Evidence collection

Tuesday, December 27, 2022 10:30 AM

Why collect evidence -

- Evidence is nothing but a proof against the suspect who committed the crime.
- Evidence collection is essential because it helps to find out the culprit and tie it up in the custody of law
- It helps to stop further crimes done by culprit
- It helps to track down other crimes done by the culprit

Options to collect evidences -

When any computer related crime happens there are two option to gather evidence for the investigators or computer forensics expert,

- Remove the system from its network and bring it offline -
  This may lead to several problems. If the attacker has implemented some program to vipe out data when system goes offline, this leads to serious problem.

- Keep the system online on its network and track down the attacker -
  If the attacker gets notified about its tracking then it can clear the evidence on the network and can affect other systems

Obstacles while collecting evidences -

- Computer crimes are difficult to investigate and track down
- Identifying the attacker is difficult because the culprit can use various techniques to hide its identity like some private server, credentials of other persons, remote access of other device, etc.
- If attacker uses bots to do crime then it becomes impossible to track down the attacker
- Even if we get the identity of the attacker though we can not say that it is the real attacker because it may be a bot

Types of evidence -

- Real evidence -
  It is the evidence that can be carried into the court room and presented to the jury. It is the most powerful evidence that speaks for itself
- Documentary evidence -
  This the evidence in the form of written document. For ex. Server logs, emails, database logs, etc
- Testimonial evidence -
  This is nothing but evidence given by witnesses on the crime
- Demonstrative evidence -
  This are the evidences that needs to be demonstrated in front of the jury to be proven

Rules of evidence -

- Admissible -
  The evidence must be hold up in the court
- Authenticate -
  The evidence must be genuine. It must be related to the incident.
- Complete -
  The evidence must cover all aspects of the incident and provides all required info on the incident
- Reliable -
  The evidence must be reliable and trustworthy. Reliability is achieved using forensic techniques and methodology.
  The experties of the specialist also matters
- Believable -
  The evidence must be acceptable in the court. The data provided must be believable and match with other results by specialists

Volatile evidence -

- The evidence which is in always state of change is called as volatile evidence
- The data stored in volatile parts of a device like, RAM, virtual memory, secondary memory, etc. is said to be volatile.
- The computer forensic expert first try to collect this volatile evidences first from memory cache, main memory, routing tables, memory registers, etc.

Data Collection and archiving -

- Logs and logging -
  1.The expert runs some sort of system logging on the compromised system to check activities on the system
  2.The logs have timestamps on activities that can be used to track down the unusual user
  3.the logs data should be archived on other device or server instead of compromised system

- Monitoring -
  1.Network monitoring can be done on compromised system to track down the unusual activities
  2.Monitoring helps to find usual pattern of activities of a system and can points out the unusual ones
  3.Monitoring should be done under regulations defined

Methods of data collection -

- Honeypotting - creating some dummy system and monitor hackers activity on it and gather data for evidence against hacker
- Freezing the scene - capture the data at the time of hacking and gather data from it to be used as evidence

Chain of custody -

- Chain of custody is the documentation of data related to evidence like what data is found, how it is collected, who accessed the data and when, etc.
- The main goal of chain of custody is to ensure the integrity of the evidence
- If the chain of custody fails to show when the evidence is accessed by whom then the complete evidence becomes useless
- Following steps has to be followed to write the chain of custody and tag the evidence,

1.Document what kind of data is found
2.Where the data is found like on computer, mobile or some other electronic device
3.How the data is collected
4.How it is transported to forensic labs
5.How it is analyzed
6.What conclusions are obtained
7.Who accessed the evidence and when
8.How the evidence is presented in the court

- There are safe storages in the law enforcement authorities offices to store the evidence
- Some person or group of people are appointed to safegaurd the evidence

Preserving the digital crime scene -

- Before processing and analyzing the evidence data, it should be preserved so that the integrity of the data remains intact
- For preserving purpose data should be backed up so that it can be used for future purposes
- Full image back ups needs to be done to get exact mirror copy of original data
- Further processing should be done on the back up data instead of original data to maintain the evidence
- Tools used are SafeBack, SnapBack
- SafeBack tool is cheaper and used by various government agencies for evidence analysys
- SnapBack is alternative to the SafeBack and it is very costly
- It is not that much in use

Computer evidence processing steps -

1. Turn off the system from its network
2. Note down the hardware details of the system
3. Transport the system
4. Take back up of the data from the system
5. Ensure that during back up original data is not modified
6. Instead of exploring entire data get keywords from related people and try to find using this keywords
7. Search in unallocated space
8. Document details of the files that are found
9. Document the details of the software used for analysis of data
10. Document the findings
11. Provide entire document to the court