**Lab Practical #09:**

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

**Practical Assignment #09:**

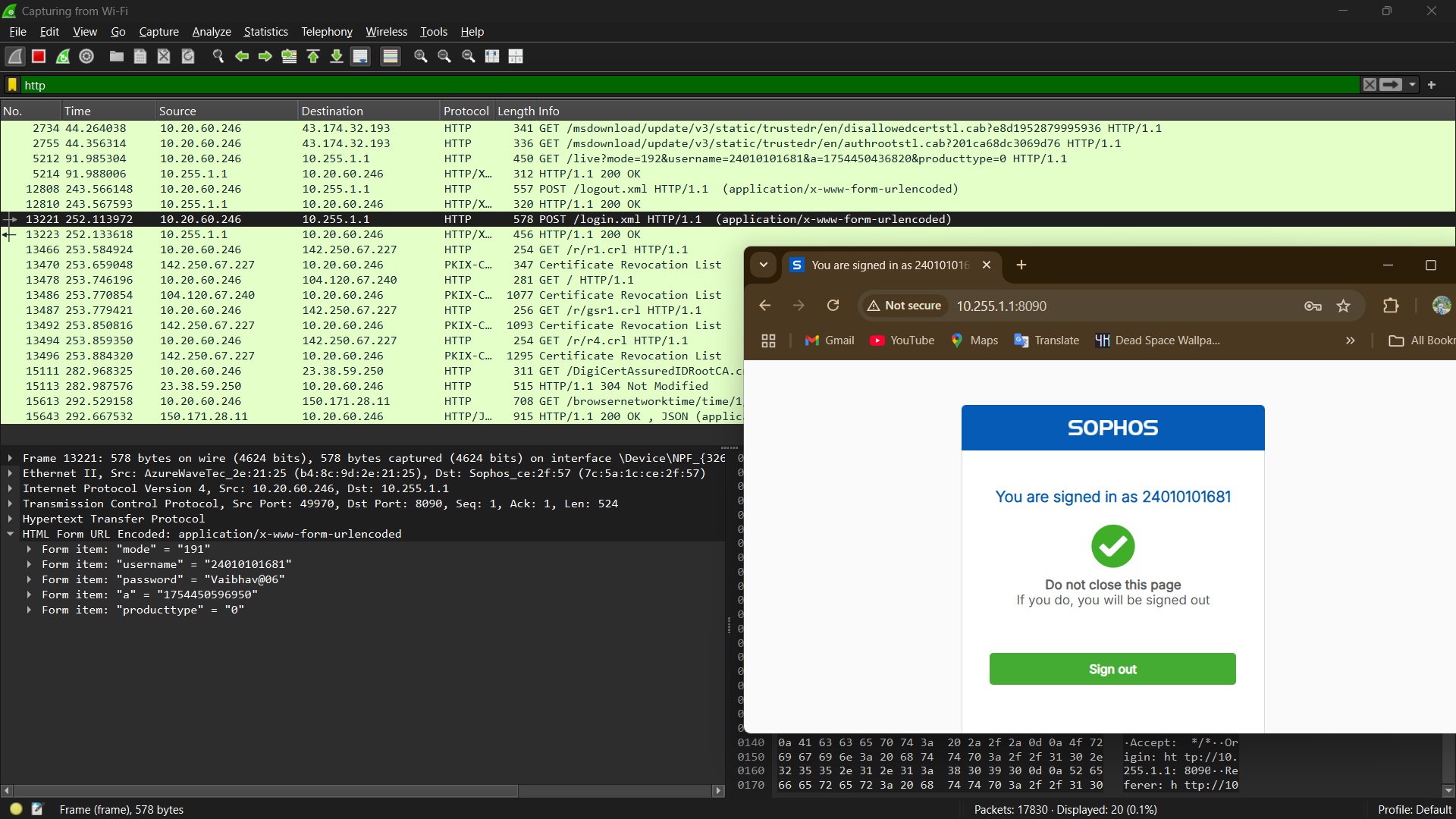
1. **Explain usage of Wireshark tool.**

**Wireshark is a free and open-source network protocol analyzer used to capture and analyze packets in real-time. It supports hundreds of protocols and displays packet details layer by layer (OSI/TCP-IP model).**

