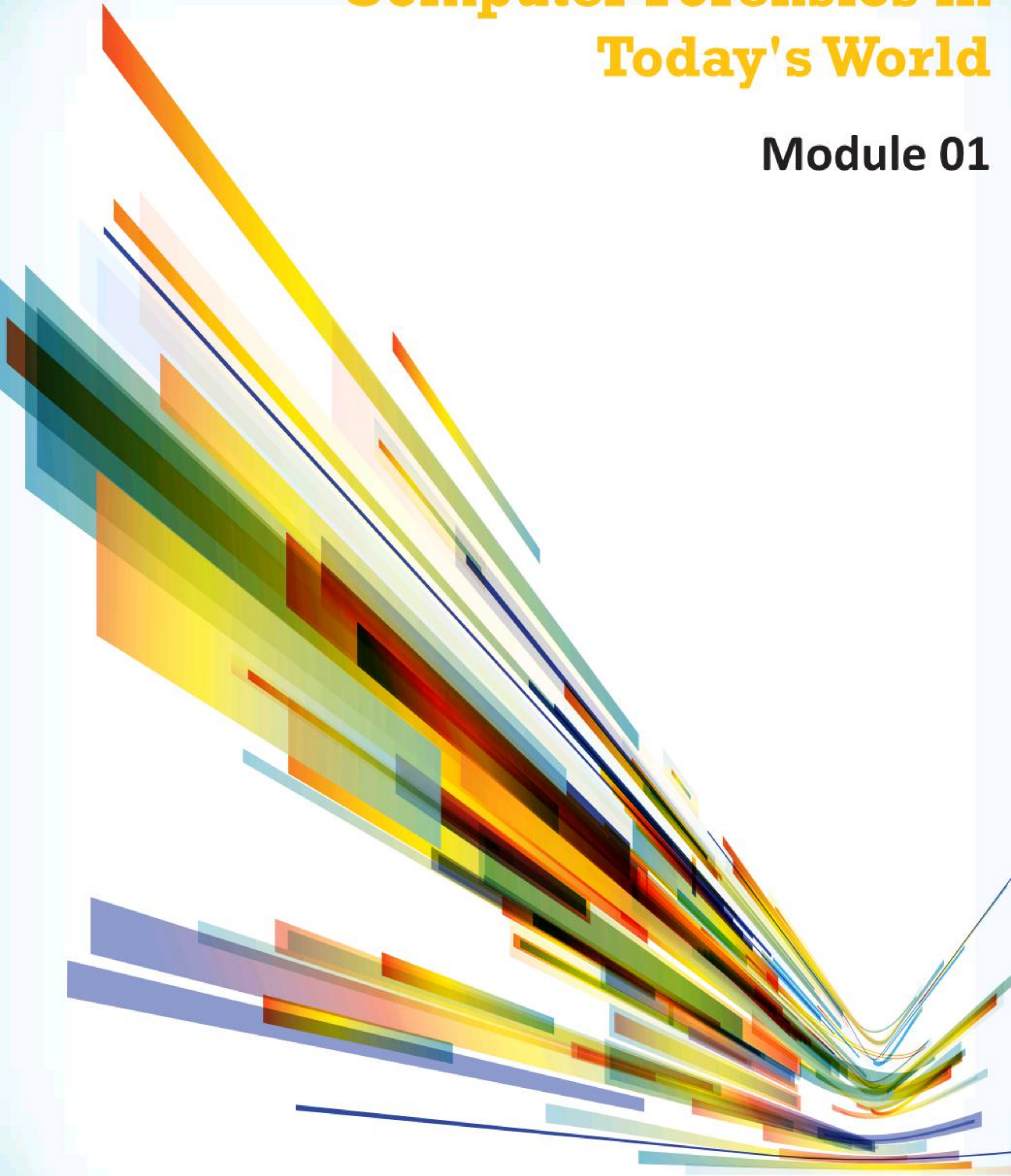


Computer Forensics in Today's World

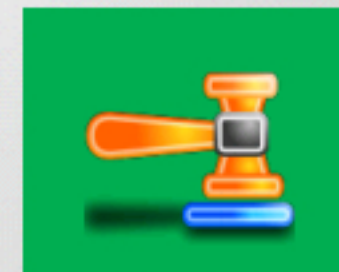
Module 01



Computer Forensics in Today's World

Module 01

Designed by **Cyber Crime Investigators**. Presented by Professionals.




Computer Hacking Forensic Investigator v9

Module 01: Computer Forensics in Today's World

Exam 312-49

Module Objectives

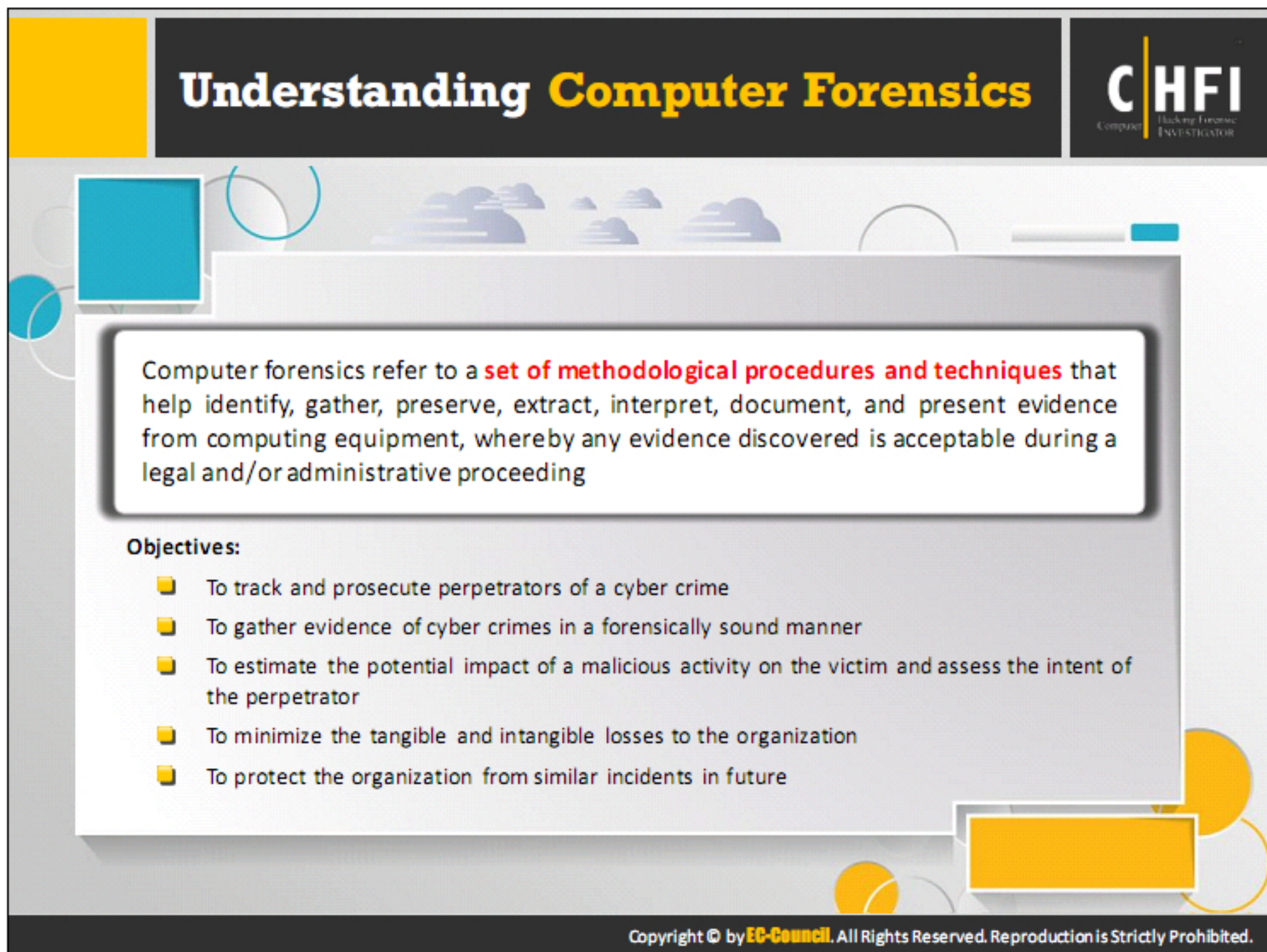


→ After successfully completing this module, you will be able to:

- 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Computer forensics plays a vital role in the investigation and prosecution of cyber criminals. The process includes acquisition, inspection, and reporting of information stored across computers and networks related to a civil or criminal incident. Forensic investigators are trained professionals who can extract, analyze, report, and investigate cases that involve technology as the source or the victim of a crime. This module introduces computer forensics in today's world. It discusses some of the most important problems and concerns that forensic investigators face today. The main objective of this module is to familiarize you with the aforementioned topics.



Understanding Computer Forensics

CHFI
Computer Hacking Forensic Investigator

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Computer forensics is a digital forensic division that deals with crimes committed across computing devices such as networks, computers, and digital storage media. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document and present evidence from computing equipment in such a manner that the discovered evidence is acceptable during a legal and/or administrative proceeding in a court of law.

