Lab Practical #09:

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

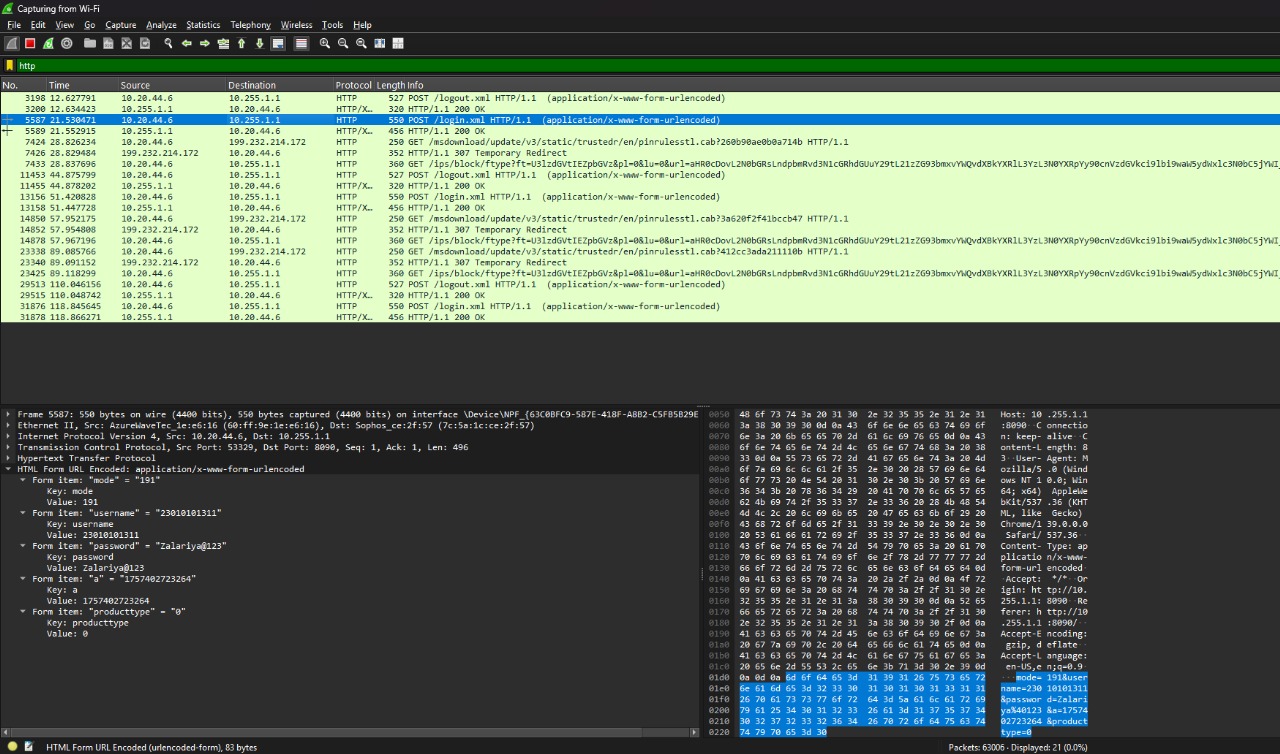
**Practical Assignment #09:**

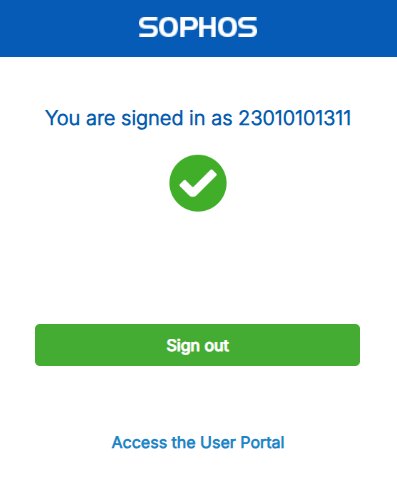
1. **Explain usage of Wireshark tool.**
2. **Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)**

