Digital Forensics

Introduction to Digital Forensics
Procedure, Tools, and Techniques

An organizational approach ...

Andrew Immerman
ahimmerman@yahoo.com

LayerOne ’06
Pasadena, CA
Agenda

1. Conceptual Introduction
2. Anatomy of Malice
3. Digital Evidence
4. Forensic Procedure
5. Forensic Tools & Techniques
6. Counter-Forensics
7. Forensic Hardening
8. Forensic Future
9. Educational Resources
**Concept:** Forensic Science

*n.* the use of science and technology to investigate and establish facts to facilitate decisive action
**Concept: Forensic Science**

*n.* the use of science and technology to investigate and establish facts to facilitate decisive action

(or)

*n.* an argumentative exercise
Concept: Digital Forensics

*n.* the use of science and technology to investigate and establish facts to facilitate decisive action

(or)

*n.* an argumentative exercise

**Subject:** Digital Data (Evidence)

**Object:** Data Storage Systems

**Objective:** Evidential Discovery
Concept: Critical Distinctions

- Forensics v. Security
  - Forensics Facilitates Discovery
  - Security Resists Discovery
Concept: Critical Distinctions

- **Forensics vs. Security**
  - Forensics Facilitates Discovery
  - Security Resists Discovery

- **Vital vs. Postmortem (vs. Recovery)**
  - Vital Forensics on Dynamic, Evolving Systems
    (Work Against Time: Order of Volatility)
  - Postmortem Forensics on Static Systems
    (Work With Time)
Concept: Critical Distinctions

- **Forensics v. Security**
  - Forensics Facilitates Discovery
  - Security Resists Discovery

- **Vital v. Postmortem (v. Recovery)**
  - Vital Forensics on Dynamic, Evolving Systems
    (Work Against Time: Order of Volatility)
  - Postmortem Forensics on Static Systems
    (Work With Time)

- **Archeology v. Geology**
  - Archeology studies (Direct) Effects of Humans
  - Geology studies Effects of Autonomous Systems
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation
   1. Discovery
      1. Discovery of Raw Data (Vital & Postmortem)
      2. Electronic Surveillance
   2. Seizure & Preservation
      1. From "LayerOne" through Abstraction Layers
      2. From Volatile to Non-Volatile
      3. Know the Geological Terrain
      4. Avoid Malware
      5. Document Everything
   3. Recognition of Digital Evidence
   4. Chain of Custody
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation

2. Duplication, Distillation, and Conversion
   1. Admissible Duplication Process
      1. Follow Industry Standards for Quality & Reliability
      2. Duplicates Must Support Independent Verification
      3. Duplicates Must be “Tamper-Proof”
   2. Distillation
      1. “If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original’.” - Federal Rules of Evidence, Rule 1001(3).
   3. Conversion
      1. Conversion for Analysis
      2. Conversion for Representation
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation
2. Duplication, Distillation, and Conversion
3. Analysis and Reporting
   1. Analysis
      2. Find the Needle in the Haystack (*Identifying Digital Evidence*)
      3. Reconstruct the Time Table (*Context of Digital Evidence*)
   2. Reporting
      1. Represent the Evidence
      2. Represent the Investigation
      3. Represent the Facts
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation
2. Duplication, Distillation, and Conversion
3. Analysis and Reporting
4. Expert Testimony
   - Experience & Expertise
   - Durable Expert Witness
   - Durable Expert Testimony
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation
2. Duplication, Distillation, and Conversion
3. Analysis and Reporting
4. Expert Testimony
5. Tactical Strategist
   1. Consult in Establishing Strategic Objectives
   2. Define Tactical Implementation Plan
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation
2. Duplication, Distillation, and Conversion
3. Analysis and Reporting
4. Expert Testimony
5. Tactical Strategist
6. Business Operations
   - Incident Response Plan (IRP)
   - Standard Operating Procedures (SOP)
   - Business Continuity Plan (BCP)
   - Disaster Recovery Plan (DRP)
   - Operational Readiness Tests (ORT)
   - Security & Privacy Policy
   - Acceptable Use Policy
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation
2. Duplication, Distillation, and Conversion
3. Analysis and Reporting
4. Expert Testimony
5. Tactical Strategist
6. Business Operations
7. Consultation
   1. Strategic Tactics
   2. Training & Education
Concept: Forensic Investigator

1. Discovery, Seizure, and Preservation
2. Duplication, Distillation, and Conversion
3. Analysis and Reporting
4. Expert Testimony
5. Tactical Strategist
6. Business Operations
7. Consultation

... and, above all else:

“If you’re not a part of the solution, there’s good money to be made in prolonging the problem.” – Despair, Inc.
Concept: Professional Requirements

- Expertise in Volatile & Non-Volatile Digital Data
- Expertise in Digital Data Tools & Techniques
- Expertise in “Government”
- Secure & Private Work Environment
- Self Knowledge
- Experience
Concept: Professional Philosophy

- Crisis Management = Art of Slowing Down
- Be Methodical
- Perform to Check-Lists
- Perform Pedantic Record-Keeping
- Build Relationships
- Anticipate Challenge & Criticism
- Never Assume Anything
- Respect Murphy’s Laws
Anatomy of Malice

Intrusion Scenario
- Reconnaissance
- Exploitation
- Reinforcement
- Consolidation
- Pillage

- Was/Is “this” inadvertent or malicious?
- Was/Is “this” the target or merely an instrument?
- Was/Is “this” a case of espionage or sabotage?
- Was/Is “this” pre-meditated?
Evidence: Incident Response

- Primary Evidence (Directly Relevant to Incident)
  - Supportive Evidence
  - Counter-Supportive Evidence
  - Controversial Evidence
Evidence: Incident Response

- Primary Evidence (Directly Relevant to Incident)
  - Supportive Evidence
  - Counter-Supportive Evidence
  - Controversial Evidence

- Secondary Evidence (Directly Relevant to Evidence)
  - Destruction
  - Concealment
  - Fabrication / Forgery
Evidence: Incident Response

- Primary Evidence (Directly Relevant to Incident)
  - Supportive Evidence
  - Counter-Supportive Evidence
  - Controversial Evidence

- Secondary Evidence (Directly Relevant to Evidence)
  - Destruction
  - Concealment
  - Fabrication / Forgery

