Doctor A Security

Forensics Analysis of Hacking Cases

Norman PAN *cisa, pdcf*

Doctor A Security Systems (HK) Ltd.

2003-09-22

npan@drasecurity.com

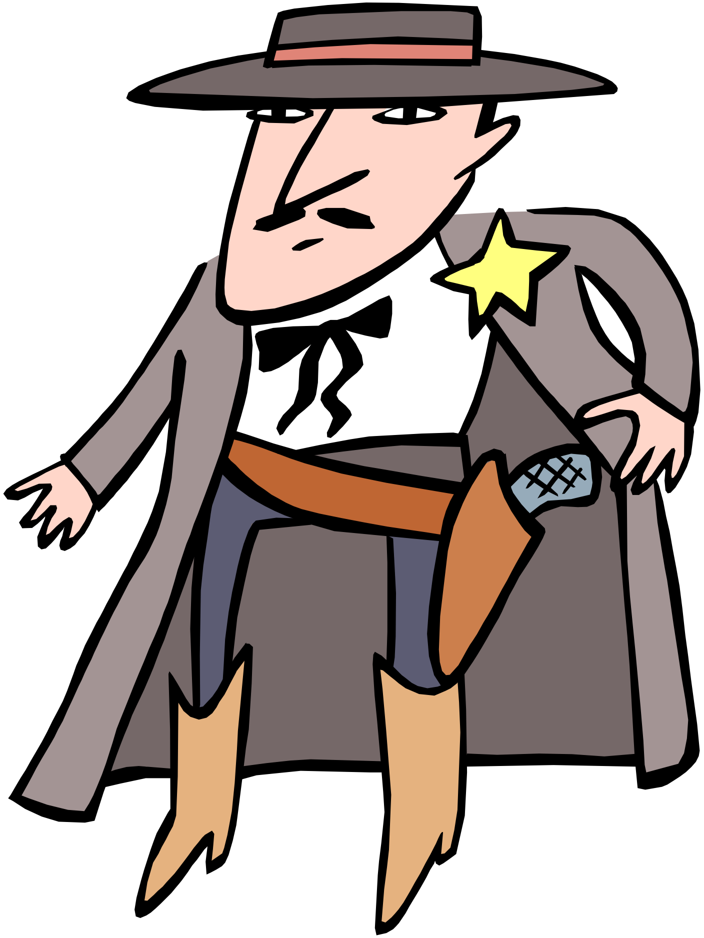
(Professional correspondence only)

Today

- Is for
  - Need to know
  - Should/should not
- Is NOT for
  - How to do
  - Legal advice

