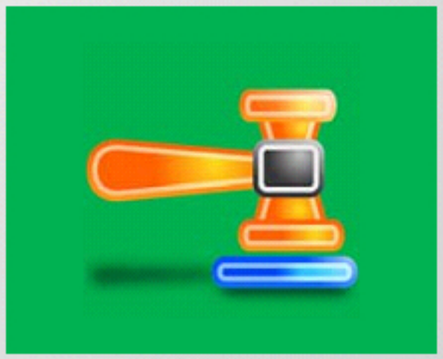
Computer Forensics in Today's World

Module 01

Designed by Cyber Crime Investigators. Presented by Professionals.



Module Objectives

C|HFI Computer Hacking Forensic Investigator

After successfully completing this module, you will be able to:

1. Define computer forensics and understand its objectives
2. Understand and classify different types of cybercrimes
3. Understand different challenges cybercrimes present to investigators
4. Understand different types of cybercrime investigations and general rules of forensics
5. Understand Rules of Evidence and recognize different types of digital evidence
6. Examine the role of computer forensics and forensics readiness in incident response plans
7. Understand need for forensic investigators and identify their roles and responsibilities
8. Review legal, privacy and code of ethics issues in computer forensics

Understanding Computer Forensics

Computer forensics refer to a **set of methodological procedures and techniques** that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal and/or administrative proceeding

Objectives:

- To track and prosecute perpetrators of a cyber crime
- To gather evidence of cyber crimes in a forensically sound manner
- To estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator
- To minimize the tangible and intangible losses to the organization
- To protect the organization from similar incidents in future

Types of Cybercrimes

- Cyber crime is defined as **any illegal act** involving a computing device, network, its systems, or its applications.
- Cyber crime can be categorized into two types based on the line of attack.

Internal Attacks

Breach of Trust by disgruntled or unsatisfied employees within the organization

Examples:

- Espionage
- Theft of Intellectual Property
- Manipulation of the records
- Trojans horse attack

External Attacks

Attackers hired either by **internal or external entities** to destroy the organization's reputation

Examples:

- SQL attack
- Brute force
- Identity theft
- Phishing/Spoofing
- Denial of Service Attack
- Cyber Defamation

Case Study 1: Insider Attack - Industrial Espionage & Loss of Trade Secrets

The Case: The Chief Information Security Officer (CISO) of a research company was made aware of unusual activity by one of the company's employees. A researcher was observed running a piece of software which they later determined to be a known hacker tool from his laptop computer. All the employee saw was a black screen with lines of white text scrolling in a rapid fashion. As all the computers used Windows operating systems and were locked down, a black screen with scrolling white text appeared peculiar to the reporter. He decided to report it. The CISO of the corporation contacted the forensic team to investigate.

The Investigation: The forensic team performed covert forensic imaging and examination of the suspect's laptop and desktop computers. The examination revealed several interesting facts. The suspect cracked the "local" admin password on both of his computers and installed a key logger on each one so as to know if someone became suspicious and accessed his computer while he was away. He intended to catch anyone trying to put any type of monitoring software on either one of his computers. For this purpose, he deployed a potent detection mechanism to alert him if he was under investigation. In his laptop, the suspect installed various hacker tools (network sniffers, password crackers, network vulnerability scanners, etc.) in addition to data scrubber software. Initially, the laptop revealed no evidence of wrongdoing due to the presence of a data scrubber, which he used periodically to clean his hard drive. Later, when the forensic team collected the network traffic and analyzed the logs, the truth was finally revealed: he had successfully compromised the entire network and cracked all other researcher's passwords. He would periodically log in to the server, access other researcher's data, and download it to his laptop to take it home. He would then remove the data from his laptop and run a scrubber software to eliminate any evidence that other scientists' data were ever present on his hard drive.

The Result: The target company maintained it to be confidential

Source: http://www.cyberdiligence.com

Case Study 2: External Attack - ABC Bank's Case

C|HFI Computer Hacking Forensic Investigator

The Case:

ABC Bank (ABC) identified unauthorized wire transfers from their environment. They needed to know when and how it happened quickly, in order to mitigate future attacks and notify affected customers. ABC engaged the Solutionary Security Engineering Research Team (SERT) to provide on-demand critical incident response services.

