Mustansiriyah University

College of Science – Department of CS/Cybersecurity

By

Prof. DR. Bashar ALEsawi

Introduction To Digital Forensics

2023-2024/ 2nd – Semester

Digital Forensics: An Introduction

Digital Forensics is the application of scientific methods in preserving, recovering, and investigating digital evidence in a Digital crime scenario. It can be correctly defined as, collection, examination, analysis, and documentation by using scientifically proven methods to investigate a digital crime and present it before the court.

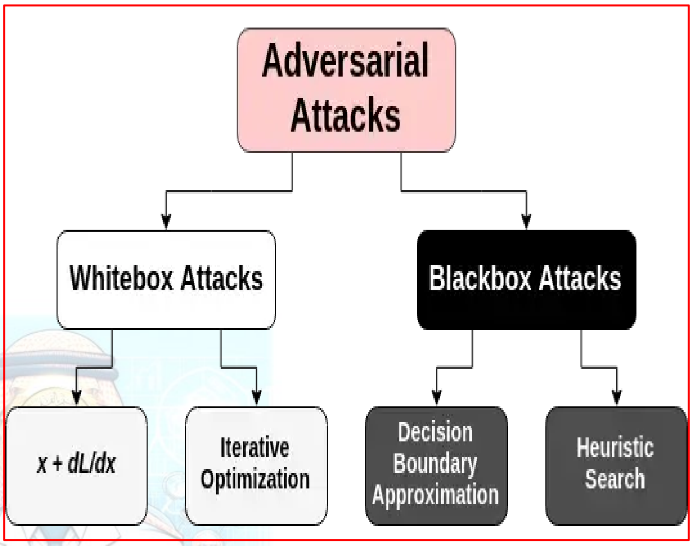
Table of Contents:

What is Digital Forensics?

Digital forensics is a branch of forensic science that uses scientific understanding to acquire, evaluate, record, and present digital evidence related to computer crime in court. The main goal is to ***figure out what happened, when it happened, and who did it***. These investigations include user laptops, computers, mobile phones, network devices, Webcams, tablets, camcorders, IoT and smart home devices, and storage media such as USB drives, CD/DVD, SD cards, and tapes, among other digital systems and devices that can send, receive, and store digital data.

Digital Forensics is also defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases. Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

- ***Data breaches, phishing, ransomware, DoS assaults, and SQL Injunctions*** are all examples of cyberattacks on digital systems that may be investigated using **Digital Forensics**.
- ***Cyberespionage*** or ***Adversarial assaults*** (لتجسس الإلكتروني أو الاعتداءات العدائية) that compromise accounts and services, unauthorized system and network access, or other associated cyberattacks that cause commercial or reputational harm are all included in this category.



https://www.labellerr.com/blog/what-are-adversarial-attacks-in-machine-learning-and-how-can-you-prevent-them/

Digital Forensics Goals:

The basic goal of digital forensics is to investigate crimes committed with computer systems that store and process digital data and to extract forensic' digital evidence to present in court. This is achieved in the following ways using digital forensics:

- Follow court-approved technological methods to preserve and recover evidence.
- Assigning responsibility for an activity to the person who initiated it.
- Determining data breaches inside a company.
- Identifying the extent of any damage that may occur as a result of a data breach.
- Compiling the findings into a formal report that may be submitted in court.
- Providing expert evidence in court as a guide.

- اتباع الأساليب التكنولوجية المعتمدة من قبل المحكمة لحفظ الأدلة واسترجاعها.
- إسناد مسؤولية النشاط إلى الشخص الذي تم تحديده.
- تحديد خروقات البيانات داخل الشركة.
- تحديد مدى أي ضرر قد يحدث نتيجة لخرق البيانات.
- تجميع النتائج في تقرير رسمي يمكن تقديمه إلى المحكمة.
- تقديم أدلة الخبراء في المحكمة كدليل.

Challenges faced by Digital Forensics

Here, are major challenges faced by the Digital Forensic:

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- Large amount of storage into Terabytes that makes investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

Defining Cybercrime (Digital Crime):

Any illegal activity carried out on a computer or via a computer network, such as the internet, is referred to as cybercrime.

&

وفقا لوزارة العدل الأمريكية،
يتم تعريف الجريمة
السيبرانية على أنها أي
سلوك غير قانوني يتم
القيام به ضد أو باستخدام
جهاز كمبيوتر أو شبكة
كمبيوتر.

According to the US Department of Justice, cybercrime is defined as any unlawful behavior done against or with the use of a computer or computer network. The fundamental motivation for cybercrime is financial gain (for example: spreading malware to steal access codes to bank accounts).

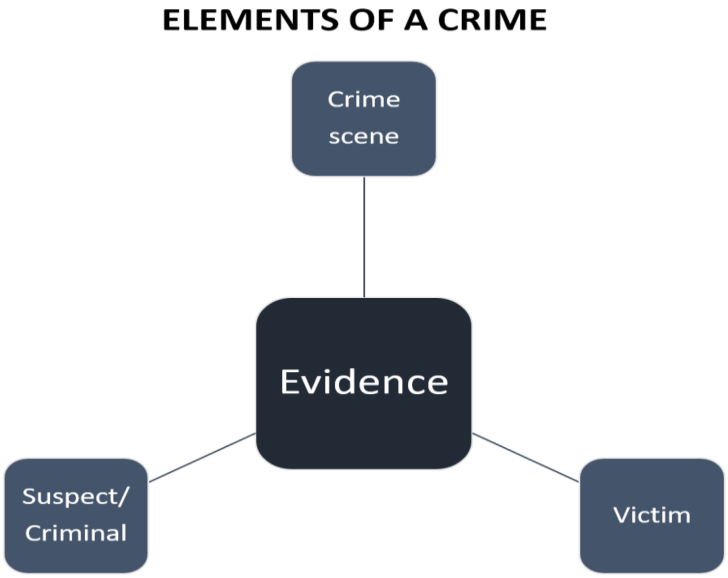
Sources of cybercrime

Insider threats and external attacks are the two primary sources of cybercrime.

- **Insider threats**: Since they might go unnoticed for a long period, this is the most significant cyber risk threatening enterprises today. Employees —or other persons working within the target company, such as former employees, third-party contractors, or business associates—with authorized access to the target organization’s computing systems and/or information about its cybersecurity procedures and defenses—commit insider attacks.
- **External attacks**: These attempts are typically carried out by skilled hackers who operate from outside the target company. These are the most typical types of cyberattacks against organizations all across the world. A black hat hacker may attempt to enter the target company’s networks from another country to get illicit access.

Elements of a Digital Crime

To prove a digital crime, as an investigator you should have the following elements to bring out a conclusion. All the elements will be related to one another in a more or so.



1) Digital Crime:

A digital crime scene refers to the virtual or electronic environment where a cybercrime or digital incident has occurred. It involves the collection, analysis, and preservation of digital evidence to investigate and understand the nature of the cybercrime. Digital crime scenes can include a wide range of scenarios, such as hacking, data breaches, computer intrusions, malware attacks, and other cybercrimes.

Key characteristics of a digital crime scene include:

1. **Virtual Nature:**
    - Unlike traditional crime scenes, digital crime scenes exist in the virtual world. They involve computer systems, networks, and digital devices where electronic evidence is stored.
2. **Data and Artifacts:**
    - Digital crime scenes contain electronic data and artifacts that can serve as evidence. This may include files, logs, system configurations, network traffic, and other digital traces left behind by cybercriminals.
3. **Dynamic Environment:**
    - Digital environments are dynamic and can change rapidly. Therefore, digital crime scene investigators must work efficiently to preserve and collect evidence before it is altered or compromised.
4. **Specialized Tools:**
    - Investigating digital crime scenes requires the use of specialized tools and techniques. Digital forensics tools help investigators collect, analyze, and preserve electronic evidence in a forensically sound manner.
5. **Remote Investigations:**
    - Digital crime scenes may involve remote systems and networks. Investigators may need to conduct remote forensic analysis or collaborate with entities across different geographical locations to gather evidence.
6. **Multidisciplinary Approach:**
    - Digital crime scene investigations often involve a multidisciplinary approach, combining expertise in computer science, cybersecurity, law enforcement, and legal procedures.
7. **Legal Considerations:**
    - Evidence collected from digital crime scenes must adhere to legal standards and be handled in a manner that ensures its admissibility in court. Chain of custody, proper documentation, and forensic best practices are crucial.

2) What is Victim:

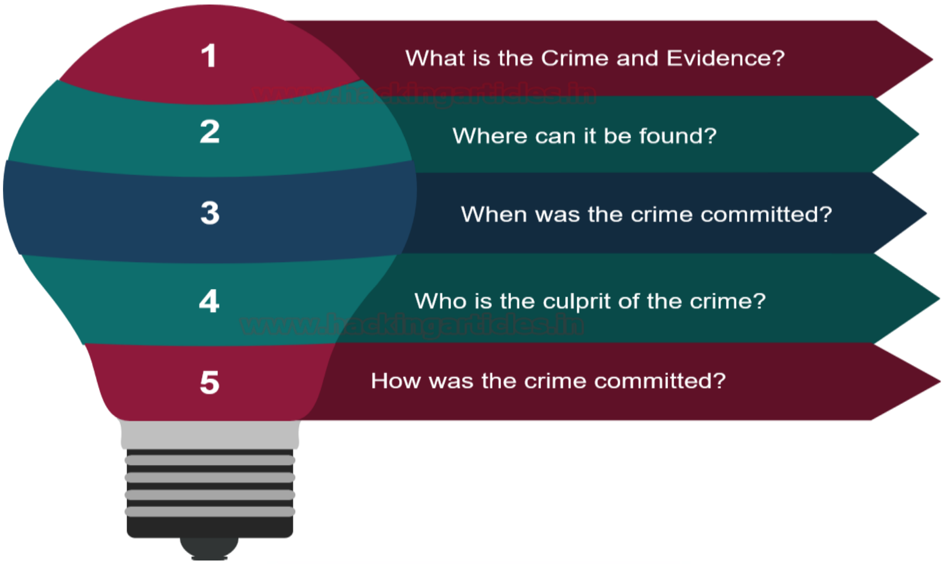
In digital forensics, a "victim" refers to an entity or individual that has experienced harm, damage, or compromise as a result of a cybercrime or digital incident. The term is used to describe the target or subject of the malicious activity, and the victim could be an individual, an organization, or even a system.

Key points related to victims in digital forensics include:

1. **Individuals or Organizations:**
   - Victims can be individuals who have had their personal information compromised or misused, or organizations that have suffered from cyberattacks such as data breaches, ransomware attacks, or other forms of digital crimes.
2. **Harm or Compromise:**
   - The harm or compromise experienced by the victim can take various forms, including unauthorized access to sensitive data, financial losses, disruption of services, reputation damage, or other negative impacts resulting from cyber incidents.
3. **Forensic Investigation:**
   - Digital forensic investigators work to uncover the details of cybercrimes and the impact on the victim. They analyze digital evidence to determine the extent of the compromise, identify the methods used by attackers, and gather information that can be used for attribution or legal action.
4. **Incident Response:**
   - In addition to forensic investigation, victims often engage in incident response activities to mitigate the impact of the cyber incident. This can include isolating affected systems, removing malware, restoring services, and implementing measures to prevent future incidents.
5. **Legal Considerations:**
   - Victims play a crucial role in legal proceedings related to cybercrimes. The evidence collected during digital forensic investigations is often used to build a case against perpetrators, and victims may be involved in legal actions or cooperate with law enforcement agencies.
6. **Notification and Communication:**
   - In cases of data breaches or other incidents involving personal information, victims may need to be notified about the breach. Effective communication with affected individuals or organizations is an essential aspect of handling digital incidents.

