Computer Crime, Incident Response, and Digital Forensics

Ed Crowley

Spring 10

Today's Topics

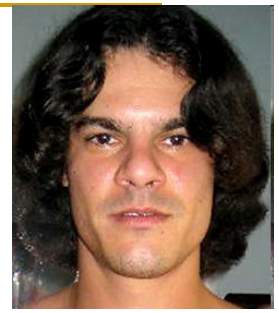
- Computer Crime
  - Threat
  - Attack Statistics & Trends
  - Corporate Concerns
  - Selected Costs
  - Selected Laws
- Incident Response
- Digital Forensics
  - Development
  - Methodology
- CF Categories
  - Disk Forensics
  - System Forensics
  - Network Forensics
  - Internet Forensics
- Digital Evidence
  - Rules of Evidence
    - Daubert Rule
- Case Demonstration

Who am I?

- NSA Certified
  - INFOSEC Assessment Methodology
  - INFOSEC Evaluation Methodology
- Usual Certifications from the usual suspects
  - Security + Certified, other certifications from Cisco, CompTIA, Microsoft
  - Earned CISSP from ISC^2
- Military Police Academy Graduate
  - Trained in Investigative Techniques
- Former:
  - IS Director
  - Academic Computing Researcher

Please note that I am not a lawyer.
As you would expect, nothing here should be construed as legal advice.

Threats & Threat Agents



Albert Gonzalez

Alexey Ivanov
and
Vasiliy Gorshkov

Ehud Tenenbaum

Robert Morris

Identity Theft

Attack Trends Overview

- Automation: increasing attack speeds
- Increasingly sophisticated attack tools
- Faster vulnerability discovery
- Increasing permeable firewalls
- Increasingly asymmetric threat
- Increasing threat from infrastructure attacks

--CERT/CC

  - Increasingly, attacks combine social engineering and technical attributes.
  - As lower ISO levels become secure, attacks move up the model.
- Most recent US Javelin data showed that 9.3M individuals (or 4.25% of all adults) are victims of identity fraud on an annual basis.

Corporate Concerns One

- FBI's CCIPs (Computer Crime and Intellectual Property Section) web site documents that over 50% of the intrusions investigated and referred for federal prosecution involved intruders with a relationship to the company they attacked.

- Of Fortune 500 organizations, 27% have defended themselves against claims of sexual harassment stemming from inappropriate email.
  - Includes Chevron and Microsoft that settled sexual harassment suits based on circulated emails for $2.7 million a piece.

- *Patricia Y. Logan*

Corporate Concerns Two

- IT staff can be involved in investigations for civil litigation, as well as investigations for a wide range of potential crimes including:
  - Breaches of confidentiality
  - Deliberate corruption of data
  - Fraud
  - Vandalism
  - Child pornography
  - Theft
  - Hate speech
  - Identity theft
  - Copyright violation
  - Extortion
  - Industrial espionage and systems sabotage.
- IT staff use some of the same computer forensic skills practiced by law enforcement, but investigations often require an extension of those skills to meet the unique nature of corporate surveillance and investigation.

  - *Patricia Y. Logan*

Selected Costs

- SirCam: 2.3 million computers affected
  - Clean-up: $460 million
  - Lost productivity: $757 million
- Code Red: 1 million computers affected
  - Clean-up: $1.1 billion
  - Lost productivity: $1.5 billion
- Love Bug: 50 variants, 40 million computers affected
  - $8.7 billion for clean-up and lost productivity

http://energycommerce.house.gov/107/hearings/11152001Hearing420/McCurdy724.htm

- U.S. Identity fraud crimes now total $52.6B annually (up 2.3% from the previous survey), with a per-individual total of $5,686 per victim, according to the Javelin study.

Trends Summary

- …organizations relying on the Internet face significant challenges to ensure that their networks operate safely and that their systems continue to provide critical services even in the face of attack.

--CERT/CC

- By inference, any organization utilizing digital devices faces analogous challenges…
- Until preventative security techniques are perfected, IR and forensics skills will be necessary.