In short, computer forensics deals with the process of finding evidence related to a digital crime to find the culprits and initiate legal action against them.

Objectives:

- Identify, gather, and preserve the evidence of a cybercrime.
- Track and prosecute the perpetrators in a court of law.
- Interpret, document and present the evidence to be admissible during prosecution.
- Estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator.
- Find vulnerabilities and security loopholes that help attackers.
- Understand the techniques and methods used by attackers to avert prosecution, and overcome them.
- Recover deleted files, hidden files, and temporary data that could be used as evidence.
- Perform incident response to prevent further loss of intellectual property, finances and reputation during an attack.

- Have knowledge about the laws of various regions and areas, as digital crimes are omnipresent and remote in nature.
- Know the process of handling multiple platforms, data types and operating systems.
- Understand the usage of proper tools for forensic investigations.

Why and When Do You Use Computer Forensics?

There has been an exponential increase in the number of cybercrimes and litigations involving large organizations. This has highlighted the need for computer forensics. Organizations need to employ the services of a computer forensics agency or hire a computer forensics expert to guard against computer incidents or solve crimes that involve the use of computers and related technologies. The staggering financial losses caused by computer crimes have also contributed to the renewed interest in computer forensics.

Why Do You Use Computer Forensics?

It is essential to use computer forensics to:


- Prepare for incidents in advance to ensure integrity and continuity of network infrastructure.
- Identify and gather evidence of computer crimes in a forensically sound manner.
- Offer ample protection to data resources and ensure regulatory compliance.
- Protect the organization from similar incidents in future.
- Help counteract online crimes such as abuse, bullying, and reputation damage.
- Minimize the tangible and intangible losses to the organization or an individual.
- Support prosecution of the perpetrator of an incident.

When Do You Use Computer Forensics?

Computer forensics can be helpful against all types of security and criminal incidents that involve computer systems and related technologies. As observed by various industry surveys, most organizations seek the help of computer forensics to:

- Prepare for incidents by securing and strengthening the defense mechanism as well as filling the holes in security
- Gain knowledge of the regulations and comply with them.
- Report the incidence of a breach of contract.
- Identify the actions needed as incident response.
- Act against copyright and intellectual property theft/misuse.
- Settle disputes among employees or between the employer and employees.
- Estimate and minimize the damage to resources.
- Set a security parameter and create the security norms for forensic readiness.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Cybercrime refers to “any illegal act that involves a computer, its systems, or its applications.” Once investigators start investigating a crime scene, they must remember that under computer forensics, cybercrimes are most often intentional and not accidental. The type of a cybercrime depends on the tools of the crime and its target.

The tools of the crime refer to various hacking tools used to commit the crime. They include the computer or workstation used for the crime including hardware such as the keyboard, the mouse, and the monitor. Forensic investigators usually take all such tools into custody to use them as evidence.

The target of the crime refers to the victim, which can be corporate organizations, websites, consulting agencies, and government bodies. Targets can also include the virtual environment that can act as digital evidence on account of an incident. A system becomes the target for reasons such as stealing, modifying or destroying the data; Trojan attacks; unauthorized access; a Denial of Service attack (DoS); or a Man in the Middle attack (MITM).

Based on the line of attack, cybercrimes can be classified as internal attacks and external attacks.

Internal Attacks:

Insider attacks, considered as a primary threat, refer to attacks by disgruntled individuals working in the same firm or same household as the victim. The attackers have legitimate access to the system, and have specific goals and objectives. This type of attack can be extremely

difficult to detect or protect against as the attackers are aware of the loopholes, vulnerabilities and security settings of a firm.

An insider attack can affect all components of computer security, impact availability by overloading the system's processing or storage capacity, or cause the system to crash as well as cost the company millions of dollars.

Examples of internal attacks include espionage, theft of intellectual property, manipulation of records, and Trojan horse attack.

External Attacks:

External attacks originate from outside of an organization or can be remote in nature. Such attacks occur when there are inadequate information security policies and procedures. According to various security reports, on average, a company becomes the target of intrusions every 15 minutes from an external source. Due to such numerous attempts, it is difficult to track down and prosecute the suspect of an external attack. The suspect may be operating from a machine that is across the world.

Attackers use the system as a tool to crack passwords; escalate privileges; launch Trojans, worms, and botnets; and engage in e-mail snooping and phishing.

Examples of external attacks include SQL attack, bruteforce cracking, identity theft, phishing/spoofing, denial of service attack, and 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>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Case:

One of the employees made the Chief Information Security Officer (CISO) of a research company aware of unusual activity. 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 employees 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 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. This is to know if someone became suspicious and accessed his computer while he was away. He would 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, 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 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

CHFI
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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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. Because the attacker used the cloud to mask the attack, SERT wrote special tools to analyze the multi-host command and control the attacker used. While reverse engineering malware identified during the attack, SERT experts pieced together the precise methods the attacker used 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 improving 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 customers not affected. It also helped to prevent additional fraudulent wire transfers from occurring.

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.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Computer crimes pose new challenges for investigators due to the following inherent characteristics.

- **Speed:** Advancing technology and the increasing speed of accessing data have boosted the alacrity of cybercriminals. Conversely, investigators require authorization and warrants before starting any legal procedure. This has resulted in an increasing number of cybercrimes, many more than can be handled by the investigative authorities.
- **Anonymity:** Cyber criminals can easily hide their identity by masquerading as some other entity or by hiding their IP addresses using proxies. Digital crimes also include cases where the attackers first steal the identity from a person and then use it to commit the crime.
- **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, and radio signals. The volatile data needs special tools to identify, gather, handle, interpret and present the data. Lack of such tools has become a challenge for the investigators.
- **Global origin and difference in laws:** The perpetrators can initiate a crime from any part of the world, whereas the authorities have jurisdiction over domestic crimes only. Very few cyber laws are present that empower authorities of one jurisdiction to try perpetrators present in another distant jurisdiction. Lack of such laws is helping the attackers avert prosecution even if the authorities have strong evidence against them.


- **Limited legal understanding:** Many victims are unaware of the law violated during the incident and fail to defend their claim. Besides, the limited technological knowledge of some prosecutors also causes dismissal of the trial.

Other challenges include the failure of private firms to report cybercrimes, lack of knowledge and skills to tackle advanced attacks, giving undue importance to high-loss cases, failure to link different attacks, and lack of coordination between cybercrime and local authorities.

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.**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Cybercrime investigation is the process of studying a digital crime, its impact and other details to identify the source and perpetrators of the attack and prove their guilt. It involves the painstaking collection of clues and forensic evidence, analysis of the evidence, reconstruction of the incident and presentation of the evidence in such a way that it is admissible in a court of law.

As the crime is digital, it is inevitable that there will be at least one electronic device found during the investigation, be it a computer, a cell phone, a printer, or a fax machine. Skilled investigators should analyze such devices with utmost caution and care, as they may be of critical importance for the investigation and reveal valuable evidence to help solve the case.


Therefore, the investigator must perform the forensic analysis of the information contained in the device and present it in a manner suitable for a court of law.

Types of approaches to manage cybercrime investigation include:

- Civil
- Criminal
- Administrative

These types of approaches have different processes such as collection of data, analysis, and presentation 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	Civil Cases
<ul style="list-style-type: none">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.	<ul style="list-style-type: none">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.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Civil cases involve disputes between two parties, which may include an individual versus a company, an individual versus another individual, or a company versus another. They relate to violation of contracts and lawsuits, where a guilty verdict generally results in monetary damages to plaintiff. Criminal cases include crimes that are considered harmful to the society and involve action by law enforcement agencies against a company, individual or group of individuals in response to a suspected violation of law. A guilty outcome may result in monetary damages, imprisonment, or both.

Criminal Cases:

As criminal cases involve actions that are against the norms of society, the burden of proving the accused guilty lies entirely on the prosecution.

Civil Cases:

Civil cases involve a plaintiff and defendant, wherein the plaintiff registers the case and is responsible for the burden of proof, while the authority hears both parties and passes the judgement based on the evidence presented.



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>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ALLEGED RAPE

The Case:

An attorney who was 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 that what had happened a few nights earlier was not the beginning of a relationship but was rather just a one nightstand, 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 subsequently was arrested and charged with rape.

The Investigation:

If the accused were 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 analysis of the image revealed numerous deleted text messages, which clearly showed the incident, was totally

consensual. About 100 deleted text messages were recovered, exchanged after the alleged rape took place where she was referring 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

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>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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 new high-level executive they had recently hired 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 where the executive lead. The client stated that court documents were alleging that, before his departure, the executive had copied the plaintiff's trade secrets to an external drive and had emailed close to one 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 forensics team had taken. 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 limited 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.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Administrative Investigation refers to an internal investigation by an organization to discover if its employees, clients and partners are abiding by the rules or policies. Most organizations limit administrative investigations to staff members, while some include partners along with corporations and individuals linked to the organization.

- Involves an agency or government performing inquiries to identify facts with reference to its own management and performance
- Non-criminal in nature and related to misconduct or activities of an employee that includes but are not limited to:
 - Violation of organization's policies, rules, or protocols
 - Resources misuse or damage or theft
 - Threatening or violent behavior
 - Improper promotion or pay rises
 - Corruption and bribery
 - Sexual Exploitation, harassment and abuse
- 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://einvestigate.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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. 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 GDF collected in a forensically sound manner from the systems it investigated, 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 having the digital evidence to use in finalizing the issues related to the investigation and was able to make important deadlines with regards to certain SEC filings.