- Types of Evidence
  - Fossilized Artifacts (Archeology)
  - Residual Evidence (Geology)
Evidence: Government

Questions
1. What are the objectives of “this” forensic investigation?
2. Who will receive “this” forensic analysis?
3. What are the subjects of “this” forensic investigation?
4. What governs “this” forensic investigation?
Evidence: U.S. Court

Applicable Types of Law
- Electronic Search & Seizure Law
- Electronic Surveillance Law
- Admissibility of Digital Evidence
Evidence: U.S. Court

Applicable Types of Law
- Electronic Search & Seizure Law
- Electronic Surveillance Law
- Admissibility of Digital Evidence

Applicable Law
- U.S. Constitution
- Federal Rules of Evidence (FRE)
- Case Law (Stare decisis)
- Contract Law
Evidence: U.S. Court: Admissibility

1. Legal Search & Seizure (Criminal Procedure)
Evidence: U.S. Court: Admissibility

1. Legal Search & Seizure (Criminal Procedure)
2. Authenticated
   1. Authenticity
   2. Documentation
   3. Preservation
Evidence: U.S. Court: Admissibility

1. Legal Search & Seizure (Criminal Procedure)
2. Authenticated
   1. Authenticity
   2. Documentation
   3. Preservation
3. Best Evidence Rule
   - FRE 2004 Rules 401 - 403, 1001 - 1004
   - Frye Standard (Frye v. U.S., 1923)
   - Coppolino Standard (Coppolino v. State, 1968)
   - Marx Standard (People v. Marx, 1975)
   - Daubert Standard (Daubert v. Merrell Dow, 1993)
Evidence: U.S. Court: Admissibility

1. Legal Search & Seizure (Criminal Procedure)

2. Authenticated
   1. Authenticity
   2. Documentation
   3. Preservation

3. Best Evidence Rule
   - FRE 2004 Rules 401 - 403, 1001 - 1004
   - Frye Standard (Frye v. U.S., 1923)
   - Coppolino Standard (Coppolino v. State, 1968)
   - Marx Standard (People v. Marx, 1975)
   - Daubert Standard (Daubert v. Merrell Dow, 1993)

4. Exceptions to the Hearsay Rule
   - Documentary & Digital Evidence
   - FRE 2004 Rules 801 - 804
   - State v. Armstead, 1983
Evidence: Viability

1. Admissible
   ✓ (Covered Earlier)
2. Applicable
   ✓ Real & Relevant
3. Verifiable
   ✓ Independently Verifiable Authenticity
4. Reliable
   ✓ Industry Accepted Tools & Techniques
   ✓ Non-Contaminated
5. Receivable
   ✓ Presentable
   ✓ Understandable
   ✓ Believable
6. Complete
   ✓ Self-Contained
   ✓ Exculpatory
7. Convincing
Forensic Procedure

1. Preparation
2. Collection
3. Preservation
4. Analysis
5. Presentation
**Procedure: Preparation**

1. Incident Statement
   - Discovery Timeline
   - Initial Hypotheses
   - Mitigating Actions
Procedure: Preparation

1. Incident Statement
2. Establish & Prioritize Objectives
   - SMART Objectives
Procedure: Preparation

1. Incident Statement
2. Establish & Prioritize Objectives
3. Establish Constraints (Rules of Engagement)
   - Regulatory
   - Security & Privacy
   - IRP, BCP
   - Court Orders
Procedure: Preparation

1. Incident Statement
2. Establish & Prioritize Objectives
3. Establish Constraints (Rules of Engagement)
4. Mobilize Team
   - Coordinators, Forensic & Security Specialists, Scribe
   - Legal Counsel, Notary, Political
   - Paired Approach: Worker, Supervisor
Procedure: Preparation

1. Incident Statement
2. Establish & Prioritize Objectives
3. Establish Constraints (Rules of Engagement)
4. Mobilize Team
5. Mobilize Tools
   - Secure & Dedicated Environment
   - Identification, Capture, and Archival Tools
   - Industry Standard Tools
Procedure: Preparation

1. Incident Statement
2. Establish & Prioritize Objectives
3. Establish Constraints (Rules of Engagement)
4. Mobilize Team
5. Mobilize Tools
6. Brief Team
   1. Describe Incident
   2. Define Roles & Responsibilities
   3. Issue Credentials
Procedure: Preparation

1. Incident Statement
2. Establish & Prioritize Objectives
3. Establish Constraints (Rules of Engagement)
4. Mobilize Team
5. Mobilize Tools
6. Brief Team, and
7. Collect Incident-Relevant Materials
   1. Past & Present Specifications & Schematics
   2. Past & Present System Topologies & Diagrams
   3. Past & Present Access Control Lists
Aside: Analog & Digital Residuals

Misnomers

- "Deletion" Skips Data; Marks Space as Available
- "Overwritten" Leaves "Analog" Residuals
- "Discharged" Leaves "Digital" Residuals
**Aside: Analog & Digital Residuals**

**Misnomers**
- "Deletion"  Skips Data; Marks Space as Available
- "Overwritten"  Leaves “Analog” Residuals
- "Discharged"  Leaves “Digital” Residuals

**Interesting Tidbits**
- "Secure Deletion of Data from Magnetic and Solid-State Memory”
  Peter Gutmann, 1996
- "Data Remanence in Semiconductor Devices”
  Peter Gutmann, 2001
- **Veeco Instruments NanoTheatre**
  Atomic Force & Magnetic Force Microscopy (AFM & MFM)
  Data Storage Gallery
Procedure: Collection

Collection Challenges
First Layer Collection
+ Data Preservation
+ Data Integrity
+ Documentation
= Evidence Viability
Procedure: Collection

**Collection Challenges**

First Layer Collection
+ Data Preservation
+ Data Integrity
+ Documentation

= **Evidence Viability**

**Contamination Challenges**
- Normal Deterioration (System & User)
- Examination Contamination
- System Malfunction
- Negligence, Malpractice
- Malware: Sabotage & Espionage (User & Kernel)
- “Real-Time” Sabotage
- Tamperware (User & Kernel)
- Natural (or Unnatural) Disaster
Procedure: Collection