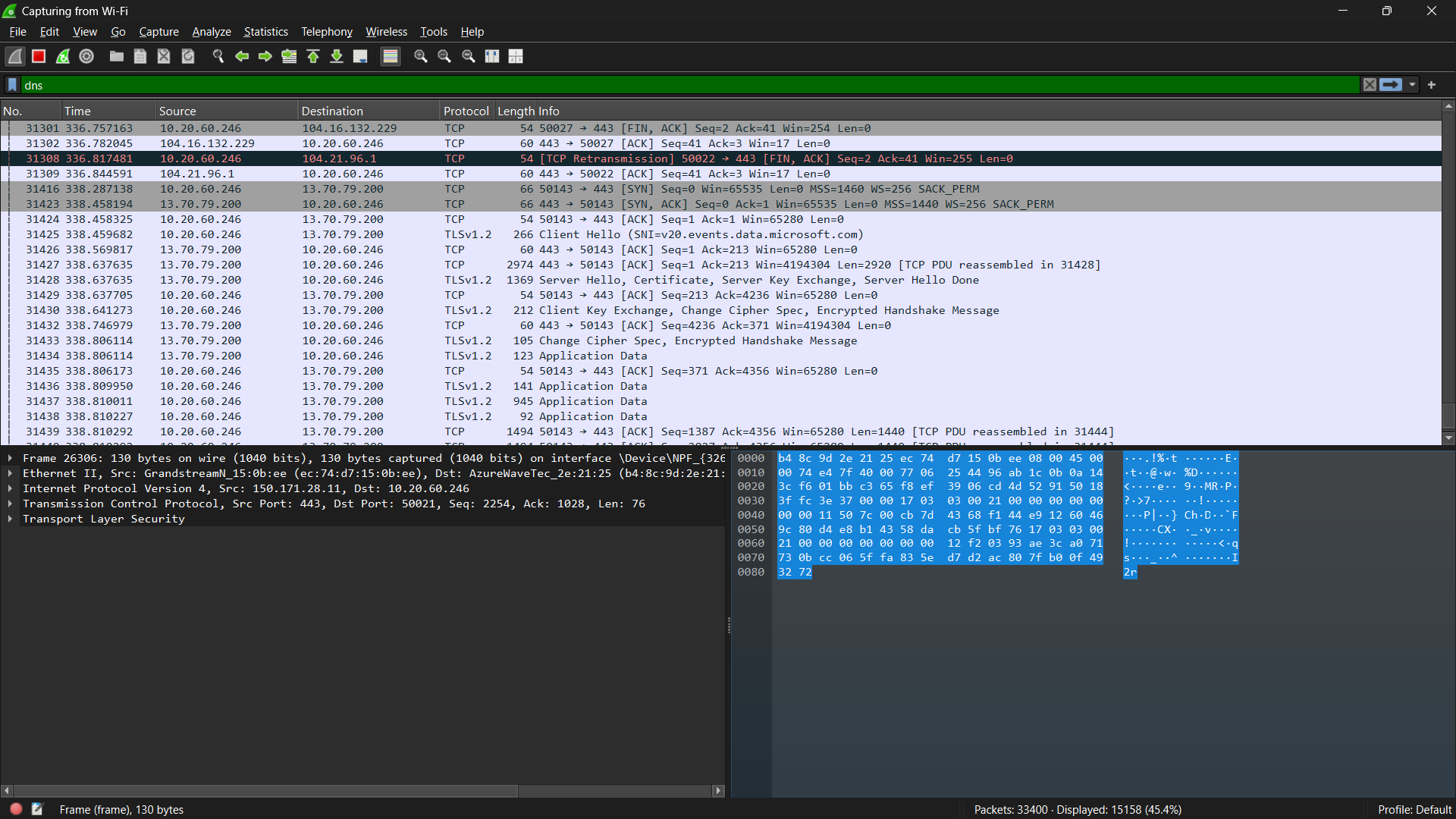
**Uses:**

* **Captures live network traffic for monitoring.**
* **Troubleshoots network issues (latency, packet loss, misconfigurations).**
* **Analyzes protocols like TCP, UDP, HTTP, DNS, etc.**
* **Detects suspicious/malicious activities for security monitoring.**
* **Helps in performance analysis and bandwidth monitoring.**
* **Useful for learning networking concepts.**
* **Should be used only on authorized networks since packet sniffing without permission is illegal.**

