Network Forensics

In network forensics, **understanding the data flow, connections, and interactions within a network is essential**. Here's an overview of important network forensics components like **DNS logs, passive DNS, NetFlow, and sampling rate**.

DNS Logs / Passive DNS

- **DNS Logs**
  - Purpose: DNS logs **capture details about DNS queries and responses**, helping trace domain name resolutions back to specific times, IPs, or users.
  - Forensics Value: Analyzing DNS logs **can reveal attempted connections to malicious domains, aiding in tracking malware or command-and-control (C2) traffic**.
- **Passive DNS**
  - Purpose: Unlike active DNS, which queries the DNS system directly, passive DNS **captures and logs DNS responses observed over time without making new queries**.
  - Forensics Value: Passive DNS data **enables investigators to review historical mappings between domain names and IPs**, even after the IP address for a domain has changed, which is useful in tracking malicious domains over time.

NetFlow

- Definition: NetFlow is **a protocol originally developed by Cisco to collect IP traffic information as it enters or exits an interface**.
- Purpose: It logs flow data, including **source and destination IPs, ports, protocol types, byte and packet counts, and timestamps**.
- Forensics Value: NetFlow data provides a high-level overview of network traffic patterns and can help detect unusual behaviors, such as unexpected outbound connections or large data transfers, which may indicate exfiltration attempts or C2 activity.

Sampling Rate

- Definition: The sampling rate refers to **the frequency at which network traffic is captured for analysis**. Instead of capturing every packet, samples of packets are collected at a predefined interval (e.g., 1 in every 1000 packets).
- Purpose: Sampling helps **reduce the storage and processing load** by capturing representative samples of network traffic rather than continuous streams.
- Forensics **Trade-off**: While sampling conserves resources, it can limit visibility and miss subtle events. A lower sampling rate (e.g., 1:100) is generally suitable for long-term traffic monitoring, but a higher rate (e.g., 1:10) or even full capture may be necessary for detailed forensic investigations of specific events.

Using These Components in Forensics

- **DNS logs and passive DNS** aid in **tracking domain resolution** over time and identifying potential malicious domain usage.

- **NetFlow** provides **a broader view of traffic patterns** and is highly useful in **identifying anomalies or suspicious flows** without needing full packet captures.
- **Sampling Rate** helps **manage data volume**, though high-fidelity investigations may require adjusting sampling rates or capturing data in real time to avoid missing key forensic evidence.

> In summary, each of these elements plays a unique role in network forensics, providing insight into network behaviors, malicious activities, and incident timelines.