1. Identify Potential Sources
   1. Data Containers
      1. Macro (System)
         1. Enterprise
         2. Host → Network (LAN, WAN)
         3. Disk → Disk Array (RAID)
         4. NAS → SAN
         5. Peripheral Devices (e.g., Key-Stroke Loggers, Print Queue)
   2. Micro (Host)
      1. Disk Storage (e.g., Fixed, Removable)
      2. Non-Volatile Memory Storage (e.g., Flash)
      3. Volatile Memory Storage (e.g., RAM)
      4. Processor Storage (e.g., Registers, Cache)
Procedure: Collection

1. Identify Potential Sources
   1. Data Containers
   2. Data Stores
      1. Master & Slave Storage
      2. Redundant & Standby Storage
      3. RAID Mirroring
      4. Data Journals, Version Control: e.g., CVS, Subversion
      5. Online & Offline Backups
      6. Filesystem Journals: e.g., ext3, reiserfs, jfs, xfs
      7. Meta Storage: e.g., NTFS MFT
      8. Permitted Transfer
      9. Disaster Recovery Sites
     10. Regulatory Compliance
     11. Filesystem Monitors: e.g., Tripwire
     12. Logs
Procedure: Collection

1. Identify Potential Sources
   1. Data Containers
   2. Data Stores
   3. Data Authenticators (Assurance)
      1. Audit Logs (e.g., Tripwire)
      2. Fingerprints, Version Control
      3. General System Logs
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
   Order of Volatility (OoV)
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda

Order of Volatility (OoV)

1. Factors (Risk of Contamination)
   1. Control Flow: Frequent → Infrequent
   2. Abstractions: Lower (System) → Upper (Application)
      Raw → Cooked
   3. Mutability: Mutable → Semi-Mutable → Immutable
   4. Volatility: Volatile → Non-Volatile (Power)
   5. Probe Stability: Safe → Unsafe
   6. Anticipated: Relevant → Irrelevant
   7. Data Stores → Data Authenticators
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
   Order of Volatility (OoV)
   1. Factors (Risk of Contamination)
   2. Containers
      1. Processor Storage
      2. Volatile Memory Storage
      3. Non-Volatile Memory Storage
      4. Disk Storage
Procedure: Collection

1. Identify Potential Sources

2. Establish Capture Agenda

   Order of Volatility (OoV)
   1. Factors (Risk of Contamination)
   2. Containers
   3. In Practice
      1. Processor State: Registers & Cache
      2. System Time/Date (UTC / GMT & Local)
      3. Kernel: Configuration, Modules, Memory, Stats
      4. Process Table: State, Memory, Files, Bindings, Trace, Stats, Shared Memory
      5. Network: ARP & DNS Cache, Bindings, Connections, Routing, Stats
      6. Main Memory, Swap
      7. BIOS, EEPROM Data
      8. File System Meta: Time/Date Stamps, Access Control, e.g. MAC, MACE, MFT
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
   Order of Volatility (OoV)
   1. Factors (Risk of Contamination)
   2. Containers
   3. In Practice
   4. Mechanisms
      1. Select Method(s) of Access
         e.g., HDD: BIOS v. Direct
      2. RAID Capture: Logical Disk
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
3. Document Scene
   - Digital Photographs, Audio/Video Records
   - Log: Time/Date, Investigators, Scene Description
   - Five Senses (Non Interference)
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
3. Document Scene
4. Contain Scene (Secure Interfaces)
   - “Cold-Turkey” Shutdown **Will** (Generally) Prevent Capture of Memory
   - “Cold-Turkey” Shutdown **Will** Prevent Capture of *Mounted* Encryption
     e.g., Cryptoloop, Win32 Encrypted File System (EFS)
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
3. Document Scene
4. Contain Scene (Secure Interfaces)

Schedule as Opportune, Applicable, and Appropriate:

1. Unusual Noise is a VERY Bad Thing
2. Freeze Memory & Filesystem
   - Forensic Kernel (System-Call) Subversion (Future?)
   - Forensic Library Subversion (Future?)
   - "Remount" Read-Only (Data & Meta)
3. Freeze Environment
   - "Real-Time" Halt & Memory Dump (Future?)
4. Freeze Network
   - Firewall: Ingress, Egress, Bi-Directional
   - Single User Mode
5. "Cold-Turkey" Shutdown (Disconnect Power)
   - Preserve v. Damage
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
3. Document Scene
4. Contain Scene
5. Capture Data
   o Capture Agenda: Respect OoV (1:1 Capture)
   o Capture Everything: e.g., dmesg → hdparm → sdfisk → dd
   o If Safe, Synchronize Memory to Disk
   o Document Everything
     o Activity / Handler Log
       o Case #, Tag #, Container Tag #
       o Time/Date, People, Roles, Process, Approval
       o Environment, Physical Configuration, Connectivity (Topology)
       o Log: Action, Result, Signature, Supervisor Sign-Off, Witnesses
     o Tamper-Proof Evidence Tagging
       o Time/Date, Make, Model, P/N, S/N, Geometry
       o Source (Physical Seizure) & Capture
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
3. Document Scene
4. Contain Scene
5. Capture Data
6. Fingerprint Capture
   o Cryptographic Hash
   o Checksum
Procedure: Collection

1. Identify Potential Sources
2. Establish Capture Agenda
3. Document Scene
4. Contain Scene
5. Capture Data
6. Fingerprint Capture, and
7. Secure Evidence
   1. Anti-Static, Tamper-Proof Envelopes
   2. Chain-of-Custody Form (Follows Evidence)
      - Transfer: Time/Date, Reason, Details
      - Source & Destination Person / Location
      - Signatures: Handlers, Supervisor
   3. Evidence Activity Form (Follows Evidence)
      - Check-In & Check-Out, Reason, Details
      - Person, Location, Log
      - Signatures: Handlers, Supervisor
   4. Secure Evidence & Documentation in Vault / Escrow (Credentials as Necessary)
Procedure: Collection (Example)

