



Forensic Readiness

Presented by:

Jack J. Murphy, Ph.D.

Corporate Capabilities

- Advanced Network Technologies
 - IPV6, MPLS/VPLS, VoIP, DWDM
 - Micromuse Netcool® Certified Government Integrator
- Enterprise Security
 - Network, Host, Application Security Solutions
 - International Information System Security Certification Consortium (ISC)2 Resources (CISSP)
- Infrastructure Applications
 - Network, Host, Application Monitoring & Management
 - Desktop/Server Software Management/Provisioning



Background

- Forensic Science—The application of science to the law
- Digital Forensic—The application of science to the identification, collection, analysis, and examination of digital evidence (DFI) while preserving the integrity of the information and maintaining a strict chain of custody for the evidence
- Types of Digital Forensic Investigation (DFI)
 - Computer
 - Network
 - Others



Background (Cont.)

- Forensic Readiness—The ability of an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation
- Anti-forensics—The application of tools and techniques to conceal or destroy information so that others cannot access it.
 - Benign uses: Donating used equipment to charity, removing data on public (kiosk) computers to preserve the users privacy, equipment disposal
 - Nefarious uses: Confounding incident responders data analysis activities



Context

- Criminal activity represents a small fraction of the need for a forensic analysis capability, e.g.,
 - Troubleshooting performance anomalies
 - Virus Remediation/Clean-up
 - IDS/Firewall/Operating System Alarm Response
- But, chain-of-custody formalisms, evidence collection/handling rules, and privacy concerns must be applied in coordination with legal and law enforcement organizations
- Specialized disciplines require specialized skills e.g., Forensic Accounting, Forensic Engineering, and Software Forensics



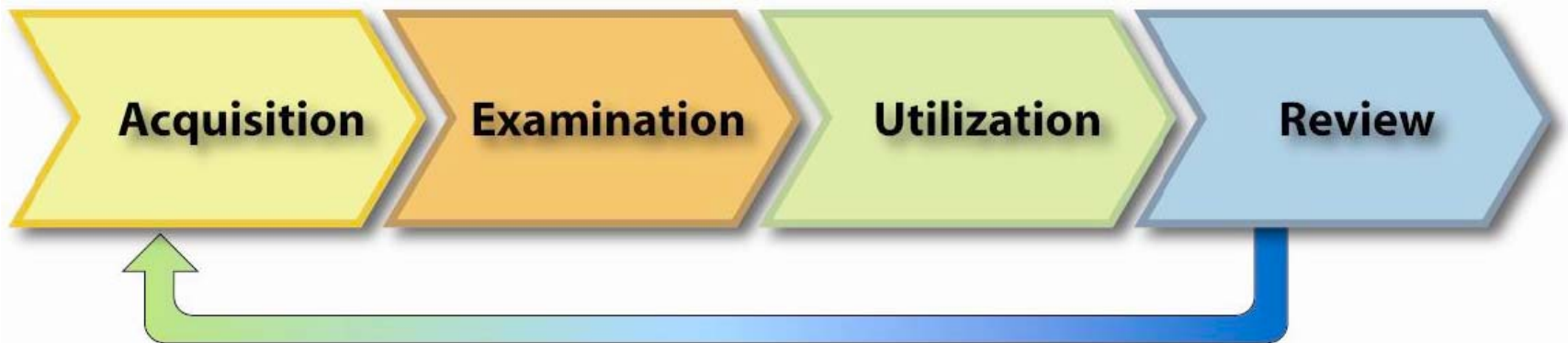
Context (cont.)

- Incident Types¹
 - Threats and extortion
 - Accidents and negligence
 - Stalking and harassment
 - Commercial disputes
 - Disagreements, deceptions, and malpractice
 - Property rights infringements
 - Economic crime (fraud, money laundering)
 - Content abuse
 - Privacy Invasion and identity theft
 - Employee disciplinary issues

1. [A 10 Step Process for Forensic Readiness](#)
International Journal of Digital Evidence
Winter 2004, Vol. 2, Issue 3



Analysis Process²



- Performed in the context of an enterprise forensic policy
 - Organization
 - Tools and Procedures
 - Roles and Responsibilities



Acquisition

- File/Mail/Application Servers
- System Log Files
- Phone Log Files
- Backup/Archive Systems
- Firewall Audit/Log Records
- IDS, Antivirus, Spyware logs
- Hard Disk/Removable Media
- ISP Log Files
- Alternative Work Place
- Adjacent systems persons
- Interviews and Paper Documents
- Keystroke monitoring
- RAM and BIOS content

