Name - Sanskruti Sachin Chumble
Std - SYBtech . Div - A
Roll No - 9

CLF Assignment-1 (Unit 1)

Q1) Define System Software and application Software. Explain their roles in forensic computing, providing relevant examples.

→ i) System Software -

This refers to essential programs that manage hardware and provide a platform for application Software.
Examples including operating Systems (Windows, Linux), utilities and drivers.

Role in forensic computing : Investigators rely on OS features (eg, logs, registry, file system) to extract forensic evidence.

ii) Application Software -

These are programs designed for specific tasks, such as wordprocessing or forensic analysis tools.
Examples including EnCase, Autospy and FTK (forensic Toolkit)

Role in forensic Computing - Specialized forensic tools analyse digital artifacts like deleted files, network logs and malware.

Q.8. Compare low level and high-level programming languages. How do they influence forensic investigations, especially in malware analysis?

→

Feature	Low-level Languages	High-level Languages.
Definition	Close to hardware, requires direct memory management.	More abstract, easier to read/write.
Examples	Assembly language, C-programming.	Python, Java, C++.
Execution Speed	Faster, directly interacts with hard.	Slightly slower due to abstraction.
Use in Malware.	Often used for rootkits, key loggers.	Used for scripting-based malware (eg: python bots)

Influence on Forensic Investigations-

- Low level analysis - Reverse engineering assembly code in malware helps determine its functionality.
- High level analysis - Analysing scripts in ransomware or phishing attacks.

Example - A forensic expert decomplies a malware sample in C to understand how it modifies system registry entries.

Q.3) How do computer hardware and Software interact in digital forencis investigations? provide an example where forensic analyst ~~con~~ must consider both the aspects.

→ Forensic investigations require both hardware and Software to extract evidence.

- Hardware Considerations:
  - Hard drives store logs and deleted files.
  - RAM analysis can reveal running processes.
- Software Considerations:
  - File System analysis (NFTS, FAT) helps track file modifications.
  - Logs from OS and applications assist in tracking activities.

Example - A forensic analyst investigating a cybercrime must retrieve data from an encrypted SSD using forensic tools like FTK Imager while considering the SSD's wear-leveling feature.

Q.4) Explain the role of an OS in computer forensics How do different OS structures impact forensic recov

→ An OS manages system resources and forensic investigators analyze it for evidence.

<u>Roles in forensic</u> -

- Collects logs (windows Event logs, Linux Syslogs).

- manages file Systems (FAT32, NTFS ext4).
- Stores uses data (Registry, System cache).

Impact of OS Structures on Data Recovery:

- windows - Stores metadata in the registry making it useful for user activity analysis.
- Linux - Uses logs like /var/ log for tracking security events.
- MacOS - Has time machine backups that assist in forensic investigations.

Q.5) Discuss various types of Storage devices (HDD, SSD, Optical Disks, FD) and their significance in forensic data collection

→ i) HDD (Hard disk drive) - Magnetic Storage, Slower that SSD. It can recover deleted files using data carving.

ii) SSD (Solid-State Drive) - Flash memory, fast read/ write. TRIM feature may prevent file recovery.

iii) Optical Disks (CD / DVD) - Laser based Storage, Limited capacity. Useful for recovering archived evidence.

iv) Flash Drivers (USB, SD card) - Portable uses NAND flash memory. Often used for quick data transfers and hiding evidence.

Example - A suspect deletes files from a USB drive, but forensic tools recover from metadata analysis.