ahi@oglaroon:~# mount -o sync -n /dev/hdd1 /mnt/dev/hdd1 # <-- Mount Evidence Target
ahi@oglaroon:~# cd /mnt/dev/hdd1
ahi@oglaroon:hdd1# dd if=/dev/urandom of=hdb.img bs=1M # <-- Prime Encrypted Target
ahi@oglaroon:hdd1# LD=`losetup -f` # <-- Identify First Free Loop-Back Device (cryptoloop)
ahi@oglaroon:hdd1# losetup -e aes $LD hdb.img # <-- Establish Encrypted Loop-Back
ahi@oglaroon:hdd1# mke2fs –b 4096 –m 0 $LD # <-- Make File-Based Filesystem
ahi@oglaroon:hdd1# mount -o sync -n $LD /mnt/nam/hdb.img # <-- Mount Filesystem
ahi@oglaroon:hdd1# cd /mnt/nam/hdb.img
ahi@oglaroon:hdb.img# dmesg | tee dmesg.`date +%Y%m%d-%H%M%S` | grep [hs]d[a-z] # <-- Find Source
ahi@oglaroon:hdb.img# hdparm -i /dev/hdd | grep "UDMA modes" # <-- Query uDMA Modes of Target
ahi@oglaroon:hdb.img# hdparm -Igi /dev/hdb > hdparm.`date +%Y%m%d-%H%M%S` 2>&1
ahi@oglaroon:hdb.img# grep "UDMA modes" hdparm.* # <-- Query uDMA Modes of Source
ahi@oglaroon:hdb.img# fdisk –lu /dev/hdd > fdisk.`date +%Y%m%d-%H%M%S` 2>&1 # <-- Capture Geometry
ahi@oglaroon:hdb.img# dmesg | tee dmesg.`date +%Y%m%d-%H%M%S` | grep [hs]d[a-z] # <-- Find Source
ahi@oglaroon:hdb.img# fdisk –lu /dev/hdd > fdisk.`date +%Y%m%d-%H%M%S` 2>&1 # <-- Capture Geometry
ahi@oglaroon:hdb.img# smartctl –s on /dev/hdd # <-- Activate SMART Interface
ahi@oglaroon:hdb.img# smartctl –a /dev/hdd > smartctl.`date +%Y%m%d-%H%M%S` 2>&1 # <-- Query SMART
ahi@oglaroon:hdb.img# smartctl –a /dev/hdd > smartctl.`date +%Y%m%d-%H%M%S` 2>&1 # <-- Query SMART
ahi@oglaroon:hdb.img# dmesg | tee dmesg.`date +%Y%m%d-%H%M%S` | grep [hs]d[a-z] # <-- Find Source
ahi@oglaroon:hdb.img# smartctl –a /dev/hdd > smartctl.`date +%Y%m%d-%H%M%S` 2>&1 # <-- Query SMART
ahi@oglaroon:hbd1# umount –d $LD # <-- Un-Mount & Free Loop-Back Device
Aside: Surveillance

- If Appropriate, Establish "Honey-Net"
  1. Balance Potentials: Objectives v. Liabilities
  2. Isolate "Honey-Net"
  3. Configure Active "Honey-Net" Framework (Optional)
  4. Establish Remote & Secure Data Capture
  5. Establish Intrusion Detection System (IDS)
     1. Monitoring & Notification
     2. Interior & Exterior
  6. Absolute Fail-Safe

Unix / Linux Tools
- Snort, (IDScnter), Tripwire, Nagios
- Honeynet Project
- Honeyd, The Deception Toolkit (TDK)
- tcpdump
Procedure: Preservation

1. If Safe, Synchronize Memory to Disk
2. “Cold-Turkey” Shutdown (Disconnect Power)
3. Follow “Secure Evidence” Collection
Procedure: Analysis

Diagram:

Physical Analysis
- Sectors
- Segments
- Files
- Volumes
- Swap
- Database Analysis
- Continuous
- Fragments
- Binary

Logical Analysis
- Memory Analysis
- State Analysis
- Filesystem Analysis
- Application Analysis
- Presentation

Digital Forensics
**Procedure: Analysis**

1. Establish Analysis Agenda
   1. Recombine Dataset
      - Defragmentation
      - RAID Reconstitution
   2. 1st Layer → nth Layer of Abstraction
   3. Meta → Data
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
3. Identify Artifacts
   1. Identify Intact Artifacts
   2. Identify Obfuscated Artifacts (“Carving”)
      1. Concealment
         1. “In-Band”
            • “Deleted” Data
            • Interleaved Datasets (e.g., Steganography, Deniable Encryption)
            • “Extra” / “Unused” Areas
         2. “Out-of-Band”
            • File Slack Space (e.g., ELF), Volume Slack Space
            • Non-Partitioned & Reserved Space
            • Host Protected Area (HPA)
            • False Markings & Structure (e.g., Bad Sector, Inode Disconnect)
            • Journal Hiding
            • Fragmentation
   2. Destruction
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
3. Identify Artifacts
4. Analyze Artifacts
   1. Time-Line Analysis
      1. System State
         1. Process State: e.g., Time/Date Stamps, Open Files, Trace
      2. Application
         1. "Forensic Discovery": DNS TTL
   3. Filesystem
      1. MAC: Modified, Accessed, Changed
      2. MACE: Modified, Accessed, Created, Entry
      3. Journal Entries
   4. Trace & Log File Analysis
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
3. Identify Artifacts
4. Analyze Artifacts
   1. Time-Line Analysis
   2. Contextual Analysis
      1. Common Analysis: Magic, HashDB, Patterns, Strings
      2. Specific Application Tools
e.g., DBMS, E-Mail/Client, PDA
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
3. Identify Artifacts
4. Analyze Artifacts
5. Application Analysis
   1. Passive Analysis: Strings & Instructions
   2. Active Analysis
      1. Establish Environment
         1. Virtual Filesystem Execution (e.g., chroot) (Bad)
         2. Virtual Machine (VM) Execution (e.g., VMware) (Better)
         3. Dedicated Machine Execution (Best)
      2. Establish Framework
         1. Process Analysis (e.g., strace, truss)
         2. Kernel & Library Subversion
         3. Censored Execution (e.g., Java Globe, Janus, SysTrace)
   3. Execute
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
3. Identify Artifacts
4. Analyze Artifacts
5. Application Analysis
6. Involve Specialists
   1. Prepare Assets & Objectives for Hand-Off
   2. Engage Field Experts (e.g., Filesystem, RAID, DBMS)
   3. Provide Forensic Framework
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
3. Identify Artifacts
4. Analyze Artifacts
5. Application Analysis
6. Involve Specialists
7. Theorize to Objectives
Procedure: Analysis

1. Establish Analysis Agenda
2. Duplicate for Analysis
3. Identify Artifacts
4. Analyze Artifacts
5. Application Analysis
6. Involve Specialists
7. Theorize to Objectives, and
8. Refine Process & Repeat
Procedure: Presentation

