Evidence Volatility (network vs memory vs disk)

Evidence volatility in digital forensics refers to **how quickly certain types of evidence can be lost or altered**. Understanding evidence volatility is crucial because it helps **prioritize what to capture first during an investigation**. Here's a breakdown of volatility in the context of network, memory, and disk evidence:

Network Evidence

- Volatility: **Highly** volatile, as network traffic data exists only for a brief moment while being transmitted. Once a network session ends, packets are lost unless captured in real time.
- Examples: IP addresses, active connections, port activity, DNS queries, and packet data.
- Capture Priority: **Network traffic should be captured as soon as possible**, ideally using tools like Wireshark or a network tap, as it can provide insights into an attacker's movements.

Memory Evidence (RAM):

- Volatility: **Moderately** volatile. RAM is cleared when a system is powered off or rebooted, making it transient and susceptible to quick loss.
- Examples: Running processes, active network connections, encryption keys, and user credentials.
- Capture Priority: **Memory should be captured immediately after network evidence**, often using tools like Volatility or FTK Imager. This data reveals in-memory malware, active processes, and other crucial indicators.

Disk Evidence (Storage Drives):

- Volatility: **Least** volatile among the three. Disk data persists even after power is removed, making it more stable for later analysis.
- Examples: System logs, deleted files, application data, and file system structures.
- Capture Priority: **Disk evidence can be collected last**, as it's generally persistent. However, disk data can still be altered by system processes or human actions, so it **should be imaged and preserved quickly if there's a risk of tampering**.

Summary

In forensic investigations, understanding this **volatility hierarchy (network > memory > disk)** ensures the most transient, valuable evidence is collected first, preserving critical information for analysis.