Case for discussion .. 1

Doctor A Security

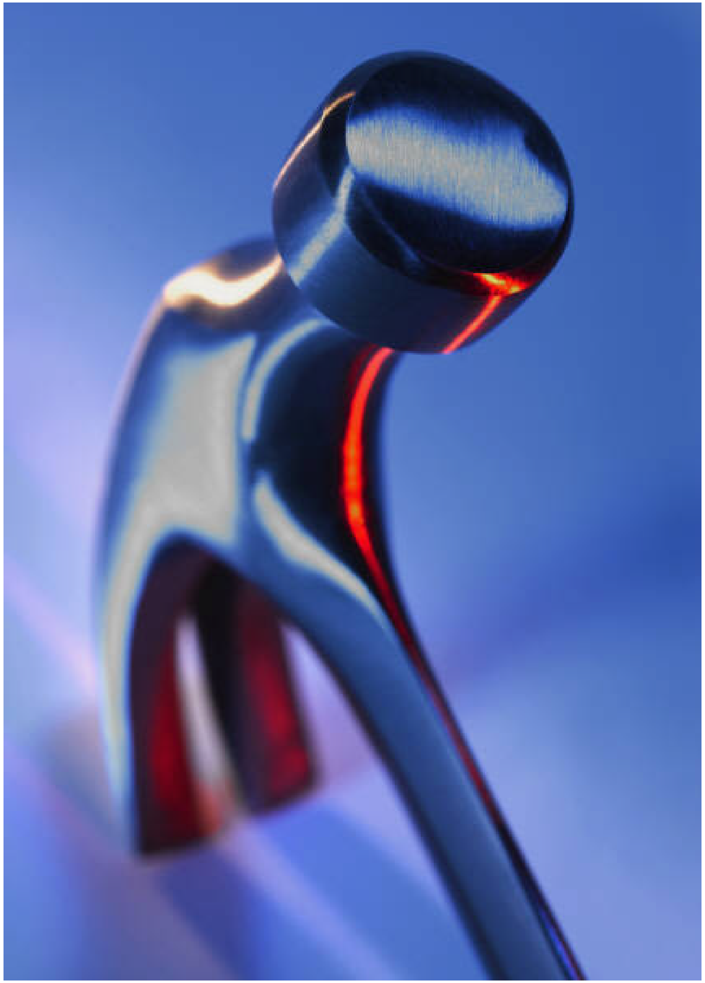


- Investigator arrived the crime scene and
- used his notebook and created a new partition in the existing USB Hard disk…

Case for discussion … 2

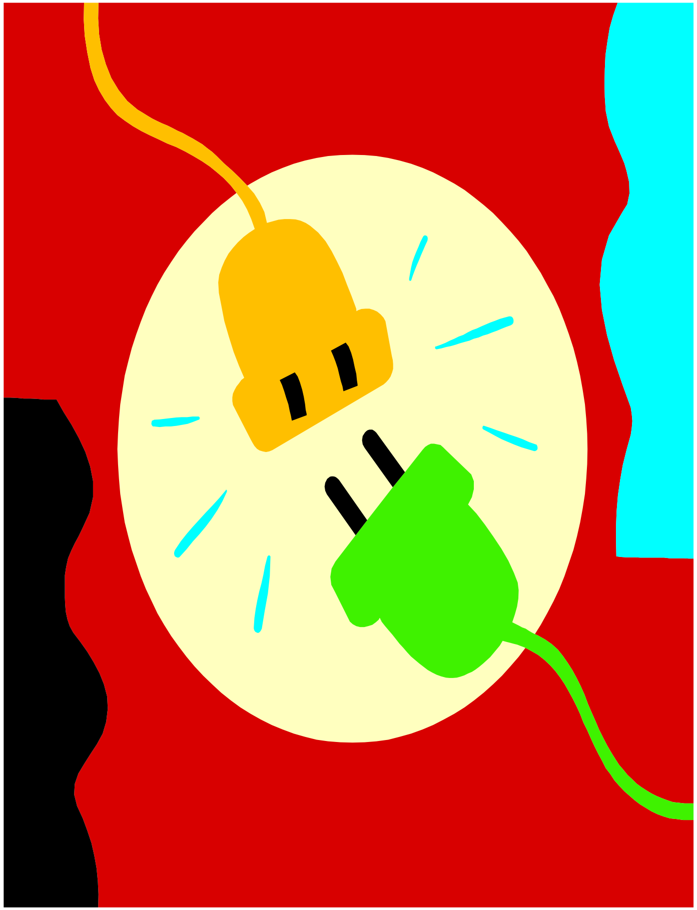
Doctor A Security

- Used a Forensic tools installed yesterday in his notebook using colleague's CD



Case for discussion … 3

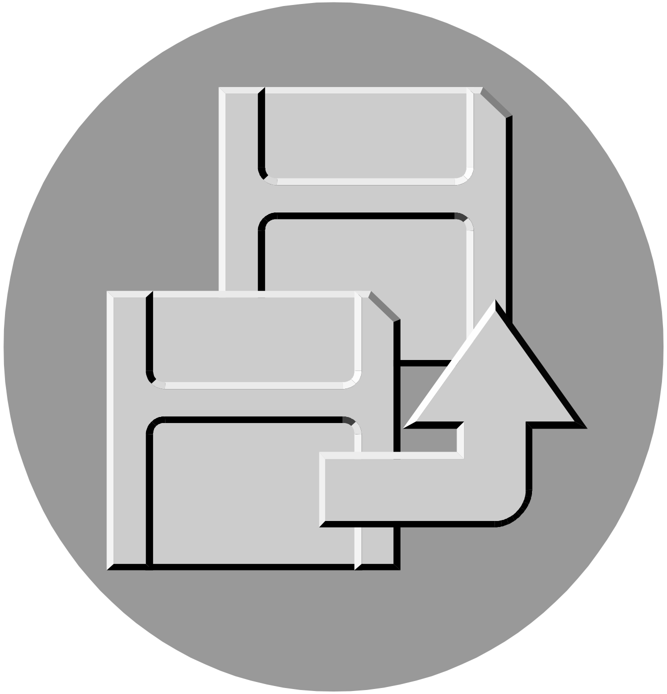
Doctor A Security



- Unplugged the power supply of the target computer

Case for discussion … 4

- Copied the files of the target computer to the Investigation newly created partition