Selected Laws

- Federal Computer Fraud and Abuse Act
- Federal Sentencing Guidelines
- Economic Espionage Act
- National Infrastructure Protection Act
- Patriots Act
- Privacy Laws
- Regulatory Laws

Privacy Laws

- Aim to protect information on private individuals from intentional or unintentional disclosure or misuse.
- Include:
  - Graham-Leach-Bliley, 1999
  - Health Insurance Portability and Accountability Act (HIPAA)
- US Privacy Laws differ from European Laws.
  - Organizational movement of individual private information across international boundaries may not be legal

Regulatory Laws

- GLB
- SOX
- HIPPA
- California SB 1386
- FERPA

Security Goals

- Historical Goals:
  - Confidentiality
  - Integrity
  - Availability
- Expanded to include:
  - Authentication
  - Non repudiation
  - Dynamic Environment

ISAlliance on Security

- "Security is not a one-time activity but rather a continuous, risk managed process,"

-- ISAlliance Executive Director Dave McCurdy.

Security Countermeasures

- Detective
  - Intrusion Detection
  - Incident Response
  - Digital Forensics
- Preventative
  - Access Control
  - Physical Security
  - Network Security

What is an Incident?

- Any adverse event that impacts an organization's security or ability to do business.
- Incident Handling
  - Addressed by establishing a Computer Incident Response Team (CIRT).
- Many incidents are the result of incompetent employees, malicious employees, other insiders, accidental actions, and natural disasters.

Carnegie Mellon's CERT

http://www.cert.org/

Why is Incident Response Required?

- Incident response is required for:
  - Rapidly detecting incidents
  - Minimizing loss and destruction
  - Mitigating exploited weaknesses
  - Restoring computing services.

NIST 800 -61

What is the Incident Response Life Cycle?

NIST 800 – 61

NIST's Computer Security Incident Handling

Figure 3-1. Incident Response Life Cycle

Incident Response Team

- Analyzes incident
  - Routine anomaly or security incident?
- Makes system viability decisions
  - Shutdown? Unplug?
- Conducts Forensics
  - Evidence search
  - Evidence preservation
- When necessary, contacts outside experts, forensic or LE
  - Calling LE may limit your ability to investigate incident
- Documents and reports incident

Incident Related Outside Communications

Digital Forensics

Attempts to determine:

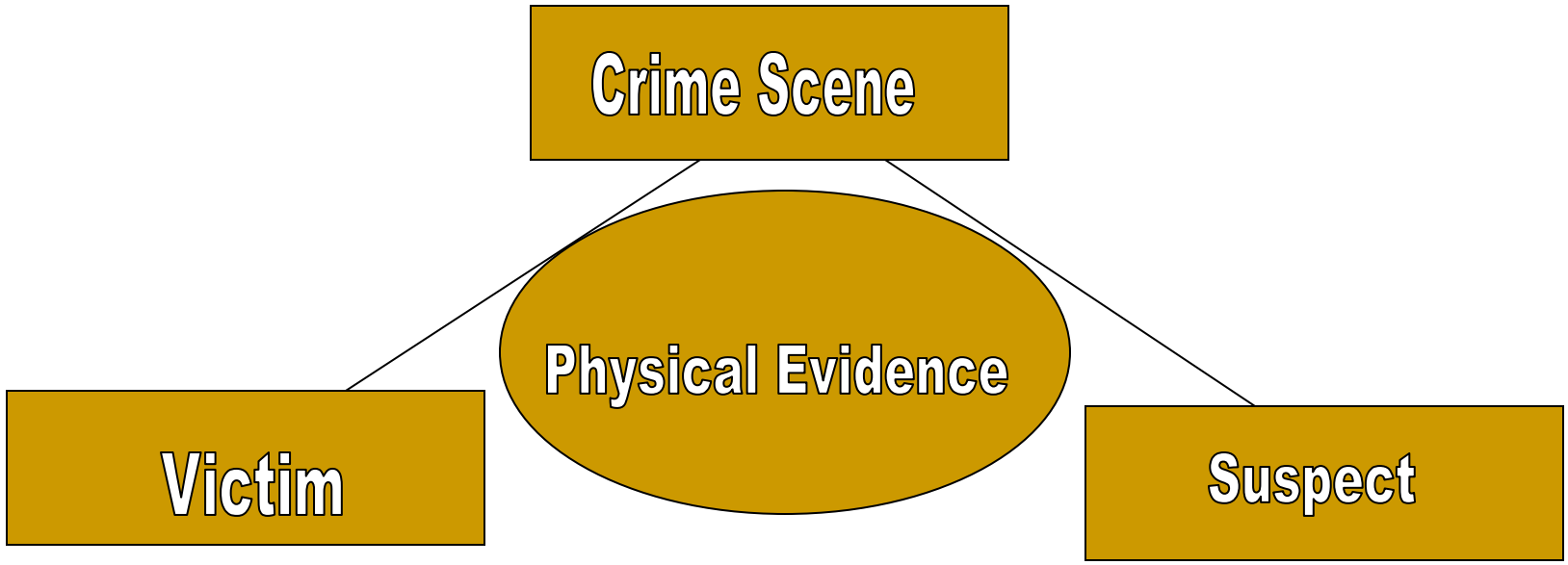
1. What happened?
2. How did it happen?
3. Who is responsible?

