Introduction to Computer Forensics

Computer forensics is the use of analytical and investigative techniques to identify, collect, examine, and preserve computer-based material for presentation as evidence in a court of law. This presentation will explore the fundamental concepts, legal requirements, and technical knowledge needed for effective digital forensic investigations.

Agenda

Fundamentals

- What is computer forensics?
- Goals of digital forensics
- Scientific approach

Technical Knowledge

- Hardware fundamentals
- Software & operating systems
- Networks & connectivity

Legal Framework

- The Daubert standard
- Relevant US laws
- Federal guidelines

By the end of this presentation, you will understand the basic concepts of forensics, how to maintain the chain of custody, the technical knowledge required, and the legal framework governing computer forensics.

What is Digital Forensics?

YouTube

Understanding Digital forensics In Under 5 Minutes | EC-Council

Thanks to advanced technologies, hackers have become adept at infiltrating networks. However, even cybercriminals leave traces behind. Digital forensics...

What is Computer Forensics?

Forensics

The use of analytical and investigative techniques to identify, collect, examine, and preserve evidence for presentation in a court of law.

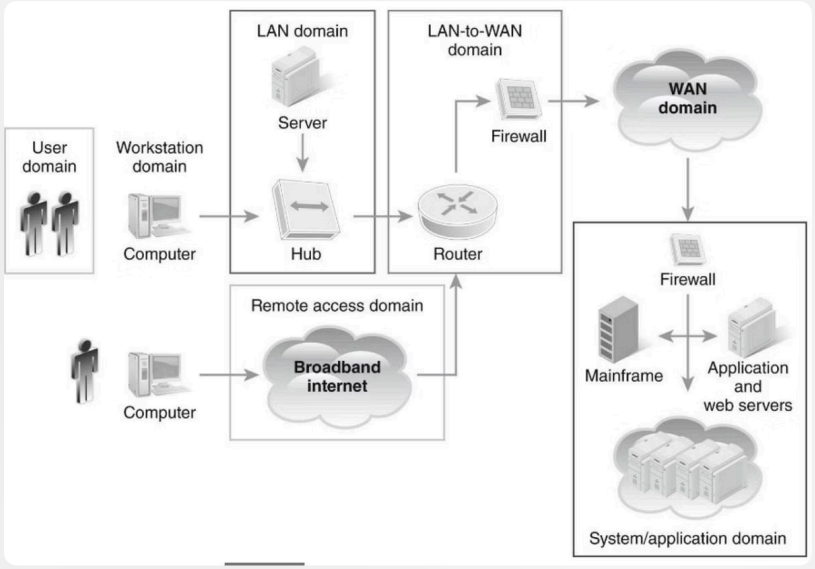
Computer Forensics

The application of these techniques specifically to computer-based material.

Digital Forensics

An expansion of computer forensics to include smartphones, smart watches, and other digital media and devices.

The field has evolved from focusing solely on computers to encompassing all forms of digital evidence, requiring specialized tools and techniques.



Goal of Digital Forensics

The primary goal is to recover, analyze, and present computer-based material in such a way that it can be used as evidence in a court of law.

Integrity and Security

The emphasis must be on maintaining the integrity and security of evidence throughout the investigation process.

Stringent Guidelines

A forensic specialist must adhere to stringent guidelines and avoid taking shortcuts that could compromise evidence.

Comprehensive Coverage

Digital forensics covers the seven domains of a typical IT infrastructure.

The Scientific Approach to Digital Forensics

Collecting

Evidence must be collected using specific procedures to ensure admissibility in court. The method of collection directly impacts whether evidence will be accepted.

Analyzing

The most challenging and time-consuming part, requiring strong scientific knowledge to interpret data effectively. Investigators must meticulously examine evidence like solving a complex puzzle.

Presenting

Translating complex technical information into clear, plain English for the court. Effective communication, possibly aided by visuals, is crucial for a successful outcome.

Computer forensics requires a thorough understanding of scientific methods, processes, and relevant disciplines, particularly computer hardware, operating systems, and basic computer networks.