Goals of Digital Forensic Investigation

As a digital forensic investigator, you should have a goal for investigation. Depicted below are the five most important goals of investigation;

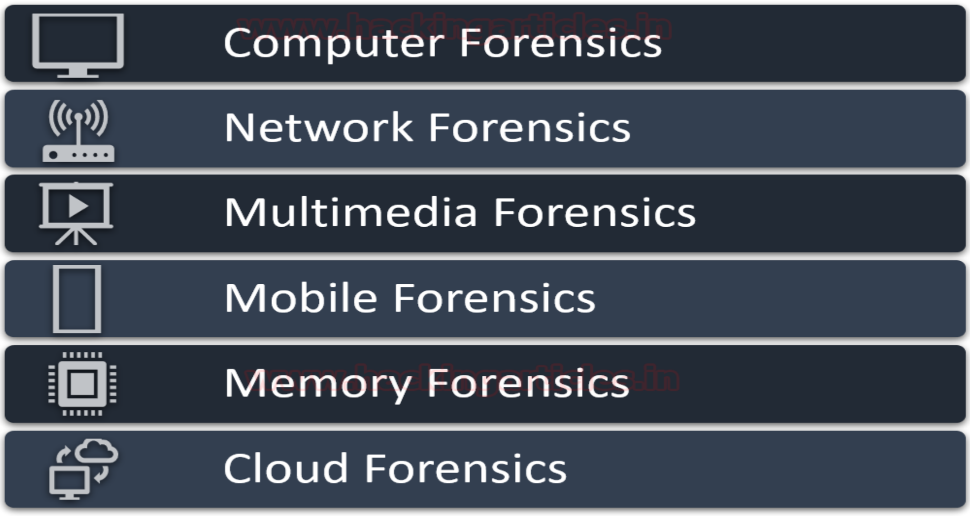

1
What is the Crime and Evidence?
2
Where can it be found?
3
When was the crime committed?
4
Who is the culprit of the crime?
5
How was the crime committed?

Classification of Digital Forensics

Digital forensics is a very broad term that has various classifications within it. The most popular forensic investigations are as follow:

1. **Computer Forensics:** It is the most primitive type of digital forensics which usually was introduced in the early evolution of computer systems. It includes investigating computers, laptops, logs, USB drives, hard drives, Operating systems, etc.
2. **Network Forensics:** It includes investigating by analyzing network events, intrusion, and data packets that were transmitted to detect network attacks.
3. **Multimedia Forensics:** It comprises of investigation of images, audio, and video files that are recovered as evidence in a digital crime scene.
4. **Mobile Forensics:** It comprises of investigation of smartphones like android, iOS, etc for finding digital evidence and recovering the deleted data important for the case.
5. **Memory Forensics:** It is the forensic investigation of the memory or ram dump of the system to find out volatile memory like chat history, clipboard history, browser history, etc.
6. **Cloud Forensics:** Considering the virtual storage are in demand, the investigation of the cloud environment also plays a key role in a digital crime scene for gathering evidence.

The classification of digital forensics isn't limited to the above diagram and as t can be classified into more depending on the cases.



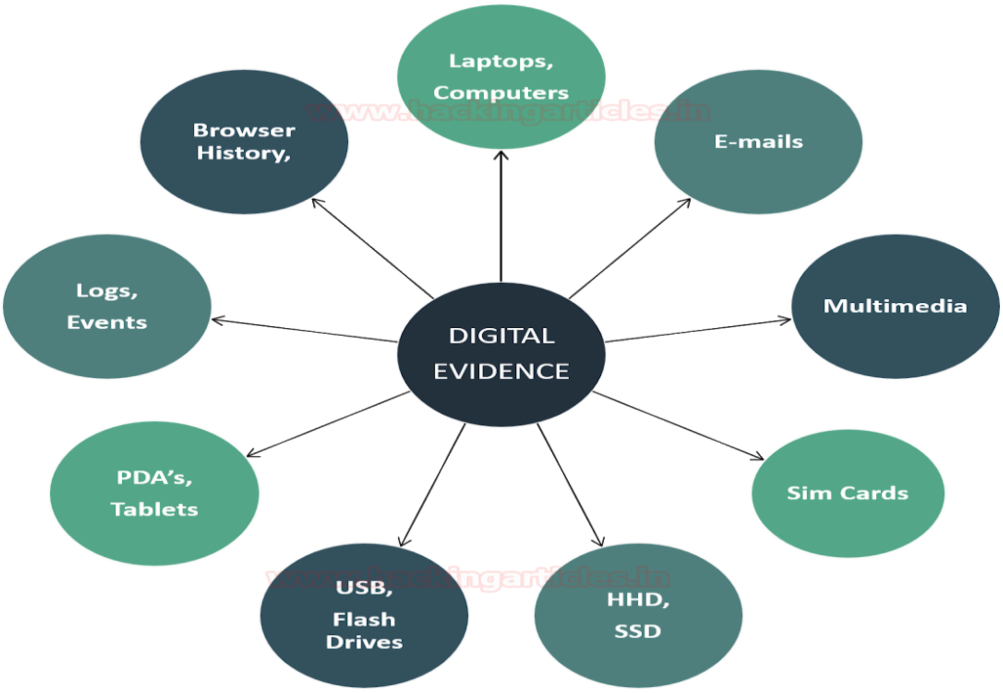
Digital Evidence

Digital evidence or electronic evidence can be defined as any object that stores digital information and transmits it in any form which was used in the act of crime or in supporting the investigation of the case in a trial before the court.

The evidence found at the crime scene should have two key properties

1. They should be admissible in the court
2. They should be authentic.

The ***digital evidence*** can be like of various types and should be availed ethically by following the prescribed guidelines of investigations. Here are a few digital evidences in the diagram below, but the list goes on.



Acquiring digital evidence:

It is a critical step in the digital forensic process. It involves gathering data from various sources, such as computers, mobile devices, storage media, and networks, while ensuring the preservation and integrity of the evidence. Here are some common methods of acquiring digital evidence:

1. Live acquisition: This method involves collecting data from a live or running system. It typically includes capturing volatile data such as running processes, network connections, and system information.

2. Disk imaging: Disk imaging involves creating a bit-for-bit copy or "image" of an entire storage device, such as a hard drive or solid-state drive (SSD). The imaging process ensures that all the data, including deleted or hidden files, is preserved.

3. File-level acquisition: In some cases, it may be necessary to acquire specific files or directories rather than imaging an entire storage device. This method allows for targeted collection of relevant files while reducing the amount of data to be processed. It is important to maintain the integrity of the files and document their metadata, such as timestamps and permissions.

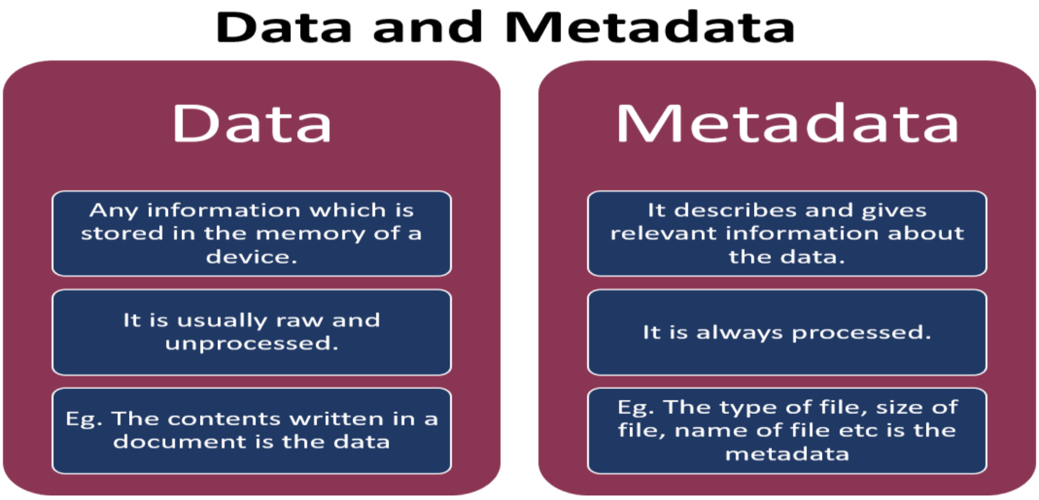
4. Mobile device acquisition: Mobile devices such as smartphones and tablets often contain valuable evidence. Specialized tools and techniques are used to acquire data from these devices. Depending on the device and its security features, acquisition methods can vary and may include logical acquisition (extracting data through the device's operating system) or physical acquisition (acquiring a bit-by-bit image of the device's storage).

5. Network traffic capture: In cases involving network-related investigations, capturing and analyzing network traffic can provide valuable evidence. This can be done using packet capture tools or network monitoring software. It allows the examiner to analyze communication patterns, identify suspicious activities, and extract relevant data from network packets.

6. Cloud-based data acquisition: With the increasing use of cloud services, it may be necessary to acquire data stored in the cloud for forensic analysis. Cloud service providers often offer APIs or tools that enable legal and authorized access to user data. The acquisition process may involve requesting data from the cloud provider or using specialized tools to extract data from cloud backups or synchronized devices.

Understanding Data and Metadata

The difference between the data and the metadata for the forensic investigation can be easily understood with the help of the diagram below;



Data and Metadata

Data

Any information which is stored in the memory of a device.

It is usually raw and unprocessed.

Eg. The contents written in a document is the data

Metadata

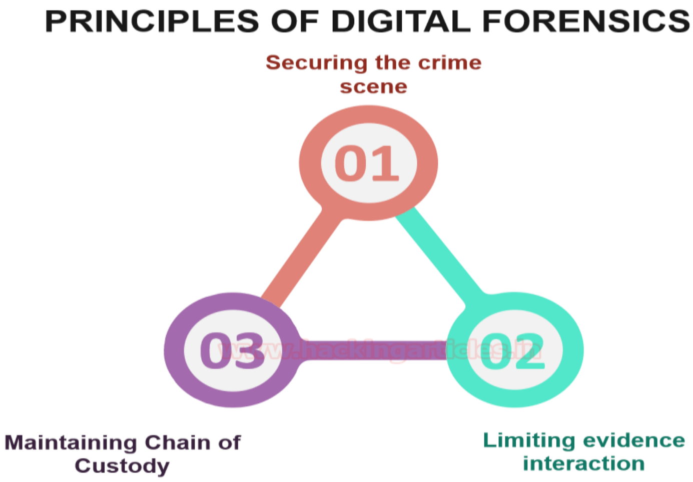
It describes and gives relevant information about the data.

It is always processed.

Eg. The type of file, size of file, name of file etc is the metadata

Principles of Digital Forensics

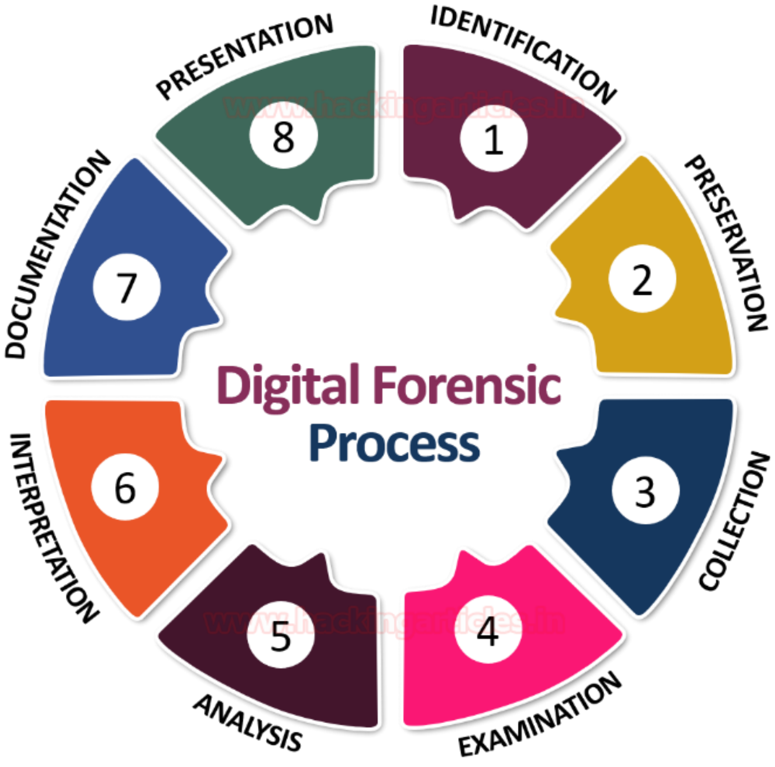
1. **Securing the Crime Scene:** This is the most primary principle of Digital Forensics. As an investigator you should prohibit any access to your suspected digital evidence, document all processes and connections, disconnecting wireless connections, etc. to keep your evidence secure.
2. **Limiting evidence Interaction:** As an investigator, you should make sure that your evidence is having a limited interaction by capturing the ram and can also perform cold boot attacks on the evidence.
3. **Maintaining Chain of Custody:** Chain of custody is a record of sequence in which the evidence was collected, date and timestamps at the collection, the investigator who accessed and handled it, etc.