- Structure
  1. Describe Objectives
  2. Assert Conclusions
     1. State Conclusion
     2. Present Relevant Evidence
     3. Present Logical Analysis
  3. Table of Evidence
     1. Describe Collection
     2. Describe Handling
Procedure: Presentation

- Structure
- Guidelines
  - Evidence: Admissible, Applicable, Verifiable, Reliable, Receivable, Complete, and Convincing
  - Be Structured & Organized
  - Be Clear, Concise, and Cogent
  - Be Objective
  - Anticipate Challenges
  - Presentation = Testament
Procedure: Presentation

- Structure
- Guidelines
- Formalize
  - Digital Encryption
  - Digital Signing
Aside: Recovery

**Restore Operational Continuity**

1. Incident Response Plan (IRP) Check-List
2. Establish / Refine Policies & Procedures
   - Incident Response Procedure (IRP)
   - Disaster Recovery Plan (DRP)
   - Business Continuity Plan (BCP)
3. Restore Service & Data-Set
4. Restore & Confirm System Integrity
   - Eliminate Malware
   - Eliminate Tamperware
5. Provision Up-to-Date Security (Local & Remote)
   - IPS, IDS
   - Auditable
6. Provision Up-to-Date System Health Management
   - Monitoring → Containment → Notification → Recovery
7. Provision Secure, Incremental Archival & Backup Solutions
8. Enable Services
Tools & Techniques
Live Response: Unix & Linux Tools

Disk, Volume, and Filesystem Query
- Disk: dd, hdpam, smartctl, sync
- Volume: dd, df, disktype, fdisk, mount, tune2fs
- Filesystem: cd, stat, du, find, cat, dd, file, ar
- ELF: ldd, nm, objdump, readelf, size

Process Query
- ps, pstree, gprof, strace, top
- fuser, lsoc

Memory Query
- free, ipcs, vmstat

Network Query
- arping, ping, nmap, ping, traceroute
- nc, netstat, tcpdump
- ifconfig, iwlist, iwconfig
- ethereal, iptraf, ipppstats
- nessus, cryptcat

History Query
- history, last, lastb, lastcomm, w, who

System Query
- dmesg, iostat, lspci, lsmod, sar, uname, uptime

Data Stream Manipulation
- grep, hexdump, od, xxd, strings, wc, tee
- awk, sed
- md5sum
- less, more, sort, uniq
- bzcat, bzless, bzmore
- iconv

Additional Tools
- Bash, Perl + CPAN, expect
- dcf1-dd, ned/odd, rex
- chkrootkit, ClamAV
- xargs
- openssl, ssh, losetup
- foremost
- hydra
- cdrecord

Linux Locations
- /home/*/.history*
- /{bin,boot,dev,etc,home,lost+found}
- /{mnt,opt,proc,root,sbin,tmp,usr,var}
- /dev/{hd?*,sd?*}, /dev/{mem,kmem}
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo .* *
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo .* *
# date "+%F %X %Z"
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo .* *
# date "+%F %X %Z"
# hdparm –A 1 –X udma6 –a 256 –c 1 –d 1 –m 16 /dev/hd?* (Dangerous)
# mount –o noatime,nodev,noexec,ro ...; mount –o sync ...
# dcfldd if=[...] of=[...] bs=128 conv=noerror,notrunc,sync \  
  hashwindow=1024 hashlog=[...] errlog=[...]
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo .* *
# date "+%F %X %Z"
# hdparm -A 1 -X udma6 -a 256 -c 1 -d 1 -m 16 /dev/hd?* (Dangerous)
# mount -o noatime,nodev,noexec,ro ...; mount -o sync ...
# dcfldd if= [...] of= [...] bs=128 conv=noerror,notrunc,sync \
  hashwindow=1024 hashlog= [...] errlog= [...] 
# find / -noleaf -printf "%F %i %A® %C® %T® %U=%u:%G=%g %m %s %d %n %p\n"
# find / -noleaf -type f -printf "%i " -exec md5sum -b "{}" \

Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo .* *
# date "+%F %X %Z"
# hdparm -A 1 -X udma6 -a 256 -c 1 -d 1 -m 16 /dev/hd?* (Dangerous)
# mount -o noatime,nodev,noexec,ro ...; mount -o sync ...
# dcfldd if=[...] of=[...] bs=128 conv=noerror,notrunc,sync \
   hashwindow=1024 hashlog=[...]
# find / -noleaf -printf "%F %i %A@ %C@ %T@ %U=%u:%G=%g %m %s %d %n %p\n"
# find / -noleaf -type f -printf "%i " -exec md5sum -b "{}" \;
# who -a
# last -aix
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo .* *
# date "+%F %X %Z"
# hdparm -A 1 -X udma6 -a 256 -c 1 -d 1 -m 16 /dev/hd?* (Dangerous)
# mount -o noatime,nodev,noexec,ro ...; mount -o sync ...
# dcfldd if=[...], of=[...], bs=128, conv=noerror,notrunc,sync,hashwindow=1024, hashlog=[], errlog=[]
# find / -noleaf -printf "%F %i %A@ %C@ %T@ %U=%u:%G=%g %m %s %d %n %p\n"
# find / -noleaf -type f -printf "%i " -exec md5sum -b \\n# who -a
# last -aix
# netstat -anv 2>&1
# netstat -aiv 2>&1; netstat -arnv 2>&1
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo ./* *
# date "+%F %X %Z"
# hdparm -A 1 -X u DMA6 -a 256 -c 1 -d 1 -m 16 /dev/hd?* (Dangerous)
# mount -o noatime,nodev,noexec,ro ...; mount -o sync ...
# dcfldd if= [...] of= [...] bs=128 conv=noerror,notrunc,sync \  
  hashwindow=1024 hashlog= [...] errlog=[]
# find / -no leaf -printf "%F %i %A@ %C@ %T@ %U=%u:%G=%g %m %s %d %n %p\n"
# find / -no leaf -type f -printf "%i " -exec md5sum -b "{}" \\
# who -a
# last -aix
# netstat -a nv 2>&1
# netstat -aiv 2>&1; netstat -arnv 2>&1
# ps axww -o start_time,pid,ppid,ruid,rgid,euid,egid,fuid,fgid,  
  %cpu,%mem,stat,cputime,etime,ni,ignored,rss,cmd -forest
# pstree -Gachlnpu
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