While most computer crimes are not prosecuted, we should still consider acceptability in a court of law as our standard for investigative practice.

-- Kruise and Hiese

Forensics are based upon Locard's Exchange Principle

Locard's Exchange Principle



- Anyone, or anything, entering a crime scene
  - Takes something of the scene with them, and
  - Leaves something behind when they depart.
  - Principle holds within a system, within a network, and within the Internet.

Forensic Interests

- Traditional
  - Fingerprints
  - Hairs and Fibers
  - Ballistics
  - DNA Collection and Testing
- Digital
  - Filesystems
  - Slack space
  - Logs
  - Keyloggers
  - E-mail

Computer Forensics Defined

- Computer Forensics
  - Name for the field of investigating computer crime.
  - Relatively young.
- Generally, it (Computer Forensics) is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. (NIST 800-86)

Computer Forensics Defined

- Unique issues associated with computer crime cases include:
  - Logical analysis of digital information required
  - Compressed investigation time frame (detective)
  - Intangible (digital) information
  - Potential interference with the normal conduct of the business

Computer Forensics

- Developed outside of the main traditions of Forensics Science

- Forensic Science implies:
  - Repeatability of investigations
  - Testing of methods
  - A normal process of determining “what is generally scientifically agreed” via peer reviewed journal articles

--Peter Sommer

Note many authorities consider Network Forensics a separate discipline.

A Brief CF Development Timeline

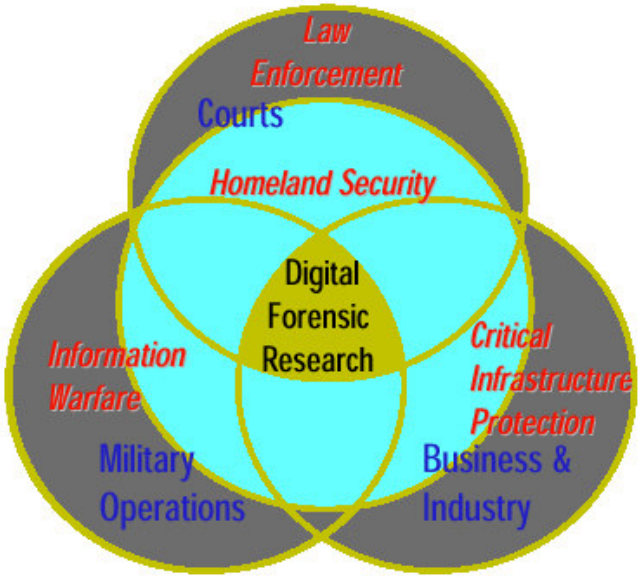
- Early ’90s, feeling that digital evidence might be important
- Mid ’90s, Law Enforcement discovers computer crime and computer evidence.
  - Kiddie porn, traveler crimes, and the threat of computer crime
  - LE struggles to understand how to respond

A Brief CF Development Timeline

- Mid 90's, LE experiments with Computer Forensic delivery models.
  - LE forms units, specialties, and labs.
  - Begins to develop CF policies and procedures
- Late 90s,critical mass achieved
  - CF critical to many cases
- Note, CF was developed from the bottom up.