PRINCIPLES OF DIGITAL FORENSICS
Securing the crime scene
01
02
03
Maintaining Chain of Custody
Limiting evidence interaction

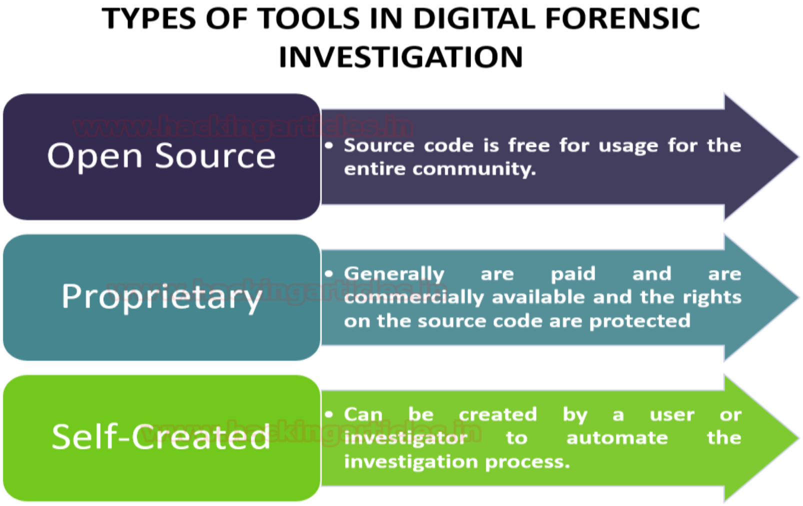
Process of Digital Forensic Investigation

1. **Identification:** This is the first step that an investigator takes at the crime scene is to identify the purpose of the investigation and recognize the potential digital evidence. (ماهو الغرض من التحقيق وما هي الأدلة الرقمية المتوفرة).
2. **Preservation:** This is the next step where the investigator has to be careful as he should make sure that the evidence has not tampered which may complicate the investigation (التأكد من عدم التلاعب بالأدلة).
3. **Collection:** This step involves acquiring the evidence most appropriately without causing any harm to the evidence and packing it in a Faraday Bag. (جمع الأدلة دون التأثير عليها ووصعها في حقيبة لهذا الغرض تسمى فاراداي).
4. **Examination:** This step is a precursor to performing any analysis of the evidence. This step requires careful inspection of the evidence for any other secondary details. (يتظمن الفحص خطوة سابقة للتحليل لغرض الحصول على ادلة فرعية من الرئيسية).
5. **Analysis:** In this step, the investigator carries out the most crucial things like joining the bits and pieces of the pieces of evidence, retrieving deleted files, etc. (في هذه الخطوة ، يقوم المحقق بتنفيذ أهم الأشياء مثل ضم أجزاء وأجزاء من الأدلة ، واسترداد الملفات المحذوفة).
6. **Interpretation:** This step involves concluding the investigation finding after reconstruction of the crime scene. (تتضمن هذه الخطوة الانتهاء من نتائج التحقيق بعد إعادة بناء مسرح الجريمة).
7. **Documentation:** usually involves preparing a detailed report or a document on the entire investigation. (تتضمن هذه الخطوة عادة إعداد تقرير مفصل أو وثيقة عن التحقيق بأكمله).
8. **Presentation:** mandatory step only when it is asked for cross-examination which is to be mentioned in very simple terms of understanding for commoners. (هذه خطوة إلزامية فقط عندما يطلب منها الاستجواب الذي يجب ذكره بعبارات فهم بسيط للغاية لعامة الناس).



Types of Tools

An investigator needs to have the right set of tools for conducting a digital forensic investigation. It is for the investigator to decide the tool appropriate for the case. The tools also depend on the application based on hardware and software. The types of tools can be classified into three types; Open Source, Proprietary, and Self-created.


TYPES OF TOOLS IN DIGITAL FORENSIC INVESTIGATION
Open Source
• Source code is free for usage for the entire community.
Proprietary
• Generally are paid and are commercially available and the rights on the source code are protected
Self-Created
• Can be created by a user or investigator to automate the investigation process.

Here's a brief overview of the three types of tools you mentioned:

Open Source Tools

Open Source tools are freely available and can be modified by anyone. They are often developed by a community of users and developers. Examples include:

- **Autopsy**: A digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools.
- **Wireshark**: A network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network.

Proprietary Tools

Proprietary tools are owned by a company and require a purchase or subscription. They often come with customer support and regular updates. Examples include:

- **EnCase**: Provides an end-to-end solution covering forensic acquisition to reporting.
- **AccessData FTK**: A court-cited digital investigations platform built for speed, stability, and ease of use.

Self-Created Tools

Self-Created tools are developed in-house for specific needs that may not be met by existing open source or proprietary tools. These are tailored to the unique requirements of the investigation and can be:

- Scripts written in Python or another language to automate certain tasks.
- Custom applications designed to interact with unique systems or proprietary hardware.

Each type of tool has its own advantages and disadvantages.

Open source tools are cost-effective and highly customizable, but may lack dedicated support. Proprietary tools often come with robust features and support, but can be expensive. Self-created tools offer the most customization and integration into existing systems but require development time and expertise.

In practice, an investigator might use a combination of these tools.

For instance, they might use an open source tool like Wireshark to capture network traffic, a proprietary tool like EnCase for deep analysis, and a self-created script to automate the extraction of specific data types.

The choice of tools is indeed a critical decision for the investigator and should be guided by the nature of the investigation, the types of data involved, and legal considerations.

إن اختيار الأدوات هو في الواقع قرار حاسم بالنسبة للمحقق ويجب أن يسترشد بطبيعة التحقيق وأنواع البيانات المعنية والاعتبارات القانونية.

Autopsy Platform

Autopsy is a widely recognized open-source digital forensics platform. It's a graphical interface to The Sleuth Kit® and other digital forensics tools, used by law enforcement, military, and corporate examiners to investigate what happened on a computer[1]. Here are some key features and considerations for using Autopsy:

Key Features:

- **Modular Architecture**: Allows users to add new functionalities through plugins and modules.
- **File System Analysis**: Supports analysis of various file systems, including NTFS, FAT, exFAT, HFS+, and ext2/3/4.
- **Timeline Analysis**: Helps in understanding the timing of file activities.
- **Keyword Searching**: Facilitates finding specific information within the data.
- **Web Artifacts**: Extracts web browsing data to help understand user activities.
- **Registry Analysis**: Analyzes Windows registry files to extract valuable information.
- **Email Analysis**: Recovers and analyzes emails from different clients.

Considerations:

- **Training**: While Autopsy is user-friendly, proper training can maximize efficiency.
- **Community Support**: Being open-source, it has a community for support, but it might not be as immediate as proprietary tools.
- **Legal Admissibility**: The use of Autopsy in investigations should comply with legal standards to ensure evidence is admissible in court.

Autopsy is designed to be fast, thorough, and efficient, evolving with the needs of digital forensic investigators. It's free to download and use, making it an accessible tool for professionals and students alike. For more detailed information or to download Autopsy, you can visit their official website[1].

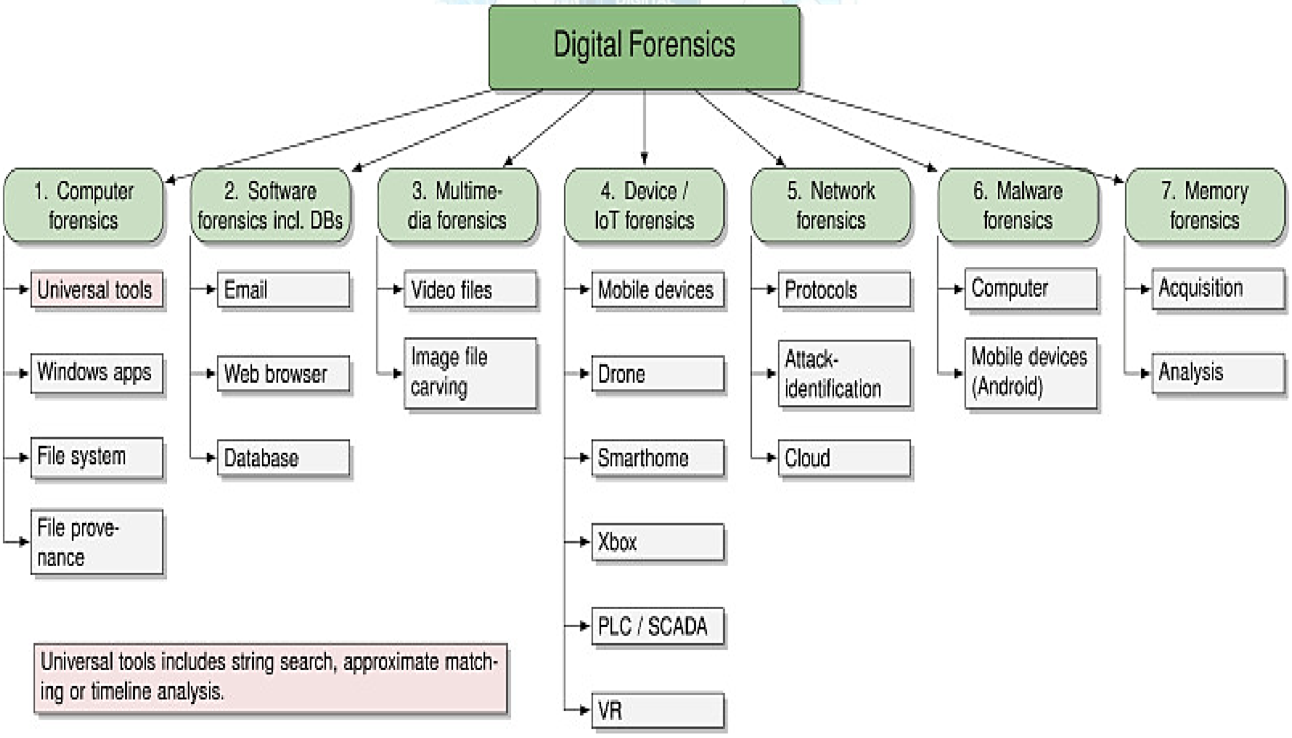
There are several example cases and tutorials on Autopsy available on YouTube. Here are a couple of notable ones:

- "Starting a New Digital Forensic Investigation Case in Autopsy 4.19+" provides a mini-course on how to use Autopsy, including setting up a new case[1].
- "Digital Forensic Investigation Case with Autopsy 4.20 | Case # 1 - 2023" is a video that delves into a forensic investigation using Autopsy, showcasing its capabilities in analyzing digital evidence[2].

Other Open-Source Platforms Forensic Tools:

Open-source forensic tools are essential for conducting digital investigations and are available for free. They can be used for various purposes such as data acquisition, analysis, and reporting. Here are some key open-source tools:

- **Wireshark**: A network protocol analyzer for capturing and analyzing network traffic.
- **The Sleuth Kit (TSK)**: A library for analyzing disk images and recovering data.
- **Volatility**: An advanced memory forensics framework.
- **CAINE**: A complete forensic environment that integrates existing software tools.
- **GRR**: A live forensics tool for remote incident management.
- **Plaso**: A tool for extracting timelines from various sources.
- **DEFT**: A Linux distribution for forensic analysis with a wide range of tools.
- **ExifTool**: For reading, writing, and manipulating metadata.