Source: <http://einvestigate.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



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A forensic examiner must keep in mind certain rules to follow during a computer forensic examination, as well as to handle and analyze the evidence. This will safeguard the integrity of the evidence and render it acceptable in a court of law.


The forensic examiner must make duplicate copies of the original evidence and start by examining only the duplicates. The duplicate copies must be accurate replications of the originals, and the forensic examiner must also authenticate the duplicate copies to avoid questions about the integrity of the evidence.

Sometimes, changes to the evidence are inevitable. For example, the system may modify the memory and/or temporary files while booting up or shutting down. These modifications are natural, and the investigators should record the extent and reason for these modifications.

The computer forensic examiner must not continue with the investigation if the examination is going to be beyond his or her knowledge level or skill level. In these circumstances, the forensic investigator must seek the assistance of an experienced specialist investigator or undergo training in that particular field to enhance his or her knowledge or skill set. It would be wise to discontinue with the investigation if it is going to adversely affect the outcome of the case.

Forensic investigators should memorize the rules enumerated in the slide.

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


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

ETI is a methodology for investigating criminal activity. It adopts a holistic approach toward any criminal activity as a criminal operation rather than as a single criminal act. ETI is a powerful methodology to identify criminals who have escaped prosecution despite their criminal organizations having ceased to exist. ETI encourages proactive action on the structure of the criminal enterprise, considering that the individual criminals commit the crimes not for personal motives but to benefit their criminal enterprise. By applying ETI with favorable state and federal legislation, law enforcement agencies can target and dismantle the entire criminal enterprise in one criminal indictment.

ETI differs from traditional investigative methods and seems to be complex and time consuming, which could affect the case-closure rates. Nevertheless, it is more effective in prosecuting criminal enterprises. ETI seems to be a good option if an investigator can identify the underlying motive as financial profit for most criminal enterprises. It analyzes the full range of criminal activities of the enterprise, determines the components that allow the enterprise to operate, and exploits the identified vulnerable areas within each component.

ETI is successful in cases involving criminal organizations that have a hierarchy of criminal activities. In such cases, the authorities can initiate the investigation from the lower level, where chances are high to identify the criminal activities with ease. The benefit of applying ETI is that the diversity of criminal organizations opens new discoverable vulnerabilities of the organizations on a large scale, which provides law enforcement agencies with opportunities to identify illicit activities.

Source: *The FBI Law Enforcement Bulletin*, by Richard A. McFeely

	<h2>Understanding Digital Evidence</h2>	 Computer Hacking Forensic Investigator
	<p>Digital evidence is defined as “any information of probative value that is either stored or transmitted in a digital form”</p>	
	<p>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</p>	
	<p>Digital evidence is circumstantial and fragile in nature, which makes it difficult for a forensic investigator to trace criminal activities</p>	
	<p>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”</p>	
<p>Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.</p>		

Digital devices used in cyberattacks and other security breaches store some data about the session, such as login user, time, type of connection, IP addresses, etc., which can act as evidence for prosecuting the attacker. Digital evidence includes all such information that is either stored or transmitted in digital form and has probative value, thus helping investigators find the perpetrator.

Digital evidence is present across computing devices, servers, routers etc. It is revealed during forensics investigation while examining digital storage media, monitoring the network traffic, or making duplicate copies of digital data.

Investigators should take utmost care while gathering and extracting the digital evidence as it is circumstantial and fragile in nature. This makes it difficult for a forensic investigator to trace the criminal activities. Investigators should be trained and skilled to extract, handle and analyze such fragile evidence.

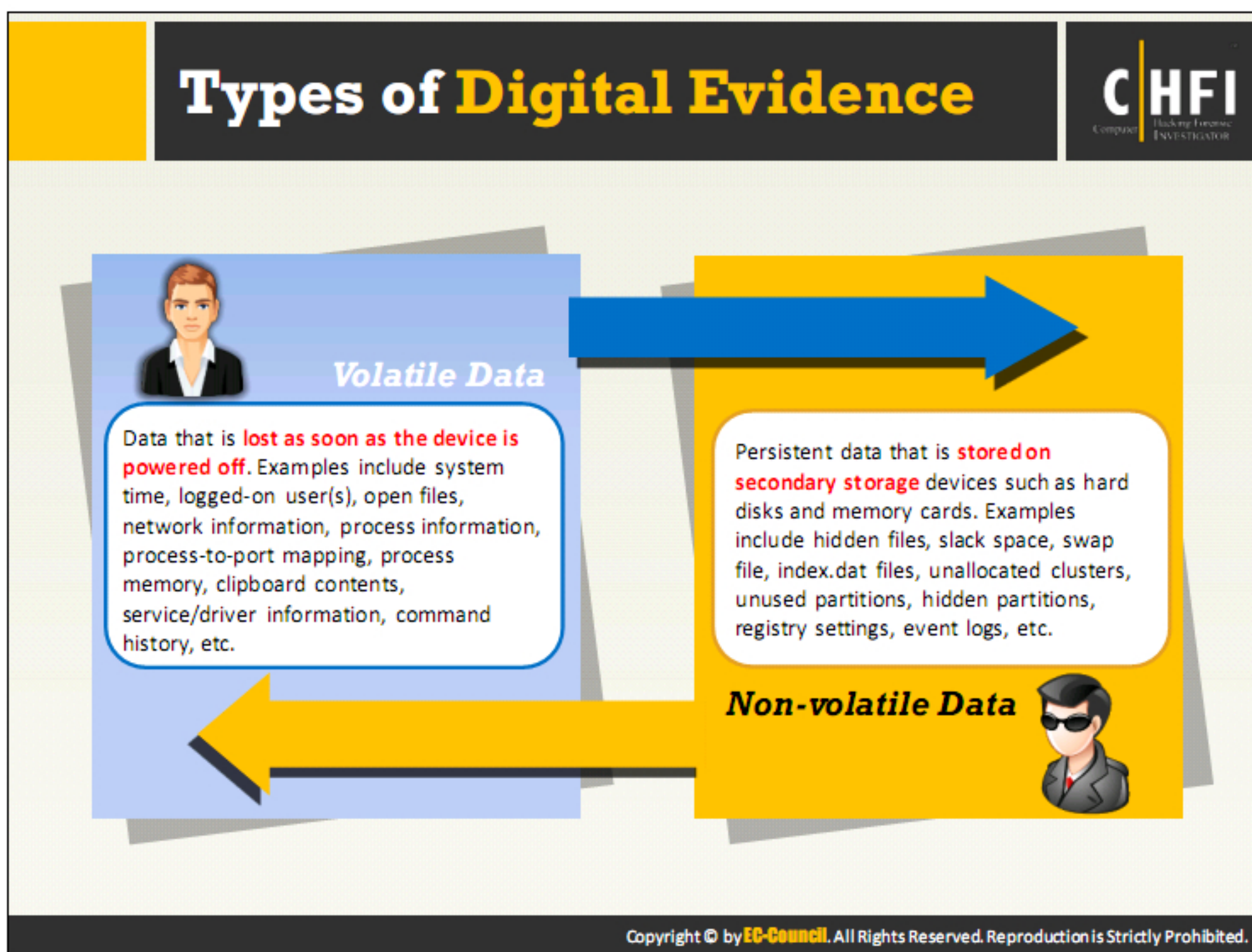
According to Locard's Exchange Principle, “anyone or anything, entering a crime scene takes something of the scene with them, and leave something of themselves behind when they leave.” For example, if information from a victim’s computer is stored on the server or system itself at the time of the crime, the investigator can get that information easily by examining log files, Internet browsing history, and so on.

Similarly, if an individual sends an intimidating message via an Internet-based e-mail service such as Hotmail, Gmail, or Yahoo Mail, the browser stores files, links, and other information on the hard disk along with the date and time of the sent information. Forensic investigators can

find plenty of digital information relating to the sent message on the victim's hard drive, including the original message.

Digital Forensics Challenges:

Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence. For example, system data that an intruder can easily change or destroy should have priority while assembling the evidence. Some of the major challenges faced by digital forensic investigators are mentioned in the aforementioned slide.



Cybercriminals directly depend on technology and digital devices to engage with the targeted system or network. Therefore, most of the evidence is present in the devices used by an attacker to connect to a network or to the computing devices of the victim. Digital evidence can be any type of file stored on a device including a text file, image, document, executable file, and application data. Most of this evidence is in the storage media of the devices.