The Investigation:

SERT identified and provided a list of compromise indicators to ABC and assisted with investigations of their network infrastructure to identify additional unauthorized remote administration or other attacker tools. Since the attacker used the cloud to mask the attack, SERT wrote special tools to analyze the multi-host command and control the attacker used. Using the reverse engineering malware identified during the attack, SERT experts pieced together the precise methods used by the attacker to obtain an initial foothold into the ABC protected network. Analysis revealed not only findings from the current incident but also aspects of security and process recommendations ABC should consider to prevent and detect future attacks. In this case, SERT also found a SQL injection attack within a cloud application used by ABC Bank that allowed controls to be bypassed.

The Result:

ABC could quickly notify only those customers affected by the attacks, avoiding the need for a broader public disclosure of the incident. Doing so reduced the overall cost of the incident and helped to preserve ABC's reputation with the unaffected customers. It also helped to prevent additional fraudulent wire transfers.

Source: https://www.solutionary.com

Challenges Cyber Crimes Present to Investigators

Cyber crimes **pose new challenges** for investigators due to their:

- **Speed**: Advancement in technology has boosted the speed with which cyber crimes are committed, whereas investigators require authorization and warrants before starting legal procedure.
- **Anonymity**: Cyber criminals can easily hide their identity by masquerading as some other entity or by hiding their IP addresses using proxies
- **Volatile nature of evidence**: Most of the digital evidence can be easily lost as it is in the form of volatile data such as logs, records, light pulses, radio signals or other means.
- **Evidence Size and Complexity**: Diversity and distributed nature of digital devices results in increased size of evidence data and complexity.
- **Anti-Digital Forensics (ADF)**: Attackers are increasingly using encryption and data hiding techniques to hide digital evidence.
- **Global origin and difference in laws**: The perpetrators can initiate the crime from any part of the world, whereas the authorities have jurisdiction over domestic crimes only.
- **Limited legal understanding**: Many victims are unaware of the law violated during the incident and fail to defend their claim.

Cyber Crime Investigation

1. The investigation of any crime involves the **painstaking collection of clues and forensic evidence** with an attention to detail.

2. It is inevitable that there will be at least one **electronic device found during the investigation**, be it a computer, cell phone, printer, or fax machine.

3. The electronic device found may be central to the investigation as it could **contain valuable evidence** for solving the case.

4. Therefore, the information contained in the device must be investigated in the **proper manner** in order to be relied upon in a court of law.

Types of cyber crime investigation cases:

- Civil
- Criminal
- Administrative

5. **Processes** such as collection of data, analysis, and presentation **differ based on the type of case**.

Civil Vs. Criminal Investigation

Civil cases are brought for violation of contracts and lawsuits where a guilty outcome generally results in monetary damages to the plaintiff, whereas criminal cases are generally brought by **law enforcement agencies** in response to a suspected violation of law where a guilty outcome may result in monetary damages, imprisonment, or both.

Criminal Cases

- Investigators must follow a set of **standard forensic processes** accepted by law in the respective jurisdiction.
- Investigators, under court's warrant, have the authority to force seize the computing devices.
- A formal investigation report is required.
- The law enforcement agencies are responsible for collecting and analyzing evidence.
- Punishments are harsh and include fine, jail sentence or both.
- Standard of proof needs to be very high.
- Difficult to capture certain evidence, e.g., GPS device evidences.

Civil Cases

- Investigators try to show some information to the opposite party to support the claims and induce them for settlement.
- Searching of the devices is generally based on mutual understanding and provides a wider time window to the opposite party to **hide the evidence**.
- The **initial reporting** of the evidence is generally informal.
- The claimant is responsible for the collection and analysis of the evidence.
- Punishments include monetary compensation.
- Poorly documented or unknown chain-of-custody for evidence.
- Sometimes, evidence can be within the third party control.

Case Study

Case Study: Criminal Case

ALLEGED RAPE

The Case: An attorney representing a local college student who had been accused of rape needed forensic expertise to prove his client`s innocence. It was told that the accused met another student at a party and had sex with her after the event in the accuser's car. The accused also stated that they continued to see each other after the alleged rape for several days, attending the same events and exchanging emails and text messages. The accused stated that after he informed the accuser what had happened a few nights earlier was not the beginning of a relationship but was rather just a one night stand, she did not react well and was extremely angry. A few weeks later she reported to the university police that she was forcibly raped by the accused. He was subsequently arrested and charged with rape.