# echo .* *
# date "+%F %X %Z"
# hdparm -A 1 -X udma6 -a 256 -c 1 -d 1 -m 16 /dev/hd?* (Dangerous)
# mount -o noatime,nodev,noexec,ro ...; mount -o sync ...
# dcfldd if= [...] of= [...] bs=128 conv=noerror,notrunc,sync \
   hashwindow=1024 hashlog= [...] errlog= [...] 
# find / -noleaf -printf "%F %i %A@ %C@ %T@ %U=%u:%G=%g %m %s %d %n %p\n"
# find / -noleaf -type f -printf "%i " -exec md5sum -b "{}" \ 
# who -a 
# last -aix 
# netstat -anv 2>&1 
# netstat -aiv 2>&1; netstat -arnv 2>&1 
# ps axww -o start_time,pid,ppid,ruid,rgid,euid,egid,fuid,fgid, 
   %cpu,%mem,stat,cputime,etime,ni,ignored,rss,cmd -forest 
# pstree -Gachlnpu 
# lsof -Rl +w 2>&1
Tools & Techniques
Live Response: Unix & Linux Tools (Examples)

```bash
# echo .* *
# date "+%F %X %Z"
# hdparm -A 1 -X 256 -c 1 -d 1 -m 16 /dev/hd?* (Dangerous)
# mount -o noatime,nodev,noexec,ro ...; mount -o sync ...
# dcfldd if= [...] of= [...] bs=128 conv=noerror,notrunc,sync
   hashwindow=1024 hashlog= [...] errlog= [...] 
# find / -noleaf -printf "%F %i %A@ %C@ %T@ %U=%u:%G=%g %m %s %d %n %p\n"
# find / -noleaf -type f -printf "%i " -exec md5sum -b "{" "
# who -a
# last -aix
# netstat -anv >&1
# netstat -aiv >&1; netstat -arnv >&1
# ps axww -o start_time,pid,ppid,ruid,rgid,euid,egid,fuid,fgid,
   %cpu,%mem,stat,cputime,etime,ni,ignored,rss,cmd -forest
# pstree -Gachlnpu
# lsof -Rl +w >&1
# mount -o loop=/dev/loop[#] [img-file] [mount-point]
```
Tools & Techniques
Live Response: Windows Tools

- ipconfig, netstat, nbtstat, userdump
- Cygwin + UnxUtils + UnxUpdates
- Sysinternals: Utilities
  - Disk: DiskExt, Diskmon, Du, EFSDump, Filemon, MoveFile, PendMoves
  - Disk: SDelete, Streams, Sync, Strings
  - Security: AccessEnum, Autologon, LogonSessions, Tokenmon
  - Security: RootKitRevealer, ShareEnum
  - Process: Autoruns, Filemon, Handle, ListDLLs, PMon, Portmon
  - Process: Process Explorer, PsFile, PsList, PsTools, Regmon
  - Network: TCPView, TCPVcon, TDIMon
  - System: CPUMon, LiveKd, LoadOrder, PsInfo, RegDelNull
- SecurityFocus: Tools
  - (Browse by Category)
- Open-Source Digital Forensics: Tools: Windows-Based
Tools & Techniques

Postmortem Response: TCT, TSK

The Coroner’s Toolkit (TCT)
- **grave-robber** ~ Data Capture & Pre-Processing
- **ils, icat, unrm, ffind, fls, ifind** ~ Low-Level File Tools
- **mactime** ~ Timeline Analysis
- **lazurus** ~ Restructuring Tool
- **pcat, memdump** ~ Low-Level Process & Full Memory Tools
- **timeout** ~ Time-Limit Executions
- **TCTUTILs** ~ TCT Extension

The Sleuth Kit (TSK)
- **fsstat, ffind, fls** ~ “File-Layer” Tools
- **icat, ifind, ils, istat** ~ “Meta-Layer” Tools
- **dcat, dls, dstat, dcalc** ~ “Data-Layer” Tools
- **jcat, jls** ~ “Journal” Tools
- **mmls, img_stat, disk_sreset, disk_stat** ~ More Tools
- **hfind, mactime, sorter, sigfind** ~ Even More Tools

- **Autopsy Forensic Browser (AFB)** ~ Interface System
- **mac-robber** ~ Timeline Analysis
Tools & Techniques
Postmortem Response: Commercial & Other Tools

Forensic Analysis
- **EnCase** ~ Guidance Software
- **Ultimate Toolkit (UTK)** ~ AccessData
- **ProDiscover** ~ Technology Pathways
- **Forensicware Solutions** ~ StepaNet Communications
- **SMART** ~ ASR Data
- **Cell & PDA Seizure** ~ Paraben Forensic: Mobile & PDA Analysis

Virtual Machines & Emulators
- **VMware**: Virtual Machines & Infrastructures
- **Cygwin**: Win32 Linux Emulator
- **PalmOS Developer Suite** ~ PalmSource

Worth Mentioning
- **Bash, Perl, expect**
- **Forensic Hash Database**
- **Penguin Sleuth**
- **galleta, pasco, rifiuti, stegdetect, libpst**
Tools & Techniques
Building a Forensic Tool-Kit

1. Forensic Workstation
   ✓ Ruggedized Workstation (Laptop)
     ✓ Lots of Fast Storage & Memory
     ✓ CD-R/RW + DVD±R/RW
     ✓ USB 2.0 + IEEE 1394b
     ✓ Multiple Gigabit Ethernet
     ✓ 802.11abg
     ✓ Spare Hi-Capacity Batteries (+ Chargers)
   ✓ Securified Kernel
     ✓ Proper Hardware Support: e.g., HDD Controllers, ...
     ✓ FS Support: e.g., fat*, ntfs, ext*, jfs, reiserfs, xfs, hpfs, hfs, nfs*, smb*, ...
     ✓ Cryptoloop, PC Card
   ✓ Encrypted Filesystem
   ✓ Time-Accurate: e.g., NTP
   ✓ Software Toolkit
Tools & Techniques
Building a Forensic Tool-Kit

