Incident Response and Corporate Forensics

Ed Crowley

ITEC 6322

Spring 10

Today's Topics

- Digital Forensics Overview
  - Corporate and Law Enforcement Forensics
  - Expected Trends Over Time
- Incident Response and Corporate Forensics Class Overview
  - Required Skills
  - Laboratory Tools
  - Incident Response, Hard Drive/System Forensics, Live System Forensics
- LiveCDs and LiveCD Tool-kits
- Toolkit Creation

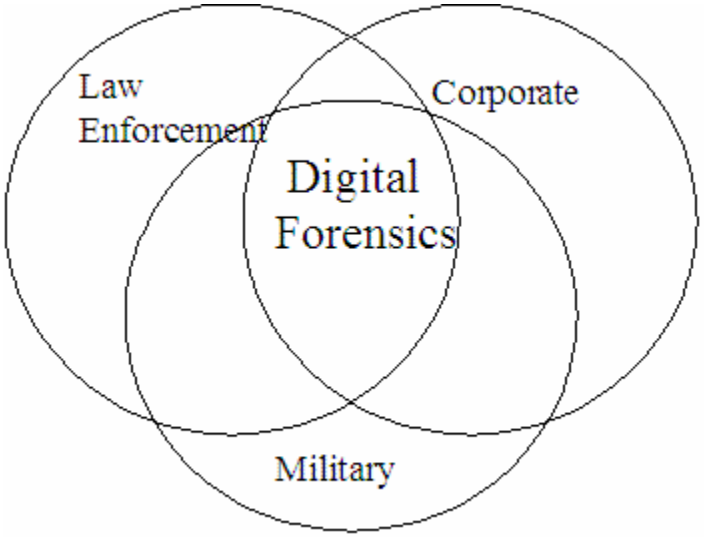
Digital Forensics Defined

The Digital Forensics Workshop [6] defines Digital Forensics (DF) as:

… the use of scientifically derived and proven methods toward the preservation, collection, validation, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Three Interest Areas

Graphically, the Digital Forensics Workshop [6], represents Digital Forensics as the overlap of three areas



Corporate and Law Enforcement (LE) Forensics

- Share a common process
- Have significant differences including:
  - Context
  - Scope
  - Outcomes
  - Tools
- Today, we'll discuss our class and related Open Source Tools and LiveCDs

Common Forensic Process

- Each group shares a common view of the four step forensics process. [7]
  1. Acquisition & Preservation
  2. Examination
  3. Analysis
  4. Presentation (*Image from NIST 800-86*)

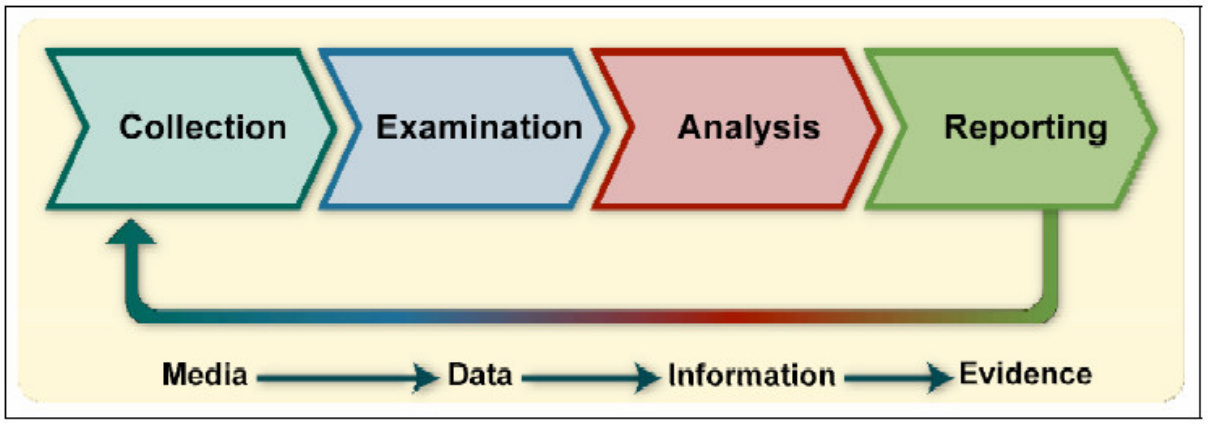


Figure 3-1. Forensic Process

Law Enforcement Forensics Focus and Practitioners

Focus

- Gather evidence for use in a criminal court.