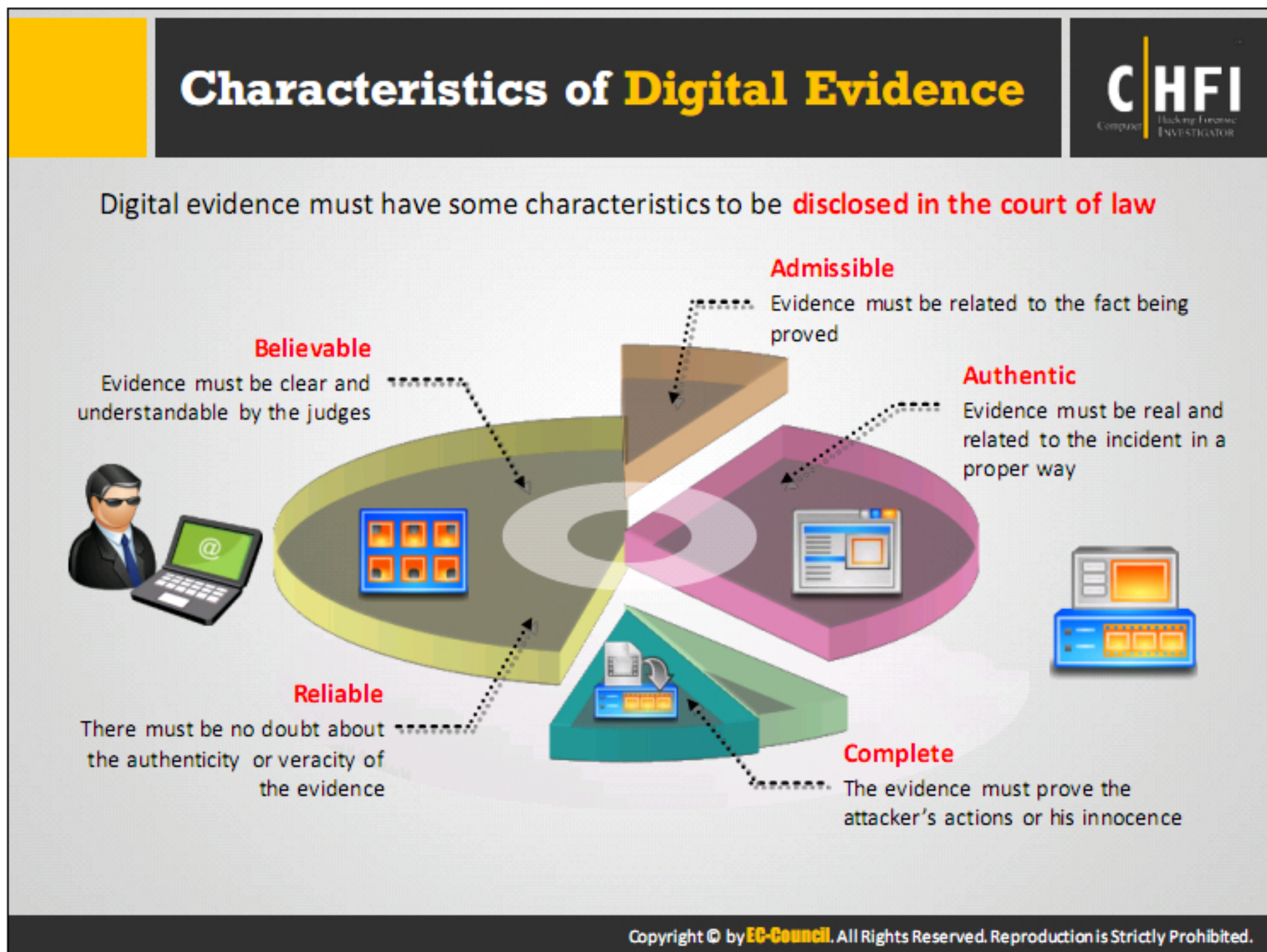
Based on the storage style and lifespan, digital evidence is of two types; volatile data and non-volatile data.

- **Volatile Data:** Volatile data refers to the temporary information on a digital device that requires a constant power supply and is deleted if the power supply is interrupted. For example, the RAM stores most volatile data and discards it when the device is switched off.

Important volatile data includes 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.

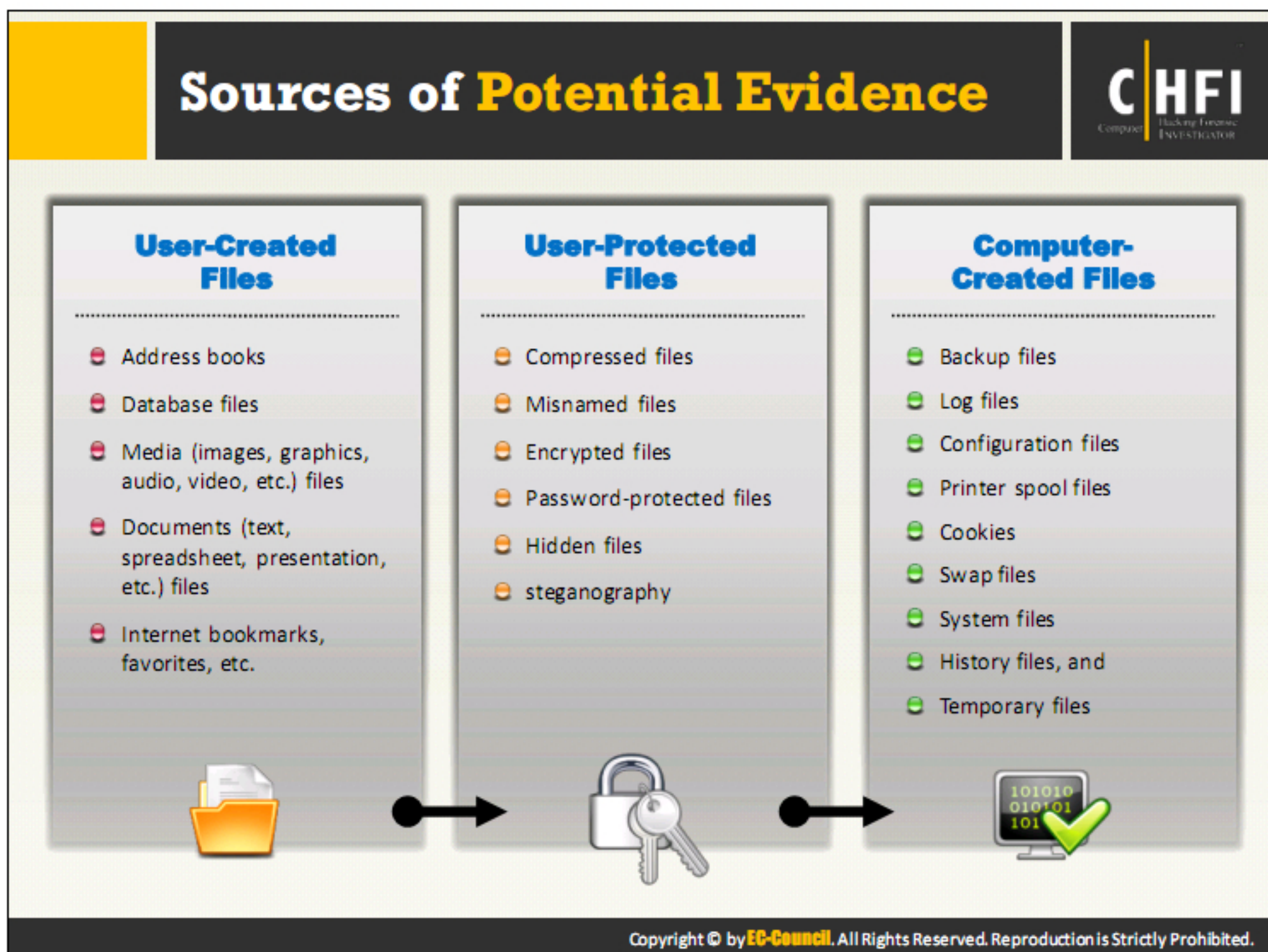
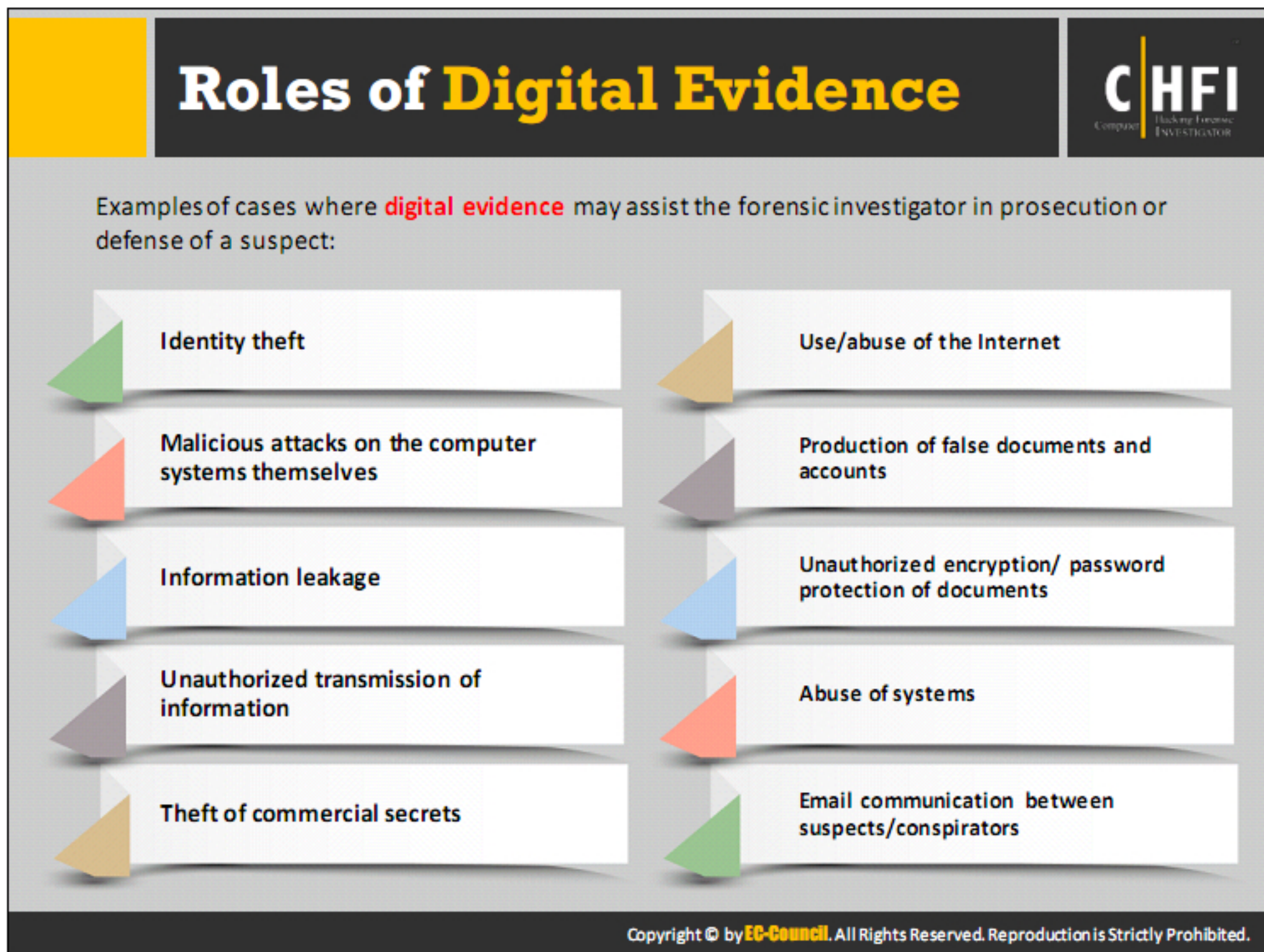
- **Non-volatile Data:** Non-volatile data refers to the permanent data stored on secondary storage devices, such as hard disks and memory cards. Non-volatile data does not depend on power supply and remains intact even when the device is switched off.