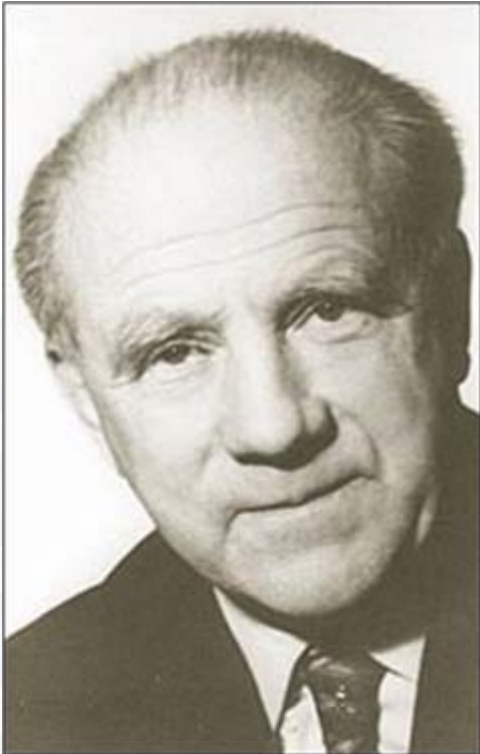


Acquisition (Cont.)

- Collecting the Data
 - Step 1—Develop a Plan
 - Likely Value Consider data sources and incident circumstances
 - Volatility Give high priority to volatile sources
 - Effort Consider time & complexity, outside experts, legal advisors, law enforcement, special equipment
 - Step 2—Collect the Data
 - Use Certified Tools for Volatile Data
 - Duplicate non-volatile data locally if possible
 - Use write blockers if possible (e.g., on workstations)
 - Step 3—Verify the Integrity of the Data (SHA-1 and/or MD-5)
 - Source
 - Copy
 - Source Again

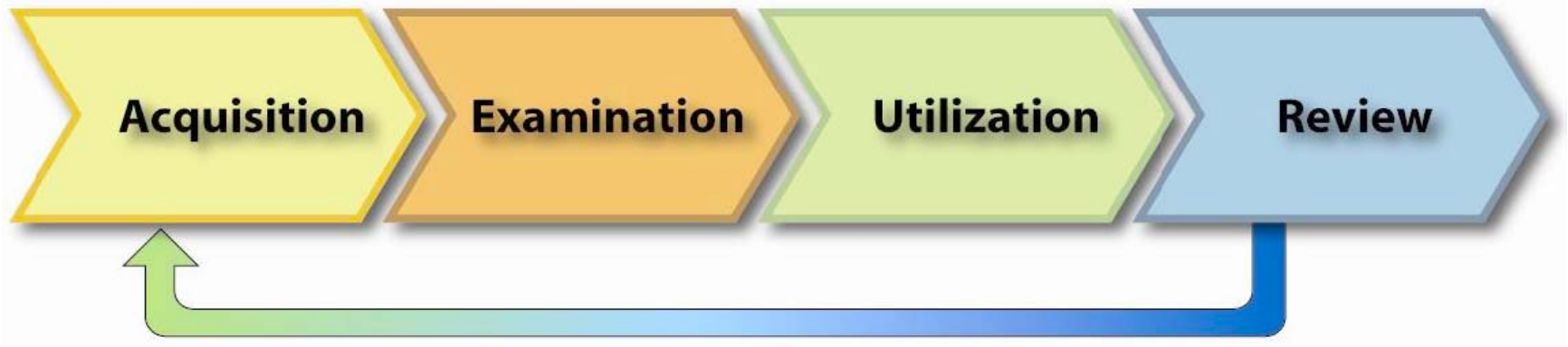


Acquisition (Cont.)



- Heisenberg Uncertainty Principle: If you know where a particle is you can't measure with precision its speed (and vice versa) without altering it!
- Forensic analyst dilemma: Any attempt to capture data precisely will most likely alter it! Despite write-blockers! And vice versa!!

Examination



- Requires sophisticated tools for
 - Discovery
 - Selection/Exclusion, Pattern Matching
 - Correlation and comparison (e.g., to a baseline config.)
- Employs scientific methods to draw conclusions



Examination (cont.)

- Challenges
 - Recovery of Deleted Files
 - Slack Space (unused space in the last block of a file or memory page)
 - Free Space (unused partition, file system, or memory blocks)
 - Missing/Renamed Files/Alternate Data-streams/File Metadata
 - Exploited File/Protocol Formats (covert channels)
 - Altered Operating System Files, Partition Table, File System, File Headers, File Names, File Extensions, File Modify/Access/Create Attribute
 - Eliminating “Safe” Files using NSRL Reference Data Set (<http://www.nsrl.nist.gov/downloads>)



Examination (cont.)