--Mark Pollitt, Director FBI National Program Office for Regional Computer Forensic Laboratories

A Digital Forensics Taxonomy



Area	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution		After the fact
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business & Industry	Availability of Service	Prosecution	Real Time

A Digital Taxonomy

- … four distinct categories of forensic consumers ...
  1. Law enforcement
  2. Business or e-commerce
  3. U.S. DOD
  4. Research and academic
- Law enforcement focuses on gathering evidence for use in prosecution
  - Within strict judicial standards.
- Business requirements are driven more by economics for use in keeping the business on track.
  - Uses reasonably effective techniques that are cost justified and fast.
- Each category represents a distinctly different approach using varied criteria.

  - Charles Boeckman, Mitre

Basic Forensics Methodology

- Without altering or damaging original source, acquire and isolate evidence
- Authenticate that recovered evidence is the same as the original.
  - Document the crime scene
  - Verify document integrity
  - Maintain chain of custody
- Establish audit trail of all processes applied to computer based evidence.
  - Must be third party repeatable
- Analyze data without modifying it.

Methodology

ACPO Guidelines

- Principle 1
  - No action taken by officers or their agents should change data held on a computer or other media which may subsequently be relied upon in court.

- Principle 2
  - In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and implications of their actions.

For further information, consult the ACPO Good Practices Guide.

Computer Forensics Development

- Disk Forensics
  - Relatively well developed
- System Forensics
  - O/S Dependent
- Network Forensics
  - Includes ID systems
- Internet Forensics
  - Includes ISP logs etc.

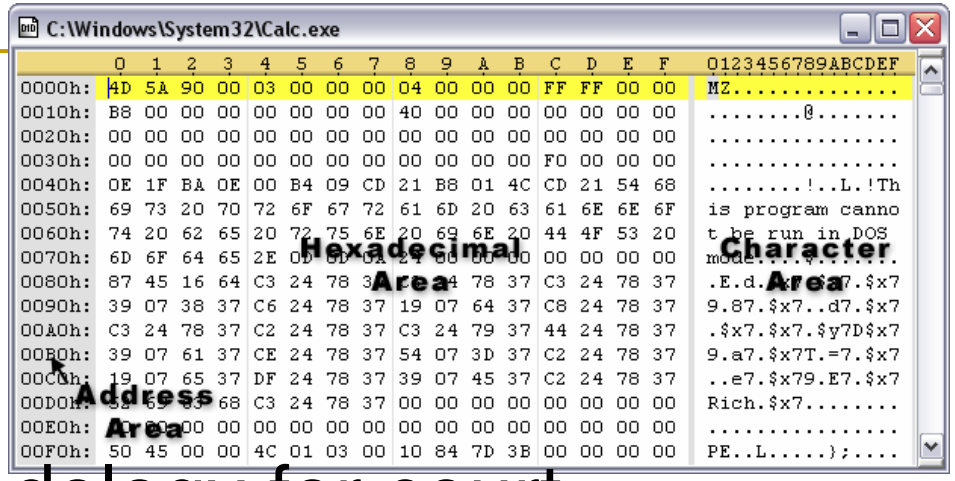
Disk Forensics Functions?

- Recover:
  - Deleted files
  - Passwords
  - Cryptographic keys
- Analyze file access, modification and creation times.
- View/analyze:
  - Logs, system, application, other …
- Identify a user or program's system activity.
- Analyze e-mail
  - Source
  - Content.

