

Date: 22/08/2024

Lab Practical #08:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #08:

1. Explain usage of Wireshark tool.

Wireshark is a network protocol analyzer that captures and inspects data traveling across a network in real-time. It's an essential tool for network administrators, cybersecurity professionals, and developers for troubleshooting, analysis, and monitoring of network traffic.

How to Use :

1. **Install Wireshark:** First, download and install Wireshark from the official website.
2. **Select a Network Interface:** When you open Wireshark, you'll see a list of network interfaces (like Wi-Fi, Ethernet). These represent the different connections your computer is using. Choose the one you want to monitor (e.g., your Wi-Fi connection).
3. **Start Capturing Packets:** Click the "Start Capturing Packets" button (the blue shark fin icon). Wireshark will begin recording all the network traffic passing through the selected interface.
4. **Analyze the Data:** As Wireshark captures packets, you'll see them listed in real-time with details like the source and destination IP addresses, protocols used, and data. You can stop the capture at any time to analyze the data more closely.
5. **Use Filters:** Wireshark lets you apply filters to narrow down the data. For example, you can filter by IP address, protocol, or even specific data within the packets.
6. **Save and Export:** Once you've captured the data you need, you can save it for future analysis or export it in various formats.

Usage:

- **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
- **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
- **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.
- **Network Troubleshooting:** Identify and diagnose issues like slow network performance, packet loss, or connectivity problems by analyzing packet data.
- **Protocol Analysis:** Examine how specific protocols (e.g., HTTP, DNS, TCP) operate on the network, helping in debugging and understanding network communication.



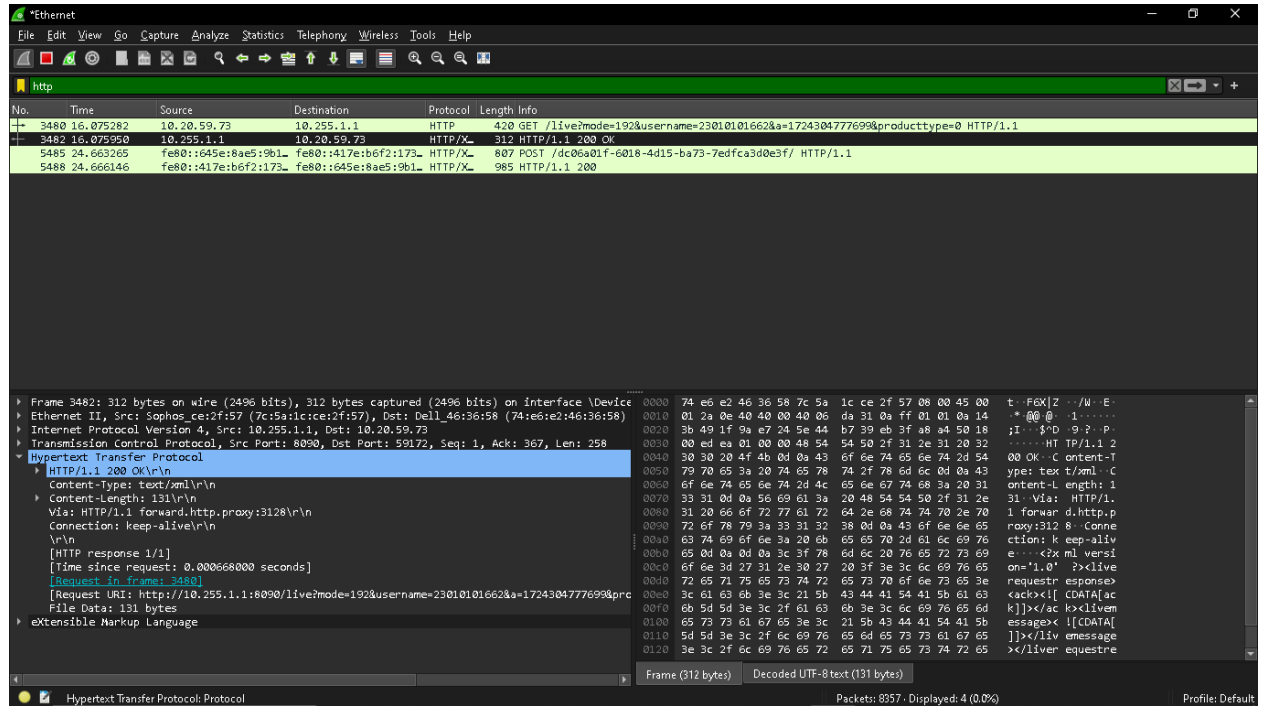
Date: 22/08/2024

- **Security Monitoring:** Detect unauthorized access, malware activity, or unusual traffic patterns that could indicate a security breach.
- **Application Performance Tuning:** Monitor and optimize the performance of networked applications by analyzing the communication between client and server.
- **VoIP Analysis:** Capture and analyze Voice over IP (VoIP) traffic to troubleshoot call quality issues and inspect SIP and RTP protocols.
- **Network Forensics:** Investigate network incidents, such as data breaches or cyberattacks, by reviewing captured packet data for evidence.
- **Learning and Education:** Study network protocols, packet structures, and traffic patterns to enhance your understanding of networking concepts.
- **Bandwidth Usage Analysis:** Monitor and analyze network bandwidth consumption to identify heavy bandwidth users or applications.
- **Network Mapping:** Visualize the flow of data across the network, helping in understanding network topology and device communication.
- **Compliance Auditing:** Ensure that network communications adhere to organizational policies and regulatory requirements by capturing and inspecting relevant traffic.