- Challenges (Cont.)
 - Detecting
 - Steganography
 - Encryption
 - Compression
 - Volatile data
 - Operating network configuration, open ports, running processes, open files, login sessions, operating system time
 - Recovering password hashes before shutdown
 - Rootkit discovery and response



Anti-Forensics

- Known Hiding Techniques
 - Media Management Layer—Hide data in unused partitions, the boot sector, or in the partition table itself
 - File System Layer—Hide data in the file system data structure itself, file slack space, inode/data-stream, or socially-engineered file/directory names, removal of open files (volatile data), and other tricky stuff
 - Application Layer—Obfuscated/offset loopback filesystems, unused fields in application file formats
 - Exploits of journaling file systems—Very tricky

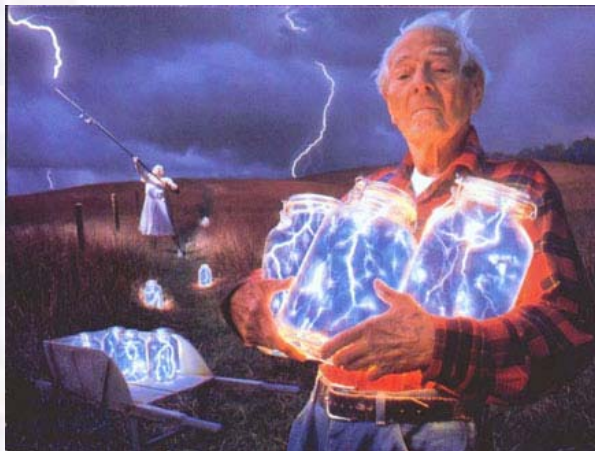


Stegananography

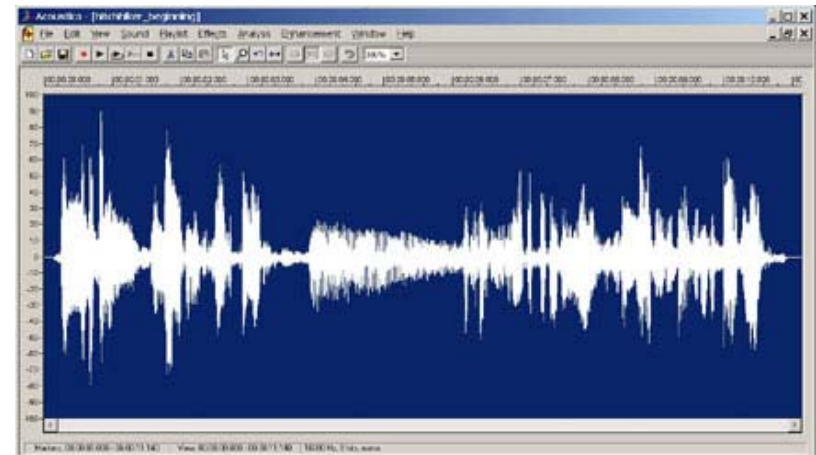
gif-it-up (color pallet)



Jphs (lossy, e.g., jpeg)



S-Tools (lossless, e.g., .wav)

