Digital Forensics

Monday, December 26, 2022 11:30 AM

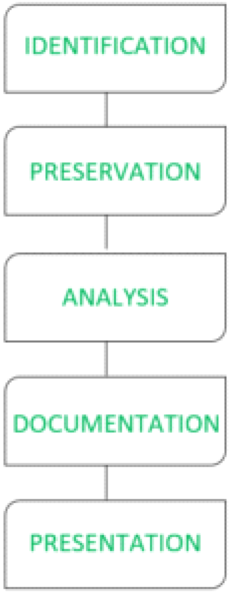
Computer forensics -

- Computer forensics is the science of investigating and analysing the electronic devices to gather evidence that can be presented in court of law.

  Types -

  1.Disk forensics
  2.Network forensics
  3.Database forensics
  4.Malware forensics
  5.Email forensics
  6.Mobile forensics

  Characteristics -



  1.Identify devices for analysis
  2.Preserve the devices in the original condition
  3.Analyse the device or data to get evidence
  4.Document the findings in non technical way
  5.Present the document in the court for further procedure

  Flow -

  1.The devices are identified
  2.The court gives permission to take custody of devices
  3.The devices are preserved
  4.Data from devices is copied for investigation
  5.Then all the findings and evidences are documented
  6.This document is presented in court

Application -

1.Email analysis
2.Cyber fraud
3.indestrial fraud
4.Crime investigation
5.Internet frauds

Use in law enforcement -

- Criminal prosecuters uses computer forensics to get evidences and use them against the suspects to prosecute them.
- It is also used in civil litigation cases land dispute, harrasment, divorce, etc. The data collected from users can be used as evidence to give verdict accordingly
- Also the Insurance companies uses digital records as evidence to rerclaim the insurances of users
- Law enforcement officials rely on computer forensics to back up the evidences in digital format
- Data recovery
- Email analysis
- Network analysis

Computer forensics assistance to HR or Employment procedings -

- Computers can be used as evidence in many Human Resources proceedings or employee termination
- The employee proceedings of sexual harassment, data compromise, misbehaviour, etc can be proven from digital data
- Data present on employee computer can be treated as evidence against him/her
- But the data can be manipulated by the employee to safegaurd its termination
- So the company or Employer should ask a computer forensics expert to recover or make copy of all the data on the employee computer before its termination
- To find the actions of culprit employee we can analyse which files has been downloaded, which sites has been visited, which data has been last modified, email tracking, etc.
- Now even if employee alters the data the employer has the copy of original data to terminate employee

Computer forensics services -

Following are some services that a Computer Forensics expert should provide,

- Data seizure
- Data recovery
- Data duplication
- Evidence documentation
- Evidence presentation
- Data conversion

Benefits of professional computer forensics methodologies -

- The crime scene involving electronic devices like computer, CCTV, mobile phone can be handled by a Professional computer forensic
- The professionals has experience of working on various technologies and devices
- They also have knowledge of various OS and database systems
- They have knowledge of data storage systems on device
- They can properly recover formatted data, can find hidden data, can find alternate ways to track down data storage
- Can analys sites and network
- They can prevent virus attacks on client computer
- They can preserve digital evidence properly without being tamperd

Steps taken by computer forensics specialist -

1.Protect the devices from any alteration
2.Discover data
3.Recover data
4.Examine data
5.Find evidences
6.Document evidences
7.Present the evidences

Military computer forensic technology -

- It is related to the analysis, extraction and preservation of digital evidence from a computer device in a military setting
- It involves analysing cyber crime, tracking down cyber terrorists, etc.
- For this the special softwares and techniques are used and also the specialists are used to extract evidences that can be used for military analysis
- In India the work on implementing computer forensics is going on

Types of business computer forensics technology -

There are various computer forensics tools and technologies used to analyze and extract data from computer in a business setting,

1.Remote monitoring of target computers
Data interception by remote transmission (DIRT) is a software sued to access data remotely
2.Creating trackable electronic document
Create trackable electronics document so that we can track who downloaded the file, who try to access it, etc.
3.Theft recovery software for personel computers like PC Phonehome

Data recovery solutions/methods -

Data recovery is the process off retrieving and analyzing data from the computer or electronic device to be used for forensic analysis and generate an evidence to be presented in court.
The experts has to follow legal regulations and frameworks to collect and analyze the evidence.

Methods for data recovery are,

1.Physical recovery

In this data is recovered by repairing damaged hardware using electronics tools
This also includes replacing hardware like hardrive, motherboard, etc.

Methods of physical recovery are,

1.Harware repair tools
2.Data recovery hardware

2.Logical recovery

In this method data is recovered using software tools from devices present on crime site

Methods are,

1.File craving - in this a software analyses the file storage and try to find a specific file
2.Data recovery software
3.Forensic software

3.Cloud recovery

When the data is not stored on actual device but on cloud storage then cloud data recovery techniques are used.

Methods are,

1.Cloud extraction tools which can retrieve data from Google drop box, Salesforce and other cloud platforms
2.Cloud forensic software
3.Networking tools

Data recovery defn -

Data recovery is the process of retrieving and analyzing the data from electronic devices to preserve, process and present the data for the legal procedings in court
This include restoring data from damaged devices, recovering deleted files, tracking networks, etc.

Data backup -

It is the methodology in computer forensics in which the data is copied from subject device and preserved for future use.

The data is backed up because for investigation the original data can not be modified.

Also in cases like if data is altered or destroyed by any person then the copy of data is present as back up.

The data can backed up in various ways like,

1.Full image backups -

In this the entire data from device is copied as it is to analyze complete data from device
This allows experts to analyze data in its original state
This also serve as dummy model of subject device for the experts to work on

2.Partial backups -

In this only investigation related data is backed up which eventually speeds up the investigation
This also saves extra space required for the full image backups

3.Cloud backups -

In this the data is backed up on cloud storage like Salesforce or Dropbox, etc.
This is most safest type of backup than other two
Because the devices on which the backup is made they can be also get damaged or altered.
Ans this backup can be accessed anywhere.

Role of data backup in data recovery -

Data backup plays vital role to preserve data at the event of data loss or corruption.
When data corruption or device failure occurs, data backup serve as another source of data to be given as evidence.
Actual data may be modified or tampered but the data backup serves as safety net for the user or organization or investigator.

Limitations of current data backup methods -

1.Offline data backup requires considerable time to backup data
2.Hard drives for backup has limited capacity
3.Backup on the same network creates burden on the network

New methods -

1.Data should be backed up in real time with minimum time
2.Data can be backed up on remote centers
3.Decentralized storage can be used to backup the data