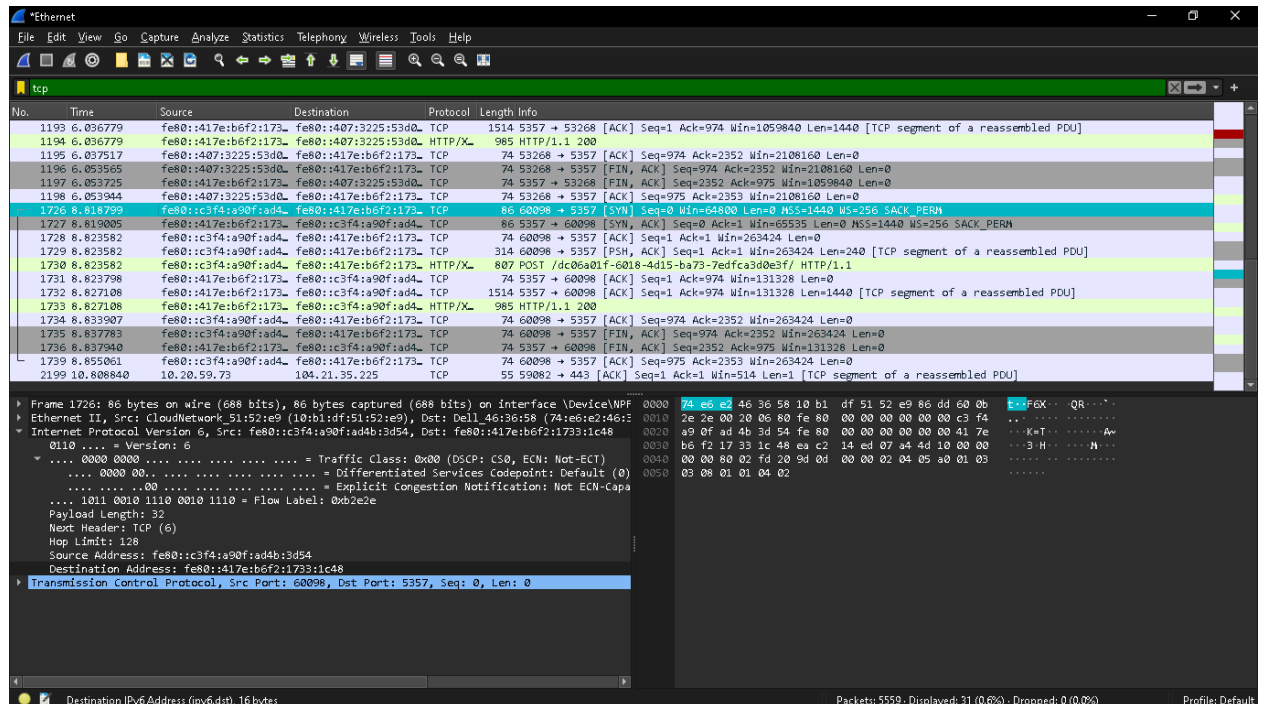
Date: 22/08/2024

2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

• HTTP :