Windows / Mac / Linux Forensics

Digital forensics on Windows, Mac, and Linux involves specialized techniques and tools tailored to the unique file systems and features of these operating systems. Here's a brief overview:

Windows Forensics

- **File Systems**: FAT, exFAT, NTFS, and ReFS.
- **Key Locations**: Recycle Bin, Registry, Event Logs, Prefetch files, and more.
- **Tools**: EnCase, FTK, and proprietary as well as open-source tools like Autopsy.

File systems are essential for storing and organizing data on storage devices. Here's a brief overview of the file systems you mentioned:

- **FAT (File Allocation Table)**: An older file system, simple and widely compatible, but with limitations in file size and partition capacity[1].
- **exFAT (Extended File Allocation Table)**: Designed for flash storage, exFAT supports larger files than FAT32 without the overhead of NTFS, making it ideal for USB drives and SD cards[1].
- **NTFS (New Technology File System)**: The standard file system for Windows, NTFS supports large volumes, file permissions, and encryption. It's more robust and feature-rich compared to FAT and exFAT[12].
- **ReFS (Resilient File System)**: Designed for data centers and enterprise environments, ReFS focuses on data resilience, high availability, and scalability

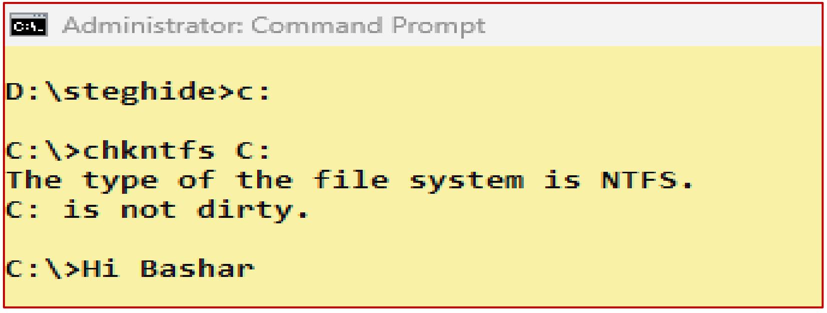
Is there a cmd command to investigate NTFS in windows

There are several CMD you can use to investigate NTFS file systems in windows:

- **chkntfs:** This command can check the NTFS file system and modify the behavior of the automatic system file checking at boot time1.
- **fsutil:** A versatile command to perform tasks related to NTFS, such as managing reparse points, sparse files, and quotas.
- **Get-Acl:** While not a CMD command, it's a PowerShell cmdlet that can be used to get the Access Control List (ACL) for files and folders to check NTFS permissions2. In CMD (cacls OR icacls).

For example, to use chkntfs to check the NTFS file system on the C: drive, you would open Command Prompt as an administrator and enter:

chkntfs C:



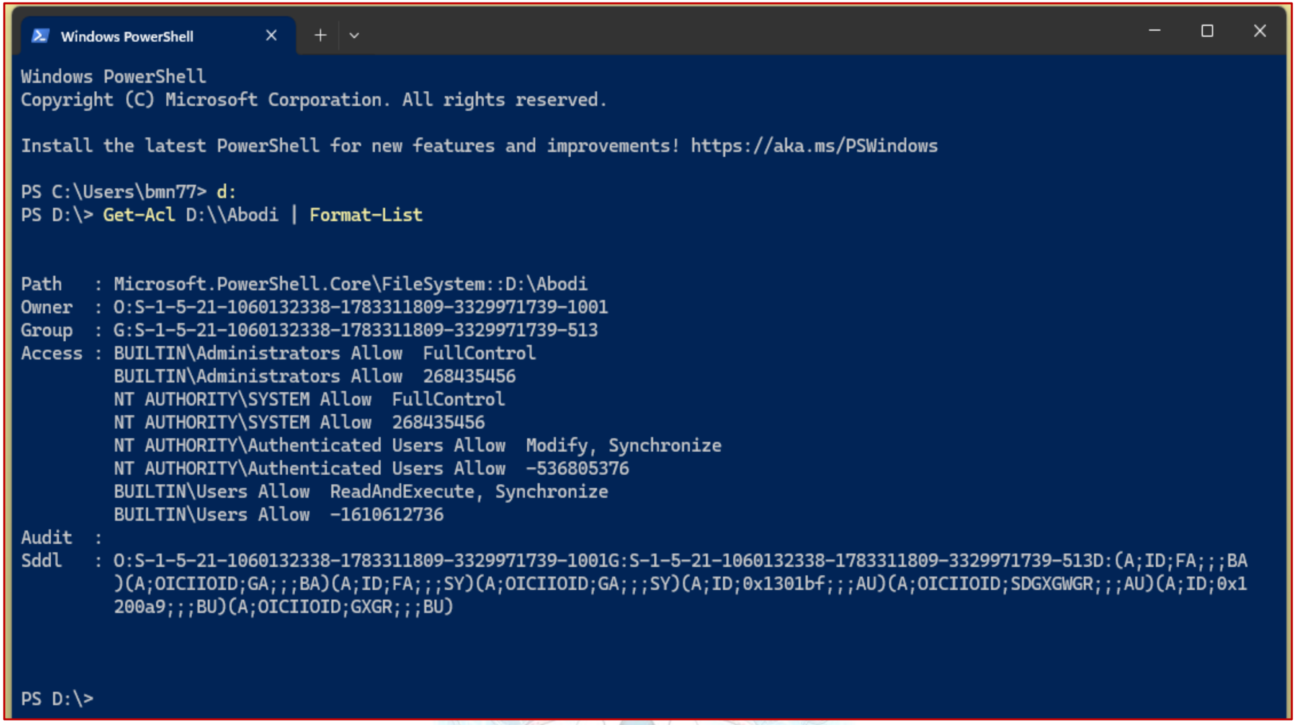
Administrator: Command Prompt

```
D:\steghide>c:

C:\>chkntfs C:
The type of the file system is NTFS.
C: is not dirty.

C:\>Hi Bashar
```

To use Get-Acl in PowerShell to check the permissions of a folder, you would enter:

```
Get-Acl D:\\"Your Folder Name" | Format-List
Get-Acl D:\\Abodi | Format-List
```

Replace "Your Folder Name" with the actual name of your folder. If the folder name contains spaces, enclose it in quotes.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\bmn77> d:
PS D:\> Get-Acl D:\\Abodi | Format-List


Path   : Microsoft.PowerShell.Core\FileSystem::D:\Abodi
Owner  : O:S-1-5-21-1060132338-1783311809-3329971739-1001
Group  : G:S-1-5-21-1060132338-1783311809-3329971739-513
Access : BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         NT AUTHORITY\Authenticated Users Allow  Modify, Synchronize
         NT AUTHORITY\Authenticated Users Allow  -536805376
         BUILTIN\Users Allow  ReadAndExecute, Synchronize
         BUILTIN\Users Allow  -1610612736
Audit  :
Sddl   : O:S-1-5-21-1060132338-1783311809-3329971739-1001G:S-1-5-21-1060132338-1783311809-3329971739-513D:(A;ID;FA;;;BA
         )(A;OICIIOID;GA;;;BA)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;0x1301bf;;;AU)(A;OICIIOID;SDGXGWGR;;;AU)(A;ID;0x1
         200a9;;;BU)(A;OICIIOID;GXGR;;;BU)



PS D:\>
```

Mac Forensics

- **File Systems**: HFS+, APFS.
- **Key Locations**: Trash, Spotlight database, Time Machine backups, and plist files.
- **Tools**: BlackBag Technologies' MacQuisition, Cellebrite, and open-source tools like Sleuth Kit.

Linux Forensics

- **File Systems**: Ext2/3/4, XFS, Btrfs.
- **Key Locations**: /var/log directory, /home directory, and more.
- **Tools**: CAINE, DEFT, and other Linux-based live CDs that provide a suite of forensic tools.

Each operating system requires a different approach to forensic analysis due to its unique structure and operation

Introduction to Programming for Digital Forensics

Digital Forensics is a field that involves the recovery and investigation of material found in digital devices, often in relation to computer crime. Python is a powerful tool in this domain due to its simplicity and the vast array of libraries available for various forensic tasks.

Example 1: Hash Function for Data Integrity

One of the core aspects of digital forensics is ensuring the integrity of data. Python's `hashlib` library can be used to create a hash of files, ensuring they have not been altered.

```
import hashlib

def generate_hash(file_path):
    with open(file_path, 'rb') as file:
        file_content = file.read()
        return hashlib.sha256(file_content).hexdigest()

# Usage
file_hash = generate_hash('example_file.txt')
print(f'The SHA-256 hash of the file is: {file_hash}')
```

This script reads a file in binary mode and generates a SHA-256 hash of its contents, which can be used to verify its integrity at any point in time.

Example 2: Extracting Metadata from Images

Images often contain metadata that can provide valuable information during an investigation. The `Pillow` library can be used to extract such metadata.

```
from PIL import Image
from PIL.ExifTags import TAGS

def extract_metadata(image_path):
    image = Image.open(image_path)
    exif_data = {
        TAGS[key]: value
        for key, value in image._getexif().items()
        if key in TAGS
    }
    return exif_data

# Usage
metadata = extract_metadata('example_image.jpg')
print(metadata)
```

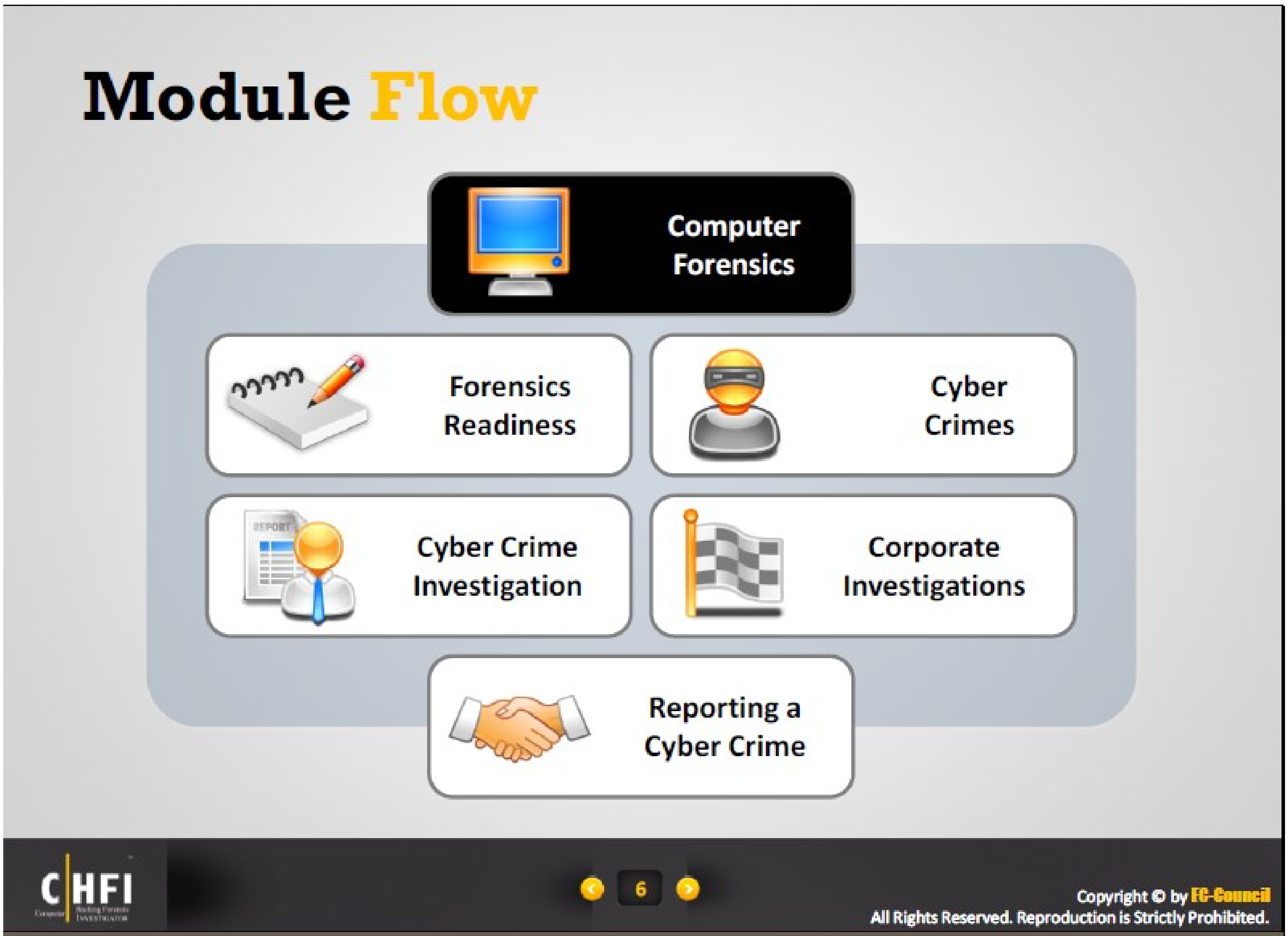
This function opens an image and extracts its EXIF metadata, which can include data like the camera model, date taken, GPS coordinates, and more.

Example 3: Analyzing Network Traffic

Network traffic analysis is crucial for identifying malicious activities. Python’s `scapy` library can be used to capture and analyze packets.