Information stored in non-volatile form includes hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs.



The digital evidence must have some characteristics to be acceptable **in a court of law**

- **Admissible**: Investigators need to present evidence in admissible manner, which means that it should be relevant to the case, act in support of the client presenting it, and be well communicated and non-prejudiced.
- **Authentic**: It is very easy to manipulate digital evidence, which raises questions of its ownership. Therefore, investigators must provide supporting documents regarding the authenticity of the evidence with details such as source and its relevance to the case. If necessary, they must also furnish details such as author of the evidence or path of transmission.
- **Complete**: The evidence must be complete, which means it must either prove or disprove the consensual fact in the litigation. If the evidence fails to do so, the court is liable to dismiss the case citing lack of strong evidence.
- **Reliable**: The forensic experts should extract and handle the evidence while maintaining a record of the tasks performed during the process to prove that the evidence is dependable. Forensic investigations must be conducted only on the copies of the evidence because the court needs to have the original evidence for future reference.
- **Believable**: Investigators and prosecutors must present the evidence in a clear and comprehensible manner to the members of jury. They must explain the facts clearly and obtain an expert opinion on the same to confirm the investigation process.



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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Sources of Potential Evidence (Cont'd)

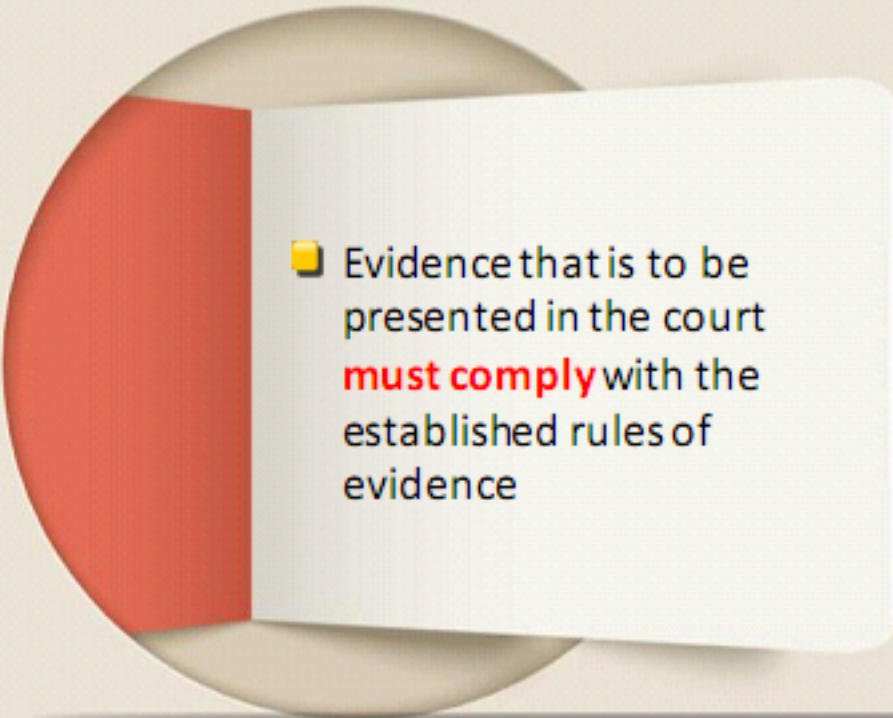


Device	Location of Potential Evidence
Removable Storage Device and Media	Storage device and media such as tape, CD, DVD, and Blu-ray have the evidence in the devices themselves
Scanner	Evidence is found by looking at the marks on the glass of the scanner
Telephones	Evidence is found through names, phone 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.


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Prior to the investigation, it is important for the investigator to understand the rules of evidence. The submission of evidence in a legal proceeding, especially in computer crime cases, can have major challenges. Specific knowledge is required to collect, preserve, and transport the evidence because the evidence obtained from a cybercrime case might vary from the traditional forms of evidence. Often, evidence associated with computer crimes is in the form of an electronic pulse, i.e., in digital form.

Prior to the legal proceeding, evidence that is to be present in court must comply with the rules of evidence, which are based on English common law. The main purpose of these rules is to be fair to both parties, prohibiting increased allegations.


The Wikipedia page on the Law of Evidence states that:

- Rules of evidence govern whether, when, how, and for what purpose a case requires proof 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


The best evidence rule is designed to prevent any alteration of digital evidence, either intentionally or unintentionally. It ensures that the court considers only the best evidence related to a specific matter or particular computer crime case.

It states that the court allows only the original evidence of any document, photograph, or recording at a trial rather than a copy, but the duplicate will also suffice as evidence under the following conditions:


- Original evidence is destroyed due to fire and flood.
- Original evidence is destroyed in the normal course of business.
- Original evidence is in possession of a third party.

It also states that the best or highest form of evidence available to any party must be presented in a court of law. If a live or original testimony form of the evidence were available, the court would not admit the duplicate copies of that testimony as evidence.

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

<p>(a) Effect of erroneous ruling</p> <ul style="list-style-type: none">➤ 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	<p>(b) Record of offer and ruling</p> <p>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</p>
<p>(c) Hearing of jury</p> <p>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</p>	<p>(d) Plain error</p> <p>Nothing in this rule precludes taking notice of plain errors affecting substantial rights although they were not brought to the attention of the court</p>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Rule 101: Scope

These rules govern proceedings in the courts of the United States and before United States bankruptcy judges and United States magistrate judges, to the extent and with the exceptions stated in rule 1101.

Rule 102: Purpose and Construction


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.

Rule 103: Rulings on Evidence

Rules of Evidence are discussed in the aforementioned slide.

Source: <http://www.uscourts.gov>


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



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Federal Rules of Evidence (Cont'd)

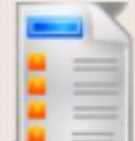




Limited Admissibility

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Rule 105: Limited Admissibility

When evidence which 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

According to Rule 801 of the Federal Rules of Evidence, Hearsay is a statement other than the one made by the declarant while testifying at an ongoing trial or hearing. It is offered as evidence to prove the truth of the matter asserted. Hearsay is not admissible except as provided by this rule or by other rules prescribed by the Supreme Court pursuant to statutory authority or by an Act of Congress.

A statement is not hearsay if it is:

1. A prior statement by a declarant witness.

The declarant testifies at the trial or hearing and is subjected to cross-examination concerning the statement, and the statement is:

- a. Inconsistent with the declarant's testimony, and was given under oath subject to the penalty of perjury at a trial, hearing, or other proceeding, or in a deposition, or
- b. Consistent with the declarant's testimony and is offered to rebut an express or implied charge against the declarant of recent fabrication or improper influence or motive, or
- c. One of identification of a person made after perceiving the person; or

2. An opposing party's statement.

The statement is offered against an opposing party and is:

- a. The party's own statement, either in an individual or a representative capacity
- b. A statement of which the party has manifested an adoption or belief in its truth, or
- c. A statement by a person authorized by the party to make a statement concerning the subject, or
- d. A statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship, or
- e. A statement by a coconspirator of a party during the course and in furtherance of the conspiracy

The contents of the statement shall be considered, but are not sufficient on their own to establish the declarant's authority under subdivision (c), the agency or employment relationship and scope thereof under subdivision (d), or the existence of the conspiracy and the participation therein of the declarant and the party against whom the statement is offered under subdivision (e).