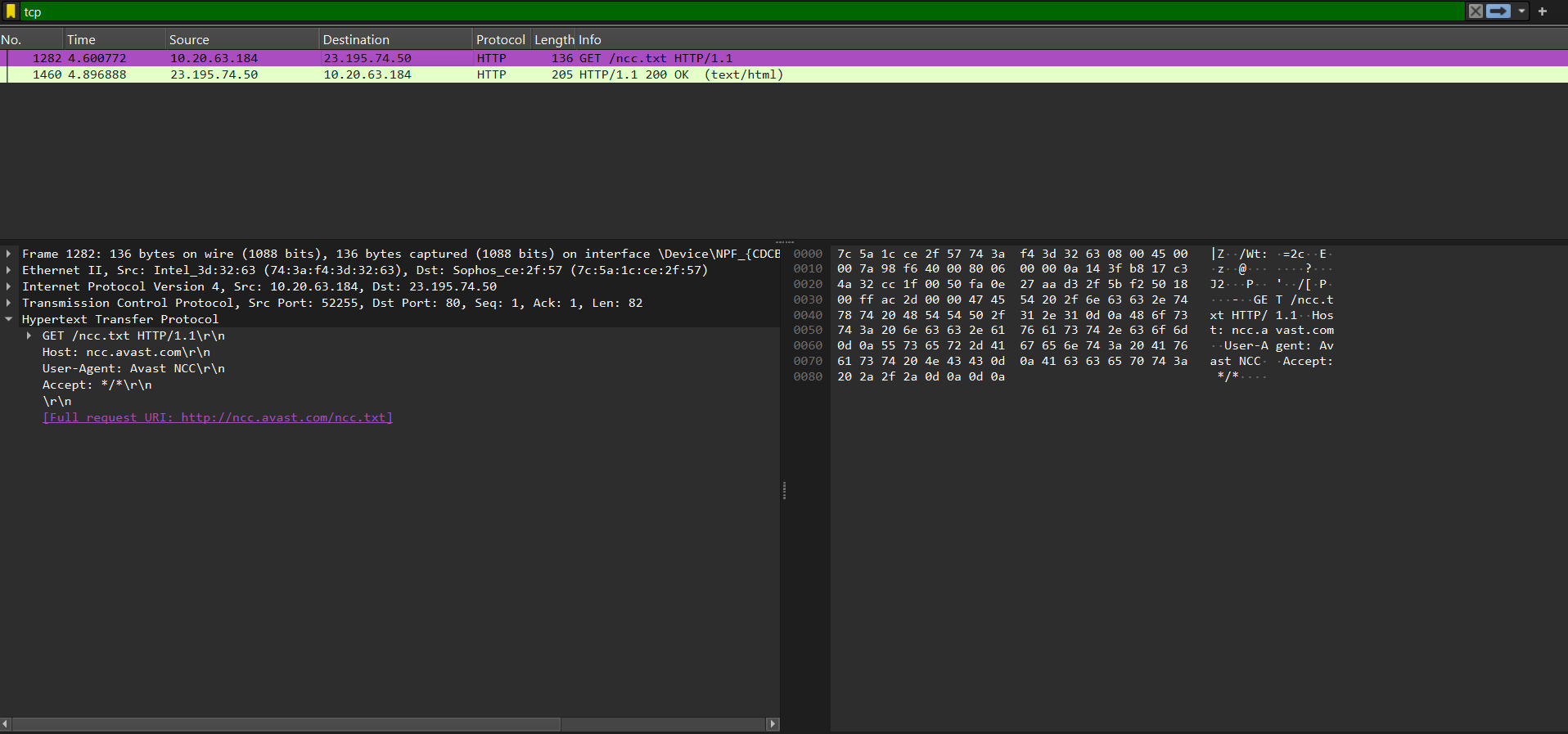
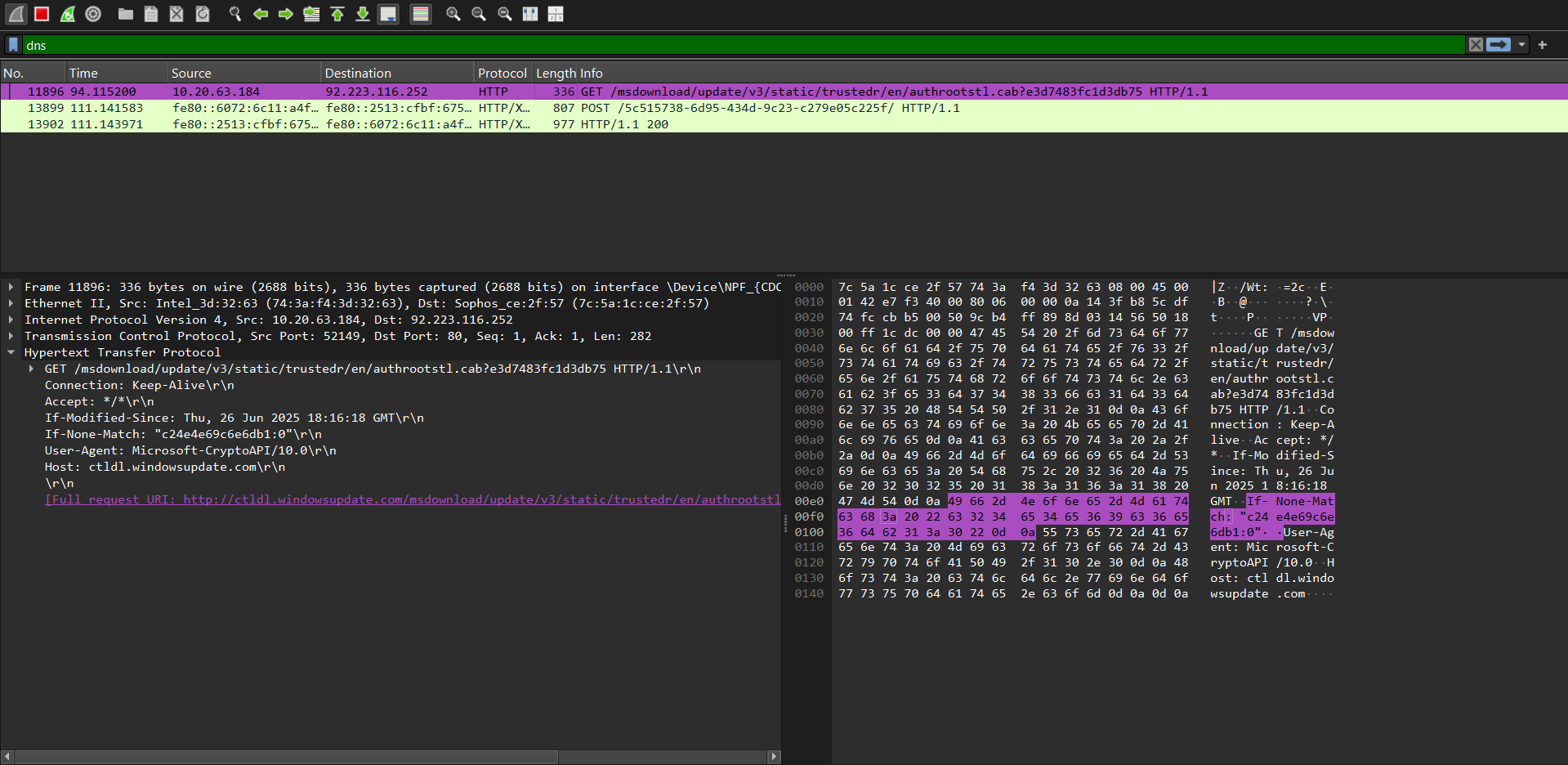
**1. Usage of Wireshark Tools**