```
from scapy.all import sniff

def packet_callback(packet):
    print(packet.show())

# Start sniffing the network
sniff(prn=packet_callback, count=10)
```

This script uses `scapy` to sniff the network and prints out the first 10 packets, allowing for further analysis of the traffic.



Module Flow

Computer Forensics

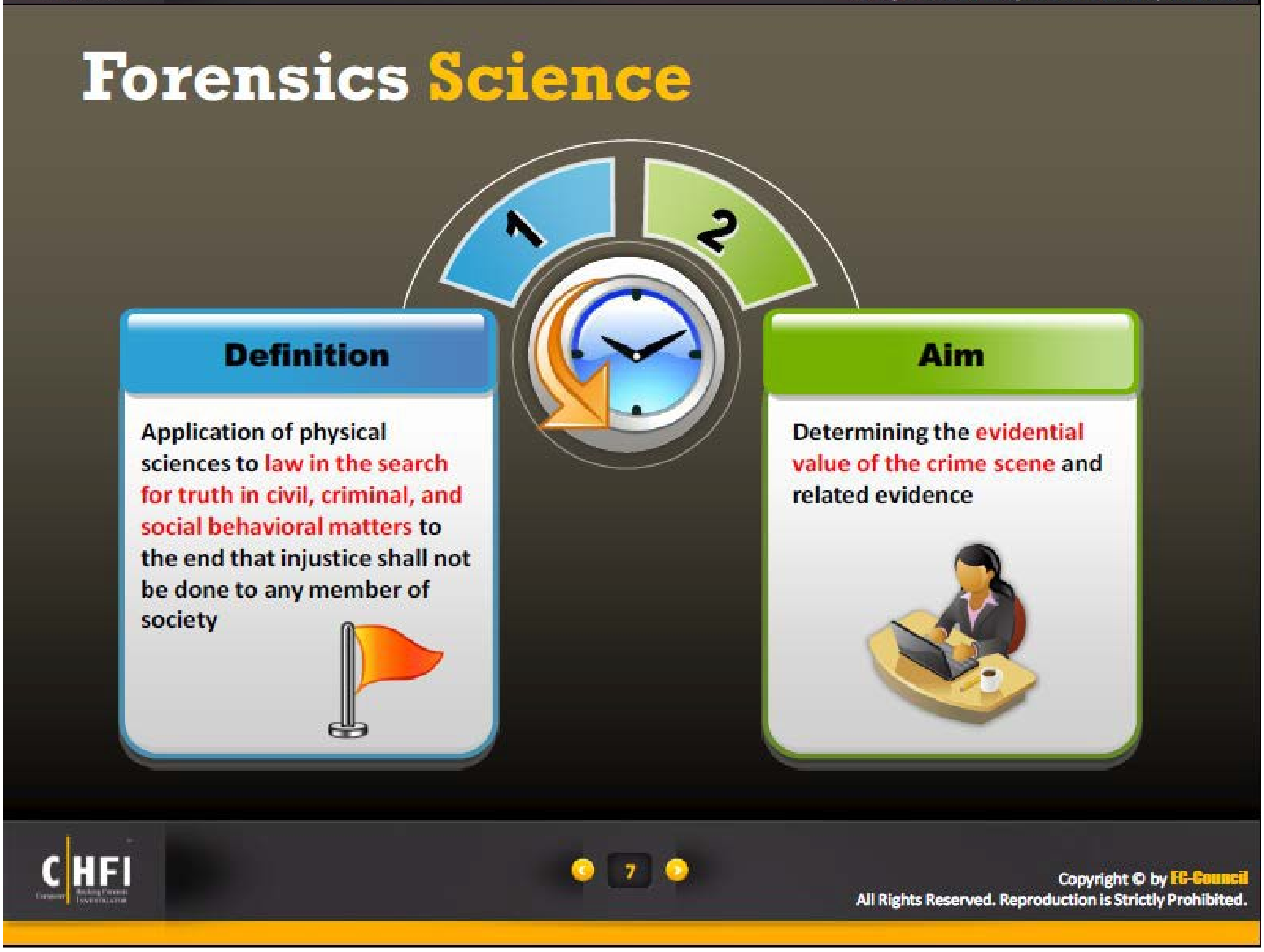
Forensics Readiness

Cyber Crimes

Cyber Crime Investigation

Corporate Investigations

Reporting a Cyber Crime



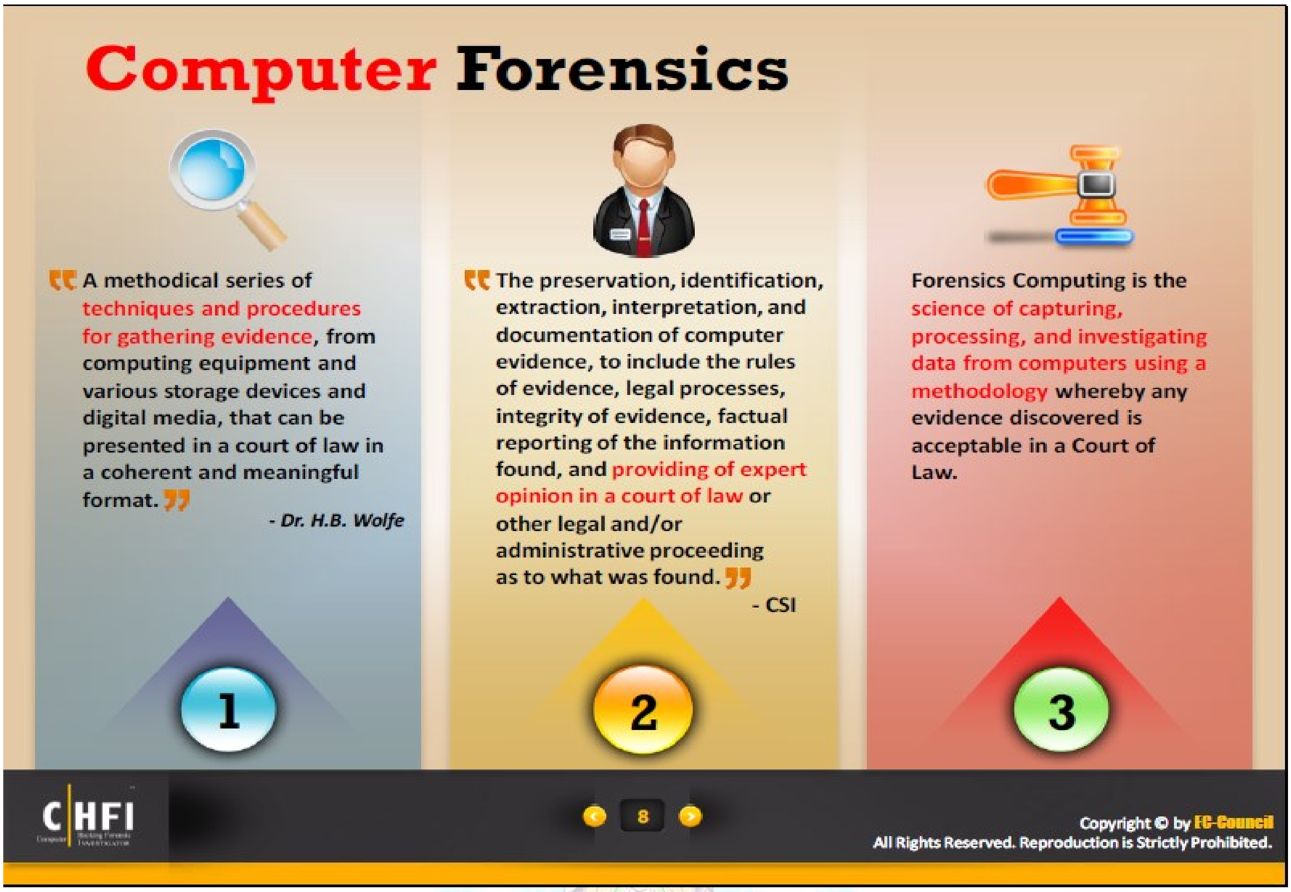
Forensics Science

Definition

Application of physical sciences to law in the search for truth in civil, criminal, and social behavioral matters to the end that injustice shall not be done to any member of society

Aim

Determining the evidential value of the crime scene and related evidence



Computer Forensics

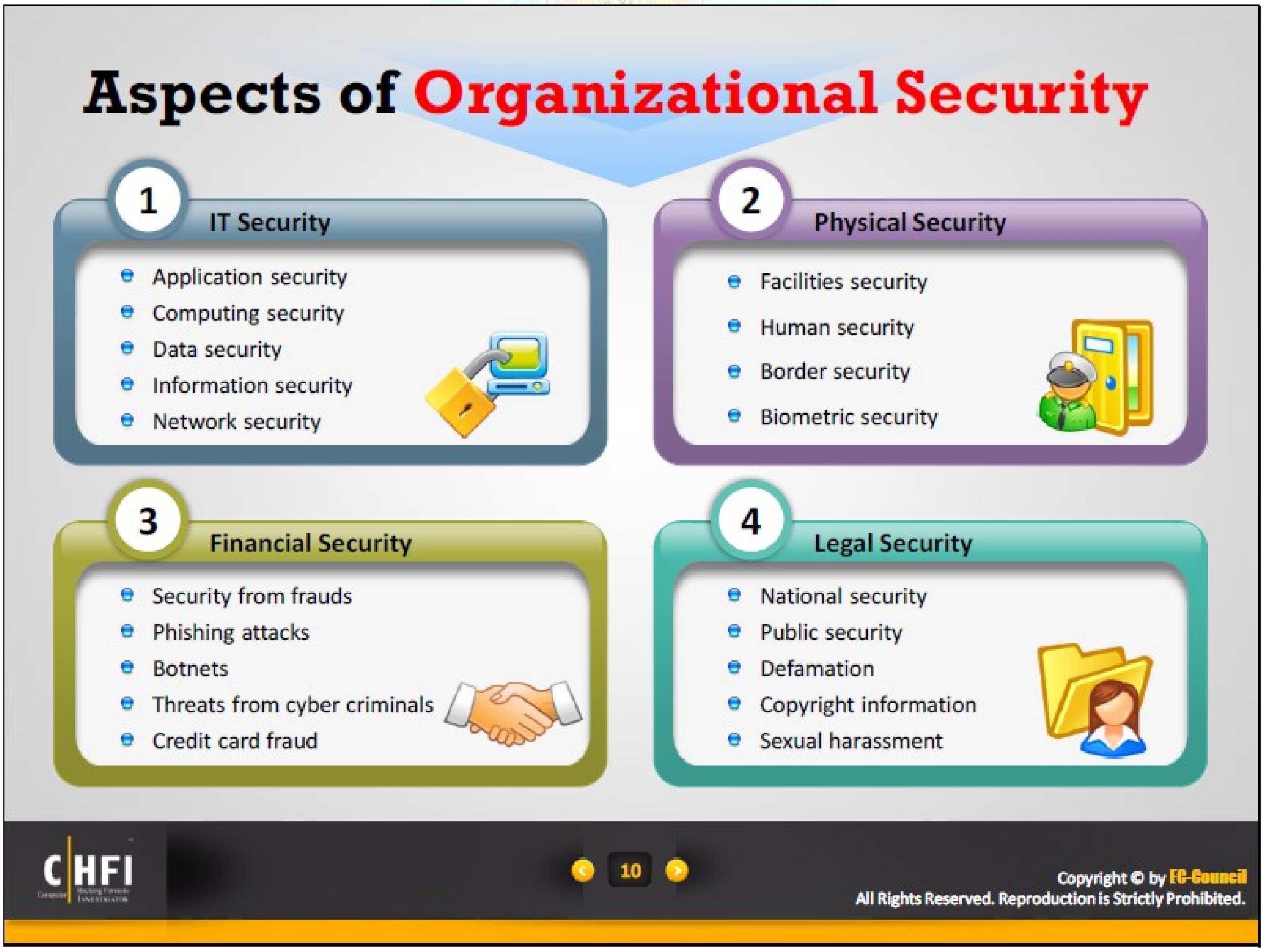
1. "A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format."

   - Dr. H.B. Wolfe

2. "The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing of expert opinion in a court of law or other legal and/or administrative proceeding as to what was found."

   - CSI

3. Forensics Computing is the science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law.



Aspects of Organizational Security

1 IT Security

- Application security
- Computing security
- Data security
- Information security
- Network security

2 Physical Security

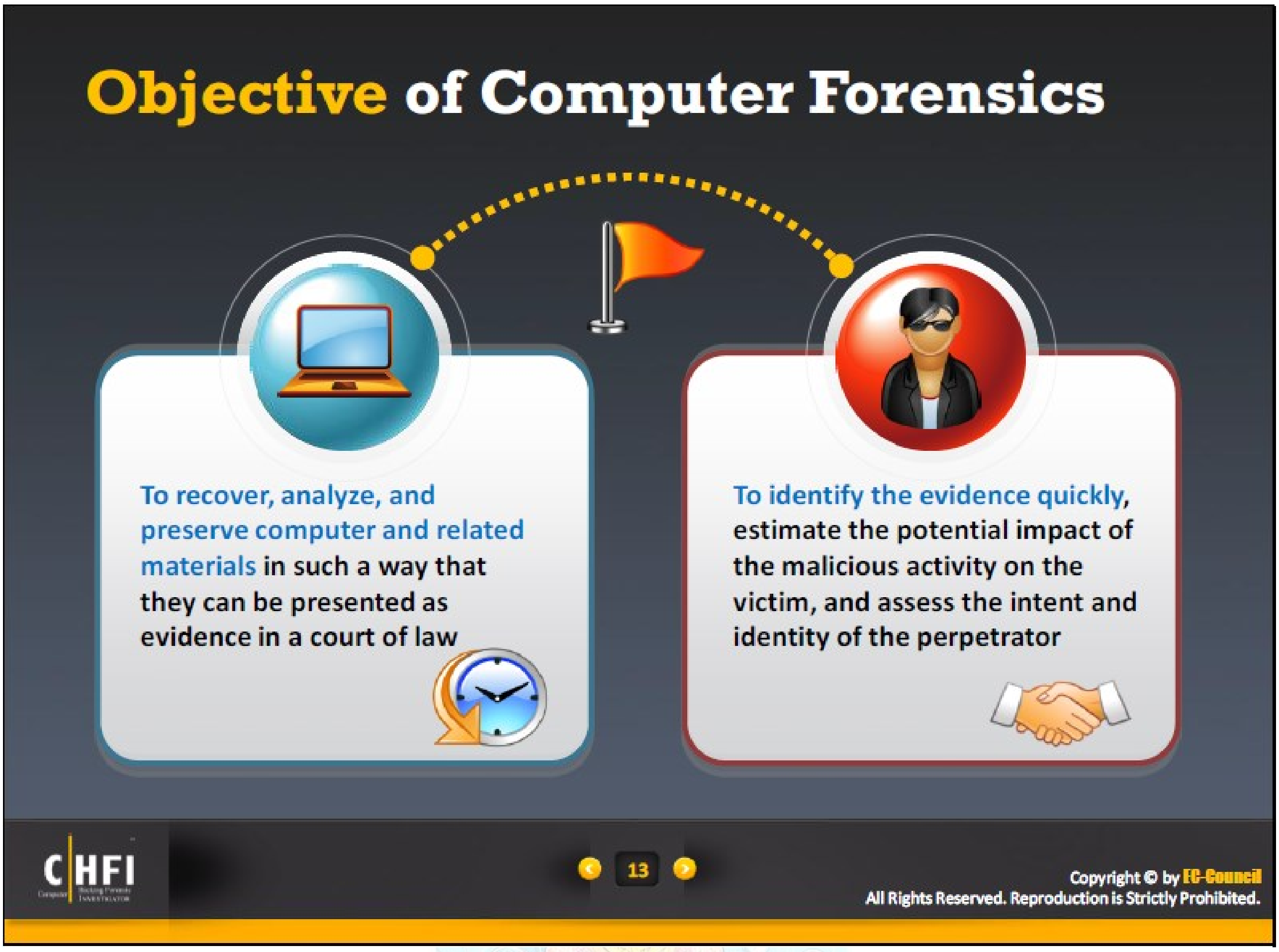
- Facilities security
- Human security
- Border security
- Biometric security

3 Financial Security

- Security from frauds
- Phishing attacks
- Botnets
- Threats from cyber criminals
- Credit card fraud

4 Legal Security

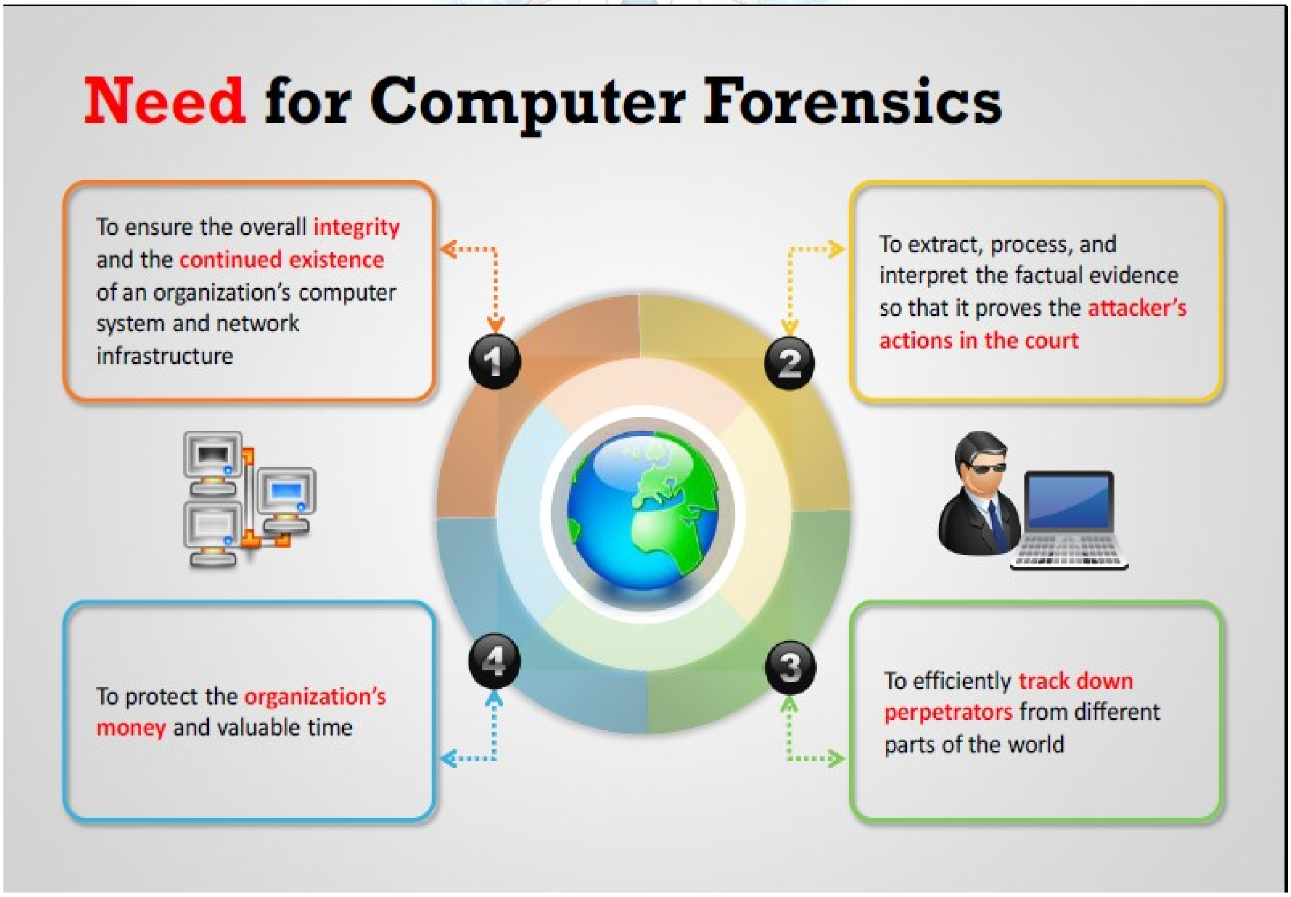
- National security
- Public security
- Defamation
- Copyright information
- Sexual harassment



Objective of Computer Forensics

To recover, analyze, and preserve computer and related materials in such a way that they can be presented as evidence in a court of law

To identify the evidence quickly, estimate the potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator



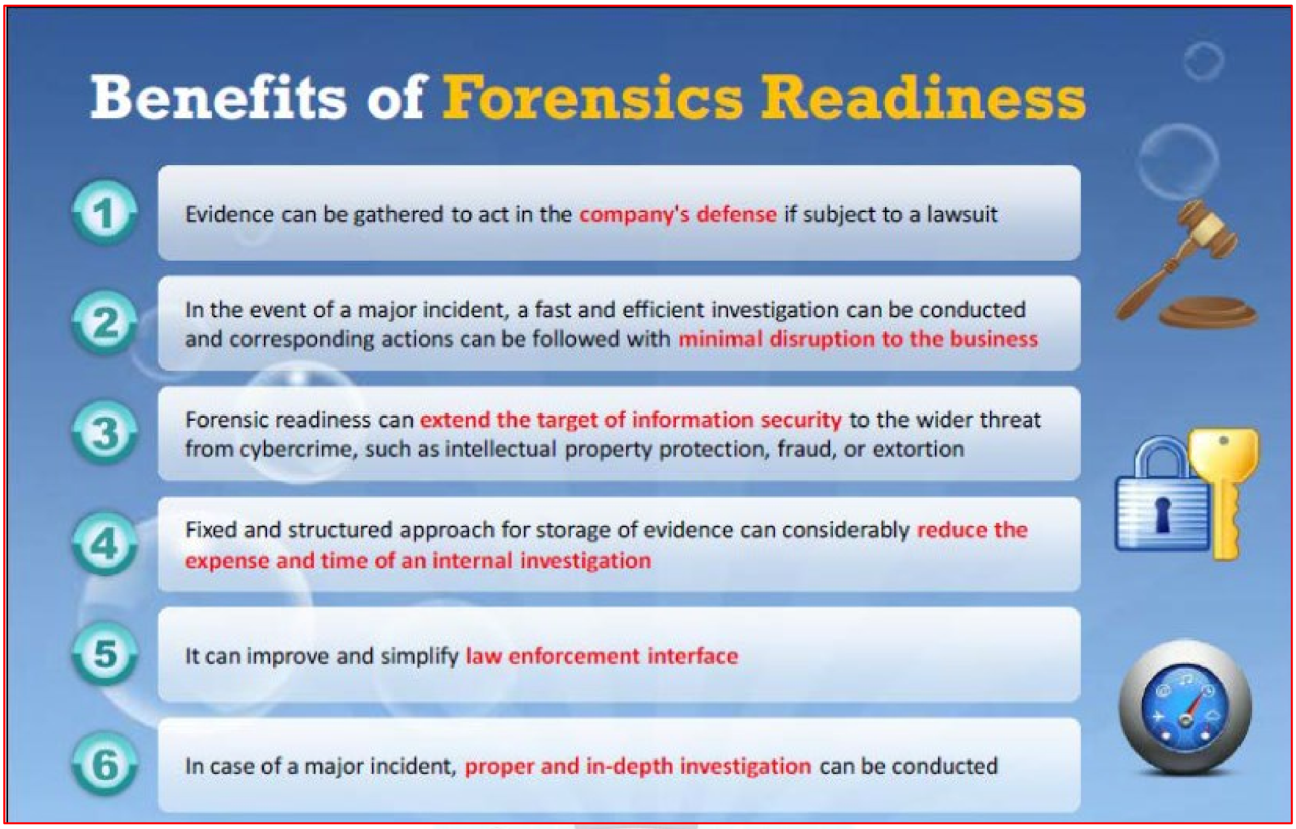
Need for Computer Forensics

1. To ensure the overall integrity and the continued existence of an organization's computer system and network infrastructure

2. To extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

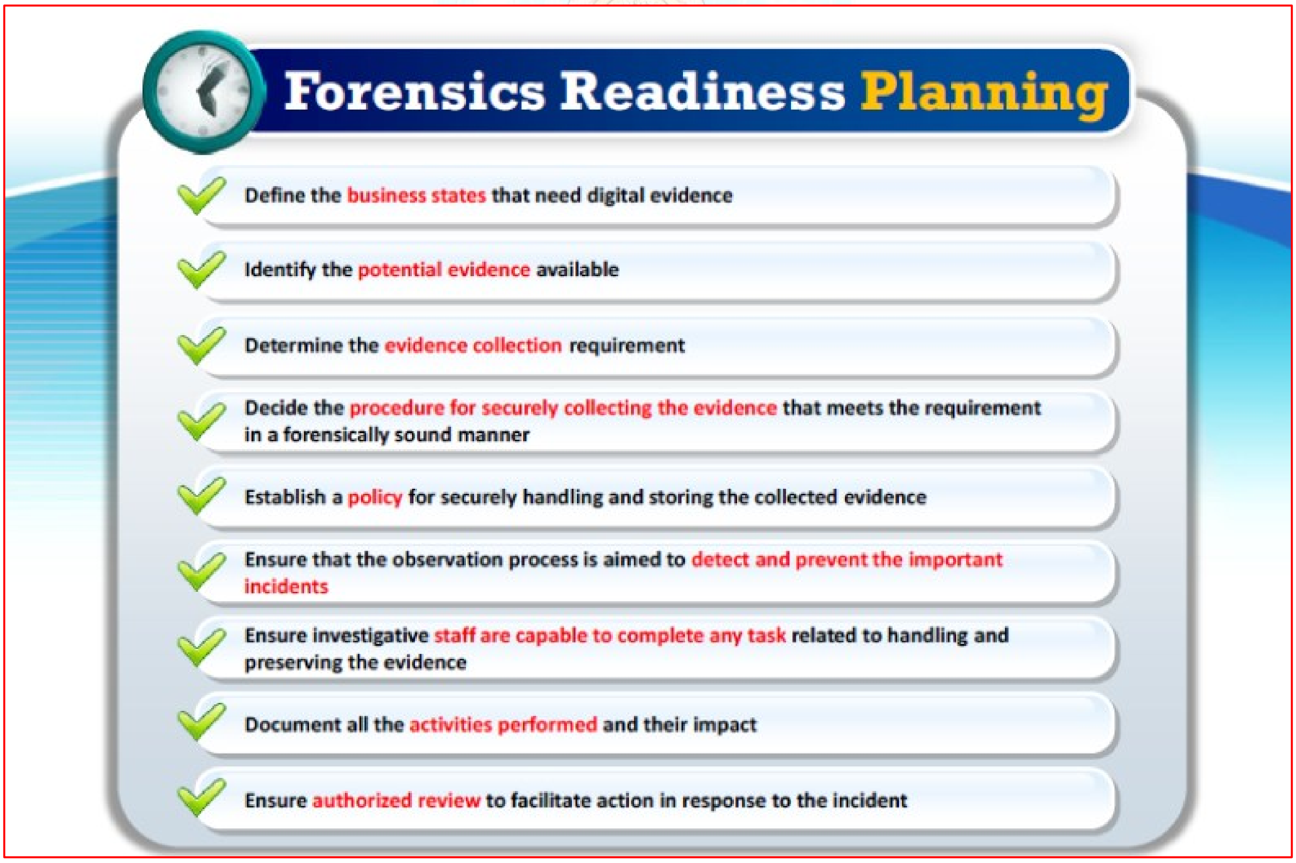
3. To efficiently track down perpetrators from different parts of the world

4. To protect the organization's money and valuable time



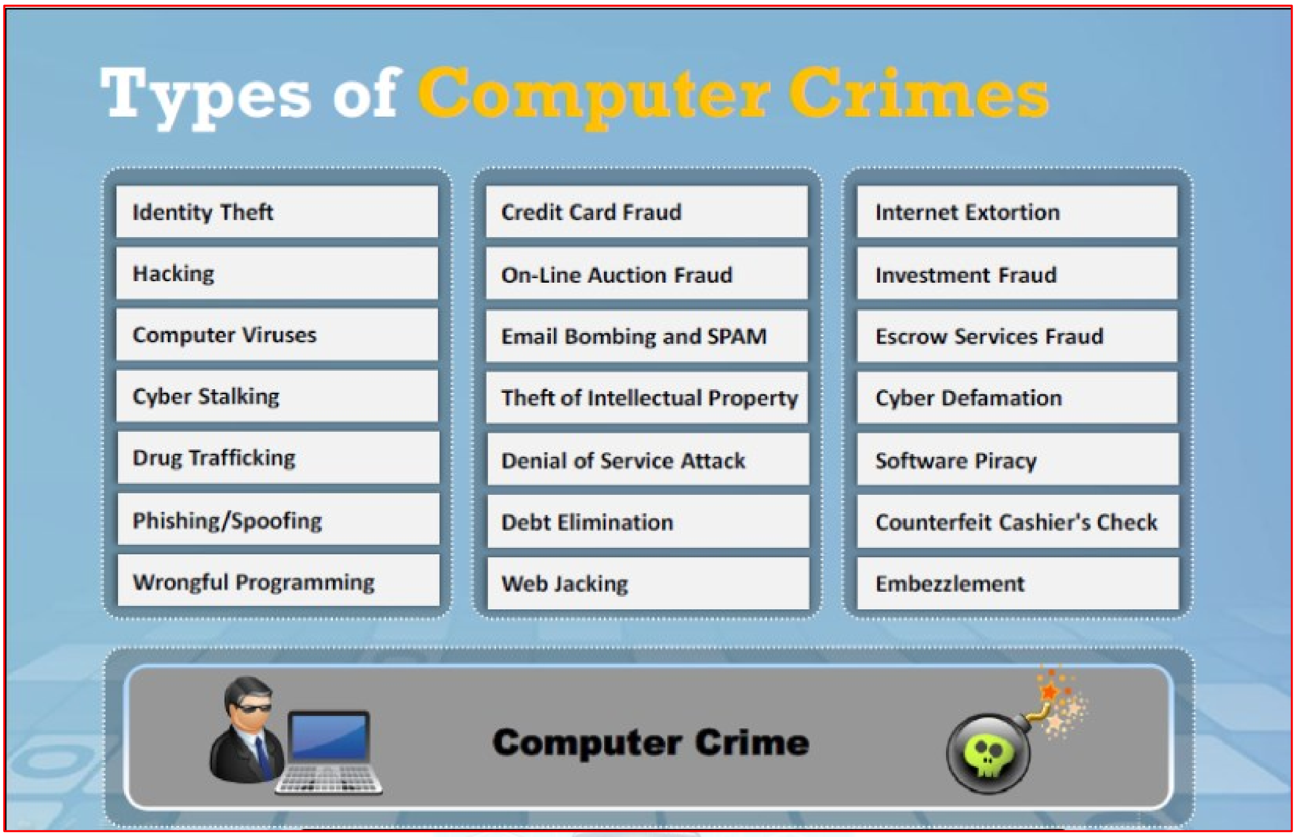
Benefits of Forensics Readiness

1. Evidence can be gathered to act in the company's defense if subject to a lawsuit
2. In the event of a major incident, a fast and efficient investigation can be conducted and corresponding actions can be followed with minimal disruption to the business
