

4. Report



Improper handling can jeopardize the evidence

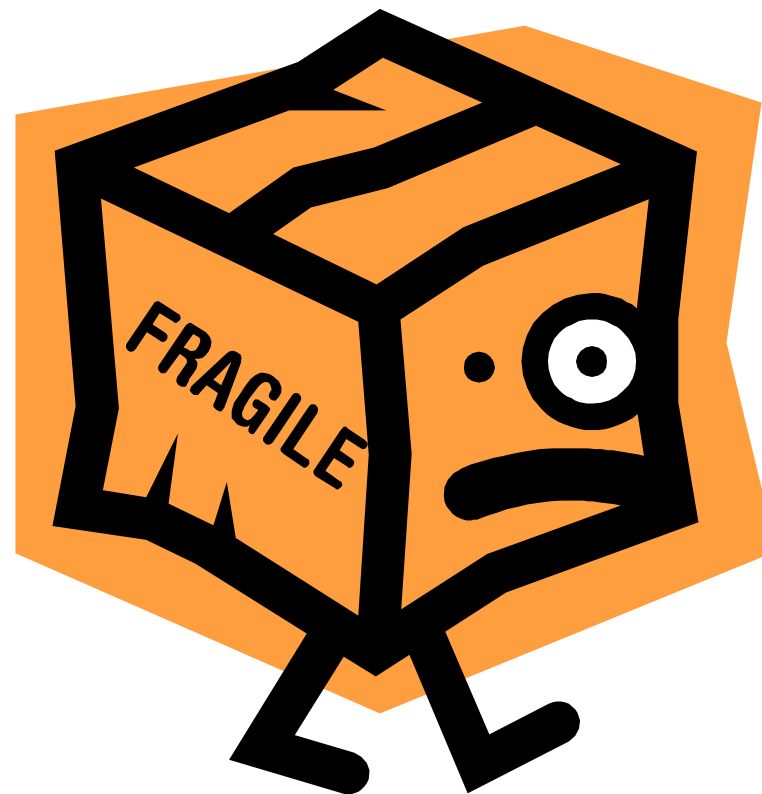
- Time to response and cover is short, usually in number of hours
- Evidence is fragile
- Need to have well prepared, tested tools
- Most important - Well trained First Responder



- **COLLECTION**
 - Search for,
 - Recognition of,
 - Collection of, and
 - Documentation of electronic evidence
- **EXAMINATION**
 - Make evidence visible
 - ❖ Recover deleted files.
 - ❖ Recover data from a reformatted drive.
 - ❖ Recover data in file slack and unallocated portions of drive.
 - ❖ Recover passwords
 - ❖ Decrypt encrypted data and messages.
 - Explain its origin and significance
- **ANALYSIS**
 - Look at the product of examination for its
 - ❖ Significance and
 - ❖ Probative value to the case
- **REPORT**



- **Fragile**, it can be
 - Altered
 - Damaged, or
 - Destroyed



- Should **NOT CHANGE** that evidence
- Handlers should be **TRAINED**
- Activity should be fully **DOCUMENTED, PRESEVED,** and available for **REVIEW.**