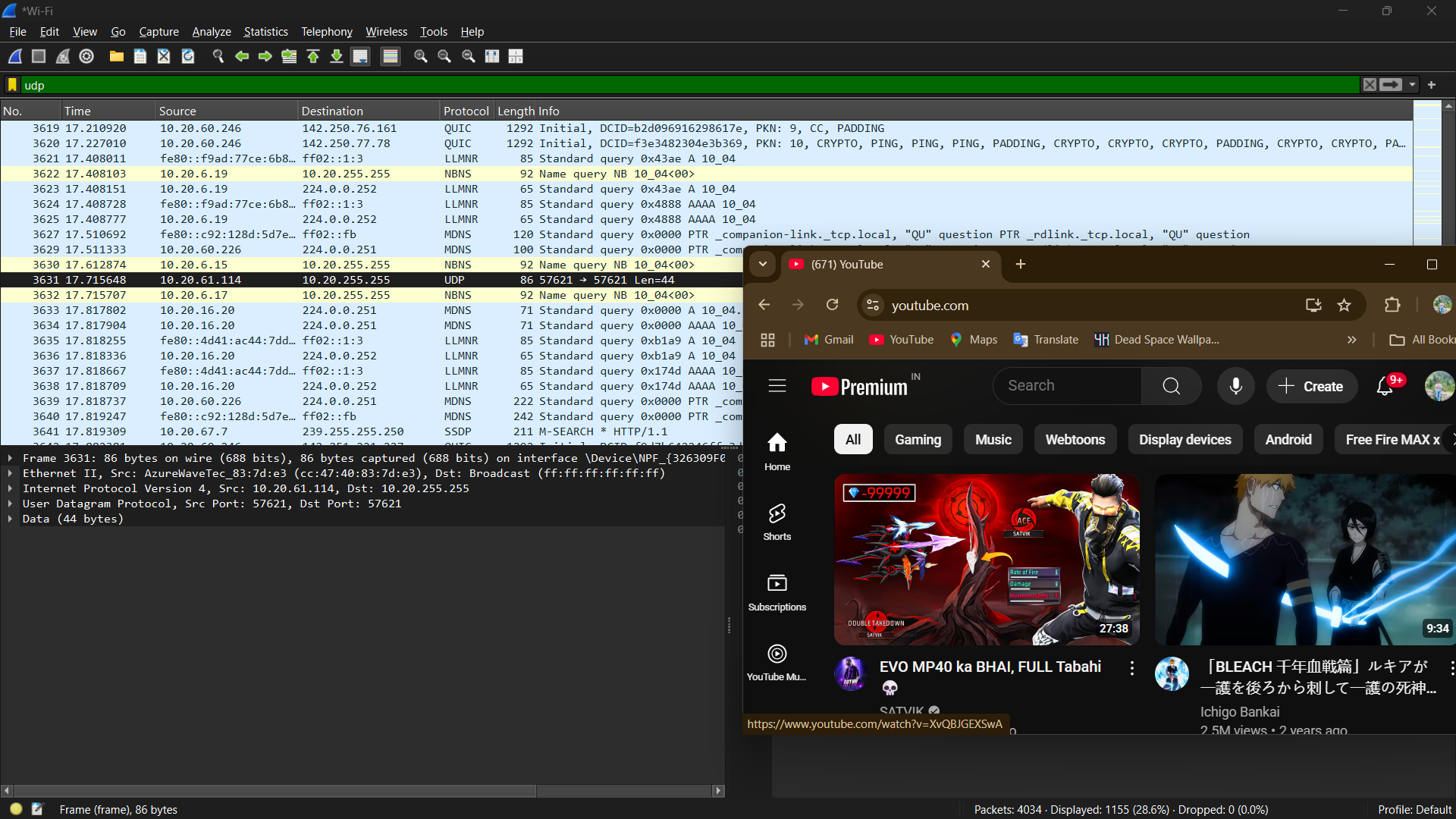
1. **Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)**
   * **HTTP**