The Investigation: If the accused was telling the truth, the key evidence would be found in his mobile phone and email. The accused stated that he had deleted emails and text messages and they were no longer available. Forensic team instructed the counsel to immediately send a "preserve records" letter to the email service provider. The letter had the necessary information on how to write and serve the letter, as well as helping him with drafting the court order to be signed by the presiding judge. Meanwhile, the team started investigating mobile phone of the accused. It was an iPhone, the team made a physical forensic image of it, and the analysis of the image revealed numerous deleted text messages that clearly showed the incident was totally consensual. About 100 deleted text messages exchanged after the alleged rape were recovered. In these messages, the accuser had referred to the event as “a magical experience,” “one of the greatest nights of her life,” etc. This proved to be smoking gun evidence of his innocence

The Result: When report was presented to the prosecutor, all charges against the accused were dropped.

Source: http://www.cyberdiligence.com

Case Study: Civil Case

THEFT OF INTELLECTUAL PROPERTY: FORTUNE 100 COMPANY CLEARED OF WRONGDOING

The Case: The chief legal counsel of a Fortune 100 Company approached forensic team, stating that a recently hired high-level executive was accused of misappropriating his previous employer's intellectual property. A lawsuit was filed in another state by his previous employer seeking an injunction on all activities of the firm involving the division led by the executive. The client stated that the court documents showed that, before his departure, the executive had copied the plaintiff's trade secrets to an external drive and had emailed about a hundred critical documents to his personal Yahoo email account.

The Investigation: Forensic team seized all home and business computers, email accounts, and external storage devices of the newly hired executive. The plan was to take custody of all misappropriated trade secrets and return them to the plaintiff. Client's attorneys briefed the judge on the actions taken by the forensics team. They informed the judge that, immediately after being made aware of the situation, they retained Cyber Diligence, Inc., which specializes in theft of intellectual property investigations, and followed recommendations on their response plan.

The Result: The judge denied the application of injunction stating that as a result of the quick and decisive action of the defendant (our client), the plaintiff did not suffer any actual damage and proceeded to instruct Cyber Diligence to isolate the executive's personal data from the data that clearly belonged to the plaintiff. The case was closed with a minimal impact on our client's operations.

Source: http://www.cyberdiligence.com

Administrative Investigation

- Administrative investigation generally involves an agency or government performing inquiries to **identify facts** with reference to its own management and performance.
- Administrative investigations are **non-criminal in nature** and are related to misconduct or activities of an employee that includes but are not limed to:
  - Violation of organization's policies, rules, or protocols
  - Resources misuse or damage or theft
  - Threatening or violent behavior
  - Improper promotion or pay rises
- Any **violation** may **result** in **disciplinary action** such as demotion, suspension, revocation, penalties, and dismissal.
- For situations like promotions, increments, transfers, etc., administrative investigations can result in positive outcomes, like modifications to existing policies, rules, or protocols.

Case Study

Case Study: Administrative Case

Banking, Corporate Fraud SOX Auditing

The Case: A medium size, publicly traded bank had gone through a series of transitions, culminating in a new Board of Directors and, because of new regulations in the financial industry, an independent Auditing Committee in accordance with the new regulations in the financial industry. The Auditing Committee charged certain officers of the Bank with engaging in suspect activities related to particular Bank expenses that were either hidden or "lost" from the purview of the normal Bank's accounting practices. A large accounting firm was hired to audit certain activities by officers of the bank. During the investigation, the auditors needed to examine several computer systems used by certain Bank employees.

The Investigation: The accounting firm retained GDF's digital forensic examiners to perform examinations of the Bank's digital assets. GDF focused its initial examination on particular desktop and network systems used by the suspect employees. Its examiners performed digital forensic analyses on those systems while simultaneously examining data supplied directly from the Bank's IT department regarding internal network and Internet-related activity of those suspect employees.

The Result: Using the digital artifacts collected by GDF in a forensically sound manner from the investigated systems, the Bank's Auditing Committee was in a better position to find that certain Bank employees had violated Bank policy and possibly certain federal regulations regarding actions by officers of public corporations. In the end, the Bank saved an enormous amount of money and time by using the digital evidence in finalizing the issues related to the investigation and was able to make important deadlines with regards to certain SEC filings.