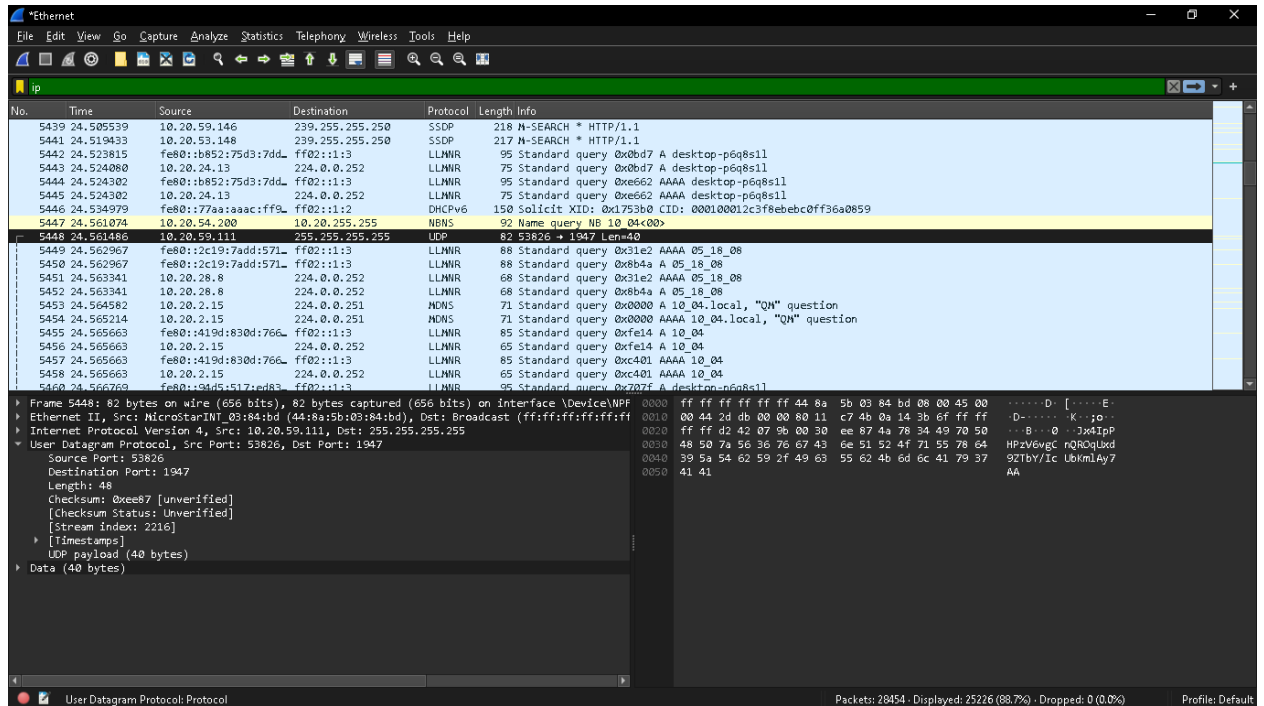


• TCP :



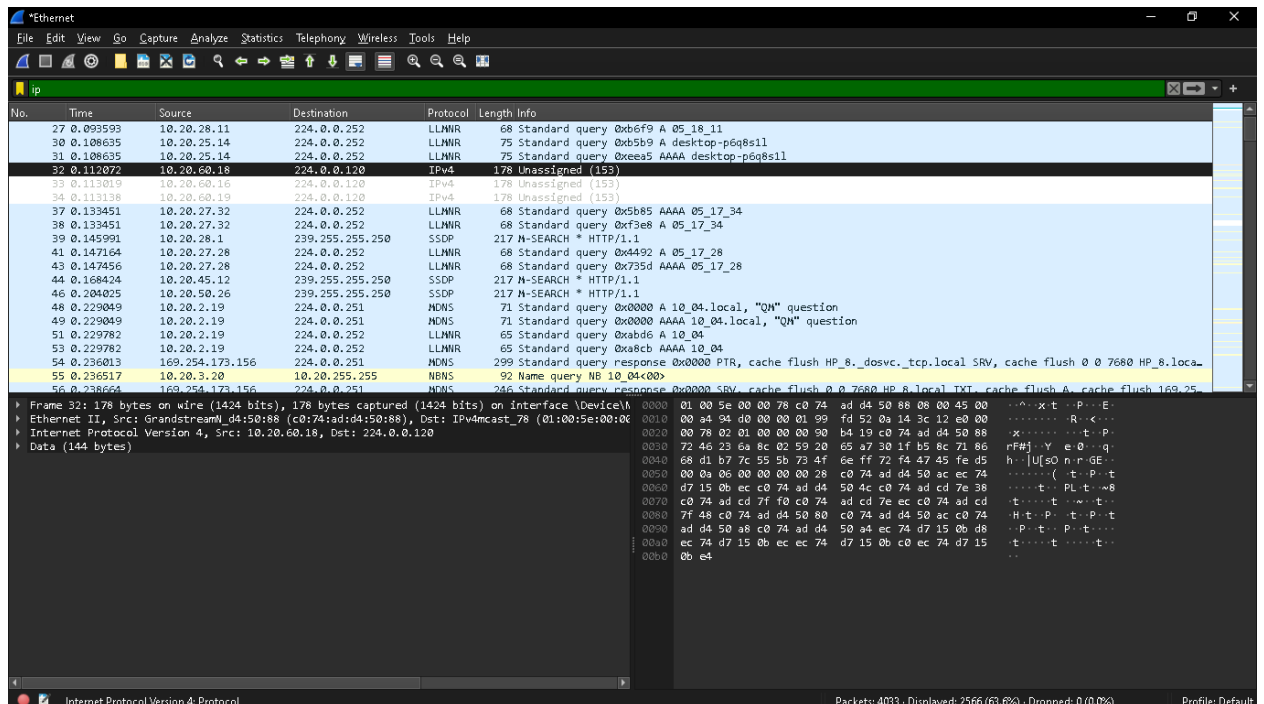
Date: 22/08/2024

• UDP :



The screenshot shows a Wireshark capture of network traffic on the 'ethernet' interface. The packet list pane displays several packets, with packet 5448 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The UDP section shows a source port of 53826 and a destination port of 1947. The packet length is 48 bytes, and the checksum is 0xee87 (unverified). The UDP payload is 40 bytes.

• IP :



The screenshot shows a Wireshark capture of network traffic on the 'ethernet' interface. The packet list pane displays several packets, with packet 32 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Internet Protocol Version 4. The IP section shows a source address of 10.20.59.111 and a destination address of 255.255.255.255. The packet length is 144 bytes.