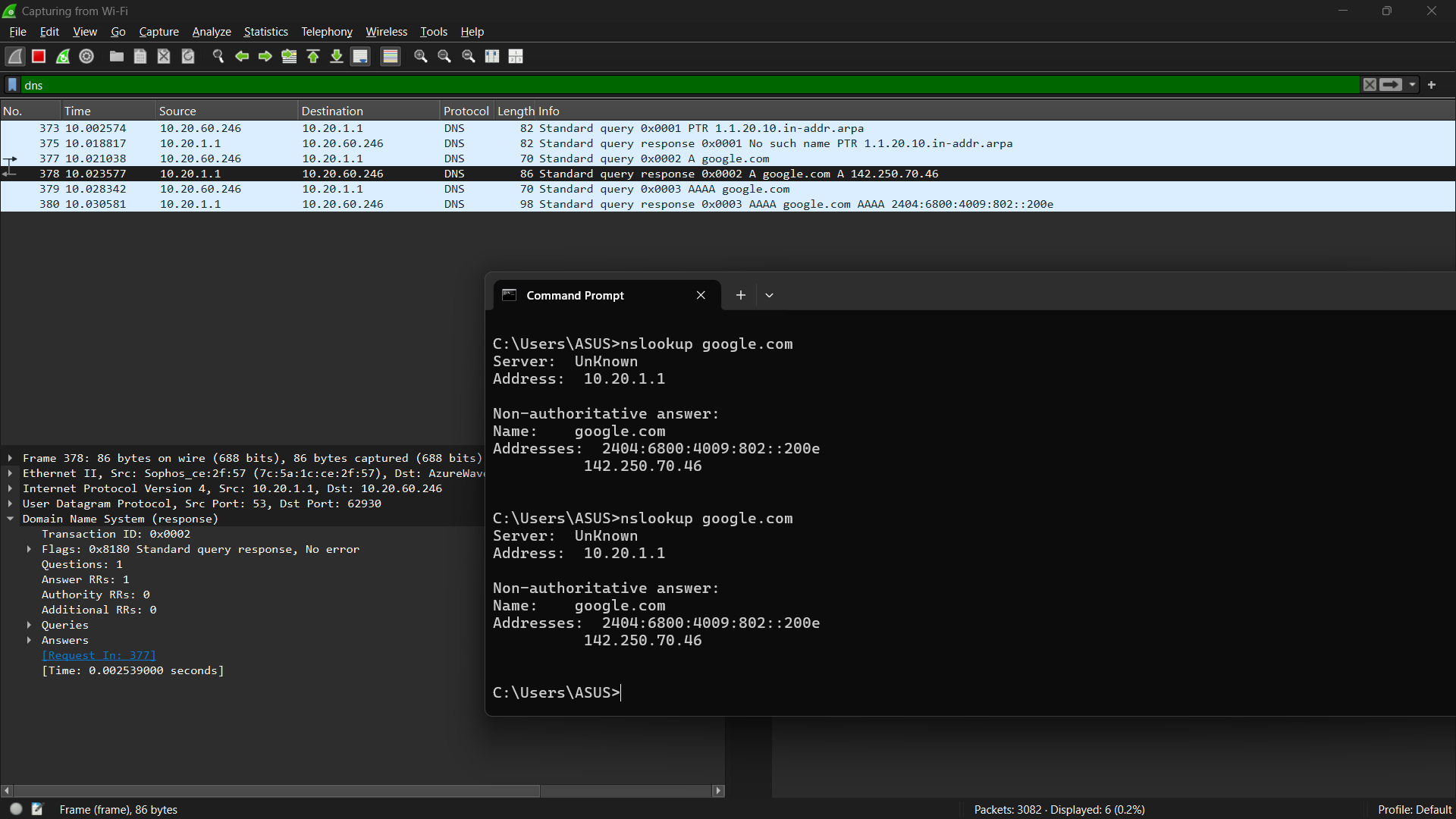
**TCP**



**UDP**



**DNS**



**ICMP**