Case for discussion … 5

- Investigator returned to office, his colleague borrowed his notebook for another case, and returned 2 days later.

The Cost of an Incident

- Intruder: 2 Hours
- the time spent to clean up after them: 80 Hours
  - not inlcude
    - ❖ Intrusion Detection (human element)
    - ❖ Forensic acquisition of disk images
    - ❖ Restoration of compromised system
    - ❖ Hardening of compromised system
    - ❖ Network scanning for other vulnerable systems
    - ❖ Communications with stakeholders

Forensic, for the sake of Forensic?

- Incident Respond Procedure… .
  - .. Snapshot of the victim machine… (?)
- Decide
  - Recovery
    - ❖Virus
    - ❖Failed Harddisk…
  - Forensic (if evidence if important)
    - ❖Substantial financial loss
    - ❖Computer crime
      - Intrusion
      - Theft of proprietary information…

Why Forensics is, a little bit, difficult?

1. Too many variables
   - Operating systems
   - Software application
   - Cryptography
   - Hardware platform
   - Law
   - International boundaries
   - Publicity

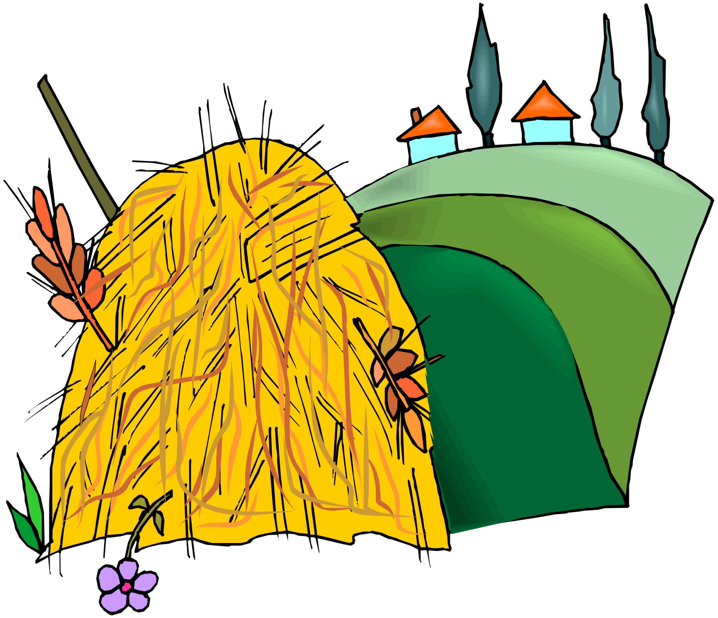
Elements of Forensic Readiness

- How Logging is Done
- What is Logged
- Forensic Acquisition
- Evidence Handling

