Computer Forensics Analysis and Validation

Tuesday, December 27, 2022 5:37 PM

What data to collect and analyze -

This depends upon following factors,

1. Nature of case - corporate case, public litigation case, fraud case, cyber attack, etc.
2. Amount of data to process
3. Search warrants and court orders
4. Scope creep - Investigation scope extends beyond original scope
5. Right to access full data

   Tool used to analyze the data -

   1.Accessdata forensic toolkit is well known software for forensic data analysys
   2.It supports various file formats
   3.It generates a log file
   4.Searching using keywords is possible
   5.It can analyze compressed files
   6.It can generate case reports

Validating forensic data -

Validating forensic data is the process of verifying integrity and authenticity of the data collected during a forensic investigation.

This helps in proving that the data is trustful and can be taken as evidence in a legal case.

Some common techniques for data validation,

1. Hash value analysis -

   In this the hash value of original data is calculated and stored.
   Then it is cross checked with some stored predetermined hash value.
   If both value matches then the integrity of data is maintained otherwise compromised
   Tools used - Hexadecimal editors

2. Metadata analysis -

   In this metadata of the files is analyzed to check its integrity
   Metadata includes info like date of creation, date of modification, last seen, etc.
   From this we can check whether data is modified or not

3. Source validation -

   In this the source of data collected is validated to ensure the data integrity
   The source system is analyzed to check whether any alterations are done or not

Data hiding techniques -

- Data hiding techniques are the methods used to conceal data so that it can not be detected in an forensic investigation.
- This methods can conceal various types of data as documents, images, etc.
- Data hiding is done to either protect the sensitive data or to hide evidence of an illegal activity.
- Techniques,

  1.Steganography -
  It is the process of hiding one type of data in other type of data.
  Ex. A message can be hided into an image

  2.Encryption -
  Encrypting the data is the way to hide the data using cryptography.
  Only people with proper key can decrypt the data

  3.Hidden partition -
  In this a hidden partition is created on the storage and data is concealed there

  4.Bit shifting -
  In this the binary representation of the data is altered by shifting the bits to left or right.
  This completely changes the data and makes it unrecognizable

  5.Marking bad clusters -
  In this some storage of system is marked as bad and data is concealed there.
  This makes OS and forensic tools to not access that cluster

Addressing data hiding techniques -

- Addressing data hiding techniques in forensic investigations involves using specialized tools and techniques to detect and extract data that has been concealed using one of the many data hiding techniques
- This may involve using forensic software or hardware tools to analyze the data on a storage device, examining metadata or other hidden data within files, or using specialized techniques to extract data from hidden partitions or marked bad clusters.
- forensic investigators may need to be familiar with a wide range of tools and techniques, and may need to use a combination of different approaches in order to detect and extract hidden data.

Remote acquisition -

- It is the method of collecting data from the device which is located remotely over the network
- This method is used when it is not possible to collect data physically or when we have to collect data while system is in use.
- Techniques used,

  1.Network forensics -
  In this the network traffic of the system is captured to access the data as evidence.
  The device should be present on the network

  2.Cloud forensics -
  Data stored in the cloud platforms may be treated as remote data.
  Collecting data from cloud platform requires various forensic tools and methods.

  3.Remote acquisition software -
  This software are specialized to access data on remote devices which are present over the network or internet.

Network forensics -

- It is the process of collecting, analyzing and preserving data from network to prepare evidence of a cybercrime or other crimes.
- It involves capturing network traffic and analyzing it to find pattern
- This pattern helps to find any anomaly or unusual activity over the network
- This also involves remote access of the data over the network
- It also helps other type of forensics to gain complete picture of the crime happened

Live acquisition -

It is the process of acquiring volatile data from the compromised system.
Volatile data is continuously changing and remains for few milliseconds on storage.
The volatile data is present on RAM, cache, registers, etc.
The volatility of the data is different for different components of the system. The investigator has to consider this and has to perform live acquisition of most volatile data first.

Two type of volatile data,

1.System info -
This includes OS info, user profiles, logs, login details, RAM info, storage type, etc.
2.Network info -
This includes info of activity of the system with other devices over the network like routing info, ARP info, etc.

Live acquisition process -

1.Note down the current date and time of the system
2.Note down the date and time of the tools used for forensics
3.Collect most volatile data first
4.Maintain log of all data collected in order
5.Collect data over the network
6.Do not shut down or restart the system
7.Do not try to use administrative utilities over the compromised system
8.Store collected data in other drive or device
9.Document all the process and data acquired.

Standard procedure for network forensics -

There is no single standard procedure for network forensic but some common methods used are,

1.For every system on the network prepare an installation image that contains info of all the apps and files installed ver the system.

2.When an intrusion is detected, try to exploit the opening point of the intrusion.

3.Before shutting down the system try to get volatile data by live acquisition

4.Compare forensic image with installation image to know which apps or files are modified.

5.Continuosly analyze the network traffic

Honeynet Project -

- Honeynet is a network of computers set up to be attacked by cyber criminal and to study tactics and techniques of the attacker.
- Just like honeypot, honeynet act as a decoy network to gather info on techniques used by attacker to get inside the network and also which systems are vulnerable to attack
- Honey also helps to find vulnerabilities in the network
- Honey consist of many number of honeypots
- It also consist of apps and services to look like some normal network
- To keep track of traffic going inside and outside the honeynet, honeywall is used.
- Honeynet project is an international organization that researches and study in honeynet technology
- It provides tools and techniques for researcher to setup honeynet
- Honeynet project has following objectives,
  1.Continue research by providing resources to the volunteers
  2.Build awareness by publishing info found from research conducted
  3.Create new tools to be used for research in honeynet

Collecting evidence in private sector incident scene -

- If a corporate investigator finds that any employee has committed or committing crime then, it can ask employer to file a case against employee
- The employer is interested in implementing its company policy not in prosecuting the employee
- Hence the investigator has to focus on securing company assets
- When an evidence is found during company policy investigation then,
  1.Comapre it with crime scene
  2.Inform the management
  3.Collect the evidence and secure it
  4.Document the findings and submit it to the company attorney

Processing law enforcement crime scenes -

1.Investigator should know criminal procedures
2.Should have knowledge on search warrants
3.Other legal knowledge

Preparing for search -

1.Getting ready with search warrant
2.Having tools required for investigation

Securing a computer crime scene -

1.Secure the crime scene with the help of police
2.Allow only authorized person to enter the crime scene

Seize the digital evidence at crime scene -

1.Seize the digital evidence as mentioned in the search warrant

Store the evidence -

1.Store the seized evidence in secure way
2.Can use Drives, cloud storage, remote systems, etc.

Obtain digital hash -

Use hashing methods like MD5 to check integrity of the data obtained

Review the entire case process.