1. Forensic Workstation
2. Hardware Kit
   ✓ High Capacity, High Speed Drives
   ✓ Single & RAID Controllers
     ✓ P/ATA: ATA-1, ATA-2, ATA-3, ATA/ATAPI-5, ATA/ATAPI-6
     ✓ S/ATA: SATA-1, SATA-2
     ✓ S/SCSI: SSA, FC-AL, SAS
   ✓ Maximum Length (Y-)Power & Data Cables
     ✓ Internal P/ATA: IDC-40, IDC-80, Molex, mIDC-44 (Male Receptacle)
     ✓ Internal S/ATA: SATA-Data, SATA-Power
     ✓ Internal P/SCSI: IDC-50(M), HPDB-68(F), SCA-80, Molex, HDI-30
     ✓ External P/SCSI: HPDB-50, HPDB-68, CN-50, VHDCI-68, DB-25, DB-50, ...
   ✓ Joints (M-to-M, F-to-F), Terminators
   ✓ Adapters & Forensic Bridges (Write Blockers)
     ✓ ATA, SCSI ↔ USB, FW
   ✓ Spare Jumpers, Screws
   ✓ Network Switch, Straight & Crossover Cables
   ✓ Power Strip, Power Extension
Tools & Techniques
Building a Forensic Tool-Kit

1. Forensic Workstation
2. Hardware Kit
3. Software Kit
   ✓ (Supplementary Tools Listed Throughout)
   ✓ Bootable CD-ROM Toolkit: e.g., Knoppix
   ✓ Script Interpreters: e.g., Bash, Perl, Expect
   ✓ OS Base & Common Device Drivers
   ✓ Scanners & Cracker: e.g., Nessus Vulnerability Scanner
   ✓ Software Write Blockers: e.g., PDBlock
Tools & Techniques
Building a Forensic Tool-Kit

1. Forensic Workstation
2. Hardware Kit
3. Software Kit
4. Additional Tools
   - Palm Pilot
   - Digital Still, Video, Audio Recorder
   - Computer Tool-Kit & Dremel
   - White-Light LED Flashlight
   - Cigarette-Lighter Inverter
   - Uninterrupted Power Supply (UPS)
Tools & Techniques
Building a Forensic Tool-Kit

1. Forensic Workstation
2. Hardware Kit
3. Software Kit
4. Additional Tools
5. Additional Supplies
   - Evidence Forms: e.g., Chain-of-Custody, Activity
   - Evidence Tags, Seals, and Anti-Static Envelopes
   - 3.5IN, CD, DVD
   - Cable Ties
   - ESD Strap or Anti-Static Surfaces / Mats
   - Pens, Pencils, Paper
Tools & Techniques
Building a Forensic Tool-Kit

1. Forensic Workstation
2. Hardware Kit
3. Software Kit
4. Additional Tools
5. Additional Supplies, and
6. Documentation (Digital, If Possible)

- Technical
  - Tool Tutorials & References
  - Common Hardware & Software Specifications & References
  - Linux Documentation Project (LDP)
  - Default Lists: e.g., Passwords, Ports, Fingerprints
  - Pocket Science & Technology References

- Guidelines
  - Performance Checklists
  - Legal References
Tools & Techniques
M1911 .45
Counter-Forensics

- Non-Destructive Techniques
  - Obfuscation
  - Intrusion Prevention

- Destructive Techniques
  - Meta Cleansing
  - Data Cleaning
Counter-Forensics: “Absolute”

#!/bin/bash

disk_sreset /dev/hda  # <-- Disable HPA
for N in 1 2 3 4 5 6 7; do  # <-- DoD Secure Standard?
    dd if=/dev/urandom of=/dev/hda bs=1024 conv=noerror
done
Counter-Forensics: Non-Destructive

- Obfuscation
  - Data Hiding & Fragmentation
  - Encoding / Encryption
  - Deniable Encryption
  - Steganography
Counter-Forensics: Non-Destructive

- **Obfuscation**
  - Data Hiding & Fragmentation
  - Encoding / Encryption
  - Deniable Encryption
  - Steganography

- **Intrusion Prevention**
  - Network Appliances: Firewall, IDS/IPS
  - Network & Host Security
Counter-Forensics: Non-Destructive

- **Obfuscation**
  - Data Hiding & Fragmentation
  - Encoding / Encryption
  - Deniable Encryption
  - Steganography

- **Intrusion Prevention**
  - Network Appliances: Firewall, IDS/IPS
  - Network & Host Security

- **Disorder ~ Chaos ~ Entropy**
  - Information Overload
  - False Positives
Counter-Forensics: Destructive

- Presence & Persistence of Residual Data
  - P. Gutmann ~ Secure Deletion of Data
  - Account for Fragmentation
  - Account for “Fossilization”
  - Account for Abstraction Layers
**Counter-Forensics: Destructive**

- **Presence & Persistence of Residual Data**
  - P. Gutmann ~ Secure Deletion of Data
  - Account for Fragmentation
  - Account for “Fossilization”
  - Account for Abstraction Layers

- **Meta Cleansing**
  - MAC(E)-Times
  - Filesystem Indices

- **Data Cleansing**
  - Cleanse Data
  - Cleanse Log Data
  - Cleanse Cache & Swap
Counter-Forensics: Tools

**Filesystem Tools**
- MetaSploit ~ Anti-Forensics Project
- TrueCrypt ~ Interleaved Cryptoloop Alternative
- PhoneBook Project ~ PhoneBook Filesystem
- NTFSHider, Clandestine FS Driver
Counter-Forensics: Tools

**Filesystem Tools**
- MetaSploit ~ Anti-Forensics Project
- TrueCrypt ~ Interleaved Cryptoloop Alternative
- PhoneBook Project ~ PhoneBook Filesystem
- NTFSHider, Clandestine FS Driver

**User & Kernel Malware**
- Sabotage & Espionage, Backdoors
- Tamperware
- SISW’05: t0rn, Dica, Lrk5, Flea, SAdoor, ulogin, Adore, Knark
- BackOrifice 2k, Hacker Defender, FU, AFX RootKit
- (See [http://www.rootkit.com/](http://www.rootkit.com/))
Counter-Forensics: Tools

**Filesystem Tools**
- MetaSploit ~ Anti-Forensics Project
- TrueCrypt ~ Interleaved Cryptoloop Alternative
- PhoneBook Project ~ PhoneBook Filesystem
- NTFSHider, Clandestine FS Driver