Expert Reports and Testimony

The Expert Report

- A formal document documenting the investigation
- Must include all tests conducted and the specialist's CV
- Must be thorough and include all pertinent information
- Written in plain English, avoiding jargon
- Must be error-free and meticulously proofread

Expert Testimony

- Based on scientific knowledge, not personal opinion
- Must always tell the truth (perjury is a felony)
- Goal is to present scientifically valid evidence
- Governed by U.S. Federal Rule of Evidence 702
- Expert can only testify about what's in their report

Court procedures dictate that expert witnesses can only testify on matters included in their expert report, making thoroughness essential.

Understanding the Field of Digital Forensics

Digital forensics has evolved from informal investigator-led methods to standardized methodologies, now encompassing all forms of digital evidence.

Military & Government

Used for intelligence gathering and criminal investigations by FBI, FTC, FDA, Secret Service, DOJ, NIST, OLES, DHS, and foreign governments.

Legal & Corporate

Used by law firms for investigations and expert testimony, by prosecutors for criminal cases, and by corporations for employee termination, IP theft, fraud, and network intrusions.

Academia & Services

Used in academic research, by data recovery firms, insurance companies for claims, and by individuals for personal claims like wrongful termination.

The field continues to expand as digital technology becomes increasingly integrated into all aspects of life.

Types of Digital Evidence

1

Real Evidence

Physical objects that can be touched and observed, such as a laptop with fingerprints.

2

Documentary Evidence

Stored information on various media (e.g., emails, logs, databases). Investigators must authenticate its genuineness.

3

Testimonial Evidence

Information from forensic specialists to support or interpret other evidence (e.g., expert testimony).

4

Demonstrative Evidence

Information that explains other evidence, often presented visually (e.g., charts, graphics). Helps explain complex technical information to the court.

Digital evidence admissibility in court hinges on proving an unbroken **chain of custody**, demonstrating that the evidence's integrity has been preserved and unaltered since collection.

Challenges in Digital Forensics

Large Volumes of Data

Digital forensics involves examining all digital media, including hidden data and metadata. The massive and growing volume of data requires significant resources and strict chain of custody.

System Complexity

Modern systems are complex with diverse data. Specialists need various tools and deep understanding of technology, legal evidence rules, chain of custody, and the Daubert standard.

Distributed Crime Scenes

Digital crime scenes are increasingly global, with evidence scattered across devices, languages, and jurisdictions. Successful investigation requires extensive international cooperation.

Growing Caseload

Demand for digital forensic specialists far outstrips their numbers, leading to growing backlogs as criminals increasingly use technology in diverse ways.

Types of Digital Forensics Analysis

01

Disk Forensics

Analyzing storage media, including recovery of deleted data.

02

Email Forensics

Tracing email origins and content for investigations.

03

Network Forensics

Monitoring and analyzing network traffic.

04

Internet Forensics

Reconstructing online activity.

01

Software Forensics

Analyzing malicious code (malware).

02

Live System Forensics

Examining real-time memory for system abuse.

03

Cell-phone Forensics

Analyzing mobile device content, often involving specific laws like FISA and the PATRIOT Act.

Each type requires specialized knowledge, tools, and techniques to effectively extract and analyze evidence.

General Guidelines for Digital Forensics

Chain of Custody

The most vital principle, requiring a continuous, documented record of evidence control from seizure to court presentation. Failure to maintain proper chain of custody can lead to evidence exclusion.

Don't Touch the Suspect Drive

Minimize interaction with the original suspect system to prevent changes. Create a forensic copy using specialized tools and work with that copy instead.

Document Trail

Comprehensive documentation is essential, including who was present during seizure, what was connected, screen content, specific tools used, and who accessed the evidence.

Secure the Evidence

Forensic labs typically have locked rooms with restricted access, and evidence is secured in a safe. Every reasonable precaution must be taken to prevent tampering.

Hardware Knowledge for Forensics

Memory Types

Understanding volatile memory (RAM) vs. non-volatile memory (ROM, PROM, EPROM, EEPROM) is crucial for determining what data persists after power loss.

Storage Devices

Knowledge of HDDs vs. SSDs, including interfaces (SCSI, IDE/EIDE/PATA, SATA) and how data is organized (sectors, clusters, tracks) is essential for forensic analysis.

System Components

Digital forensic examiners need a deep understanding of device hardware (CompTIA A+ level for PCs) to comprehend component function and data storage.