Source: http://evestigate.com

Rules of Forensics Investigation

- Limited access and examination of the **original evidence**
- Record **changes** made to the evidence files
- Create a **chain of custody** document
- Set **standards** for investigating the evidence
- Comply with the **standards**
- Hire **professionals** for analysis of evidence
- Evidence should be strictly **related** to the incident
- The evidence should comply with the **jurisdiction standards**
- Document the **procedures** applied on the evidence
- Securely **store** the evidence
- Use recognized **tools** for analysis

Enterprise Theory of Investigation (ETI)

The Enterprise Theory of Investigation (ETI) has become the **standard investigative model** used by the FBI when conducting investigations against major criminal organizations

Rather than viewing criminal acts as isolated crimes, the ETI attempts to show that **individuals commit crimes in furtherance of the criminal enterprise itself**; in other words, individuals commit criminal acts solely to benefit their criminal enterprise

By applying the ETI with favorable state and federal legislation, **law enforcement can target and dismantle entire criminal enterprises** in one criminal indictment

Understanding Digital Evidence

Digital evidence is defined as “any information of **probative value** that is either stored or transmitted in a digital form”

Digital information can be gathered while examining digital **storage** media, **monitoring** the network traffic, or making duplicate copies of digital data found during forensics investigation

Digital evidence is **circumstantial** and **fragile** in nature, which makes it difficult for a forensic investigator to trace criminal activities

According to **Locard's Exchange Principle**, “anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave”

Types of Digital Evidence

Volatile Data

Data that is **lost as soon as the device is powered off**. Examples include system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, command history, etc.

Persistent data that is **stored on secondary storage** devices such as hard disks and memory cards. Examples include hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, event logs, etc.

Non-volatile Data

Characteristics of Digital Evidence

Digital evidence must have some characteristics to be **disclosed in the court of law**

Admissible

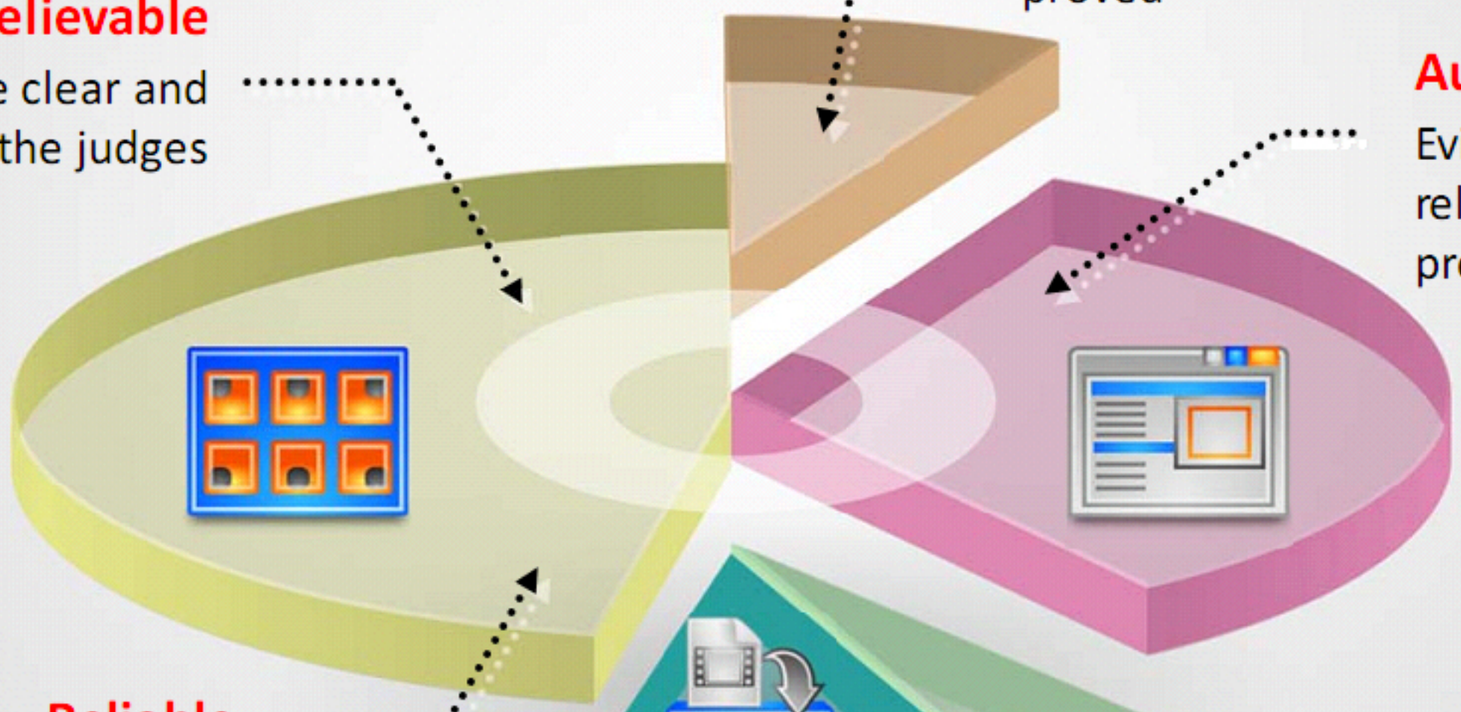
Evidence must be related to the fact being proved