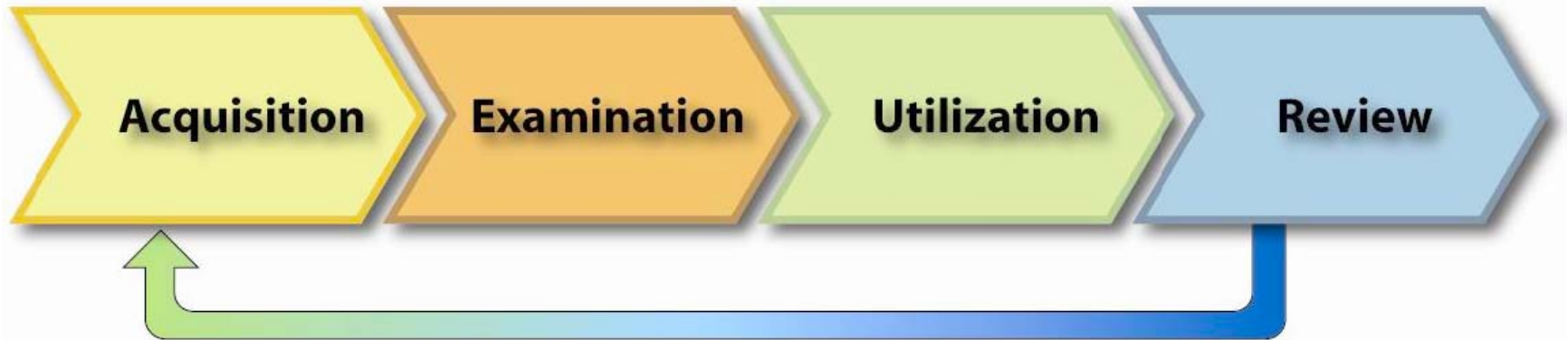


Cryptography

- Kerckhoff's Principle: The security of a cryptosystem shall not be based on keeping the algorithm secret but solely on keeping the key secret.
- In other words, assume your opponent knows the cryptosystem being used.
- Encrypted files look a lot like compressed files—Need to determine file format (<http://www.wotsit.org>)
- Need to recover keys (if possible) from volatile storage/memory (e.g., swap file or memory dump)



Utilization



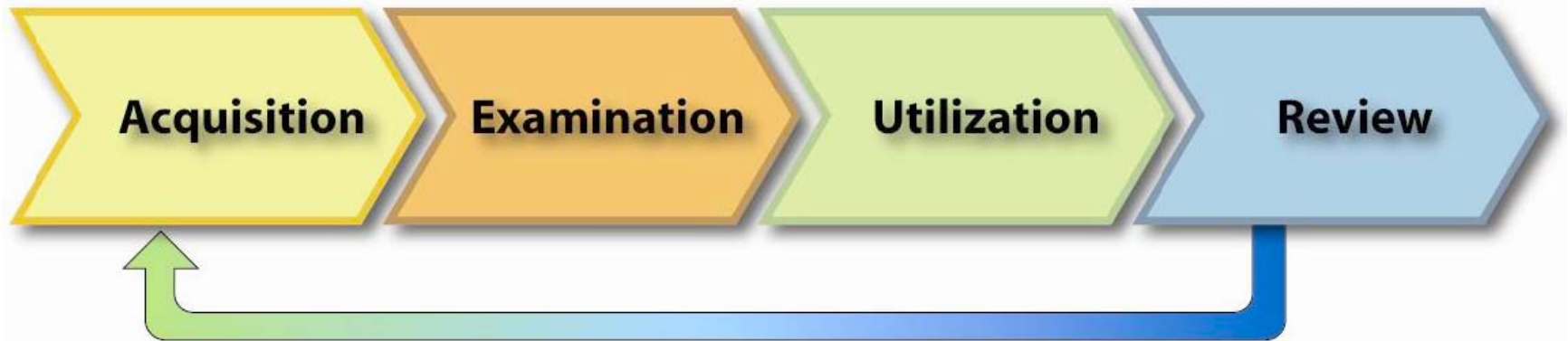
- Requires
 - Understanding of the purpose of the investigation
 - Presentation skills and audience analysis
 - Objectivity

Data Utilization

- Factors Affecting Data Utilization
 - Data Reduction—Purpose is to present only the necessary & relevant facts, to the proper people only, to help them understand what occurred and what might need to be done
 - Alternatives—In the absence of conclusive data about what happened, fairly consider alternative explanations and present them
 - Audience—The CXO needs are different; so are the security, system administrator, and others responsible for daily operations
 - Actionable—For prevention, legal/administrative response, and follow-on investigation not forensic related



Review



- Hot Wash—Formal, Structured Review
 - What went right, What went wrong
 - Process/Procedure/Policy Review
 - Training/Tool Improvements
 - Team Peer Review
 - Implement and Validate Changes



Preparing for an Investigation

- Three Aspects:
 - Prevention
 - Detection
 - Response
- A 30 minute attack required an average of 48 hours of forensic investigation by the best and brightest investigators³
 - Only includes examination phase--no acquisition, utilization, or review
 - Doesn't count outages, cleanup, etc.
 - And none of 13 teams found everything!

<ul style="list-style-type: none"> • NETWORK VULNERABILITY ASSESSMENT • APPLICATION ASSESSMENT 	<ul style="list-style-type: none"> • HOST HARDENING • FORENSIC READINESS • POLICY WRITING 	<ul style="list-style-type: none"> • INTRUSION DETECTION • INCIDENT RESPONSE PLANNING 	INCIDENT	<ul style="list-style-type: none"> • FORENSIC ACQUISITION • INCIDENT RESPONSE 	<ul style="list-style-type: none"> • EXAMINATION • UTILIZATION • REVIEW 	<ul style="list-style-type: none"> • PROSECUTION • INTRUDER TRACKING
------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------	-----------------	-------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------

3. <http://www.honeynet.org>

Preparing for an Investigation (cont.)