Software & File Systems Knowledge

Operating Systems

- **Windows:** Registry is crucial for forensic analysis
- **Linux:** Valuable for forensics due to open-source nature
- **Mac OS:** Based on FreeBSD, a UNIX clone

File Headers

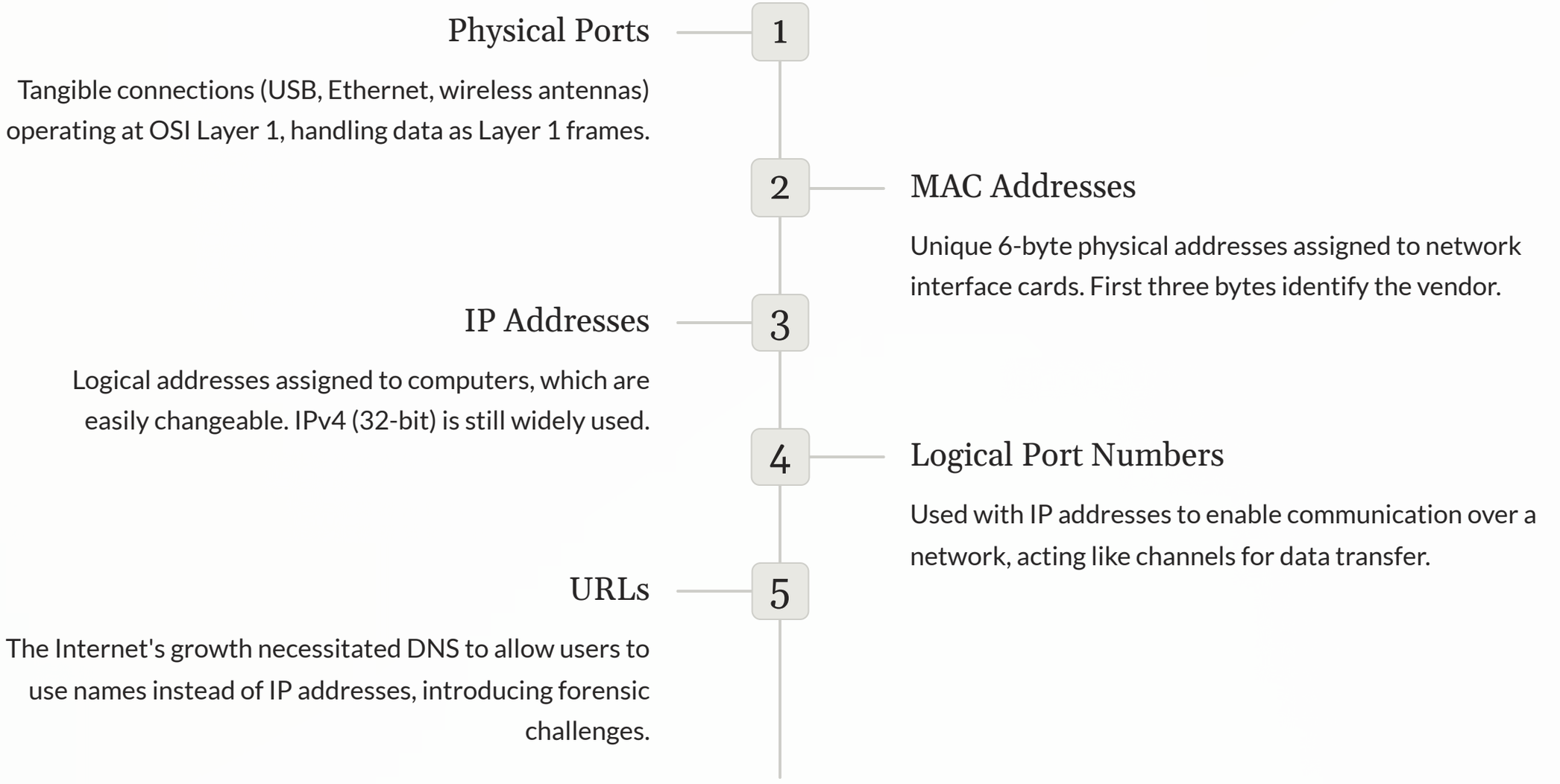
Understanding file headers is crucial as they provide accurate information about the file regardless of its extension.

File Systems

- **FAT:** Older Microsoft system with various versions
- **NTFS:** Modern Windows file system with larger volume support
- **ReFS:** Newer, more resilient Microsoft file system
- **APFS:** Default for Apple computers since macOS 10.13
- **EXT:** Linux's primary file system (currently EXT4)
- **ReiserFS:** Journaling file system for Linux

Journaling file systems maintain a log of all file transactions, enabling recovery after crashes.