Practitioners

- Sworn law enforcement officers work in a team with:
  - District attorneys
  - Judges
  - Related judicial officers.
- Information gathered and processes utilized, are evaluated against, relatively, well defined judicial standards.

Corporate Forensics
Focus and Practitioners

Focus

- Maintain enterprise operations.

Typical, practitioners

- Decentralized IT staffers working with a centralized incident response/computer forensic (IR/CF) team. Normal team includes representatives from:
  - Corporate IT
  - HR
  - Legal
- Information gathered here, is used to support a corporate decision and/or to defend the corporation in civil court
- Note IR teams may be dynamic

Corporate Responsibilities

- Maintenance of digital assets including corporate processes
  - Includes internal system and network monitoring.
- Liaison with external law enforcement.
  - Since a corporation may lose control over any investigation referred to law enforcement, liasnon is considered a significant issue.

Table 1 - Digital Forensics Goals and Environments

Area	Primary Goal	Secondary Goal	Environment
Law Enforcement	Prosecution	N.A.	After the fact
Business & Industry	Availability of Service	Prosecution	Real Time

Corporate Trends

- Increasing utilization of digital assets.
- Increasing accountability for employee's use of digital assets.
  - Already, twenty-seven percent of the Fortune 500 have defended themselves against sexual harassment claims stemming from inappropriate email. [5]
  - A recent American Management Association study (1997-2000) indicated that:
    - Sixty-three percent of surveyed private sector companies monitor workers' Internet connections
    - Forty-seven percent store and review employee e-mail. [5]

Increasing Regulatory Environment

- Ongoing legislation and regulation such as:
  - PCI DSS
  - Sarbanes-Oxley (SOX)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - California SB1366
- All require corporations to provide assurance of regulatory compliance.
- Not unusual for IT department to be the lead in developing assurance of regulatory compliance.

Incident Response (IR) Goals

Given an incident, answer three questions:

- What happened?
- How did it happen?
- Who is responsible?

- Requires appropriate methodologies for evidence
  - Collection
  - Preservation
  - Analysis
  - Presentation
- Implies knowledge of incident response frameworks

Corporate Forensic (CF) Goals One

- Detect and analyze system/network anomalies.
  - During “hands on” activities:
    - Identify
    - Collect
    - Preserve
    - Analyze
  - Digital information
    - In both static (disk) and dynamic (system, network, and internet) contexts.

Class project: create an open source, custom, incident response toolkit.

Corporate Forensic (CF) Goals Two

- Identify, Collect, Preserve, and Analyze digital information that supports a corporate decision.
- May be used in Civil Court.

Required Skills

Table 2 Incident Response and Corporate Forensics Skills

Skill Areas	Hard Drive/System Forensics	Live System Forensics	Network/Internet Forensics	Tool-kit Creation
Activity	Forensic duplication System baselining Password analysis System /data integrity File recovery	Live response Log Analysis Registry forensics	Email analysis Banner grabbing ARP poisoning Network baselining Traffic analysis	Prepare custom bootable incident response Live CD

Laboratory Tools

- Free and open source tools including LiveCDs. In most cases each tool:
  - Implements a specific activity representing the application of a particular security concept.
    - May employ a unique command line interface.
  - Produces output.
- To become useful, output must first be analyzed.
- Different tools, require different amounts of analysis.

Free and Open Source Tools

Table 3 Incident Response and Corporate Forensic Tools

Skill Areas	Hard Drive/ System Forensics	Live System Forensics	Network and Internet Forensics	Tool-kit Creation
Activity	DD MD5Sum HexEdit Steganagraphy John the Ripper L0PHt Crack NMap Shred Nessus	Live response Log Analysis Registry forensics FTK Helix	Ettercap NMap NetCat Wget Hping, Fping Dig, whois,traceroute Ethereal OpenSSL	MakeISO Knoppix DSL Helix

Incident Response

- Incident response focuses on:
  - Incident response team members roles
    - Contributions of separate corporate departments.
  - Baselining process for systems and networks.

