1. How does SSL prevent network forensics - and how could forensics work despite SSL? (35)

SSL/TLS is a protocol for the secure exchange of information over the Internet.
It works by combining asymmetric (secure key exchange and authenticity) and symmetric encryption (encrypting the data) with each other and provides privacy of data, authentication of the partners, and integrity of data.

These characteristics and the encrypted traffic make forensic analysis of potentially malicious traffic difficult.
But there are still several approaches that forensic investigators can take to analyze network traffic and activities. Here are a few methods:

- **Metadata and Traffic Analysis:** Even though the content of the communication is encrypted with SSL/TLS, the metadata (such as source IP, destination IP, packet size, timing, etc.) is still visible. Analyzing these can sometimes provide valuable information. For instance, abnormal amounts of data being sent to an unfamiliar IP address could indicate a data breach.
- **Endpoint Forensics:** Instead of trying to decrypt the SSL/TLS traffic, investigators can examine the endpoints of the communication (if available). This could involve analyzing logs, checking for malware, or looking at the data stored on the devices.
- **SSL/TLS Interception:** Also known as SSL/TLS inspection or a man-in-the-middle attack, this technique allows a third-party to decrypt the SSL/TLS traffic. In a controlled environment, a security device or software is used to act as the “client” for the server, and as the “server” for the client. This allows it to decrypt, inspect, and re-encrypt traffic. This practice is controversial due to potential privacy breaches and new attack vectors.

2. In a wired network, which measures exist to acquire network data for forensic purposes? (30)

In a wired network, several measures can be taken to acquire network data for forensic purposes:

- **Network Taps:** Network taps (Test Access Points) are physical devices inserted at specific points in a network to monitor data. They can be used to capture data in transit between devices in a network, without disrupting the flow of data.
- **Port mirroring:** Port mirroring allows the duplication of network traffic from one or more ports of a switch to a designated monitoring port. Essentially, port mirroring copies the packets that pass through the specified source ports and sends them to the monitoring port for analysis or recording purposes.
- **Log Analysis:** Network devices, such as routers, switches, and firewalls, generate log files that record various activities and events. These logs can be valuable sources of information for network forensics. Analyzing log files can help identify network anomalies, track network connections, and reconstruct events during an investigation.

3. Which restrictions would you expect when trying to analyse NIDS data? (35)

Analyzing NIDS data has several challenges and restrictions, such as:

- **Encryption:** With most of the internet traffic now encrypted using protocols such as SSL/ TLS, traditional NIDS are not able to inspect the payload of the packets, making it harder to identify malicious activities.
- **False Positives/Negatives:** NIDS often generate many alerts, some of which are false positives. Distinguishing between false positives and actual threats is a significant challenge. Conversely, a system may also have false negatives, where actual threats go undetected.
- **Real-time Analysis:** For an NIDS to be effective, it must be capable of analyzing data in real-time. The sheer volume of data, combined with the need for timely detection, presents a significant performance/scalability challenge.
- **High Data Volume:** Networks, especially in large organizations, generate massive amounts of data. Analyzing this data in real-time or even in batch mode is resource-intensive.
- **Data Privacy Concerns:** Depending on jurisdiction, privacy laws may restrict the kinds of data you can collect or analyze. Even within an organization, you may need to anonymize certain data to ensure privacy.
- **NIDS Evasion Techniques:** Attackers have developed a range of evasion techniques designed to avoid detection by NIDS. These could include fragmentation attacks or covert channels.
- **Signature Limitations:** NIDS relies on signature-based detection methods, which involve matching network traffic patterns against known signatures of attacks. If a new or customized attack does not have a matching signature in the NIDS database, it may go undetected.
- **Network Segment Visibility:** NIDS typically operate at specific network segments, such as switches or routers. If the NIDS is not deployed across all network segments or lacks visibility into certain parts of the network, it may miss important network traffic and potential security incidents occurring in those segments.