Disk Forensics

- Requires (bit-stream) image copies
  - Include slack space, unallocated space, paging (swap) files, and deleted file fragments.
- Investigators must be able to demonstrate compliance with evidence rules
- Integrity can be demonstrated with a message digest.

Disk Forensics



- Well established methodology for court preservation and presentation.
- Readily available commercial tools

- Love Bug Case Study
  - Hex Editors and Microsoft Office Documents
  - Michael Buen & Onel de Guzman
  - Jurisdiction Issues

Commercial Forensics Tools

- Tools and Vendors include:
  - EnCase
    - Guidance Software Pasadena, CA
  - Forensic Tool Kit (FTK)
    - AccessData
  - SafeBack
    - New Technologies, Inc. (NTI), Gresham, Oregon

EnCase

- Considered a L.E. leader in stand-alone forensics analysis.
  - Widely accepted in court.
- Facilitates examination of files, including deleted files and unallocated data.
- Produces reports and extracts without altering original data.

FTK

- AccessData's Forensic Toolkit® (FTK) can perform complete and thorough computer forensic examinations.
- Features powerful file filtering and search functionality.
- Customizable filters allow sorting through thousands of files to quickly find evidence.
- Recognized as a leading forensic e-mail analysis tools.

Other Forensic Tools

- Linux DD
  - Used by FBI, among other tools, in Zacarias Moussaoui's Case
- Coroners Tool Kit (CTK)
  - By Dan Farmer and Wietse Venema
  - Used for investigating Unix systems
- Winhex *State-of-the-Art Software*
  - Inexpensive hex, disk, and RAM editor.
  - Data analysis features include identification of certain file types (such as images) in unknown data, like that of recovered files.
  - Includes drive imaging and deleted data recovery capabilities.
- MD5Sum, 128 bit Message Digest generator

Message Digests and Digital Signatures

- Message digests provide a method of near individualization and, therefore, are sometimes referred to as digital fingerprints.

  --Eoghan Casey

- Digital signatures add reliability to a message digest
  - Essentially, a digital signature indicates that a given (trusted) individual calculated the message digest of a certain file.

System Forensics

- Includes ambient data such as:
  - Swap (paging) Files
  - Temporary Files
  - File Systems
  - Other data such as command history, registry files, …
- Internet Tokens
- Key Loggers
  - Alexey Ivanov and Vasiliy Gorshkov, Invita Case Study