Network Knowledge for Forensics



Digital forensics divides data into "at rest" (stored) and "in motion" (transmitted). Investigators need strong knowledge of network components and protocols to analyze both.

Basic Network Utilities for Forensics

Ipconfig

Provides network and internet connection information, including your own IP address and the default gateway IP.

Ping

Sends an echo packet to test if a machine is reachable and measure round-trip time. Output includes "time to live" (TTL).

Tracert

Shows the path and hops packets take to a destination, useful for basic troubleshooting but not reliable for forensics.

These basic utilities can be executed from a command prompt (Windows) or shell (UNIX/Linux) and provide valuable information for initial investigation.

Challenges: Obscured Information & Anti-Forensics

Obscured Information

- Data hidden or made unreadable through encryption, steganography, compression, or proprietary formats
- Used by cybercriminals to evade forensic examination
- Also used by companies to protect sensitive information
- Decrypting such data is challenging; may need to extract evidence live

Anti-Forensics

- **Data destruction:** Wiping memory buffers, overwriting data
- **Data hiding:** Storing in obscure locations, altering filenames
- **Data transformation:** Disguising information
- **File system alteration:** Corrupting file system structures

Cybercriminals are increasingly aware of digital forensics capabilities and actively use techniques to hinder investigations, often by using public networks or destroying service information.

The Daubert Standard

The Daubert standard is a legal rule guiding judges on whether expert scientific testimony is admissible in court. It requires assessing if the testimony's reasoning and methodology are scientifically valid.

Key Factors

- Testability of the theory or technique
- Peer review and publication
- Known or potential error rates
- Existence of standards controlling the technique
- General acceptance in the relevant scientific community

Implications for Forensics

- Use widely accepted methods and tools
- Meticulously document everything
- Maintain strict chain of custody
- Failure to meet Daubert can lead to evidence being inadmissible

US Laws Affecting Digital Forensics

Digital forensics is governed by laws, often requiring evidence extraction by law enforcement or licensed private investigators, unless permitted by the information owner.

Privacy Laws

- Federal Privacy Act of 1974
- Privacy Protection Act of 1980
- Electronic Communications Privacy Act of 1986
- Children's Online Privacy Protection Act of 1998

Security Laws

- Computer Security Act of 1987
- USA PATRIOT Act
- 18 USC 1030 (Computer Fraud)
- Digital Millennium Copyright Act

Surveillance Laws

- Foreign Intelligence Surveillance Act of 1978
- Communications Assistance to Law Enforcement Act of 1994
- Unlawful Access to Stored Communications
- Wireless Communications and Public Safety Act of 1999

Investigators must know their jurisdiction's legal requirements to ensure evidence admissibility.

Warrants and Fourth Amendment

Fourth Amendment Protections

Protects against unreasonable searches and seizures, particularly regarding privacy and the necessity of warrants.

Reasonable Expectation of Privacy

Law enforcement actions that violate a person's "reasonable expectation of privacy" without a warrant generally constitute a Fourth Amendment search.

Consent Issues

Complex in computer crime cases. Key questions include scope of consent and who is the proper party to consent.

Warrantless Searches

Exceptions exist, such as border crossings and imminent danger of evidence destruction.

Scope of Warrant

Crucial not to exceed the scope of a warrant. *United States v. Schlingloff* highlights that illegal images found within the scope of a legitimate search are admissible.

Federal Guidelines for Digital Forensics

FBI Guidelines

- Preserve a system's state during an incident
- Back up all data, including logs and altered files
- Activate auditing software
- Secure diverse evidence types
- Always work with copies, not originals

Secret Service "Golden Rules"

- Ensure scene safety
- Preserve computer evidence immediately
- Confirm legal basis for seizing a computer
- Avoid accessing computer files
- If evidence destruction is suspected, immediately shut down
- Photograph computer screens and location

Regional Computer Forensics Laboratory (RCFL)

- National network of forensic labs and training centers
- Funded and supported by the FBI
- Examines digital evidence for criminal and national security investigations
- Provides expertise to all levels of law enforcement
- Conducts extensive digital forensics training

When setting up a forensic lab or entering the field, consult these federal guidelines as they are particularly important for ensuring proper procedures.