Digital Forensic Fundamentals

Introduction to Digital Forensics

Forensics is the application of methods and procedures to investigate and solve crimes. The branch of forensics that investigates cyber crimes is known as **digital forensics**. **Cyber crime** is any criminal activity conducted on or using a digital device.

Digital Forensics Methodology

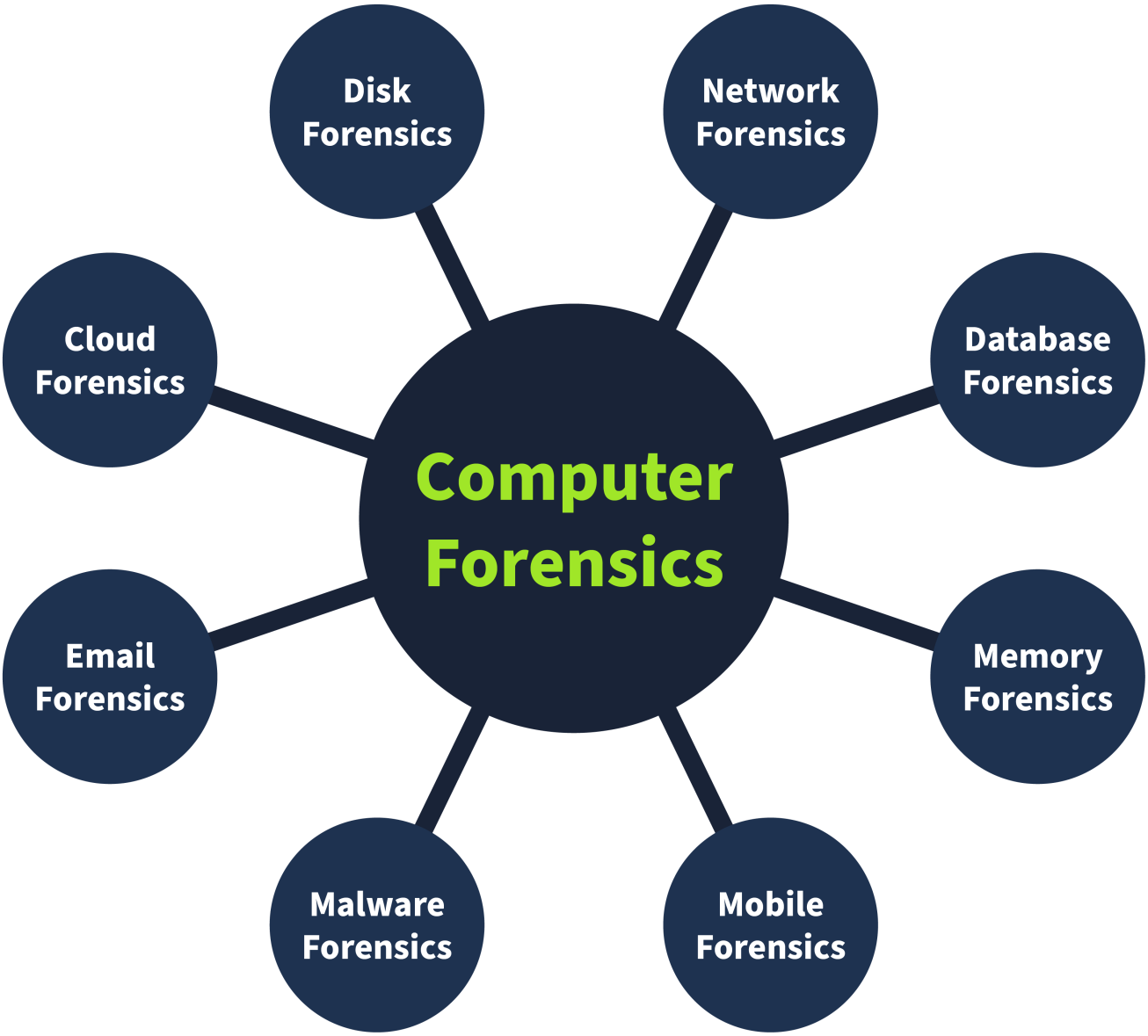
the National Institute of Standards and Technology (NIST) defines a general process for every case.