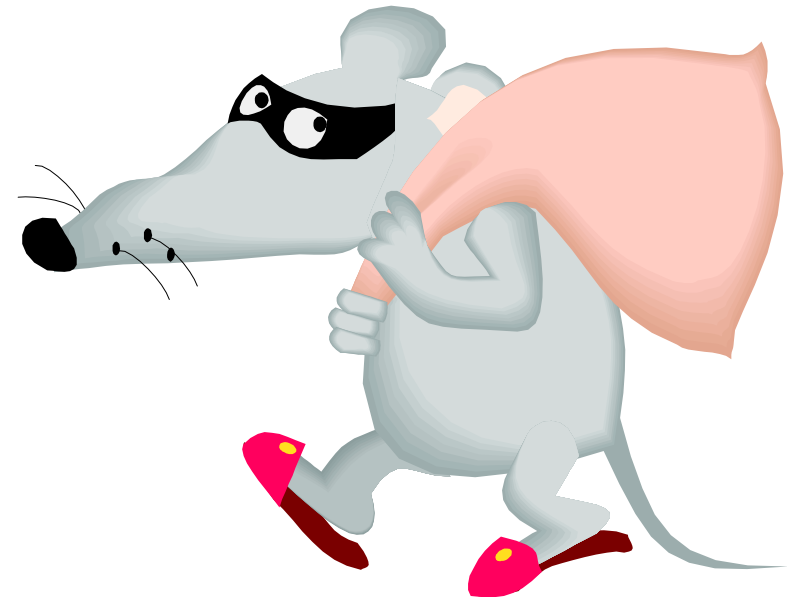


- He plugged an external USB hard disk and copied all the files of the compromised systems to the external hard disk.
- Consider
 - He changed the status of the compromised systems by plugging in a new hardware whereas the compromised system was still active
 - He COPIED all the files!!!
 - ❖ How about deleted files, hidden files?
 - ❖ Where was the integrity of the evidence?

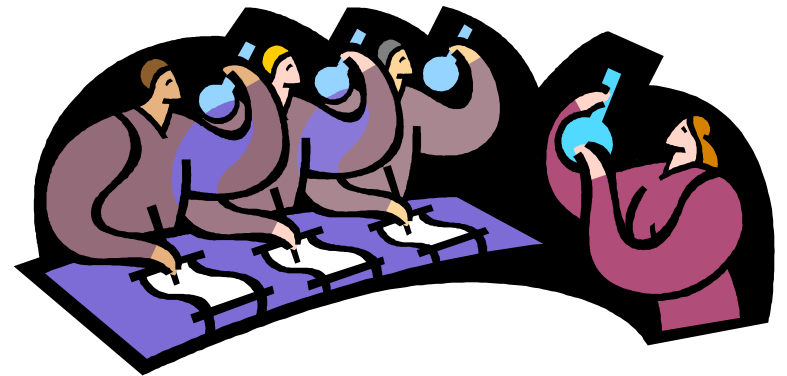
- Crime Category
 - Auction Fraud
 - Child exploitation/Abuse
 - Computer Intrusion
 - Death Investigation
 - Domestic Violence
 - Economic Fraud
 - ❖ Counterfeit
 - E-mail threats
 - Extortion
 - Gambling
 - Identity Theft
 - Narcotics
 - Prostitution
 - Software piracy
 - Telecommunication Fraud



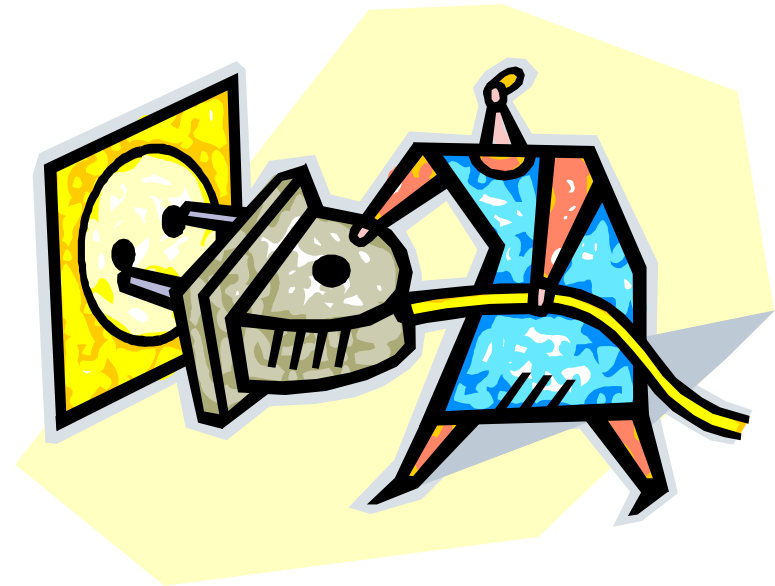
- Computer crime
- Internal Malicious use of computer
- Computer incidents for further investigation



- Computers
- Floppy diskettes
- Memory cards
- Ext. Hard drives, zip drives
- Modems
- Network equipment,
 - Routers
 - Wireless Access points
- Pagers
- PDA
- Printers
- Scanners
- Telephone, mobile
- Facsimile Machine
- GPS