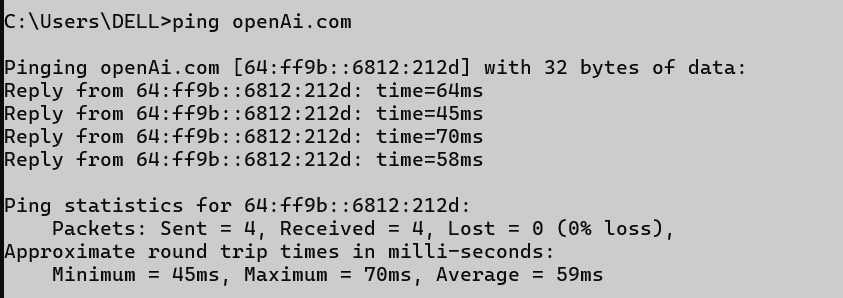
1. **Captures Network Traffic**
2. Wireshark records the data packets that travel over a network (like Wi-Fi or LAN).
3. It helps in monitoring what is happening in real-time on the network**.**
4. **Analyzes Packets**
5. Each packet (small unit of data) can be examined to check details like source, destination, and protocol used.
6. This is useful to understand how communication happens between different devices.
7. **Troubleshooting Networks**
8. Helps in finding network issues such as slow speed, connection drops, or wrong configurations.
9. Can show errors or unusual patterns in data flow, which makes debugging easier.
10. **Supports Many Protocols**
11. Wireshark can recognize and display hundreds of protocols (HTTP, TCP, UDP, DNS, etc.).
12. This makes it easy to study how various applications and services communicate.
13. **Filtering and Searching**
14. Provides powerful filters to focus on specific data (e.g., only HTTP traffic or packets from a particular IP address).
15. This feature saves time and allows targeted analysis.
16. **Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)**