Collection: The first phase of digital forensics is data collection. Identifying all the devices from which the data can be collected is essential. Usually, an investigator can find personal computers, laptops, digital cameras, USBs, etc., on the crime scene.

Examination: The collected data may overwhelm investigators due to its size. This data usually needs to be filtered, and the data of interest needs to be extracted. For example, as an investigator, you collected all the media files from a digital camera on the crime scene

Analysis: This is a critical phase. The investigators now have to analyze the data by correlating it with multiple pieces of evidence to draw conclusions. The analysis depends upon the case scenario and available data.

Reporting: In the last phase of digital forensics, a detailed report is prepared. This report contains the investigation's methodology and detailed findings from the collected evidence



- **Computer forensics:** The most common type of digital forensics is computer forensics, which concerns investigating computers, the devices most commonly used in crimes.
- **Mobile forensics:** Mobile forensics involves investigating mobile devices and extracting evidence such as call records, text messages, GPS locations, and more.
- **Network forensics:** This area of forensics covers investigation beyond individual devices. It includes the whole network. The majority of the evidence found in networks is the network traffic logs.
- **Database forensics:** Many critical data is stored in dedicated databases. Database forensics investigates any intrusion into these databases that results in data modification or exfiltration.
- **Cloud forensics:** Cloud forensics is the type of forensics that involves investigating data stored on cloud infrastructure. This type of forensics sometimes gets tricky for the investigators as there is little evidence on cloud infrastructures.

- **Email forensics:** Email, the most common communication method between professionals, has become an important part of digital forensics. Emails are investigated to determine whether they are part of phishing or fraudulent campaigns.

Evidence Acquisition

Acquiring evidence is a critical job. The forensics team must collect all the evidence securely without tampering with the original data.

Proper Authorization

The forensics team should obtain authorization from the relevant authorities before collecting any data. Evidence collected without prior approval may be deemed inadmissible in court.

Chain of Custody

A chain of custody is a formal document containing all the details of the evidence. Some of the key details are listed below:

- Description of the evidence (name, type).
- Name of individuals who collected the evidence.
- Date and time of evidence collection.
- Storage location of each piece of evidence.
- Access times and the individual record who accessed the evidence.

Use of Write Blockers

Write blockers are an essential part of the digital forensics team’s toolbox. Suppose you are collecting evidence from a suspect’s hard drive and attaching the hard drive to the forensic workstation. While the collection occurs, some background tasks in the forensic workstation may alter the timestamps of the files on the hard drive.

Suppose the data was collected from the hard drive using a write blocker instead in the same scenario. This time, the suspect’s hard drive would remain in its original state as the write blocker can block any evidence alteration actions.

Windows Forensics

The most common types of evidence collected from crime scenes are desktop computers and laptops, as most criminal activity involves a personal system.

As part of the data collection phase, forensic images of the Windows operating system are taken. These forensic images are bit-by-bit copies of the whole operating system. Two different categories of forensic images are taken from a Windows operating system.

- **Disk image:** The disk image contains all the data present on the storage device of the system (HDD, SSD, etc.). This data is non-volatile, meaning that the disk data would survive even after a restart of the operating system. For example, all the files like media, documents, internet browsing history, and more.
- **Memory image:** The memory image contains the data inside the operating system's RAM. This memory is volatile, meaning the data will get lost after the system is powered off or restarted. For example, to capture open files, running processes, current network connections, etc., the memory image should be prioritized and taken first from the suspect's operating system; otherwise, any restart or shutdown of the system would result in all the volatile data getting deleted. While carrying out digital forensics on a Windows operating system, disk and memory images are very important to collect.

popular tools used for disk and memory image acquisition and analysis of the Windows operating system.

FTK Imager: FTK Imager is a widely used tool for taking disk images of Windows operating systems. It offers a user-friendly graphical interface for creating the image in various formats. This tool can also analyze the contents of a disk image. It can be used for both acquisition and analysis purposes.

Autopsy: Autopsy is a popular open-source digital forensics platform. An investigator can import an acquired disk image into this tool, and the tool will conduct an extensive analysis of the image. It offers various features during image analysis, including keyword search, deleted file recovery, file metadata, extension mismatch detection, and many more.