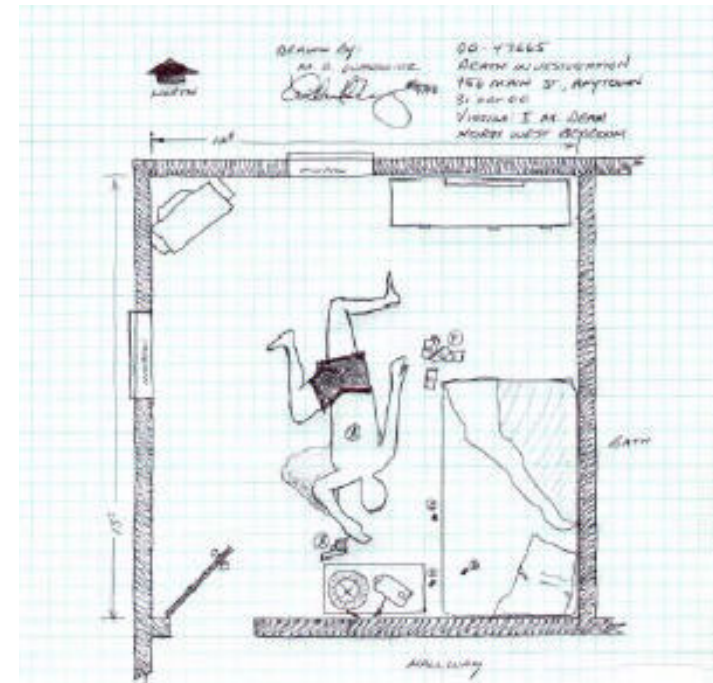
- I need to collect evidence from a Windows 2000 server, shall I unplug the power or shut it down?



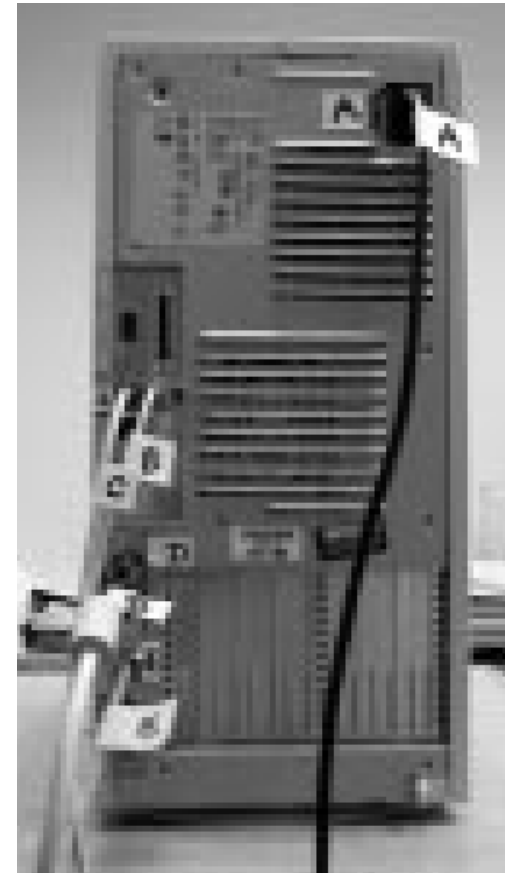
- Recognition and Identification of the evidence
 - **Securing the scene**
 - ❖ Perishable data (e.g. pagers, Caller ID boxes) should be handled in higher priority
 - ❖ Document, disconnect and label telephone lines/network cables
 - Disconnect from the wall rather than the device, if possible
 - ❖ Keyboard, Mouses
 - Finger print
 - At last
 - ❖ Conduct preliminary interviews
 - Password
 - Protective / Destructive device
 - Offsite data storage
 - Relevant documentation