Believable

Evidence must be clear and understandable by the judges

Authentic

Evidence must be real and related to the incident in a proper way



Reliable

There must be no doubt about the authenticity or veracity of the evidence

Complete

The evidence must prove the attacker's actions or his innocence

Roles of Digital Evidence

Examples of cases where **digital evidence** may assist the forensic investigator in prosecution or defense of a suspect:

- Identity theft
- Malicious attacks on the computer systems themselves
- Information leakage
- Unauthorized transmission of information
- Theft of commercial secrets
- Use/abuse of the Internet
- Production of false documents and accounts
- Unauthorized encryption/ password protection of documents
- Abuse of systems
- Email communication between suspects/conspirators

Sources of Potential Evidence

C|HFI Computer Hacking Forensic Investigator

User-Created Files

- Address books
- Database files
- Media (images, graphics, audio, video, etc.) files
- Documents (text, spreadsheet, presentation, etc.) files
- Internet bookmarks, favorites, etc.

User-Protected Files

- Compressed files
- Misnamed files
- Encrypted files
- Password-protected files
- Hidden files
- steganography

Computer-Created Files

- Backup files
- Log files
- Configuration files
- Printer spool files
- Cookies
- Swap files
- System files
- History files, and
- Temporary files

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Hard Drive	Text, picture, video, multimedia, database, and computer program files
Thumb Drive	Text, graphics, image, and picture files
Memory Card	Event logs, chat logs, text file, image file, picture file, and the Internet browsing history
Smart Card	Evidence is found in recognizing or authenticating the information of the card and the user, level of access, configurations, permissions, and in the device itself
Dongle	
Biometric Scanner	
Answering Machine	Voice recordings such as deleted messages, last number called, memo, phone numbers, and tapes
Digital Camera	Images, removable cartridges, video, sound, time and date stamp, etc.

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Handheld Devices	Address book, appointment calendars or information, documents, email, handwriting, password, phone book, text messages, and voice messages
Modem	Device itself
Local Area Network (LAN) Card/ Network Interface Card (NIC)	MAC (Media Access Control) address
Routers, Hubs, and Switches	For routers, evidence is found in the configuration files For hubs and switches, evidence is found on the devices themselves
Network Cables and Connectors	Devices themselves
Server	Computer system
Pager	It contains volatile evidence such as address information, text messages, e-mail, voice messages, and phone numbers
Printer	Evidence is found through usage logs, time and date information, and network identity information, ink cartridges, and time and date stamp

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Removable Storage Device and Media	Storage device and media such as tape, CD, DVD, and Blu-ray have the evidence in the devices themselves
Scanner	Evidence is found by looking at the marks on the glass of the scanner
Telephones	Evidence is found through names, phone numbers, caller identification information, appointment information, electronic mail and pages, etc.
Copiers	Documents, user usage logs, time and date stamps, etc.
Credit Card Skimmers	Evidence is found through card expiration date, user's address, credit card numbers, user's name, etc.
Digital Watches	Evidence is found through address book, notes, appointment calendars, phone numbers, email, etc.
Facsimile (Fax) Machines	Evidence is found through documents, phone numbers, film cartridge, send or receive logs
Global Positioning Systems (GPS)	Evidence is found through previous destinations, way points, routes, travel logs, etc.

Rules of Evidence

- Evidence that is to be presented in the court **must comply** with the established rules of evidence
- Prior to the investigation process, it is important that the **investigator understands** the rules of evidence

Definition:

- Rules of evidence govern whether, when, how, and for what purpose the proof of a case may be placed before a trier of fact for consideration
- The trier of fact may be a judge or a jury, depending on the purpose of the trial and the choices of the parties

Best Evidence Rule

- Best evidence rule is established to **prevent any alteration of digital evidence** either intentionally or unintentionally

- It states that the court only allows the **original evidence of a document, photograph, or recording** at the trial rather than a copy, but the duplicate will be allowed as an evidence under the following conditions:
  - **Original evidence destroyed due to fire/flood**
  - **Original evidence destroyed in the normal course of business**
  - **Original evidence in possession of a third party**