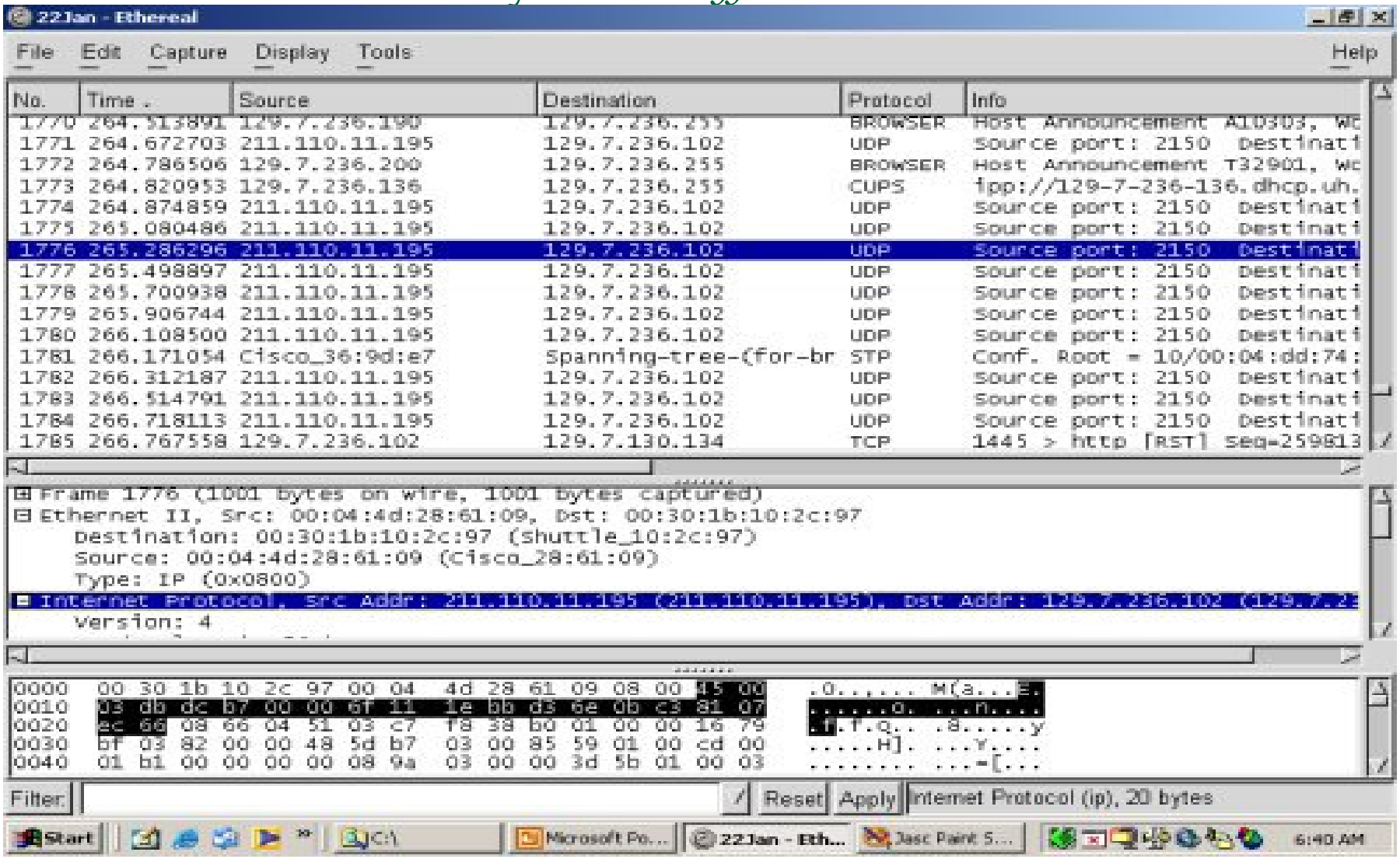
Computer System Addresses

- Logical or IP addresses
  - Public IP addresses assigned by ARIN
- Physical or MAC addresses
  - MAC addresses are burned in.
  - Address ranges are assigned to vendors by the IEEE.
  - Have been used to identify a particular computer
    - Melissa and the Love Bug Virus authors identified this way

Network Forensics

- Evidence collected from normal operation
  - Logs
  - Intrusion Detection Systems
- Evidence collected in specific surveillance
  - Extended logs
  - Sniffers
- IP headers contain source and destination IP addresses
- DataLink headers contain source and destination MAC addresses