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

CHFI
Computer Hacking Forensic Investigator

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Rule 803. Hearsay Exceptions; Availability of Declarant Immaterial

The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

1. **Present sense impression:** A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.
2. **Excited utterance:** A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.
3. **Then existing mental, emotional, or physical condition:** A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of declarant's will.
4. **Statements for purposes of medical diagnosis or treatment:** Statements made for purposes of medical diagnosis or treatment and describing medical history, or past or present symptoms, pain, or sensations, or the inception or general character of the cause or external source thereof insofar as reasonably pertinent to diagnosis or treatment.

- 5. Recorded recollection:** A memorandum or record concerning a matter about which a witness once had knowledge but now has insufficient recollection to enable the witness to testify fully and accurately, shown to have been made or adopted by the witness when the matter was fresh in the witness' memory and to reflect that knowledge correctly. If admitted, the memorandum or record may be read into evidence but may not itself be received as an exhibit unless offered by an adverse party.
- 6. Records of regularly conducted activity:** A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11) , Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.
- 7. Absence of entry in records kept in accordance with the provisions of paragraph (6):** Evidence that a matter is not included in the memoranda reports, records, or data compilations, in any form, kept in accordance with the provisions of paragraph (6), to prove the nonoccurrence or nonexistence of the matter, if the matter was of a kind of which a memorandum, report, record, or data compilation was regularly made and preserved, unless the sources of information or other circumstances indicate lack of trustworthiness.
- 8. Public records and reports:** Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.
- 9. Records of vital statistics:** Records or data compilations, in any form of births, fatal injuries, deaths, or marriages, if the report there of was made to a public office pursuant to requirements of law.
- 10. Absence of public record or entry:** To prove the absence of a record, report, statement, or data compilation, in any form, or the nonoccurrence or nonexistence of a matter of which a record, report, statement, or data compilation, in any form, was regularly made and preserved by a public office or agency, evidence in the form of a certification in accordance with rule 902, or testimony, that diligent search failed to disclose the record, report, statement, or data compilation, or entry.

- 11. Records of religious organizations:** Statements of births, marriages, divorces, deaths, legitimacy, ancestry, relationship by blood or marriage, or other similar facts of personal or family history, contained in a regularly kept record of a religious organization.
- 12. Marriage, baptismal, and similar certificates:** Statements of fact contained in a certificate that the maker performed a marriage or other ceremony or administered a sacrament, made by a clergyman, public official, or other person authorized by the rules or practices of a religious organization or by law to perform the act certified, and purporting to have been issued at the time of the act or within a reasonable time thereafter.
- 13. Family records:** Statements of fact concerning personal or family history contained in family Bibles, genealogies, charts, engravings on rings, inscriptions on family portraits, engravings on urns, crypts, or tombstones, or the like.
- 14. Records of documents affecting an interest in property:** The record of a document purporting to establish or affect an interest in property, as proof of the content of the original recorded document and its execution and delivery by each person by whom it purports to have been executed, if the record is a record of a public office and an applicable statute authorizes the recording of documents of that kind in that office.
- 15. Statements in documents affecting an interest in property:** A statement contained in a document purporting to establish or affect an interest in property if the matter stated was relevant to the purpose of the document, unless dealings with the property since the document was made have been inconsistent with the truth of the statement or the purport of the document.
- 16. Statements in ancient documents:** Statements in a document in existence twenty years or more, the authenticity of which is established.
- 17. Market reports, commercial publications:** Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations.
- 18. Learned treatises:** To the extent called to the attention of an expert witness upon cross-examination or relied upon by the expert witness in direct examination, statements contained in published treatises, periodicals, or pamphlets on a subject of history, medicine, or other science or art, established as a reliable authority by the testimony or admission of the witness or by other expert testimony or by judicial notice. If admitted, the statements may be read into evidence but may not be received as exhibits.
- 19. Reputation concerning personal or family history:** Reputation among members of a person's family by blood, adoption, or marriage, or among a person's associates, or in the community, concerning a person's birth, adoption, marriage, divorce, death, legitimacy, relationship by blood, adoption, or marriage, ancestry, or other similar fact of personal or family history.
- 20. Reputation concerning boundaries or general history:** Reputation in a community, arising before the controversy, as to boundaries of or customs affecting lands in the

community, and reputation as to events of general history important to the community or State or nation in which located.

- 21. Reputation as to character:** Reputation of a person's character among associates or in the community.
- 22. Judgment of previous conviction:** Evidence of a final judgment, entered after a trial or upon a plea of guilty (but not upon a plea of nolo contendere), adjudging a person guilty of a crime punishable by death or imprisonment for more than one year, to prove any fact essential to sustain the judgment, but not including, when offered by the Government in a criminal prosecution for purposes other than impeachment, judgments against persons other than the accused. The pendency of an appeal may be shown but does not affect admissibility.
- 23. Judgment as to personal, family or general history, or boundaries:** Judgments as proof of matters of personal, family or general history, or boundaries, essential to the judgment, if the same would be provable by evidence of reputation.

Rule 804. Hearsay Exceptions; Declarant Unavailable

Following are the rules for Hearsay Exceptions; if Declarant is Unavailable

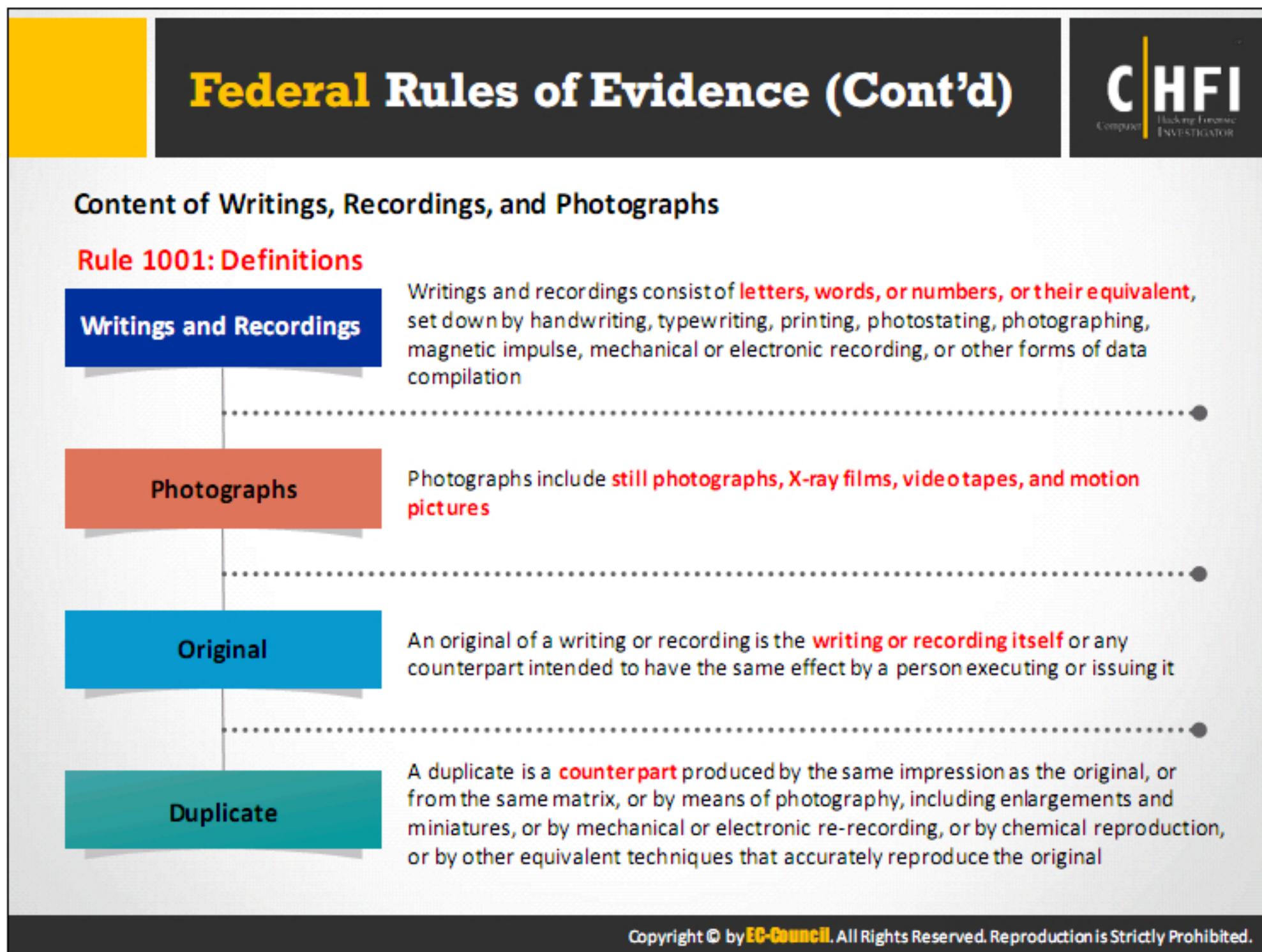
- a. Definition of unavailability:** Unavailability as a witness" includes situations in which the declarant:
 - is exempted by ruling of the court on the ground of privilege from testifying concerning the subject matter of the declarant's statement; or
 - persists in refusing to testify concerning the subject matter of the declarant's statement despite an order of the court to do so; or
 - testifies to a lack of memory of the subject matter of the declarant's statement; or
 - is unable to be present or to testify at the hearing because of death or then existing physical or mental illness or infirmity; or
 - is absent from the hearing and the proponent of a statement has been unable to procure the declarant's attendance (or in the case of a hearsay exception under subdivision (b)(2), (3), or (4), the declarant's attendance or testimony) by process or other reasonable means

A declarant is not unavailable as a witness if exemption, refusal, claim of lack of memory, inability, or absence is due to the procurement or wrongdoing of the proponent of a statement for preventing the witness from attending or testifying.