3. Forensic readiness can extend the target of information security to the wider threat from cybercrime, such as intellectual property protection, fraud, or extortion
4. Fixed and structured approach for storage of evidence can considerably reduce the expense and time of an internal investigation
5. It can improve and simplify law enforcement interface
6. In case of a major incident, proper and in-depth investigation can be conducted



Forensics Readiness Planning

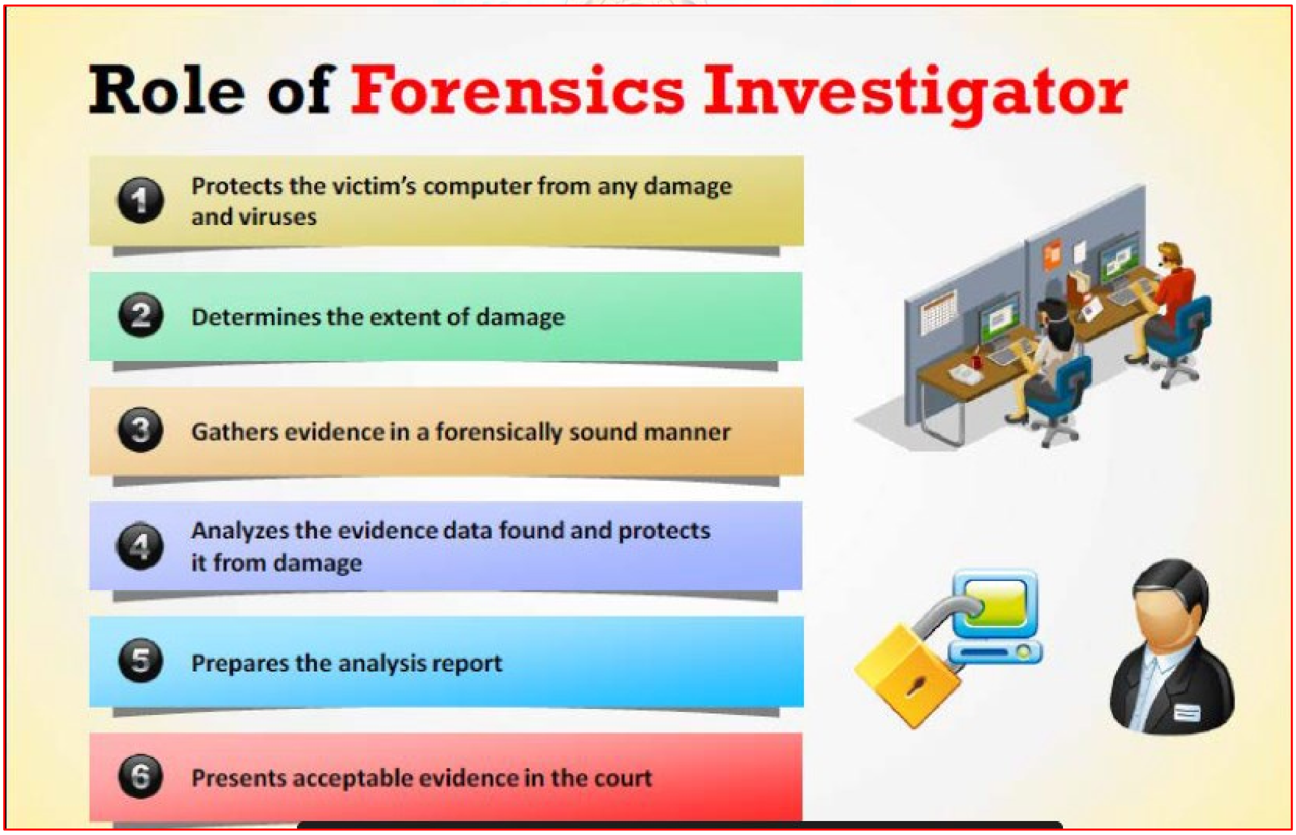
- ✓ Define the business states that need digital evidence
- ✓ Identify the potential evidence available
- ✓ Determine the evidence collection requirement
- ✓ Decide the procedure for securely collecting the evidence that meets the requirement in a forensically sound manner
- ✓ Establish a policy for securely handling and storing the collected evidence
- ✓ Ensure that the observation process is aimed to detect and prevent the important incidents
- ✓ Ensure investigative staff are capable to complete any task related to handling and preserving the evidence
- ✓ Document all the activities performed and their impact
- ✓ Ensure authorized review to facilitate action in response to the incident



Types of Computer Crimes

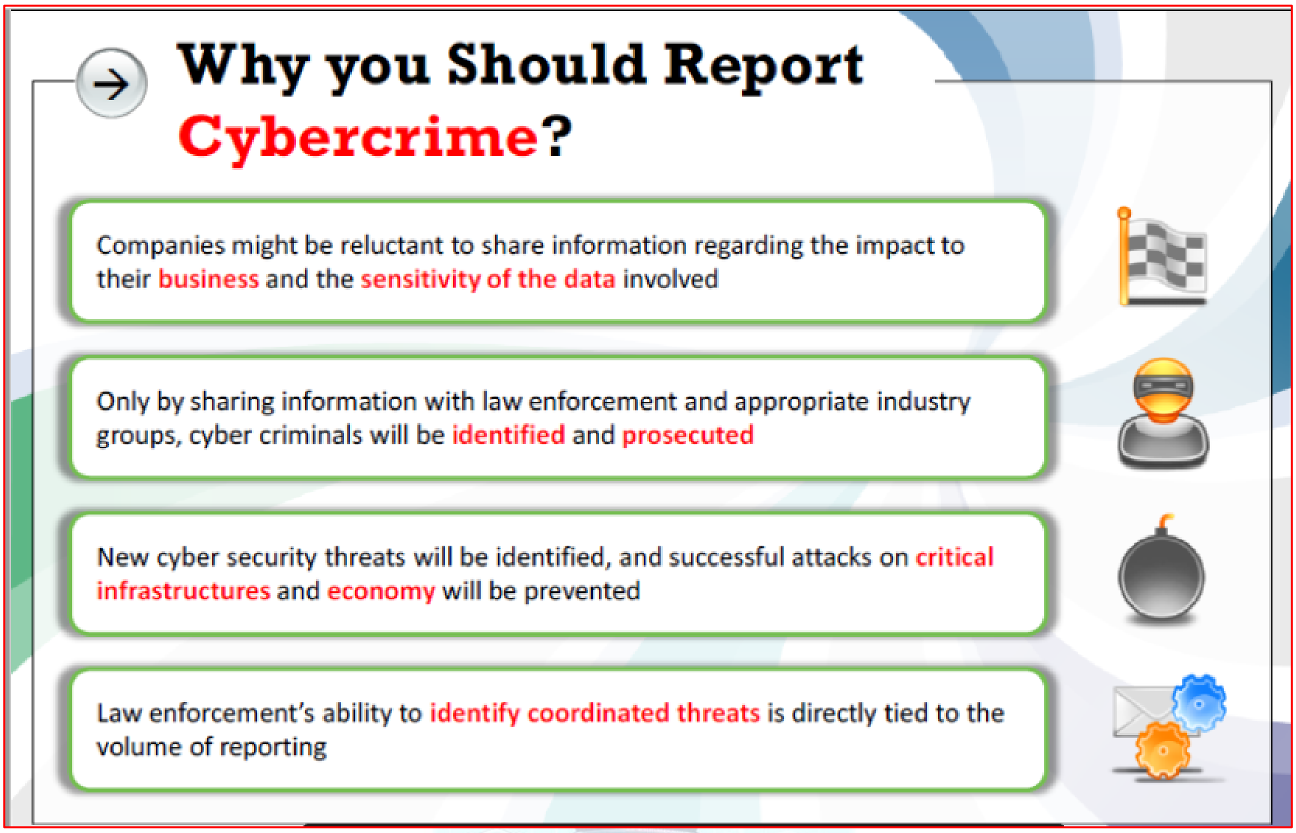
- Identity Theft
- Hacking
- Computer Viruses
- Cyber Stalking
- Drug Trafficking
- Phishing/Spoofing
- Wrongful Programming
- Credit Card Fraud
- On-Line Auction Fraud
- Email Bombing and SPAM
- Theft of Intellectual Property
- Denial of Service Attack
- Debt Elimination
- Web Jacking
- Internet Extortion
- Investment Fraud
- Escrow Services Fraud
- Cyber Defamation
- Software Piracy
- Counterfeit Cashier's Check
- Embezzlement

Computer Crime



Role of Forensics Investigator

1. Protects the victim's computer from any damage and viruses
2. Determines the extent of damage
3. Gathers evidence in a forensically sound manner
4. Analyzes the evidence data found and protects it from damage
5. Prepares the analysis report
6. Presents acceptable evidence in the court



Why you Should Report Cybercrime?

- Companies might be reluctant to share information regarding the impact to their business and the sensitivity of the data involved
- Only by sharing information with law enforcement and appropriate industry groups, cyber criminals will be identified and prosecuted
- New cyber security threats will be identified, and successful attacks on critical infrastructures and economy will be prevented
- Law enforcement's ability to identify coordinated threats is directly tied to the volume of reporting

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."

"No fingerprints, no picture ID, no Social Security number. I'm afraid your baby presents a serious security risk."

Prof. Bashar Al-Esawi
Command Prompt Commands for Basic Forensic Tasks

1. Viewing System Information:

- **systeminfo**: Displays detailed system information, including OS version, installation date, and hardware details.