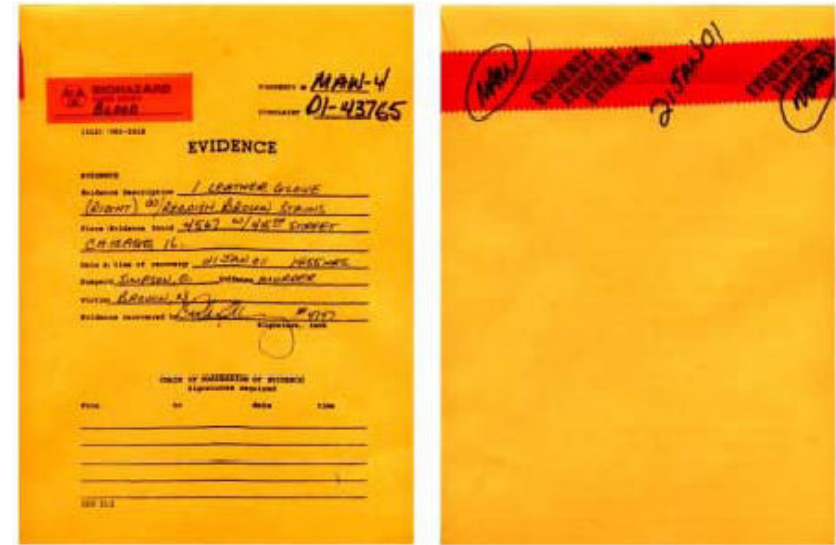
- **Documentation of the scene**
 - Physical scene
 - ❖ Mouse on the left ...
 - ❖ Photograph entire site
 - ❖ Photograph screens
 - Providing chain-of-custody documentation
 - ❖ track who had access, start when the data is first considered as potential evidence and should continue through presentation of the item as evidence in court.



- **Collection and preservation of the evidence**
 - Stand-alone PC
 - ❖ Monitor
 - Monitor is on, PC was active
 - Monitor is on and screen is blank (or screen saver)
 - Monitor is off.
 - ❖ Remove the Power (and battery)
 - Switch? Power cables?
 - Network Computers, servers
 - ❖ Too complex
 - Don't forget
 - ❖ PDA, USB harddisk



- **Packaging and transportation of the evidence**
 - Label, Label, Label (do you have enough labels)
 - Transporting the evidence
 - ❖ Paper char at 460F
 - ❖ Data start disappearing at 120F



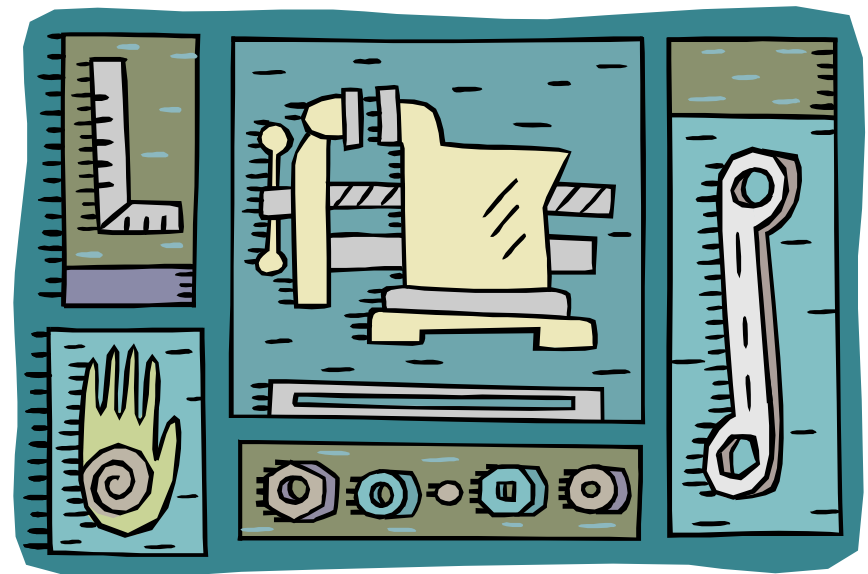
- Preserve evidence in its original state
 - One or more individuals should be trained as First Responders
 - The First Responder will manage the case, according to best practice, when an event has been identified until a qualified forensics professional arrives on the scene
 - Actual case handling should be delegated to professionally trained electronic forensics experts



- I have some spare Hard Disks which were un-plugged from old Windows computers, can I use this for storing evidence?
 - Yes?
 - No?
- Quick Answer:
 - Use forensically sterile media
 - ❖ No viruses
 - ❖ No contamination by previously examined data
 - ❖ No contamination by other data

Are you prepared?

- Notebook computers
 - Licensed software
 - External HD cases (with large size, sterile HD, of course)
 - Bootable CD (preferably in Linux)
 - Network cables
- Misc.
 - Camera
 - Label tag
 - Anti-Electro-static bag
 - Tape
 - Glove...
- Training
- Procedures
- Etc.....



- <http://www.crazytrain.com/papers.html>
- http://www.dfrws.org/dfrws2002/papers/Papers/Jesse_Kornblum.pdf
- <http://www.knoppix.net/>
- Search Internet by
 - First Responder
 - Bootable Linux