1.What is the memory forensic method?

Memory forensics is a vital form of cyber investigation that allows an investigator to identify unauthorized and anomalous activity on a target computer or server. This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a memory dump.

2.What are the different types of memory forensics?

Some of the most common memory forensics frameworks are Autopsy, Magnet RAM Capture, and REMnux. These frameworks can help investigators to conduct memory forensics in a more efficient and user-friendly way. Jon H. Digital Forensics, Incident Response and PFI Core Investigator.

3.What is the difference between memory forensics and disk forensics?

Unlike hard-disk forensics where the file system of a device is cloned and every file on the disk can be recovered and analyzed, memory forensics focuses on the actual programs that were running on a device when the memory dump was captured.

4.What is volatility tool used for?

Volatility can be used during an investigation to link artifacts from the device, network, file system, and registry to ascertain the list of all running processes, active and closed network connections, running Windows command prompts, screenshots, and clipboard contents that ran within the timeframe of the incident.

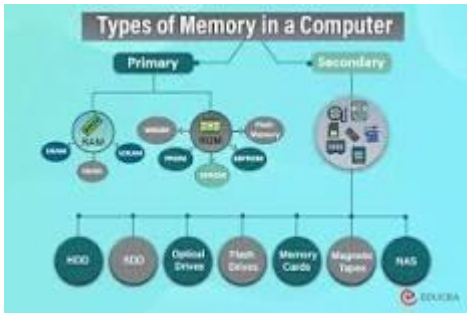
5.What are the phases in memory forensics?

The digital forensic process consists of five steps: evidence acquisition, memory forensics, analysis of selected files, disk forensics, and reporting.

6.How is forensic data stored?

The two basic types of data that are collected in computer forensics are persistent data, or data stored on a local hard drive (or another device) which is preserved when the computer is turned off and volatile data, or data that is stored in memory and lost when the computer loses power.

7.What are the 2 main types of memory?



A computer contains two types of memory: primary (volatile) and secondary (non-volatile). Primary memory (RAM and ROM) allows quick data access and temporary storage for running programs, while secondary memory (HDDs, SSDs, etc.) provides long-term data storage.

8.Why is memory forensic important?

The Importance of Memory Forensics

Memory forensics can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes.

9.What is forensic image?

A forensic image (forensic copy) is a bit-by-bit, sector-by-sector direct copy of a physical storage device, including all files, folders and unallocated, free and slack space.

10.What is a forensic tool?

Digital forensics tools are hardware and software tools that can be used to aid in the recovery and preservation of digital evidence. Law enforcement can use digital forensics tools to collect and preserve digital evidence and support or refute hypotheses before courts.