- **NOTE**: A **hotfix** is a software update, patch, or solution designed to address a specific issue or problem in a software application. It is typically released quickly to resolve critical issues, bugs, or vulnerabilities that may have been identified after the official release of the software.

2. Listing Files and Directories:

- **dir**: Lists files and directories in the current directory.
- **dir /s**: Lists files recursively in the current directory and its subdirectories.

3. Gathering Network Information:

- **ipconfig /all**: Displays network configuration details, including IP addresses, MAC addresses, and DNS settings.

4. Retrieving Event Logs:

- **wevtutil qe Security**: Retrieves security-related events from the Windows Event Log.

5. Examining Registry:

- **reg query HKEY_LOCAL_MACHINE\SOFTWARE**: Displays information from the Software registry hive.
- **reg query HKEY_CURRENT_USER\Software**: Displays information from the current user's Software registry hive.

6. Checking Active Processes:

- **tasklist**: Lists all running processes on the system. ("PID" stands for "Process ID,")
- **tasklist /svc**: Lists running processes along with their services.

7. Accessing Disk Information:

- **wmic diskdrive list brief**: Displays information about the disk drives installed on the system.
- **wmic logicaldisk get caption,description**: Lists logical disk information.

8. Checking System Drivers:

- **driverquery**: Displays a list of all installed device drivers.

Note:

- These commands provide basic information and can serve as a starting point for a forensic investigation.
- For a comprehensive forensic analysis, specialized forensic tools and methodologies are essential.
- Always ensure legal authorization and adherence to proper forensic procedures when conducting investigations.

Command Prompt (CMD) offers various commands that can be useful in digital forensics for data acquisition, analysis, and system information retrieval. Here are a few more commands that can be effective in digital forensics:

1. Disk Imaging and Acquisition:

- **dd**: Though not a native CMD command, it's a powerful tool for creating disk images. It's available on various Unix-based systems but can be used on Windows via third-party software or WSL (Windows Subsystem for Linux).

2. File and Directory Analysis:

- **find**: Searches for specific text within files.
    - Example: **find /I "keyword" C:\path\to\file.txt**

Explanation:

- `findstr`: This is the command used for searching strings in files.
- `/I`: This switch makes the search case-insensitive.
- /S: This switch tells findstr to search for the specified string in all subdirectories of the specified path.
- `"C:\path\to\file.txt"`: Replace this with the full path to the text file you want to search within.

- **findstr**: Searches for strings in files. It supports regular expressions for advanced searches.
