Cyber Forensics

Unit-1

Computer Forensics:

- Introduction to Digital Forensics and its phases
- Preparing for Digital Investigations, Data Acquisition and Processing Crime Incident Scenes
- Understanding File Systems and recovery
- Data Encryption and Compression
- Automated Search Techniques, Forensics Software

Network Forensic:

- Introduction to Network Forensics and tracking network traffic
- Reviewing Network Logs, Network Forensics Tools, Performing Live Acquisitions
- Order of Volatility, and Standard Procedure.

Cell Phone and Mobile Device Forensics:

- Overview
- Acquisition Procedures for Cell Phones and Mobile Devices

Internet Forensic:

- Introduction to Internet Forensics, World Wide Web Threats, Obscene and Incident transmission
- Domain Name Ownership Investigation, Reconstructing past internet activities and events

What is Digital Forensics?

- Emerging discipline in computer security
  - "voodoo science"
  - No standards, few research
- Investigation that takes place after an incident has happened
- Try to answer questions: Who, what, when, where, why, and how

Types of investigations

- Determine what the incident was and get back to a working state
- Internal investigation
  - Should be based on IR policy
  - May lead to criminal investigation
- Criminal investigation
- Support for “real world” investigations

What is Computer Forensics?

- Collection, preservation, analysis and presentation of computer-related evidence
- Determining the past actions that have taken place on a computer system using computer forensic techniques

What is the Purpose of Computer Forensics?

- Classic Forensics
- Computer forensics uses technology to search for digital evidence of a crime
- Attempts to retrieve information even if it has been altered or erased so it can be used in the pursuit of an attacker or a criminal
- Incident Response
  - Live System Analysis
- Computer Forensics
  - Post-Mortem Analysis

Typical Investigations

- Theft of Company Secrets (client, customer or employee lists)
- Employee Sabotage
- Credit Card Fraud
- Financial Crimes
- Embezzlement (money or information)
- Economic Crimes
- Harassment
- Child Pornography
- Major Crimes
- Identity Theft

Media Devices that hold Potential Data

- Computers and laptops
- iPads
- iPods
- Smartphones and most other cell phones
- MP3 music players
- Hard Drives
- Digital Cameras
- USB Memory Devices
- PDAs (Personal Digital Assistants)
- Backup Tapes
- CD-ROMs & DVD's

Computer Forensic Capabilities

- Recover deleted files
- Find out what external devices have been attached and what users accessed them
- Determine what programs ran
- Recover webpages
- Recover emails and users who read them
- Recover chat logs
- Determine file servers used
- Discover document's hidden history
- Recover phone records and SMS text messages from mobile devices
- Find malware and data collected

Who uses Computer Forensics?

- Law Enforcement
- Private Computer Forensic Organizations
- Military
- University Programs
- Computer Security and IT Professionals

Law Enforcement

- Local, State and Federal levels
- Several detectives at local levels
  - Inadequate funding
- State Police
- FBI's Computer Analysis and Response Team (CART)
- Regional Computer Forensics Laboratories (RCFLs)
  - Philadelphia
- Primarily use EnCase

Private Computer Forensic Organizations

- Radley Forensics
- Computer Forensics Associates
- Bit-X-Bit
- Empire Investigation LLC
- Marmo Technology
- Advanced Forensic Recovery of Electronic Data
- Philadelphia Computer Forensics
- Philadelphia Computer Forensics Analysis and Investigations
- New York Computer Forensic Services
- Speckin Forensic Laboratories

Military

- Test, identify, and gather evidence in the field
  - Specialized training in imaging and identifying multiple sources of electronic evidence
- Analyze the evidence for rapid intelligence gathering and responding to security breach incidents
  - Desktop and server forensic techniques

University Programs

- Bachelors and Masters degrees
  - Incident response techniques
  - Well funded research area
  - Many free sources of test images to practice on
- Community colleges
  - Partnering with 4-year universities to complete associates and bachelors degrees
  - Great for working professionals
  - Flexible schedules and affordable tuition

Computer Security Professionals and IT Personnel

- Network traffic
- Compromised networks
- Insider threats
  - Disloyal employees
- Malware
- Breach of contracts
- E-mail Fraud/Spam
- Theft of company documents

Important Factors

- Legal procedures
  - Not compromising evidence
- Treat every piece of evidence as it will be used in court
- Documentation*
- Chain of Custody
- Write Blocks
- Imaging
  - Bit by bit copy of a piece of electronic media (Hard drive)

What Should be Avoided During an Investigation?