Federal Rules of Evidence

These rules shall be construed to **secure fairness in administration, elimination of unjustifiable expense and delay**, and promotion of growth and development of the law of evidence to the end that the truth may be ascertained and proceedings justly determined

Rulings on Evidence

(a) Effect of erroneous ruling

- Error may not be predicated upon a ruling which excludes evidence unless a substantial right of the party is affected
- **Objection** - In case the ruling is one admitting evidence, a timely objection or motion to strike appears of record, stating the specific ground of objection, if the specific ground was not apparent from the context
- **Offer of proof** - In case the ruling is one excluding evidence, the substance of the evidence was made known to the court by offer or was apparent from the context within which questions were asked

(b) Record of offer and ruling

The court may add any other or further statement which shows the character of the evidence, the form in which it was offered, the objection made, and the ruling there on. It may direct the making of an offer in question and answer form

(c) Hearing of jury

Proceedings shall be conducted, to the extent practicable, so as to prevent inadmissible evidence from being suggested to the jury by any means, such as making statements or offers of proof or asking questions in the hearing of the jury

(d) Plain error

Nothing in this rule precludes taking notice of plain errors affecting substantial rights although they were not brought to the attention of the court

Federal Rules of Evidence (Cont'd)

Preliminary Questions

Questions of admissibility generally

- Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b)
- In making its determination, it is not bound by the rules of evidence except those with respect to privileges

Relevancy conditioned on fact

- When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition

Testimony by accused

- The accused does not, by testifying upon a preliminary matter, become subject to cross-examination as to other issues in the case

Hearing of jury

- Hearings on the admissibility of confessions shall in all cases be conducted out of the hearing of the jury
- Hearings on other preliminary matters shall be conducted when the interests of justice require, or when an accused is a witness and so requests

Weight and credibility

- This rule does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility

Federal Rules of Evidence (Cont'd)

Limited Admissibility

When evidence that is admissible as to one party or for one purpose but not admissible as to another party or for another purpose is admitted, the court, upon request, shall restrict the evidence to its proper scope and instruct the jury accordingly

1

Hearsay Rule

- Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted
- It is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress

2

Statements That Are Not Hearsay

- Prior statement by witness
- Admission by party-opponent

- https://www.rulesofevidence.org

3

Federal Rules of Evidence: Hearsay Rule (Cont'd)

Rule 803. Hearsay Exceptions - Availability of Declarant Immaterial

Even if the declarant is available as a witness, some of them are not excluded by the Hearsay Rule:

- Present sense impression
- Excited utterance
- Statements for purposes of medical diagnosis or treatment
- Recorded recollection
- Records of regularly conducted activity
- Absence of entry in records kept in accordance with the provisions
- Public records and reports
- Records of vital statistics

Rule 804. Hearsay Exceptions; Declarant Unavailable

If the declarant is unavailable as a witness, the following are not excluded by the Hearsay Rule:

- Former testimony
- Statement under belief of impending death
- Statement against interest
- Statement of personal or family history

Federal Rules of Evidence (Cont'd)

Content of Writings, Recordings, and Photographs

Rule 1001: Definitions

Writings and Recordings

Writings and recordings consist of **letters, words, or numbers, or their equivalent**, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other forms of data compilation

Photographs

Photographs include **still photographs, X-ray films, video tapes, and motion pictures**

Original

An original of a writing or recording is the **writing or recording itself** or any counterpart intended to have the same effect by a person executing or issuing it

Duplicate

A duplicate is a **counterpart** produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques that accurately reproduce the original

Federal Rules of Evidence (Cont'd)

Rule 1002: Requirement of Original

To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress

Rule 1003: Admissibility of Duplicates

A duplicate is admissible to the same extent as an original unless

1) A genuine question is raised as to the authenticity of the original, or
2) In the circumstances it would be unfair to admit the duplicate in lieu of the original

Rule 1004: Admissibility of Other Evidence of Contents

The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if:

1) Originals are lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith
2) Original is not obtainable. No original can be obtained by any available judicial process or procedure
3) Original is in possession of the opponent. At the time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing
4) Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue

Scientific Working Group on Digital Evidence (SWGDE)

C|HFI Computer Hacking Forensic Investigator

Principle

In order to ensure that the digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system.

Standards and Criteria 1.1

All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

Standards and Criteria 1.2

Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.

Standards and Criteria 1.3

Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.

Scientific Working Group on Digital Evidence (SWGDE) (Cont'd)

Standards and Criteria 1.4

The agency must maintain written copies of appropriate technical procedures.