- During incident response, corporate professionals must be prepared to appropriately:
  - Acquire
  - Duplicate
  - Analyze and
  - Report evidence

Hard Drive/System Forensics

- Most mature digital forensics layer.
  - Data Dump (DD) or FTK Imager or other tools can be used to create forensic disk copies.
    - Once duplicate drive copy is made, it must be analyzed.
    - Must also be shown to be identical to original
      - An appropriate cryptographic tool ca demonstrate that duplicate is identical.
    - Analysis includes recovering hidden information.
- Related services, such as log analysis are also important.
  - Students learn to gather and analyze related system and network logs.
  - With windows, registry forensics is also significant.
- Live system forensics can recover unique and valuable information.

Live System Forensics

- Live response refers to gathering volatile information prior to powering system down.
  - Certain information, such as current network connections and running processes, are only available while the machine is running.
- Goal: acquire relevant volatile system data while it exists.

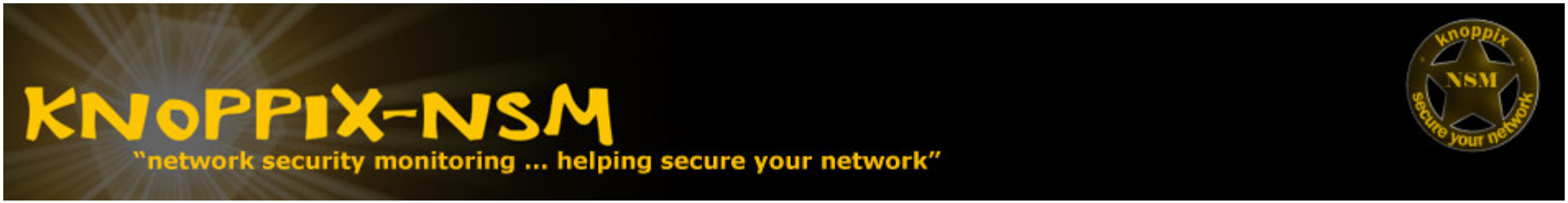
Network and Internet Forensics

- Establishing a network baseline.
  - When anomaly occurs, the current network operational profile is then contrasted to (normal) baseline.
  - In theory, the differences should point to the problematic layer.
- Network baseline lab activities include work with active tools such as NMap and Fping.
- Students also work with passive tools such as the Ethereal (Wireshark) protocol analyzer.

LiveCD Tool-kits

- Variety of free and open source forensic tools.
- LiveCDs may include Knoppix, Helix, and Back Track.
  1. Knoppix: a general purpose LiveCD that allows the students to work with many Linux based utilities.
  2. Helix: formerly a Knoppix based LiveCD focusing on digital forensics. (Now by subscription.)
  3. Back Track: a security focused livecd.

Knoppix and Helix



Toolkit Creation

- As a class project, each student creates a customized IR Tool Kit.
  - Each project focuses on a particular security problem that the tool kit addresses.
    - Each student designs and builds a custom tool kit that implements a solution.
  - In the past, the project involved remastering Knoppix. Now, it involves creating a custom USB.

Questions?

References

1. Fernandez, J., Smith,S., Garcia,M.,and Kar,D., Computer Forensics – A Critical Need In Computer Science Program, Consortium for Computing Sciences in Colleges, 2005.

2. Grance, T., Kent, K., Kim, B., Computer Security Incident Handling Guide, SP 800-61, National Institute of Standards and Technology, 2004.

3. e-fense, Helix LiveCD, http://www.e-fense.com/helix/index.php, 2006.

4. Knoppix, Klaus, Knoppix LiveCD, http://knoppix.net, 2006.

5. Logan, P., Corporate Computer Forensics: Opening Opportunities for Students, Colloquium for Information Systems Security Education, 2005.

6. Palmer, G., A Road Map for Digital Forensic Research, Report from the First Digital Forensic Research Workshop (DFRWS), 2001.

7. Pollitt, Mark; Six Blind Men from Indostan, www.dfrws.org/2004/bios/day1/D1-Pollitt-Keynote.ppt, 2004.