DumpIt: DumpIt offers the utility of taking a memory image from a Windows operating system. This tool creates memory images using a command-line interface and a few commands. The memory image can also be taken in different formats.

Volatility: Volatility is a powerful open-source tool for analyzing memory images. It offers some extremely useful plugins. Each artifact can be analyzed using a specific plugin. This tool supports various operating systems, including Windows, Linux, macOS, and Android.

Practical Example of Digital Forensics

Pdfinfo displays various metadata related to a PDF file, such as title, subject, author, creator, and creation date

```
root@tryhackme:~# pdfinfo DOCUMENT.pdf
Creator:        Microsoft® Word for Office 365
Producer:       Microsoft® Word for Office 365
CreationDate:   Wed Oct 10 21:47:53 2018 EEST
ModDate:        Wed Oct 10 21:47:53 2018 EEST
Tagged:         yes
UserProperties: no
Suspects:       no
Form:           none
JavaScript:     no
Pages:          20
Encrypted:      no
Page size:      595.32 x 841.92 pts (A4)
Page rot:       0
File size:      560362 bytes
Optimized:      no
PDF version:    1.7
```

Photo EXIF Data

EXIF stands for Exchangeable Image File Format; it is a standard for saving metadata to image files. Whenever you take a photo with your smartphone or with your digital camera, plenty of information gets embedded in the image. The following are examples of metadata that can be found in the original digital images:

- Camera model / Smartphone model
- Date and time of image capture
- Photo settings such as focal length, aperture, shutter speed, and ISO settings

phones are equipped with a GPS sensor, finding GPS coordinates embedded in the image is highly probable.

There are many online and offline tools to read the EXIF data from images. One command-line tool is `exiftool`

```
root@tryhackme:~# exiftool IMAGE.jpg
[...]
GPS Position : 51 deg 31' 4.00" N, 0 deg 5' 48.30" W
[...]
```

I used PDF info on ransom-letter.pdf

```
root@ip-10-82-118-181:~/Rooms/introdigitalforensics# pdfinfo ransom-letter.pdf
Title:          Pay NOW
Subject:        We Have Gato
Author:         Ann Gree Shepherd
Creator:        Microsoft® Word 2016
Producer:       Microsoft® Word 2016
CreationDate:   Wed Feb 23 09:10:36 2022 GMT
ModDate:        Wed Feb 23 09:10:36 2022 GMT
Tagged:         yes
UserProperties: no
Suspects:       no
Form:           none
JavaScript:     no
Pages:          1
Encrypted:      no
Page size:      595.44 x 842.04 pts (A4)
Page rot:       0
File size:      71371 bytes
Optimized:      no
PDF version:    1.7
```

and found the author of the file

I then used the exiftool on letter-image.jpg to find where the kidnappers took the image

```
root@ip-10-82-118-181:~/Rooms/introdigitalforensics# exiftool letter-image.jpg
ExifTool Version Number         : 11.88
File Name                       : letter-image.jpg
Directory                       : .
File Size                       : 124 kB
File Modification Date/Time     : 2022:02:23 08:53:33+00:00
File Access Date/Time           : 2022:02:23 09:12:00+00:00
File Inode Change Date/Time     : 2022:03:04 12:15:19+00:00
File Permissions                : rwxr-xr-x
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Little-endian (Intel, II)
Compression                     : JPEG (old-style)
Make                            : Canon
Camera Model Name               : Canon EOS R6
Orientation                     : Horizontal (normal)
X Resolution                    : 300
Y Resolution                    : 300
Resolution Unit                 : inches
Software                        : GIMP 2.10.28
```

It gave me a gps location

```
Digital Creation Date/Time      : 2021:11:05 14:06:13+03:00
Circle Of Confusion             : 0.043 mm
Depth Of Field                  : 0.06 m (0.76 - 0.82 m)
Field Of View                   : 54.9 deg
Focal Length                    : 50.0 mm (35 mm equivalent: 34.6 mm)
GPS Position                    : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
Hyperfocal Distance             : 20.58 m
Light Value                     : 7.9
Lens ID                         : Canon EF 50mm f/1.8 STM
root@ip-10-82-118-181:~/Rooms/introdigitalforensics#
```

where i pasted this in googlemaps to find the street name in which the image was taken which was milk street