Standards and Criteria 1.5

The agency must use hardware and software that are appropriate and effective for the seizure or examination procedure.

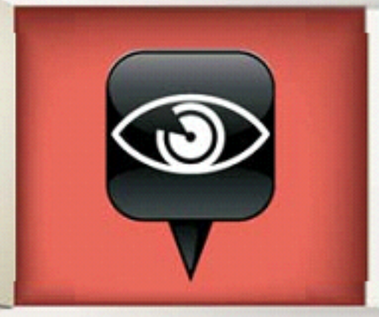
Standards and Criteria 1.6

All activities relating to the seizure, storage, examination, or transfer of the digital evidence must be recorded in writing and be available for review and testimony.

Standards and Criteria 1.7

Any action that has the potential to alter, damage, or destroy any aspect of the original evidence must be performed by qualified persons in a forensically sound manner.

Forensics Readiness



- Forensic readiness refers to an organization's ability to **make optimal use of digital evidence** in a limited period of time and with minimal investigation costs

Benefits:

- Fast and efficient investigation with **minimal disruption to the business**
- Provides **security** from cybercrimes such as intellectual property theft, fraud, or extortion
- Offers structured storage of evidence that reduces **expense** and time of an **investigation**
- Improves **law enforcement interface**
- Easy identification of **evidence** related to the potential crimes
- Proper usage of evidence for positive outcome of any **legal prosecution**
- Helps the organization use the **digital evidence** in its own defense
- Blocks the attackers from covering their tracks
- Limits the cost of **regulatory** or legal requirements for **disclosure of data**
- Averts similar **attacks** in the future

Forensics Readiness Planning

- Forensics readiness planning refers to a **set of processes** required to achieve and maintain forensics readiness

01 Identify the **potential evidence** required for an incident

02 Determine the **source of the evidence**

03 Define a **policy that determines the pathway** to legally extract electronic evidence with minimal disruption

04 Establish a **policy** for securely **handling and storing** the collected evidence

05 Identify if the incident requires **full or formal investigation**

06 **Train the staff** to handle the incident and preserve the evidence

07 Create a **special process** for documenting the procedure

08 Establish a **legal advisory board** to guide the investigation process

Computer Forensics as Part of Incident Response Plan

- Incident response is a **process of responding to incidents** that may have occurred due to security breach in the system or network

  - Goal is to **handle the incidents** in a way that minimizes the damage and reduces recovery time and costs
  - Role of an incident response professional includes **identifying how breach occurred**, how to locate the method of breach, and how to mitigate the breach

- On the other hand, computer forensics is a **legal process** of finding and analyzing the evidence to determine the culprit behind the incident

- Organizations often include **computer forensics as part of incident response** plan so as to track and prosecute perpetrators of an incident

Need for Forensic Investigator

C|HFI Computer Hacking Forensic Investigator

Cybercrime Investigation

A forensic investigator, by virtue of his or her skills and experience, **helps organizations and law enforcement agencies** investigate and prosecute the perpetrators of cyber crimes

Sound Evidence Handling

If a technically inexperienced person examines the computer involved in the crime, it will almost certainly result in rendering any evidence found inadmissible in a court of law

Incident Handling and Response

Forensic investigators **help organizations to maintain forensics readiness**, and implement effective incident handling and response

Roles and Responsibilities of Forensics Investigator

A forensic investigator performs the following tasks:

- Determines the extent of any damage done during the crime
- Recovers data of investigative value from computers involved in crimes
- Gathers evidence in a forensically sound manner
- Ensures that the evidence is not damaged in any way
- Creates an image of the original evidence without tampering with it to maintain the original evidence's integrity
- Guides the officials in carrying out the investigation. At times, it is required that the forensic investigator produce the evidence, describing the procedure involved in its discovery.
- Reconstructs the damaged disks or other storage devices, and uncovers the information hidden on the computer
- Analyzes the evidence data found
- Prepares the analysis report
- Updates the organization about various attack methods and data recovery techniques, and maintains a record of them (following a variant of methods to document) regularly
- Addresses the issue in a court of law and attempts to win the case by testifying in court

What makes a Good Computer Forensics Investigator?