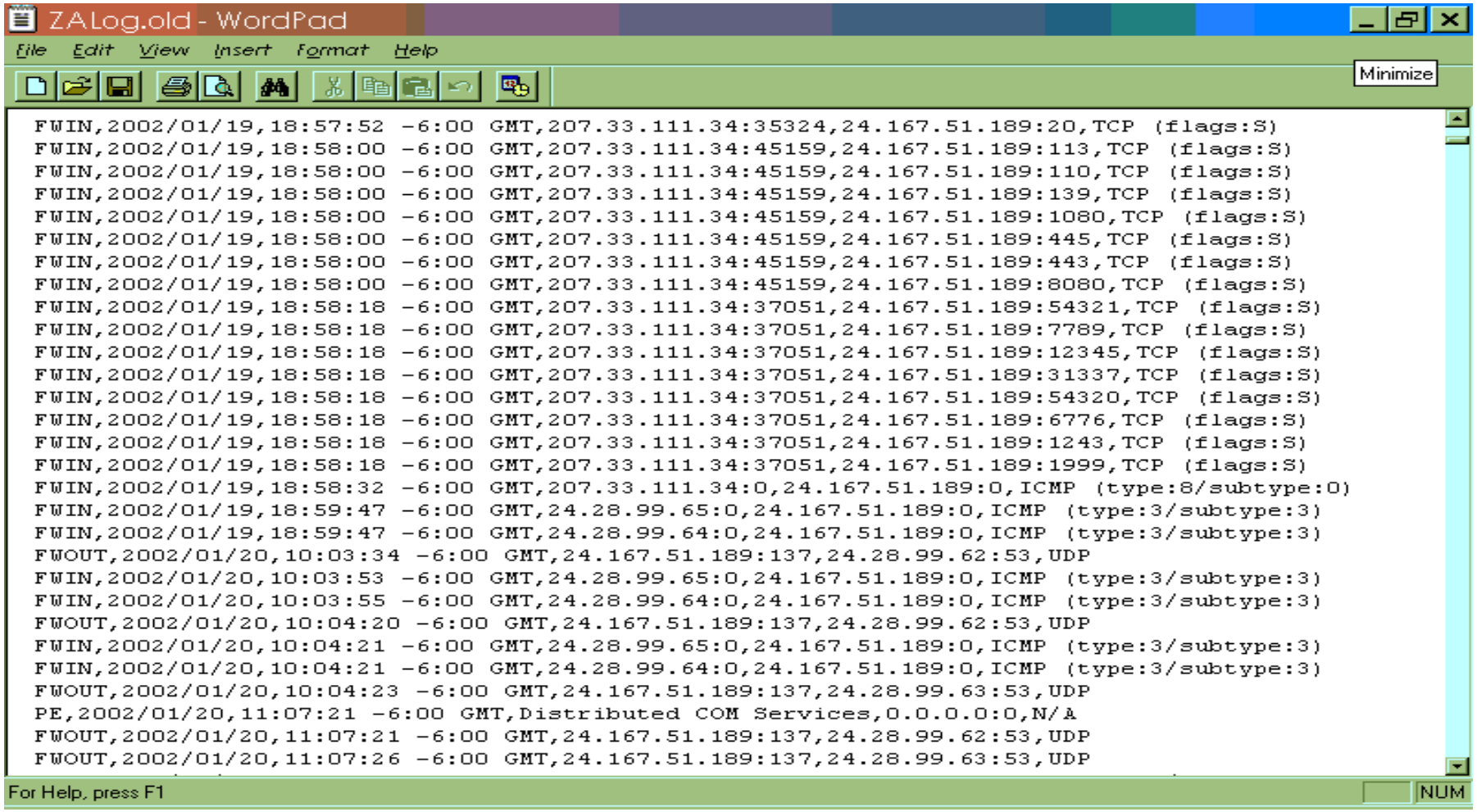
Protocol Analysis *Sniffer*



Network Forensics

- Most networks have the capability to track user activity
  - Capabilities may or may not be configured
  - May or may not be corrupted by an intruder
- Frequently involve multiple machines
- Includes discovery of IP addresses, host names, network routes and Web site information.

Sample Log File



Internet Forensics

- Remote machines on the Internet also have the capability of tracking events.
- Case Study University of Tulsa Camera Equipment Theft
  - Several thousand dollars worth of camera equipment shipped to a shack.
  - After delivery and prior to LE being notified, the shack was knocked down.
- Utilizing Internet Forensics, culprits were identified and caught.

Computer or Communications Evidence?

- May have an international scope.
  - Issues
    - Jurisdictions
    - Time and labor
- Different laws apply to unread email than to information stored on a hard drive
- Rome Labs Case Study

Digital Evidence

- Digital evidence must be authentic and must be able to be proven that it has not been modified

- Evidence Life Cycle
  - Discovery and recognition
  - Protection
  - Recording
  - Collection
  - Identification
  - Preservation
  - Transportation
  - Presentation in court
  - Return to owner

Evidence Characteristics

- Sufficient, reliable, and relevant
  - Sufficient means it must be persuasive enough to convince a reasonable person of the validity of the findings.
  - Reliable, or competent, means it must be consistent with fact.
  - Relevant means it must have a reasonable and sensible relationship to the findings.

