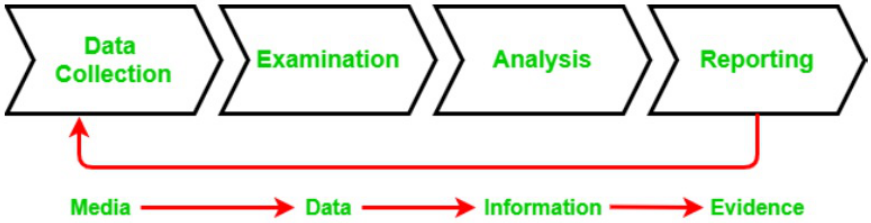
kmbh

In the early 80s PCs became more popular and easily accessible to the general population, this also led to the increased use of computers in all fields and criminal activities were no exception to this. As more and more computer-related crimes began to surface like computer frauds, software cracking, etc. the computer forensics discipline emerged along with it. Today digital evidence collection is used in the investigation of a wide variety of crimes such as fraud, espionage, cyberstalking, etc. The knowledge of forensic experts and techniques are used to explain the contemporaneous state of the digital artifacts from the seized evidence such as computer systems, storage devices (like SSDs, hard disks, CD-ROM, USB flash drives, etc.), or electronic documents such as emails, images, documents, chat logs, phone logs, etc.

Process involved in Digital Evidence Collection:

The main processes involved in digital evidence collection are given below:

- **Data collection:** In this process data is identified and collected for investigation.
- **Examination:** In the second step the collected data is examined carefully.
- **Analysis:** In this process, different tools and techniques are used and the collected evidence is analyzed to reach some conclusion.
- **Reporting:** In this final step all the documentation, reports are compiled so that they can be submitted in court.



Types of Collectible Data:

The computer investigator and experts who investigate the seized devices have to understand what kind of potential shreds of evidence could there be and what type of shreds of evidence they are looking for. So, that they could structure their search pattern. Crimes and criminal activities that involve computers can range across a wide spectrum; they could go from trading illegal things such as rare and endangered animals, damaging intellectual property, to personal data theft, etc.

The investigator must pick the suitable tools to use during the analysis. Investigators can encounter several problems while investigating the case such as files may have been deleted from the computer, they could be damaged or may even be encrypted, So the investigator should be familiar with a variety of tools, methods, and also the software to prevent the data from damaging during the data recovery process.

There are two types of data, that can be collected in a computer forensics investigation:

- **Persistent data:** It is the data that is stored on a non-volatile memory type storage device such as a local hard drive, external storage devices like SSDs, HDDs, pen drives, CDs, etc. the data on these devices is preserved even when the computer is turned off

- **Volatile data:** It is the data that is stored on a volatile memory type storage such as memory, registers, cache, RAM, or it exists in transit, that will be lost once the computer is turned off or it loses power. Since volatile data is evanescent, it is crucial that an investigator knows how to reliably capture it.

Types of Evidence:

Collecting the shreds of evidence is really important in any investigation to support the claims in court. Below are some major types of evidence.

- **Real Evidence:** These pieces of evidence involve physical or tangible evidence such as flash drives, hard drives, documents, etc. an eyewitness can also be considered as a shred of tangible evidence.
- **Hearsay Evidence:** These pieces of evidence are referred to as out-of-court statements. These are made in courts to prove the truth of the matter.
- **Original Evidence:** These are the pieces of evidence of a statement that is made by a person who is not a testifying witness. It is done in order to prove that the statement was made rather than to prove its truth.
- **Testimony:** Testimony is when a witness takes oath in a court of law and gives their statement in court. The shreds of evidence presented should be authentic, accurate, reliable, and admissible as they can be challenged in court.

Challenges Faced During Digital Evidence Collection:

- Evidence should be handled with utmost care as data is stored in electronic media and it can get damaged easily.
- Collecting data from volatile storage.
- Recovering lost data.
- Ensuring the integrity of collected data.

Recovering information from devices as the digital shreds of evidence in the investigation are becoming the fundamental ground for law enforcement and courts all around the world. The methods used to extract information and shreds of evidence should be robust to ensure that all the related information and data are recovered and is reliable. The methods must also be legally defensible to ensure that original pieces of evidence and data have not been altered in any way and that no data was deleted or added from the original evidence.

1. Digital Evidence Preservation - Digital Forensics
2. Recovering Deleted Digital Evidence
3. Early Evidence of Steganography
4. Is AI Really a Threat to Cybersecurity?
5. Top 10 Cybersecurity Tools That You Should Know
6. 6 Best Practices to Perform a Cybersecurity Audit
7. 10 Major Types of Enterprise CyberSecurity Tools
8. Future of Cybersecurity
9. Top 7 Cybersecurity Predictions for 2021
10. Unsupervised Machine Learning - The Future of Cybersecurity

Previous

Password Management in Cyber Security

Article Contributed By :

kmbh
kmbh

Vote for difficulty

Current difficulty : Easy

Easy | Normal | Medium | Hard | Expert

Article Tags : Cyber-security, Geeks-Premier-League-2022, Picked, Computer Networks, Geeks Premier League

Practice Tags : Computer Networks

Improve Article

Report Issue

GeeksforGeeks
A-143, 9th Floor, Sovereign Corporate Tower, Sector-136, Noida, Uttar Pradesh - 201305

feedback@geeksforgeeks.org

Recursion

Backtracking

AngularJS

NodeJS

Computer Science

GATE CS Notes

Operating Systems

Computer Network

Database Management System

Software Engineering

Digital Logic Design

Engineering Maths

Python

Python Programming Examples

Django Tutorial

Python Projects

Python Tkinter

OpenCV Python Tutorial

Python Interview Question

Data Science & ML

Data Science With Python

Data Science For Beginner

Machine Learning Tutorial

Maths For Machine Learning

Pandas Tutorial

NumPy Tutorial

NLP Tutorial

Deep Learning Tutorial

DevOps

Git

AWS

Docker

Kubernetes

Azure

GCP

Competitive Programming

Top DSA for CP

Top 50 Tree Problems

Top 50 Graph Problems

Top 50 Array Problems

Top 50 String Problems

Top 50 DP Problems

Top 15 Websites for CP

System Design

What is System Design

Monolithic and Distributed SD

Scalability in SD

Databases in SD

High Level Design or HLD

Low Level Design or LLD

Top SD Interview Questions

Interview Corner

Company Preparation

Preparation for SDE

Company Interview Corner

Experienced Interview

GfG School

CBSE Notes for Class 8

CBSE Notes for Class 9

CBSE Notes for Class 10

CBSE Notes for Class 11

Competitive Programming

Aptitude

English Grammar

Commerce

Accountancy

Business Studies

Microeconomics

Macroeconomics

Statistics for Economics

Indian Economic Development

UPSC

Polity Notes

Geography Notes

History Notes

Science and Technology Notes

Economics Notes

Important Topics in Ethics

UPSC Previous Year Papers

SSC/ BANKING

SSC CGL Syllabus

SBI PO Syllabus

SBI Clerk Syllabus

IBPS PO Syllabus

IBPS Clerk Syllabus

Aptitude Questions

SSC CGL Practice Papers

Write & Earn

Write an Article

Improve an Article

Pick Topics to Write

Write Interview Experience

Internships

Video Internship