- Interviewing skills to gather much information about the case from client or victim, witnesses, and suspects
- Researching skills to know the background and activities pertaining to client or victim, witnesses, and suspects
- Maintains perfect accuracy of the tests performed and their records
- Patience and the willingness to work long hours
- Excellent writing skills to detail findings in the report
- Strong analytical skills to find the evidence and link it to the suspect
- Excellent communication skills to explain their findings to the audience
- Be updated with new methodologies and forensic technology
- Well versed in more than one computer platform (includes Windows, Macintosh, and Linux)
- Knowledge of various technologies, hardware, and software
- Develops and maintains contact with computing, networking, and investigating professionals
- Be honest, ethical, and law abiding
- Knowledge of the laws surrounding the case
- Ability to control emotions when dealing with issues that induce anger
- Multi-discipline expertise related to both criminal and civil cases

Computer Forensics: Legal Issues

Digital evidence is **fragile in nature**, which makes it susceptible to changes during the course of investigation process rendering it inadmissible in the court of law

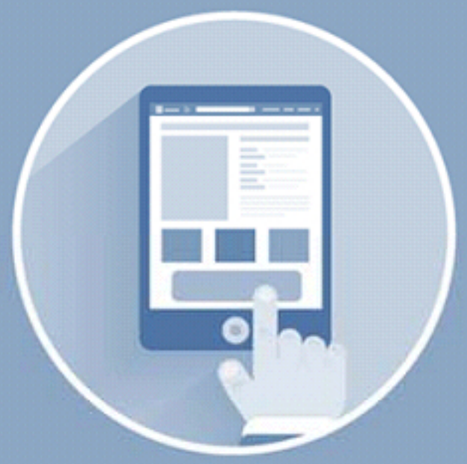
Legal system differs from one jurisdiction to the other, which makes the task of an investigator difficult as different legal systems have different rules for acquiring, preserving, investigating, and presenting the digital evidence in the court

Every legal system has a slightly different approach towards the issues related to authenticity, reliability, and completeness

The **approach of investigation differs** and evolves with changes in the technology, and the legal systems might not address these technological advances

Computer Forensics: Privacy Issues

C|HFI Computer Hacking Forensic Investigator



When retrieving evidence from a particular electronic device, investigators must be cautious to **avoid charges against unlawful search** and **seizure,** i.e., they need to be in compliance with the Fourth Amendment of the U.S. Constitution

Fourth Amendment states that the government agents may not search or seize areas or things in which a person has a reasonable expectation of privacy, without a search warrant

Note: Private intrusions not acting in the color of governmental authority are exempted from the Fourth Amendment

When dealing with the evidence related to Internet usage, investigators must **preserve** other **users' anonymity** while determining the identity of the few involved in illegal activities

Code of Ethics

- Code of ethics are the principles stated to **describe the expected behavior of an investigator** while handling a case

Computer forensic investigator should:

- Perform investigations based on well-known standard procedures
- Perform assigned tasks with high commitment and diligence
- Act with utmost ethical and moral principles
- Examine the evidence carefully within the scope of the agreement
- Ensure integrity of the evidence throughout the investigation process
- Act in accordance with federal statutes, state statutes, and local laws and policies
- Testify honestly before any board, court or trial proceedings

Computer forensic investigator should not:

- Refuse any evidence because that may cause failure in the case
- Expose confidential matters without having any authorized permission
- Exceed assignments beyond his/her skills
- Perform actions that significantly leads to a conflict of interest
- Present the training, credentials, or association membership in a wrong way
- Provide personal or prejudiced opinions
- Reserve any evidence relevant to the case

Accessing Computer Forensics Resources

Join various discussion groups and associations to access resources regarding computer forensics

- Associations offering computer forensic information:
  - Computer Technology Investigators Network

    http://www.ctin.org
  - High Technology Crime Investigation Association

    https://www.htcia.org
- Join a network of computer forensic experts and other professionals
- News services that are devoted to **computer forensics** can also be a powerful resource
- Other resources:
  - Journals of forensic investigators
  - Actual case studies

Module Summary

- Computer forensics refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document and present evidence from computing equipment that is acceptable in a court of Law
- Cyber crime is defined as any illegal act involving a computing device, network, its systems, or its applications. It is categorized into two types based on the line of attack: internal attacks and external attacks
- Computer crimes pose new challenges for investigators due to their speed, anonymity, volatile nature of evidence, global origin and difference in laws, and limited legal understanding
- Approaches to manage cyber crime investigation include: civil, criminal, and administrative
- Digital evidence is "any information of probative value that is either stored or transmitted in a digital form". It is of two types: volatile and non-volatile
- Forensic readiness refers to an organization's ability to make optimal use of digital evidence in a limited period of time and with minimal investigation costs
- Organizations often include computer forensics as part of incident response plan so as to track and prosecute perpetrators of an incident