Doctor A Security

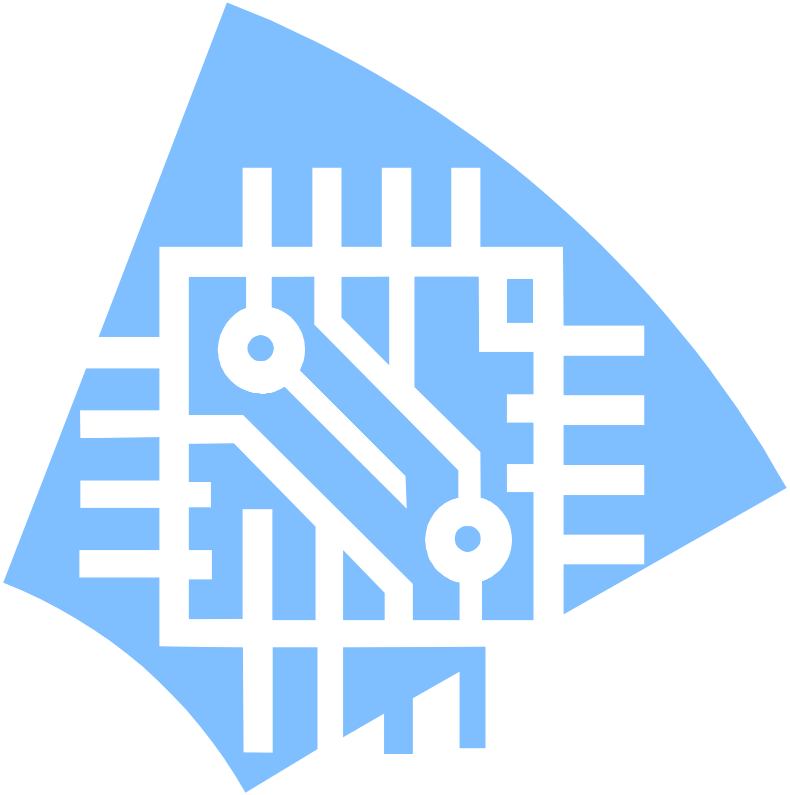
How Logging is Done

- “needle in the haystack”
  - Data from an IDS
  - Centralized logging
- Time
  - time synchronization becomes an issue.
- Permissions
- Reporting



Usefulness of Incident Data

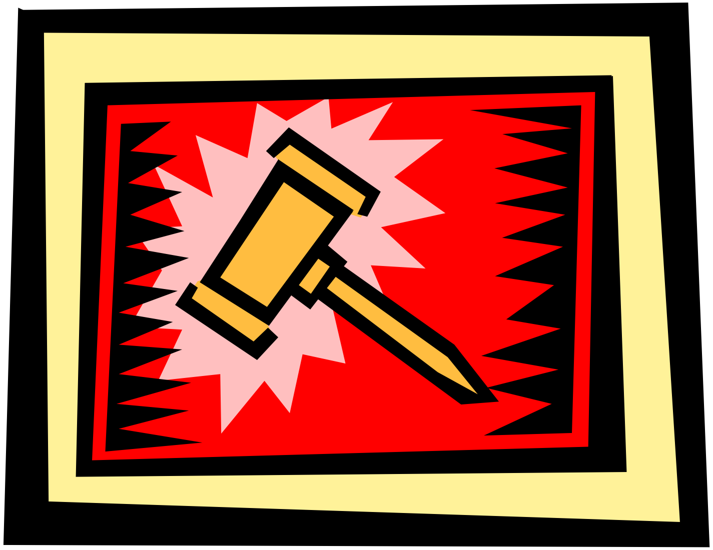
- The victim system(s) RAM, registers and raw disk
- The attacking system(s) RAM, registers and raw disk
- Logs (from the victim and attacking systems as well as intermediary systems)
- Physical security at the attacking system (e.g. camera monitoring, etc)



Solid Analysis and Case Building

- You have to defend
  - How you work
  - Why you work this way
- To Juror (non tech)
  - If you tell them you have no defined methodology
  - Acquit for Reasonable doubt
- Methodology become a Discipline
  - Think about car driving