- b. Hearsay exceptions:** The following are not excluded by the hearsay rule if the declarant is unavailable as a witness:
 - 1. Former testimony:** Testimony given as a witness at another hearing of the same or a different proceeding, or in a deposition taken in compliance with law during the same or another proceeding, if the party against whom the testimony is now offered, or, in a civil action or proceeding, a predecessor in interest, had an

opportunity and similar motive to develop the testimony by direct, cross, or redirect examination.

2. **Statement under belief of impending death:** In a prosecution for homicide or in a civil action or proceeding, a statement made by a declarant while believing that the declarant's death was imminent, concerning the cause or circumstances of what the declarant believed to be impending death.
3. **Statement against interest:** A statement which was at the time of its making so far contrary to the declarant's pecuniary or proprietary interest, or so far tended to subject the declarant to civil or criminal liability, or to render invalid a claim by the declarant against another, that a reasonable person in the declarant's position would not have made the statement unless believing it to be true. A statement tending to expose the declarant to criminal liability and offered to exculpate the accused is not admissible unless corroborating circumstances clearly indicate the trustworthiness of the statement.
4. **Statement of personal or family history**
 - (A) A statement concerning the declarant's own birth, adoption, marriage, divorce, legitimacy, relationship by blood, adoption, or marriage, ancestry, or other similar fact of personal or family history, even though declarant had no means of acquiring personal knowledge of the matter stated; or (B) a statement concerning the foregoing matters, and death also, of another person, if the declarant was related to the other by blood, adoption, or marriage or was so intimately associated with the other's family as to be likely to have accurate information concerning the matter declared.

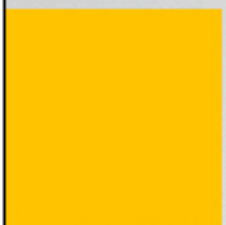


The following rules concern the contents of writings, recordings, and photographs:


Rule 1001. Definitions


For purposes of this article, the following definitions are applicable:

1. **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 form of data compilation.
2. **Photographs:** “Photographs” include still photographs, X-ray films, video tapes, and motion pictures.
3. **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. An “original” of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original.”
4. **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, which accurately reproduces 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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 Content

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

1. **Originals lost or destroyed:** All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
2. **Original not obtainable:** No original can be obtained by any available judicial process or procedure; or
3. **Original in possession of opponent:** At a 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; or
4. **Collateral matters:** The writing, recording, or photograph is not closely related to a controlling issue.

Scientific Working Group on Digital Evidence (SWGDE)

CHFI
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.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Principle 1

To ensure that digital evidence is collected, preserved, examined, or transferred in a manner that safeguards the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective system for quality control.

Standard Operating Procedures (SOPs)

Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and broadly accepted procedures, equipment, and materials.

Implementation of SOPs allows you to operate company-compliant policies and plans. It is important that no modifications are made to SOPs before implementation to achieve the desired outputs. However, if any modifications are required, they must be communicated before starting an investigation.

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.

Discussion: The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are essential to the acceptance

of results and conclusions by courts and other agencies. The development and implementation of these SOPs must be under an 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.


Discussion: Rapid technological changes are the hallmark of digital evidence, wherein the types, formats, and methods for seizing and examining digital evidence change quickly. To ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, the management must review and update SOP documents annually.

Standards and Criteria 1.3

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

Discussion: As a variety of scientific procedures may validly be applied to a given problem, standards and criteria for assessing procedures need to be flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other agencies may be useful.

Source: <http://www.fbi.gov>

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.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Standards and Criteria 1.4

The agency must maintain written copies of the appropriate technical procedures.

Discussion: Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.

Standards and Criteria 1.5

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

Discussion: Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem.

Hardware used in the seizure and/or examination of digital evidence should be in good operating condition and be tested to ensure that it operates correctly. Software must be tested to ensure that it produces reliable results for use in seizure and/or examination purposes.

Standards and Criteria 1.6

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

Discussion: In general, documentation to support conclusions must be such that, in the absence of the originator, another competent person can evaluate what was done, interpret the data, and arrive at the same conclusions as the originator.

The requirement for evidence reliability necessitates a chain of custody for all items of evidence. This implies that proper documentation must be maintained in chronological order for all digital evidence.

Case notes and records of observations must be of a permanent nature. Handwritten notes and observations must be in ink, not pencil, although pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems.

Standards and Criteria 1.7

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

Discussion: As outlined in the preceding standards and criteria, evidence has value only if it can be shown to be accurate, reliable, and controlled. A high-quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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. It includes technical and nontechnical actions that maximize an organization's competence to use digital evidence.


Forensic readiness includes the establishment of specific incident response procedures and designated trained personnel to handle the procedures in case of a breach. It enables an organization to collect and preserve digital evidence quickly and efficiently with minimal investigation costs. Such a state of readiness along with an enforceable security policy helps the organization mitigate the risk of threat from employees and prepare preemptive measures. A forensically trained and well-prepared incident response team ensures proper reaction against any mishap and the ability to handle evidence according to proper legal procedures for possible use in a court of law.

An incident response team that is forensically ready offers an organization the following benefits:

- It eases evidence gathering to act in the company's defense in case of a lawsuit.
- It enables the use of comprehensive evidence collection to act as a deterrent to insider threat and process all important evidences without fail.
- It helps the organization conduct a fast and efficient investigation in the event of a major incident and take corresponding actions with minimal disruption to day-to-day business activities.

- It facilitates a well-designed, fixed and structured approach toward storage of evidence to reduce investigation expenses and time considerably and simultaneously preserve the all-important chain of custody.
- It establishes a structured approach toward storage of all digital information, which not only reduces the cost of any court ordered disclosure or regulatory/legal need to disclose data, but also fulfils requirements under federal law (e.g., as a response to a request for discovery under the Federal Rules of Civil Procedure).
- It extends the protection offered by an information security policy to cover wider threats of cybercrime, such as intellectual property protection, fraud, or extortion.
- It demonstrates due diligence and good corporate governance of the company's information assets, as measured by the "Reasonable Man" standard.
- It ensures that the investigation meets all regulatory requirements,
- It can improve upon and make the interface to law enforcement easier.
- It improves the prospects of successful legal action.
- It can provide evidence to resolve commercial or privacy disputes.
- It can support employee sanctions up to and including termination based on digital evidence (e.g., to prove violation of an acceptable-use policy).
- It helps prevent attackers from covering their tracks.
- It limits the cost of regulatory or legal requirements for disclosure of data.
- It helps avert 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensics readiness planning refers to a set of processes required to achieve and maintain forensics readiness. The following steps describe the key activities in forensic readiness planning.

Identify the potential evidence required for an incident

Define the purpose of evidence collection and gather information to determine evidence sources that can help deal with the crime and design the best methods of collection. Produce an evidence requirement statement in collaboration with the people responsible for managing the business risk and the ones running and monitoring information systems. Possible evidence files include IT audit and device logs, network logs, and system data.

Determine the source of the evidence

Forensic readiness should include knowledge of all the sources of potential evidence present. Determine what currently happens to the potential evidence data and its impact on the business while retrieving the information.

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

Devise a strategy to ensure the collection of evidence from all the relevant sources and its preservation in a legally sound manner, while causing minimal disruption to the work.

Establish a policy for securely handling and storing the collected evidence

Secure the collected evidence in such way that it is available for retrieval whenever required in the future. Define a policy for safe storage and management of potential evidence as well as define security measures to protect legitimacy of the data and evidence integrity whenever someone tries to access, use, move, or store additional digital information. In the parlance of investigators, this is the process of continuity of evidence in the United Kingdom and chain of custody in the United States. Document the records of who held and who had access to the evidence.

Identify if the incident requires full or formal investigation

Incidents are of different types. Estimate the event and evaluate it to check if it requires a full or formal investigation or can be neglected based on its impact on the business. Escalate an incident only if it has a major impact on business continuity.

Therefore, be ready to justify any escalation to a full or formal investigation as it consumes resources as well as time.

Train the staff to handle the incident and preserve the evidence

Incident management requires a strong and well-qualified workforce, so ensure that the staff has obtained appropriate training required for fulfilling their roles. It is also necessary to ensure that staff members are competent to perform any role related to the handling and preservation of evidence.

