Wireshark

WIRESHARK

Summary:

1. Wireshark is a powerful open source network protocol analyzer used for capturing and inspecting network traffic in real time.

2. Features:
   - Packet capture - displays packet's detailed format
   - Filtering. Isolate protocols for analysis.
   - Protocol analysis - breakdown for details
   - Packet Reassembly - Fragmentation and reassembly analysis for application layer communication

3. Hands on usage:
   - Captured live traffic.
   - Used filters like http and ip.src = <IP> to narrow down packets of interest
   - Examined packet details such as source/dest IPs, ports, payload data and timestamps
   - Saved captured traffic to ip.cap file for future analysis

4. Learnings:
   - Gained insight into how data is transmitted across a network.
   - Understood structure of common network protocols and their role in communication.

Wireshark provides valuable insights into network behaviour, helps diagnose issues, and enhances understanding of protocol level communication.