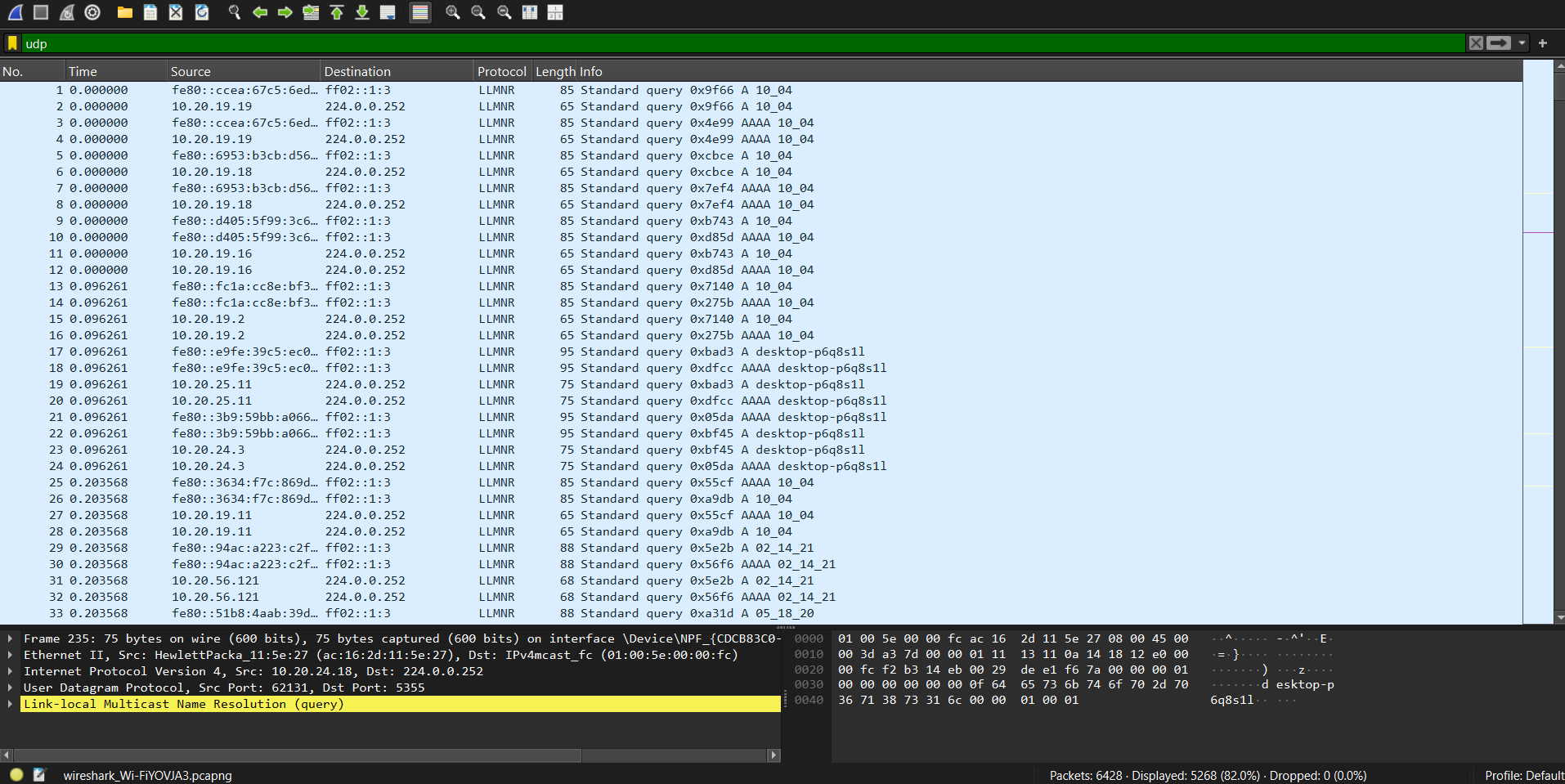
Using Wireshark, we can capture packets and analyze their headers at different layers of the OSI model. Some examples of header analysis include:  
 **• IP Header:** Contains source IP, destination IP, version, header length, TTL, and protocol type. **• TCP Header:** Includes source port, destination port, sequence number, acknowledgment number, flags, and window size.  
**• UDP Header:** Contains source port, destination port, length, and checksum. **• HTTP Header:** Includes request type (GET/POST), URL, host, user-agent, cookies, and response codes.