Create a special process for documenting the procedure

Special process of documenting is necessary to answer some questions as well as support the answers it provides. Documenting the complete process will also, help recheck the process if it yields false results and provide a backup for future reference. It will also help present the evidence in a court of law.


Establish a legal advisory board to guide the investigation process

All investigation processes should have a legal stance and the organization should seek legal advice before taking any action on the incident. This is because some incidents may damage the company's reputation. Form a legal advisory board consisting of experienced personnel who understand the company's stance and can provide sound advice on the strength of the case and suggest further action.


The legal advisory board will help the organization to:

- Manage any dangers arising from the incident.
- File the incident legally and ensure proper prosecution.
- Understand legal and regulatory constraints, and suggest necessary action.
- Handle processes such as reputation protection and PR issues.
- Design legal agreements with partners, customers, investors and employees.
- Investigate the company's commercial and civil disputes.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident response is the process of developing a strategy to address the occurrence of any security breach in the system or network. It includes the formulation of security policies and goals of incident response, creation of the incident response team, analysis of threats, establishing the methods for detecting a breach, and preparing to combat threats and mitigate damages in the event of a security breach. Organizations create incident response plans to accomplish goals such as:

- Develop and implement a strong security policy.
- Effectively monitor and analyze the systems and network traffic.
- Ensure operational logs and logging mechanisms.
- Handle the incidents in a way that minimizes damage and reduces recovery time and costs.
- Map the pathway for extracting evidence in a legally sound and acceptable manner.
- Define the role of an incident response professional, such as identifying how a breach occurred, how to locate the method of the breach, and how to mitigate the breach.

On the other hand, computer forensics is a legal process of finding, gathering, analyzing and presenting the evidence in a court of law to determine the culprit behind the incident. Organizations often include computer forensics in their incident response plan to track and prosecute perpetrators of an incident.

Need for 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



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A forensic investigator, by virtue of his or her skills and experience, helps organizations and law enforcement agencies investigate and prosecute the perpetrators of cybercrimes. If a technically inexperienced person examines the computer involved in the crime, it will almost certainly render any evidence found to be inadmissible in a court of law.

A forensic investigator performs the following tasks:

- Evaluates the damages of a security breach
- Identifies and recovers data required for investigation
- Extracts the evidence in a forensically sound manner
- Ensures proper handling of the evidence
- Acts as a guide to the investigation team
- Creates reports and documents about the investigation required to present in a court of law
- Reconstructs the damaged storage devices and uncovers the information hidden on the computer
- Updates the organization about various methods of attack 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

Forensic investigators are familiar with the current Linux, Macintosh, and Windows platforms. They also develop and maintain contact with computing, networking, and investigating professionals, who can help them overcome any difficulties during investigation.

A forensic examiner differs from a forensic investigator. The former only analyzes evidence as part of the forensic investigation process, while the latter relates it to the crime.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


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


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Digital evidence is fragile in nature, which makes it susceptible to changes during the investigation process, thus rendering it inadmissible in a court of law. Handling and safeguarding digital evidence is a difficult task because it is volatile and incorrect handling can destroy it. Forensic investigators also face many challenges when preserving digital evidence. For example, an intruder can alter system data and therefore the investigators should gather it first. Digital evidence is circumstantial, which makes it difficult for a forensic investigator to trace the system's activity.

Cybercrimes are remote in nature, which means that an attacker based in one country can breach the security of a system located in another. This makes it difficult to collect the evidence and prosecute the perpetrator. Besides, legal systems differ from one jurisdiction to the other and have different rules for acquiring, preserving, investigating, and presenting the digital evidence in a court. This complicates the task of the investigator.


In this light, investigators should read and understand the rules of investigation, analysis, presentation and prosecution that apply in various regions relevant to a case. Each legal system has a slightly different approach toward the issues related to authenticity, reliability, and completeness. Therefore, the investigators should strictly comply with the rules of the region for better prosecution. Rapid technological changes have also raised certain problems for the investigators. Consequently, investigators need to adapt and change their approach in accordance with such technological changes; particularly so because the legal systems might not address these technological advances. Conversely, changing technologies also make it difficult to train the investigators to handle all such changes.

Computer Forensics: Privacy Issues






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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Cybercrime investigators need to obtain a warrant from the authorities to search the victim or attacker system. The warrant should mention all the devices that must be investigated. When retrieving evidence from a particular electronic device, investigators must be cautious to avoid charges such as unlawful search and seizure; i.e., they need to comply with the Fourth Amendment of the U.S. Constitution.


The Fourth Amendment states that 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 do not come under the Fourth Amendment.

When dealing with evidence related to Internet usage, investigators must preserve anonymity of other users. This is important because they come across the identities of all users connected with the target system while identifying the few involved in illegal activities.

Investigators should take permission from the owners of the data or system before publicizing the data present on the investigated system. They should ensure that their acts do not raise any privacy concerns with the owner of the system.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Accessing Computer Forensics Resources




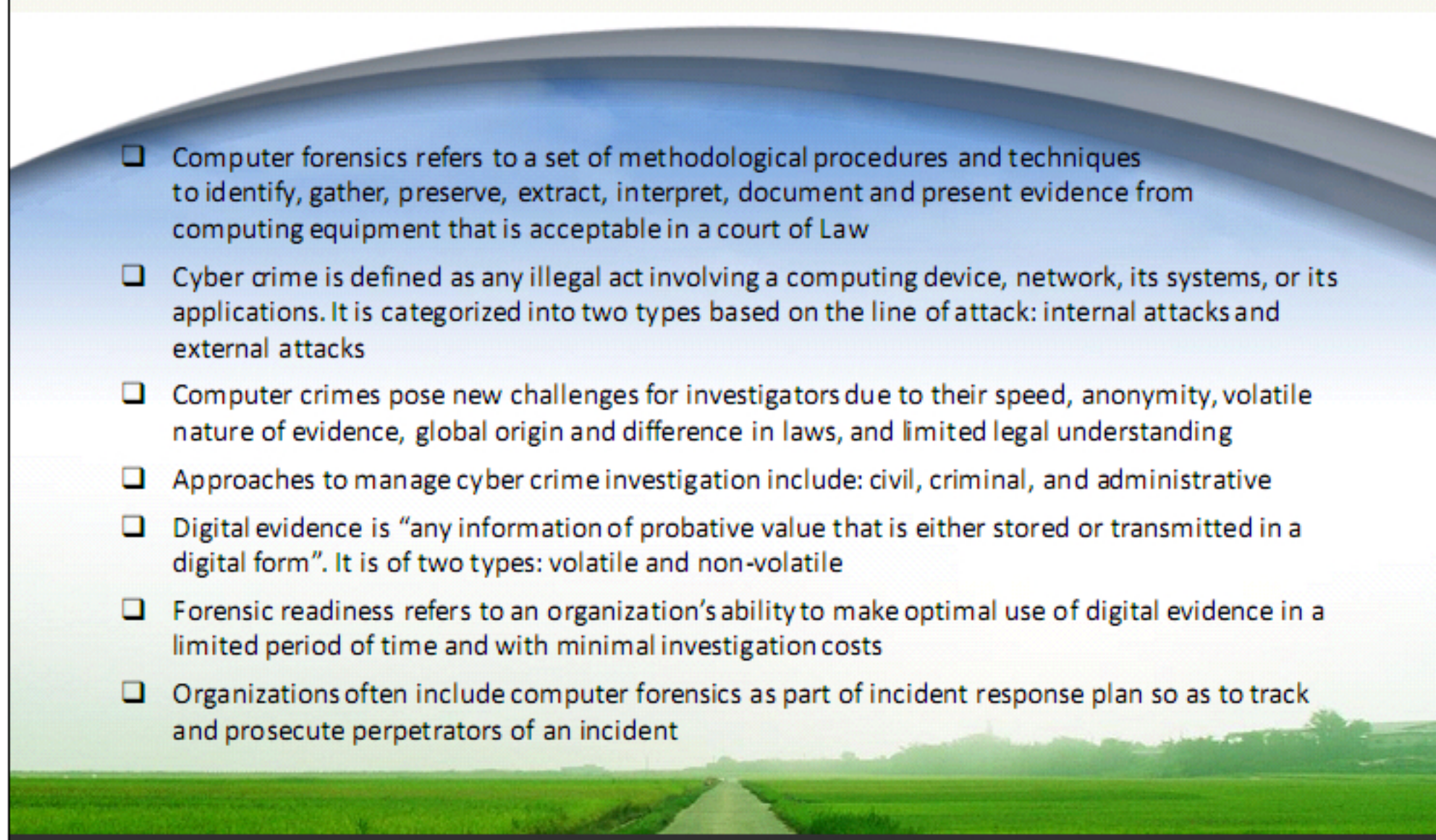
Join various discussion groups and associations to access resources regarding computer forensics

- 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In this module, you have learnt about the computer forensics, its processes and techniques, the devices involved, challenges for investigators, different types of cybercrimes, digital evidence and its types, and the process of keeping an individual or an organization forensic-ready. These topics will help you understand the forensic investigation process and other activities that can influence the process.