Document Everything



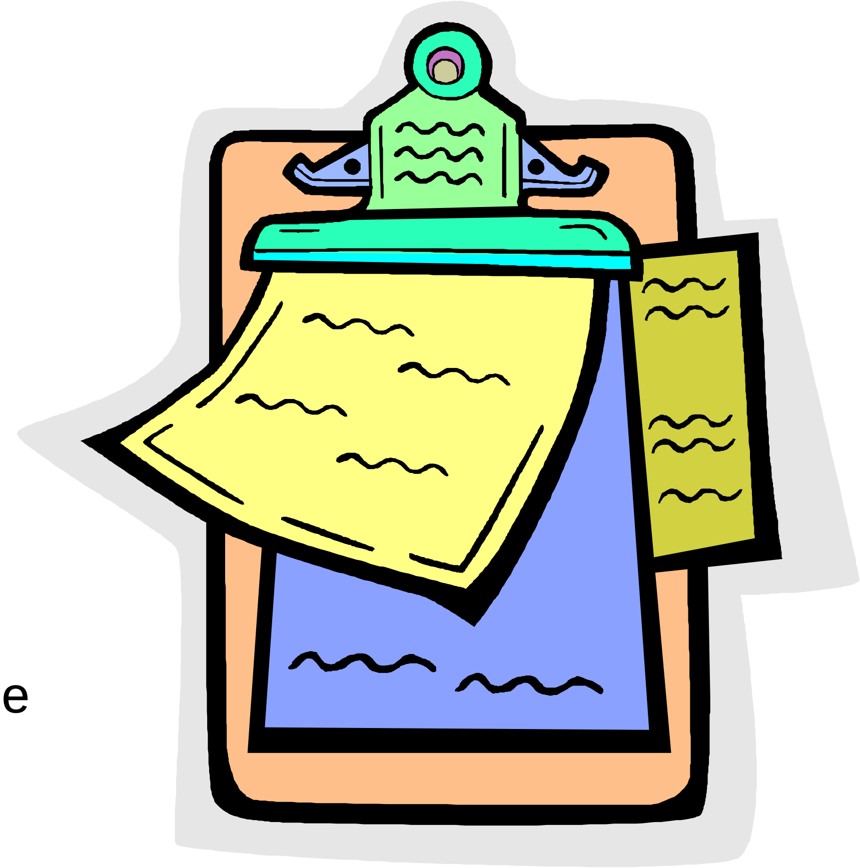
- REFUTE because of mishandling??
- Chain of evidence
  - 1 x Conduction the investigation
  - 1 x Document
- What
  - Time
  - Date
  - Steps were taken
  - Name involved
  - Whose authority's for step.

Crime Scene … . 1

- Snapshort
  - Photograph the scene
  - Note the scene
    - ❖ Personal items
  - Photograph the actual evidence
    - ❖ E.g. What's on the screen
  - Open the case carefully
  - Photograph the internal
  - Document the internals (e.g. Serial#, cable config – IDE, SCSI…)

Crime Scene … 2

- Label the evidence
  - Consistently
- Photograph the evidence with label
- Document who did what at when.
- Custodian double checked your list, initials next to yours while at the scene
- Videotape the team entrance and evidence transport, if possible



Evidence transportation

- Legal authority?
- Guard against electrostatic discharge

Preparing the Evidence

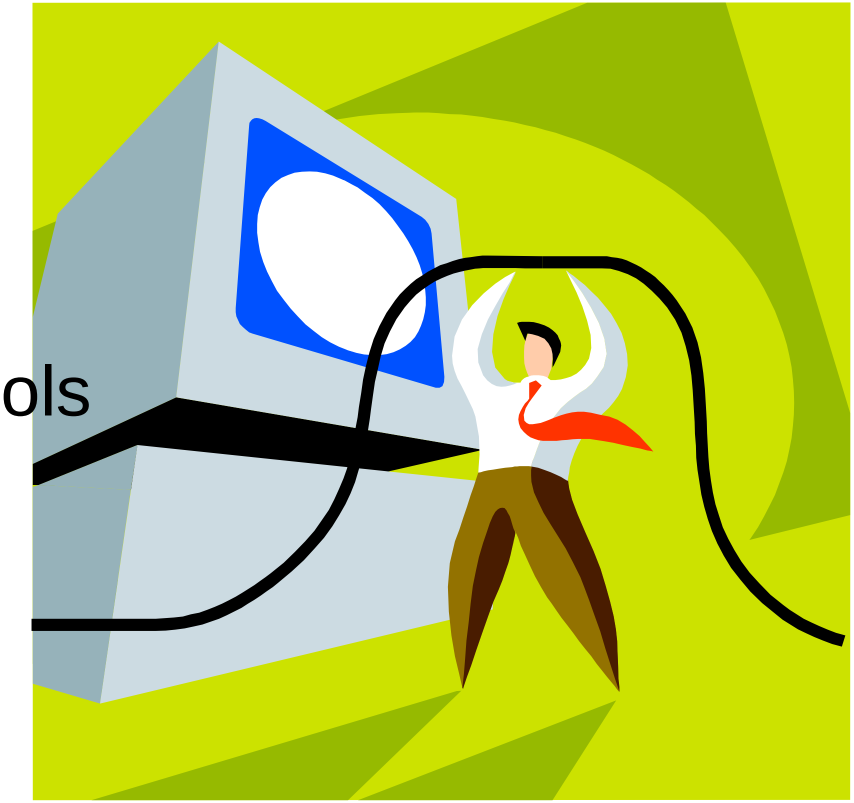
- Unpack the evidence
  - Document date, … .
- Visually examine
- Duplicate IMAGE of hard drive
  - Turn off virus scanning software
  - Record the time/date of the CMOS
    - ❖ Time zone
    - ❖ Accurate
- Make a second copy
- Seal the original evidence
  - Electrostatic safe
  - Catalog it
  - Initial by everyone touched.