    - Example: **findstr /S /I "keyword" C:\path\to\directory\*.***

3. System Information Retrieval:

- **systeminfo**: Retrieves detailed system information, including OS version, system manufacturer, BIOS version, etc.
- **tasklist**: Lists all running processes on the system.
- **driverquery**: Lists installed device drivers.

4. Network Analysis:

- **netstat**: Displays active network connections, listening ports, and network statistics.
- **arp**: Displays and modifies the IP-to-physical address translation tables.

5. File Analysis and Manipulation:

- **certutil**: Performs various operations on certificate files.
- **attrib**: Displays or changes file attributes.

6. Time and Date Information:

- **time /T**: Displays the current system time.
- **date /T**: Displays the current system date.

1. **Network Information:**
   - **ipconfig**: Display information about the computer's network configuration.
   - **netstat**: Show active network connections and listening ports.
   - **arp**: View and modify the ARP cache.
2. **Process Analysis:**
   - **tasklist**: List all running processes on the system.
   - **taskkill**: Terminate a running process.
3. **User Account Information:**
   - **whoami**: Display information about the current user.
   - **net user**: List user accounts on the system.
4. **Registry Analysis:**
   - **reg query**: Query the Windows Registry for information.
   - **regedit**: Open the Registry Editor for manual inspection.
5. **Log Analysis:**
   - **eventvwr.msc**: Open the Event Viewer to analyze system logs.
   - **wevtutil**: Work with event logs from the command line.
6. **Disk Analysis:**
   - **chkdsk**: Check and repair file systems on a disk.
   - **diskpart**: Manage disk partitions.
7. **Timestamp Analysis:**
   - **wmic**: Access the Windows Management Instrumentation Command-line interface for various system information, including timestamps.

To search for a keyword in a file using `wmic`, you might need to combine it with other commands.

```
wmic datafile where "drive='C:' and path='\\path\\to\\directory\\' and extension='txt'" get /value | findstr /I "keyword"
```

8. **File Hashing:**
   - **certutil -hashfile <filename>**: Calculate the hash value (MD5, **SHA-1**, SHA-256, etc.) of a file.

how to use Steghide:

Embedding Data:

To hide data within an image file, you can use a command like this:

```
steghide embed -ef d:\aaa.txt -cf d:\myPICAI.jpg -sf d:\outputbmn.jpg
```

- `-ef secret.txt`: Specifies the file containing the data you want to hide.
- `-cf original_image.jpg`: Specifies the cover (original) image file.
- `-sf output_image.jpg`: Specifies the output image file with the embedded data.

You'll be prompted to enter a passphrase to secure the embedded data.

Extracting Data:

To extract the hidden data from the steganographic image, you can use a command like this:

```
steghide extract -sf d:\outputbmn.jpg
```