**User & Kernel Malware**
- Sabotage & Espionage, Backdoors
- Tamperware
- SISW’05: t0rn, Dica, Lrk5, Flea, SAdoor, ulogin, Adore, Knark
- BackOrifice 2k, Hacker Defender, FU, AFX RootKit
- (See [http://www.rootkit.com/](http://www.rootkit.com/))

**Absolute Tools**
- Foundry, Crucible, and Gas Mask
- HERF Gun
Bash ~ Russian Roulette

#!/bin/bash

if [ $( $RANDOM % 6 ) == 0 ]; then
    echo “Have a nice day!”
    find / -type f -exec shred -uzn 7 "{" \;
fi
Forensic Hardening

**Security by Design & Practice**
- Identify Past, Present, and Future Vulnerabilities
- Network Security: Firewall, IDS, IPS, FO/LB, VLAN, VPN
- Host Security: Firewall, IDS, IPS, SSL
- Data Security: Encryption, Obfuscation
- External, Demilitarized Logging
- External, Demilitarized System Health Management
- Redundant, Non-Homogenous Architecture
- Strict Authentication & Access Control
- Secure Application Development
- Application Firewalls
- Scheduled Probes
- Scheduled ORTs
- Strict Government (Policies & Procedures)
Forensic Future

- Forensic Hardening
- Preventative v. Reactive Forensics
- Low Layer Backups
- Improved File Carving Tools
- Improved Cracking Tools
- Improved Response through Effective IDS & Monitoring
- Improved Tools to “Freeze” Live Machine
- Education
Resources: Organizations

- Carnegie Mellon ~ SEI CERT
  “First Computer Security Incident Response Team”
  http://www.cert.org/

- Purdue ~ CERIAS
  Center for Education & Research in Information Assurance & Security
  http://www.cerias.purdue.edu/

- NIST ~ CSD CSRC
  National Institute of Standards & Technology
  Computer Security Division: Computer Security Resource Center
  http://csrc.nist.gov/

- Symantec ~ SecurityFocus
  “Most Comprehensive & Trusted, Vendor-Neutral, ...”
  http://www.securityfocus.com/
Resources: Internet

- AccessData ~ http://www.accessdata.com/
- Argus ~ http://www.qosient.com/argus/
- Cfengine ~ http://www.cfengine.org/
- Coroner’s Toolkit ~ http://www.porcupine.org/forensics/tct.html
- Default Password List ~ http://www.phenoelit.de/dpl/dpl.html
- Despair ~ http://www.despair.com/
- Digital Forensics Research Work-Shop ~ http://www.dfrws.org/
- dmidecode ~ http://www.nongnu.org/dmidecode/
- Digital Intelligence Forensic Solutions ~ http://www.digitalintelligence.com/
- DriveSavers Data Recovery ~ http://www.drivesavers.com/
- Ethereal ~ http://www.ethereal.com/
- FatBack ~ http://www.sourceforge.net/projects/biatcux/
- Foremost Carving Tool ~ http://foremost.sourceforge.net/
- ForInSect ~ http://www.forinsect.de/
- grsecurity ~ http://www.grsecurity.com/
- Guidance Software ~ http://www.guidancesoftware.com/
Resources: Internet

Resources: Internet

- Penguin Sleuth Kit ~ http://www.linux-forensics.com/
- Phenoelit: Lands of Packets ~ http://www.phenoelit.de/
- RootKit Magazine ~ http://www.rootkit.com/
- Root Secure ~ http://www.rootsecure.net/
- SecuriTeam ~ http://www.securiteam.com/
- SecurityFocus ~ http://www.securityfocus.com/
- Secure Programming ~ http://www.dwheeler.com/secure-programs/
- Sleuth Kit Project ~ http://www.sleuthkit.org/
- Snort ~ http://www.snort.org/
- SysInternals ~ http://www.sysinternals.com/
- TaoSecurity ~ http://www.taosecurity.com/
- Tableau ~ http://www.tableau.com/
- USENIX ~ http://www.usenix.com/
- Veeco NanoTheatre ~ http://www.veeco.com/nanotheatre/
- WinInternals ~ http://www.wininternals.com/
- WikiPedia ~ http://www.wikipedia.com/
Resources: People

- Brian Carrier, Ph.D ~ TSK, AFB
- Eoghan Casey ~ Cyber Security & Investigations
- Dan Farmer ~ TCT, Titan, SATAN
- Orin Kerr, J.D. ~ Criminal Procedure & Cyber Law
- Bruce Schneier ~ Blowfish, TwoFish, Counterpane
- Wietse Venema ~ TCT, SATAN, Postfix
Resources: Books

- Forensic Discovery ~ D. Farmer, W. Venema
- Real Digital Forensics ~ K.J. Jones, R. Beijtlich, C.W. Rose
- File System Forensic Analysis ~ B. Carrier
- Handbook of Computer Crime Investigation ~ E. Casey
- Applied Cryptography, 2nd Edition ~ B. Schneier
- Pocket Ref, Pocket PCRef ~ T.J. Glover
- Programming Perl, 3rd Edition ~ L. Wall, J. Orwant, T. Christiansen
- Exploring Expect ~ D. Libes
- Understanding the Linux Kernel, 3rd Edition ~ D.P. Bovet, M. Cesati
Resources: Books

Douglas Adams

- Hitch-Hiker’s “Trilogy”
  2. Restaurant at the End of the Universe
  3. Life, the Universe, and Everything
  4. So Long, and Thanks For All the Fish
  5. Mostly Harmless

- Dirk Gently
  - Dirk Gently Holistic Detective Agency
  - The Long Dark Tea-Time of the Soul
Resources: Commercial

- KPMG ~ Forensic
- Navigant Consulting ~ Discovery Services
- LexisNexis ~ Applied Discovery
- Kroll ~ OnTrack

- DriveSavers ~ Data Recovery

- Tableau ~ Forensic Bridges
- Paraben Corporation ~ Cell & PDA Seizure Tool-Box
- PCCables.com ~ Lots of Cables & Stuff
- Guidance Software ~ EnCASE
- Ultimate Toolkit (UTK) ~ AccessData

- Axis Microsystems ~ ForensicPC
- Nessus Security Scanner
- Internet Security Systems (ISS)
- Axent Technologies
- eEye Digital Security
Peace Out!

If you’d like a copy of this presentation, please check the LayerOne website (http://www.layerone.info/) in the near future. Also, please do feel free to e-mail me at ahimmerman@yahoo.com.

Thank you for joining me,

Andrew