Digital Forensics

Risk Management and Information Systems Security Consulting Services

January 2011
UMiami alumnus
- Bachelors: Information Systems and Marketing
- MS Computer Science / MBA Information Systems
- Telecommunications Certification
- Total Qualitt Certification

Systems and Network Consultant
- Various

Infrastructure and Security Manager
- Sony Latin America, Inc.

IS Security Consultant
- Enterprise Risk Management

CISSP, CISA, PCI QSA

Member of: IIA, ISSA, ISACA, Infragard, SFTA
Agenda

- What is digital forensics?
- Digital forensics taxonomy
- Methodology
  - System description
  - Evidence collection
  - Analysis
  - Reporting
- Demonstration
What is Forensic Science?

Science - Organized study of natural phenomena
Science - Application of the scientific method
Forensis – Latin meaning public, forum, discussion
Forensic – belonging to, suitable for use in courts or public for a
Forensic Science – any science used for the purpose of law
The Three Elements

Science

Evidence

Law
Digital Forensics definition

Forensics is most often understood to refer to the process or processes by which digital evidence is identified, preserved, analyzed and presented.
Computer Forensics Taxonomy

Victim

Subject

Network

Network Forensics

Media Forensics
The overall forensic investigation methodology has the following 4 phases:

- System Description
- Evidence Collection
- Analysis
- Reporting
System Description

Determine what the workstation or server is utilized for.

- Affect the way the investigation is executed.
- Unplug the machine or not?
- Shutdown, power off or not?
- Determine type of file system in use
Evidence Collection

Evidence is defined as everything that can be collected from the system under investigation.

- IMPORTANT -> Avoid data loss
- Preserve the evidence – Volatile
  Memory, Network status and connections, Processes running, Swap files.
- Chain of custody
  Establishes continuity of possession
  Proof of integrity
Identification

Direct

- Use indelible marker to place case, item number, date and initials on item.
- Sharpie or Etching is best.

Indirect

- Place item in a sealed container
- Record serial numbers and description

Combined evidence
Chain of Custody

Refers to:

- Unbroken control of evidence from seizure to court
- The paper/electronic record which demonstrates this control

Is the most often used challenge to seized evidence

A successful challenge may weaken or eliminate evidence from consideration at trial

 Applies to original, copy and derivative evidence
Evidence Examples
File Systems

A system for organizing directories and files, generally in terms of how it is implemented in the disk operating system.

Units are called sectors (512 bytes or 2 to the power of 9)

Sectors are organized in clusters or Allocation Units.
Collecting Evidence (cont.)

Sanitize the hard drive you will use to store the evidence (Wipe programs)

Ensure that it is not possible to overwrite the evidence

- Use a hardware device to write protect the accesses

  - **Windows:**
    - HKLM\System\CurrentControlSet\Control\StorageDevicePolicies
    - WriteProtect{REG_DWORD}=1
  
  - **Unix:** mount the device with the read-only option
    - mount -o ro,loop,nodev,noexec images/honeypot.hda8.dd mnt
    - mount -r /dev/sda1 /mnt/usb
Collecting Evidence (cont.)

Backup tools - don’t work

Commercial tools: Encase, Image, Forensic Toolkit, Forensic Replicator

**DD** is a common UNIX program whose primary purpose is the low-level copying and conversion of files.

**DCFLDD** is the DD version with Steroids

Other tools: PCAT, WMFT, Memdump
Analysis

Real investigation takes place

Two steps:

- Settings goals and criteria
- Timeline creation – bedrock of the investigation. Everything centers around it. Map of activities.
- Data Recovery – Key function of forensics.
Examining Media

Goals

Software tools & Methodology

Media

Criteria

What the customer wants

The Examiner's notion of what's in/out

Data
Setting Goal & Criteria

“I’m looking for:”
- The Case

Who
What
When
Where
How
Why

“In what objects will I find:”
- The Evidence
Data Recovery

What data we should recover?

- Create a dirty word list
- Extract unallocated disk units
- Search the image using the dirty list
Reporting

- Examination Output and Reporting:
  - Ensure on preservation of the provided documentation
  - Ensure on proper format
  - Ensure on the output clarity and documentation logic
  - Ensure it meets the examination goals and scope
Report

- Is treated as a legal document
- Represents the results of the forensic exam
- Informs and states an opinion
- Will be the basis for testimony examination
  - Associated with lab notes and exhibits
Quality Assurance

- Report with notes and printout are reviewed
  - Self-review
  - Peer review
  - Admin review
- Release a report only once the proper QA has been completed
- Any conflicts should be resolved prior to submission
  - Can’t pull a report back
Forensic Information Theory

- Media
- Data
- Information
- Evidence
Exhibit Presentation

♦ Exhibits are connected to the testimony as facilitating objects

♦ They are not considered as evidence by themselves

♦ They need to be backed up by illustration, oral representation, and explanation.

♦ Support technical documentation to jury
Ensure on Illustration

♦ Reason to have exhibits:
  – Illustrate on the described technology
  – Illustrate any associated process
  – Illustrate findings and results
Exhibit Characteristics

♦ Size
  – Should be viewable, noted and readable by anyone in the jury
♦ Should be clear and concise
♦ Should present a point
♦ Simple yet efficient
♦ Of professional quality
Exhibit Characteristics

- The following should be clear and easily identifiable:
  - Case numbers
  - Item numbers
  - Physical/Logical locations
  - etc

- Separate exhibits by item/section
  - Technical
  - Logical
  - etc
Demonstration Case

An anonymous caller has informed a corporate security department that a trusted employee, Jack Lansky, has been selling the company’s secrets to a corporate spy. The caller alleges that Lansky has sent company proprietary and/or Trade Secret information to Russians in return for a trip to the Caribbean. Based on this information, security officers began an investigation.

Facts:

- Lansky has been reported being on a cruise at the Caribbean
- Lansky is a top level engineer who has access to the company's confidential and sensitive information
- There was found a 1GB DataTraveler Kingston USB drive on Lansky’s desk drawer. The company already did their internal investigation, and decided to handle the USB drive’s image acquisition and handling of chain of evidence. They didn’t find anything of value regarding the case.
- Company decides to hire us for a second opinion on the case and the USB drive image. We are denied access to image Lansky’s workstation. We further ask for a copy of the workstation’s registry, which is provided to us.
Questions

It's QUESTION TIME!!