- Changing data
  - Changing time or date stamps
  - Changing files
- Overwriting unallocated disk space
  - This can happen when re-booting
- Verify Hash values from images

Computer Forensic Tools

- Parse through the created image
  - Built in system parser
- Rebuilds both active and deleted files
- Open source
- Commercial sources

Common Computer Forensic Software

- ArcSight Logger
- Netwitness Investigator
- Quest Change Auditor
- Cellebrite
- Physical Analyzer
- Lantern
- Access Data's Forensic Toolkit (FTK)
- EnCase Cybersecurity
- EnCase eDiscovery
- EnCase Portable
- EnCase Forensic*

EnCase Forensic

- Acquisition
- Reporting
- EnScript :
  - Scripting facility
  - Various API's for interacting with evidence
- Collect, Analyze and examine data
  - Deleted files
  - Unallocated space
  - File slack
- Duplicates of original data (Imaging)
  - Accuracy can be verified by hash and Cyclic Redundancy Check values

Typical investigation phases

1. Acquisition
2. Recovery
3. Analysis
4. Presentation

Phase 1: Acquisition

- Analogous to crime scene in the “real world”
- Goal is to recover as much evidence without altering the crime scene
- Investigator should document as much as possible
- Maintain *Chain of Custody*

Acquisition (2)

- Determine if incident actually happened
- What kind of system is to be investigated?
  - Can it be shut down?
  - Does it have to keep operating?
- Are there policies governing the handling of the incident?
- Is a warrant needed?

Acquisition (3)

- Get most fleeting information first
  - Running processes
  - Open sockets
  - Memory
  - Storage media
- Create 1:1 copies of evidence (imaging)
- If possible, lock up original system in the evidence locker

Phase 2: Recovery

- Goal is to extract data from the acquired evidence
- Always work on copies, never the original
  - Must be able to repeat entire process from scratch
- Data, deleted data, “hidden” data

File systems

- Get files and directories
- Metadata
  - User IDs
  - Timestamps (MAC times)
  - Permissions, …
- Some deleted files may be recovered
- Slack space

File deletion

- Most file systems only delete directory entries but not the data blocks associated with a file.
- Unless blocks get reallocated the file may be reconstructed
  - The earlier the better the chances
  - Depending on fragmentation, only partial reconstruction may be possible

Slack space

- Unallocated blocks
  - Mark blocks as allocated to fool the file system
- Unused space at end of files if it doesn't end on block boundaries
- Unused space in file system data structures

Steganography

- Data hidden in other data
- Unused or irrelevant locations are used to store information
- Most common in images, but may also be used on executable files, meta data, file system slack space

Encrypted data

- Depending on encryption method, it might be infeasible to get to the information.
- Locating the keys is often a better approach.
- A suspect may be compelled to reveal the keys by law.

Recovery (cont.)

- Locating hidden or encrypted data is difficult and might even be impossible.
- Investigator has to look at other clues:
  - Steganography software
  - Crypto software
  - Command histories

File residue

- Even if a file is completely deleted from the disk, it might still have left a trace:
  - Web cache
  - Temporary directories
  - Data blocks resulting from a move
  - Memory

Phase 3: Analysis

- Methodology differs depending on the objectives of the investigation:
  - Locate contraband material
  - Reconstruct events that took place
  - Determine if a system was compromised
  - Authorship analysis

Contraband material

- Locate specific files
  - Databases of illegal pictures
  - Stolen property
- Determine if existing files are illegal
  - Picture collections
  - Music or movie downloads

Locating material

- Requires specific knowledge of file system and OS.
- Data may be encrypted, hidden, obfuscated
- Obfuscation:
  - Misleading file suffix
  - Misleading file name
  - Unusual location

Event reconstruction

- Utilize system and external information
  - Log files
  - File timestamps
  - Firewall/IDS information
- Establish time line of events

Time issues

- Granularity of time keeping
  - Can't order events that occur in the same time interval
- Multiple systems:
  - Different clocks
  - Clock drift
- E-mail headers and time zones

The needle in the haystack

- Locating files:
  - Storage capacity approaches the terrabyte magnitude
  - Potentially millions of files to investigate
- Event reconstruction:
  - Dozens, hundreds of events a second
  - Only last MAC times are available
  - Insufficient logging

Compromised system

- If possible, compare against known good state
  - Tripwire
  - Databases of “good” files
- Look for unusual file MACs
- Look for open or listening network connections (trojans)
- Look for files in unusual locations

Unknown executables

- Run them in a constrained environment
  - Dedicated system
  - Sandbox
  - Virtual machine
- Might be necessary to disassemble and decompile
  - May take weeks or months

Authorship analysis

- Determine who or what kind of person created file.
  - Programs (Viruses, Tojans, Sniffers/Loggers)
  - E-mails (Blackmail, Harassment, Information leaks)
- If actual person cannot be determined, just determining the skill level of the author may be important.

Phase 4: Presentation

- An investigator that performed the analysis may have to appear in court as an expert witness.
- For internal investigations, a report or presentation may be required.
- Challenge: present the material in simple terms so that a jury or CEO can understand it.

Forensics Tools

- Acquisition
  - dd, pdd
  - SafeBack, …
- Recovery
  - Encase
  - TCT and SleuthKit
- Analysis
  - ?
- Presentation
  - ?