Forensic Acquisition

- to preserve the entire digital crime scene with minimal or no modification of data.
- Order Of Volatility (OOV) which implies that collecting some data impacts other data.
  - CDROM based tool kit

Imaging

- Backup
  - MAC?
  - Deleted files?
- Live system?
- Open source tools
- Cryptographic hashes
- Shutdown vs Poweroff
- Copy of the copy



Evidence Handling … 1

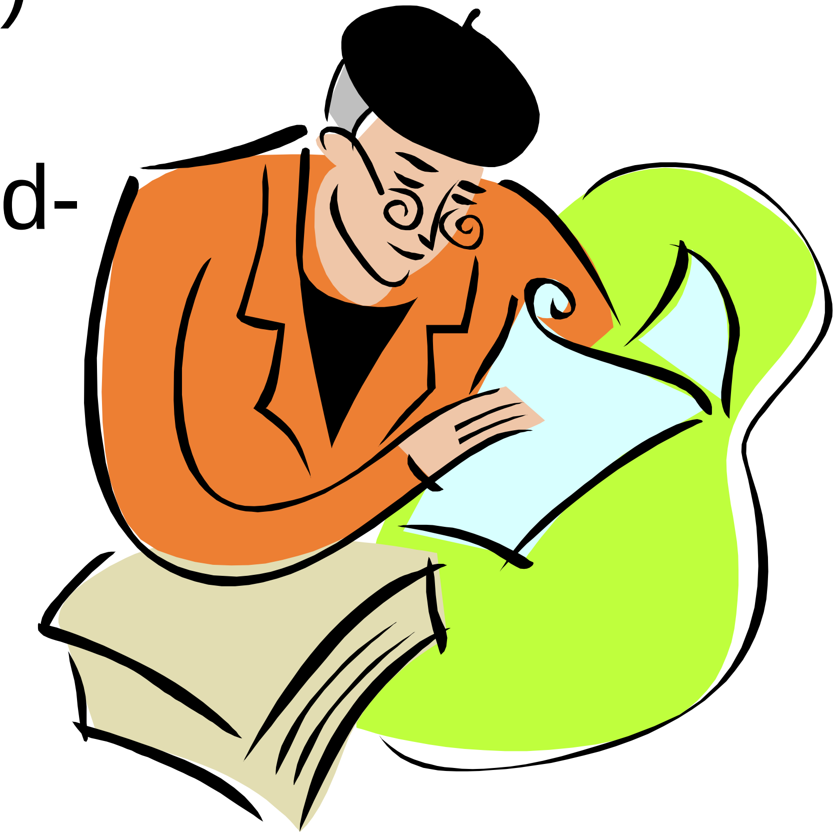
- Chain of Custody
  - track who had access
- start when the data is first considered as potential evidence and should continue through presentation of the item as evidence in court.

Evidence Handling … 2

- Physical Transport
  - FBI
- Storage
  - Paper char at 460F
  - Data start disappearing at 120F

Examination of Evidence

- disk image(s) should be mounted read-only



Now, you have the evidence…

- Where do we start?
- Think like an Intruder
- And Let's start …

Some useful links

General

- http://www.cybercrime.gov/
- http://www.e-evidence.info/
- http://www.forensix.org/

Tools

- http://www.sleuthkit.org/
- http://fire.dmzs.com/