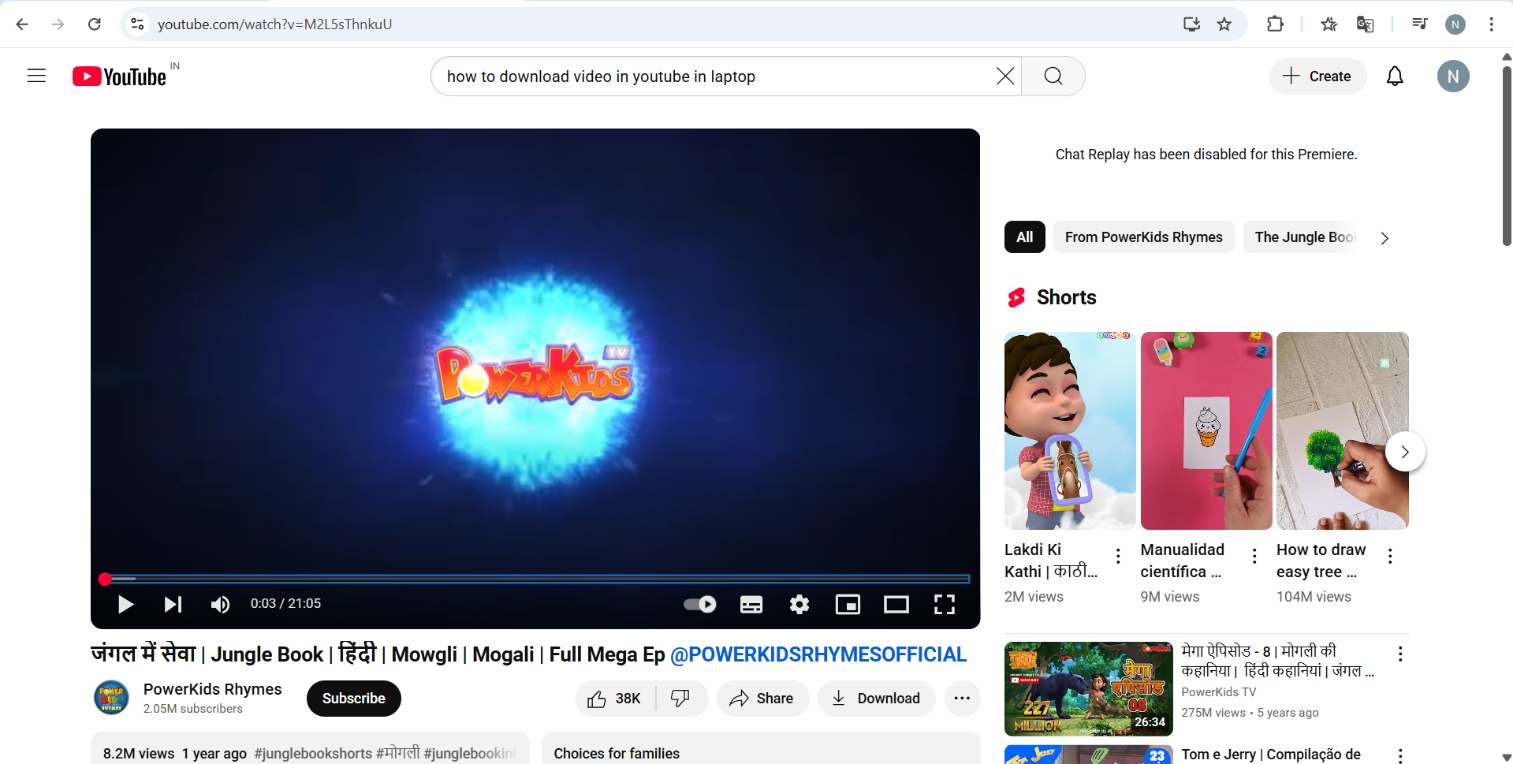
1. **HTTP**

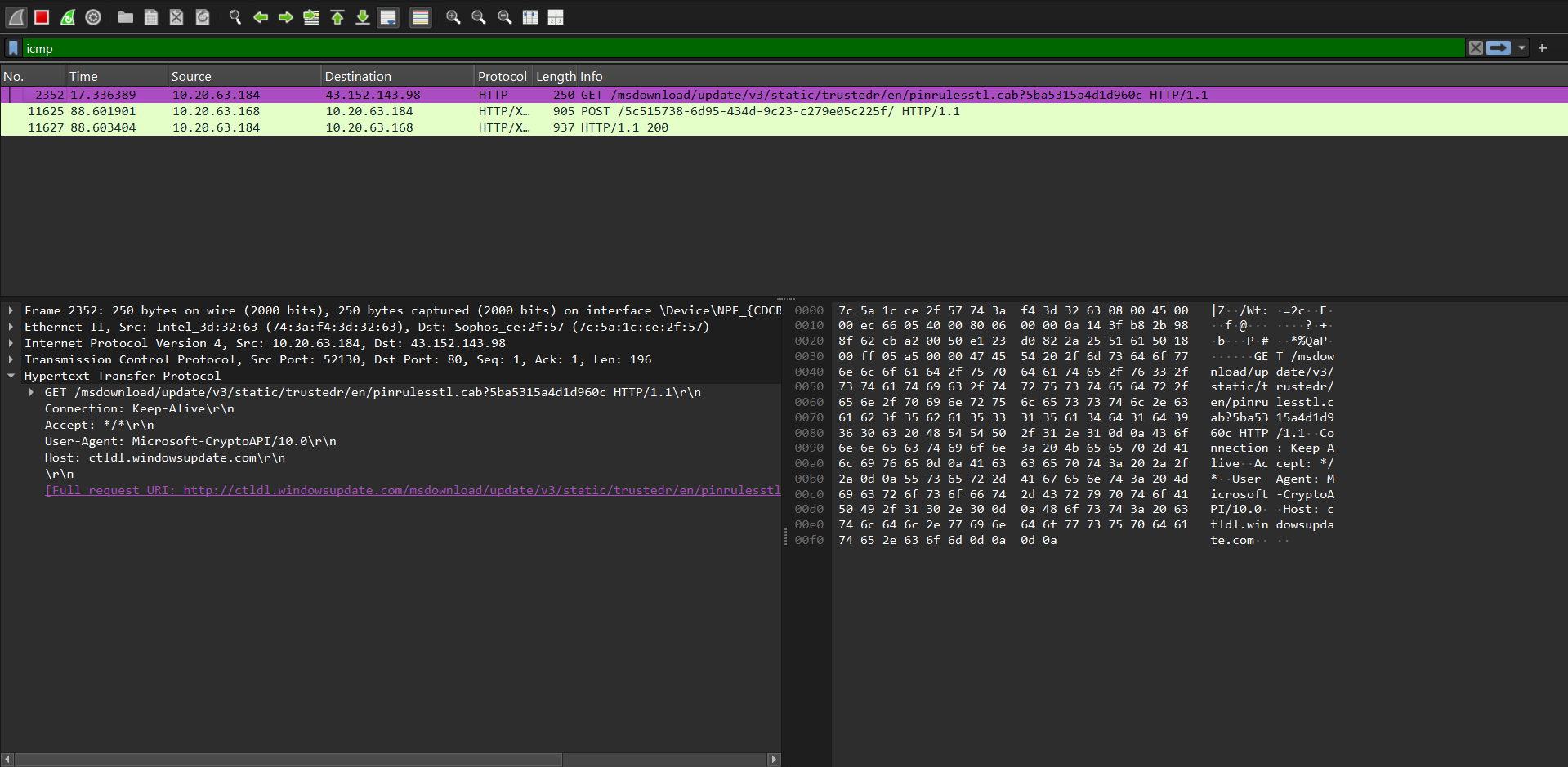
****

1. **TCP**
2. **DNS**



1. **UDP**



1. **ICMP**