- Prevention
 - Implement policies that support cyber forensics
 - Retaining Information
 - Planning the Response
 - Training
 - Accelerating the Investigation
 - Preventing Anonymous Activities
 - Protecting the Evidence
 - Policy Characteristics
 - User Focused
 - Monitoring
 - Acceptable use
 - Organizational
 - Roles/Responsibilities
 - Incident Response Guidelines
 - Forensic Team
 - Closely linked to Business Continuity Plan



Preparing for an Investigation

- Detection
 - Implement technologies that support cyber forensics
 - NTP, backup, IDS, system logs, unique identification
 - CCTV, RFID, honeypots
 - Implement processes that support cyber forensics
 - Train people on the processes and technologies



Preparing for an Investigation

- Response
 - Team Composition
 - Forensics Team
 - Subject/Suspect/Staff
 - HR/PR Staff
 - Process/Data Owners
 - Management
 - Claimant
 - Corporate Security
 - IT Staff
 - Legal
 - Follow the analysis process
 - Operating procedures should address quarantine guidelines
 - Follow evidence handling procedures (rules of evidence)
 - Important note: Containment and recovery objectives compete with forensic objectives (the Heisenberg Principle)



Preparing for an Investigation (cont.)

- Factors affecting the time and cost
 - How logging is done
 - What is logged
 - IDS
 - Forensic Acquisition Phase of Analysis Process
 - Evidence Handling



A 10 Step Approach to Forensics Readiness

- Define the business scenarios that require digital evidence
- Identify available sources/types of evidence
- Establish evidence collection requirements
- Establish a capability to securely gather legally admissible evidence
- Establish a policy for storage/handling of evidence
- Ensure monitoring is targeted to detect/deter major incidents
- Identify circumstances requiring escalation to full/formal investigation
- Train staff on incident awareness/roles/law
- Document incidents and impact base on evidence
- Ensure legal review to facilitate action in response to an incident



Forensic Readiness Costs

- Updates to policy
- Improvements in training
- Systematic evidence gathering
- Secure storage of evidence
- Incident preparation
- Legal advice
- Developing an in-house DFI capability



Forensic Readiness Benefits

- Enterprise defense
- Deterrent to insider threat
- Minimal disruption to the business in the event of an incident
- Reduced cost/time for internal investigation
- Extends information security to the wider threat from cyber crime
- Demonstrates due diligence and good enterprise governance
- Demonstrates compliance with regulatory requirements
- Improve the prospect for successful legal action
- Supports employee sanctions based on digital evidence



Other “Best Practices”

- Establish a Tools Library consisting of NIST evaluated Forensic Tools
 - AccessData Forensic Toolkit (FTK)
(<http://www.accessdata.com/>)
- Have a baseline image for each host type
- Consider certification
 - Certified Cybercrime First Responder (CCFR)
 - Certified Computer Forensics Technician (CCFT)
 - Certified Forensic Computer Examiner (CFCE)
 - Certified Information System Auditor (CISA)



Tools

- Software-based Disk Imaging Tools
 - Linux dd, EnCase, SafeBack, ILook
- Hardware-based Disk Imaging Tools
 - SOLO Forensics, Solitaire
- Software-based Write-blockers
 - PDBlock, Writeblocker XP
- Hardware-base Write-blockers
 - FastBloc, SCSIBlock
- Forensic Boot CD
 - Helix/Knoppix



Resources

- NIST Special Publication 800-86 Guide to Computer and Network Data Analysis-Applying Forensic Techniques to Incident Response (Aug. 2005 draft)
- NIST Special Publication 800-61 Computer Security Incident Handling Guide
- Computer Forensic Tool Testing (<http://www.cftt.nist.gov>)
- National Software Reference Library (NSRL) Reference Data Set (RDS) (<http://www.nsrl.nist.gov/downloads>)
- The Ultimate Collection of Forensic Software (<http://www.tucofs.com>)
- File format specifications (<http://www.wotsit.org>)
- HoneyNet Project (<http://www.honeynet.org>)
- A Ten Step Process for Forensic Readiness, International Journal of Digital Evidence, Vol 2, Issue 3



Services

- Data Recovery
 - Data Recovery Services, DriveSavers, Ontrack Data Recovery
- Off-Site Backup
 - SunGard



Contact Info

- Internet: <http://www.dexisive.com/>
- E-mail: info@dexisive.com
- Phone: 703-934-2030
- Mail: 4031 University Drive
Suite 200
Fairfax, VA 22030