Rules of Evidence

- Distinguish between hearsay and direct evidence
- Require proof of authenticity and integrity
  - Chain of custody requires that:
    - No information has been added or changed
    - A complete copy was made
    - A reliable copying process was used
    - All media was secured.
- Message Digest demonstrates integrity
- Digital Signature demonstrates authentication and non repudiation

Evidence Handling

- If evidence is handled improperly, investigation may be comprised.
- A documented chain of custody must include:
  - Who collected the evidence?
  - How and where?
  - Who took possession?
  - How was it stored and protected?
  - Who took it out of storage?

Common Enterprise Problems

- No established incident response team.
  - Evidence compromised while gathered
- No established incident response policies
  - Evidence may be compromised prior to gathering
- Inappropriate methodology
  - Peer review
- Broken chain of custody
  - Appropriate evidence was gathered but can not be presented in court

Who Gathers Forensic Evidence?

- Incident Response Team, or other trained professionals, respond to an incident.
- Specific actions should be based on the specific incident and the organization's Incident Response Policy.
- An incident response team ensures that:
  - There is a group of properly skilled professionals.
  - There is a standard set of procedures
  - Resources and processes are available when an incident occurs.
- Incident Response Team gathers evidence.

Types of Evidence

- Best evidence -- Original or primary evidence
- Secondary evidence -- A copy or oral description
- Conclusive evidence -- Incontrovertible: overrides all other evidence
- Hearsay Evidence -- (3rd party) not generally admissible

Hearsay Rule

Key for Computer Generated Evidence

- Second Hand Evidence
- Admissibility Based on Veracity and Competence of Source

- Exceptions: Rule 803 of Federal Rules of Evidence allows Business Documents created at the time by person with knowledge, part of regular business, routinely kept, supported by testimony.

Hearsay Exceptions

- Computer generated records and other business records can fall into this category
- Exceptions if records:
  - Are made during the regular conduct of business and authenticated by witnesses familiar with them
  - Relied upon in the regular course of business
  - Made by a person with knowledge of the records
  - In the custody of the witness on a regular basis

System Logs as Evidence

- According to the US Federal Rules of Evidence:

  Log files that are created routinely an contain information about acts and events made at specific times by, or from information transmitted by, a person with knowledge

- Are not excluded by the hearsay rule.

Daubert Rules

To assist the lower courts in applying Daubert, the Court provided the following list of factors that courts should consider before ruling on the admissibility of scientific evidence:

1. Whether the theory or technique has been reliably tested;
2. Whether the theory or technique has been subject to peer review and publication;
3. What is the known or potential rate of error of the method used; and
4. Whether the theory or method has been generally accepted by the scientific community.

Surveillance, Search, and Seizure

- Computer surveillance pertains to events, which passively or actively monitors events by using network sniffers, keyboard monitors, wiretaps, and line monitors
- Active monitoring may require a search warrant.
- To legally monitor an individual, the person had to have been warned ahead of time that her activities may be subject to this type of monitoring.
  - Organizational policy

Guidelines for Searching and Seizing Computers

- US Federal Guidelines for Searching and Seizing Computers (DOJ 1994)

  http://www.usdoj.gov/criminal/cybercrime/searching.html

For Further Study

- Eoghan Casey; Digital Evidence and Computer Crime; Academic Press; March 15, 2000; ISBN: 012162885X
- Kruse and Heiser Computer Forensics: Incident Response Essentials; Addison-Wesley Pub Co; September 26, 2001; ISBN: 0201707195
- http://www.cybercrime.gov
- http://www.first.org/
- http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm

For Further Study

- http://www.opensourceforensics.org/
- http://en.wikipedia.org/wiki/Comparison_of_hex_editors
- http://www.htcia.org/links.shtml
- http://www.isaca.org/Content/ContentGroups/Member_Content/Journal1/20023/Computer_Forensics_Emerges_as_an_Integral_Component_of_an_Enterprise_Information_Assurance_Program.htm
- http://www.e-fense.com/helix/

Questions?