**Lab Practical #08:**

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

**Practical Assignment #08:**

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

**Packet Capture**

Wireshark captures packets in real-time as they are transmitted over a network. It can capture data from various network interfaces such as Ethernet, Wi-Fi, and others. This ability to capture packets is fundamental for analyzing network issues.

**Protocol Analysis**

Wireshark provides detailed information about different network protocols. It decodes the data in captured packets and presents it in a human-readable format. It supports hundreds of protocols, including common ones like TCP, UDP, HTTP, DNS, and more. This is invaluable for diagnosing network problems and understanding how applications communicate over the network.

**Troubleshooting Network Issues**

Network administrators use Wireshark to troubleshoot various network problems such as slow performance, connectivity issues, and suspicious activities. By analyzing the captured packets, they can identify errors, latency, or misconfigurations that might be causing problems.

**Security Analysis**

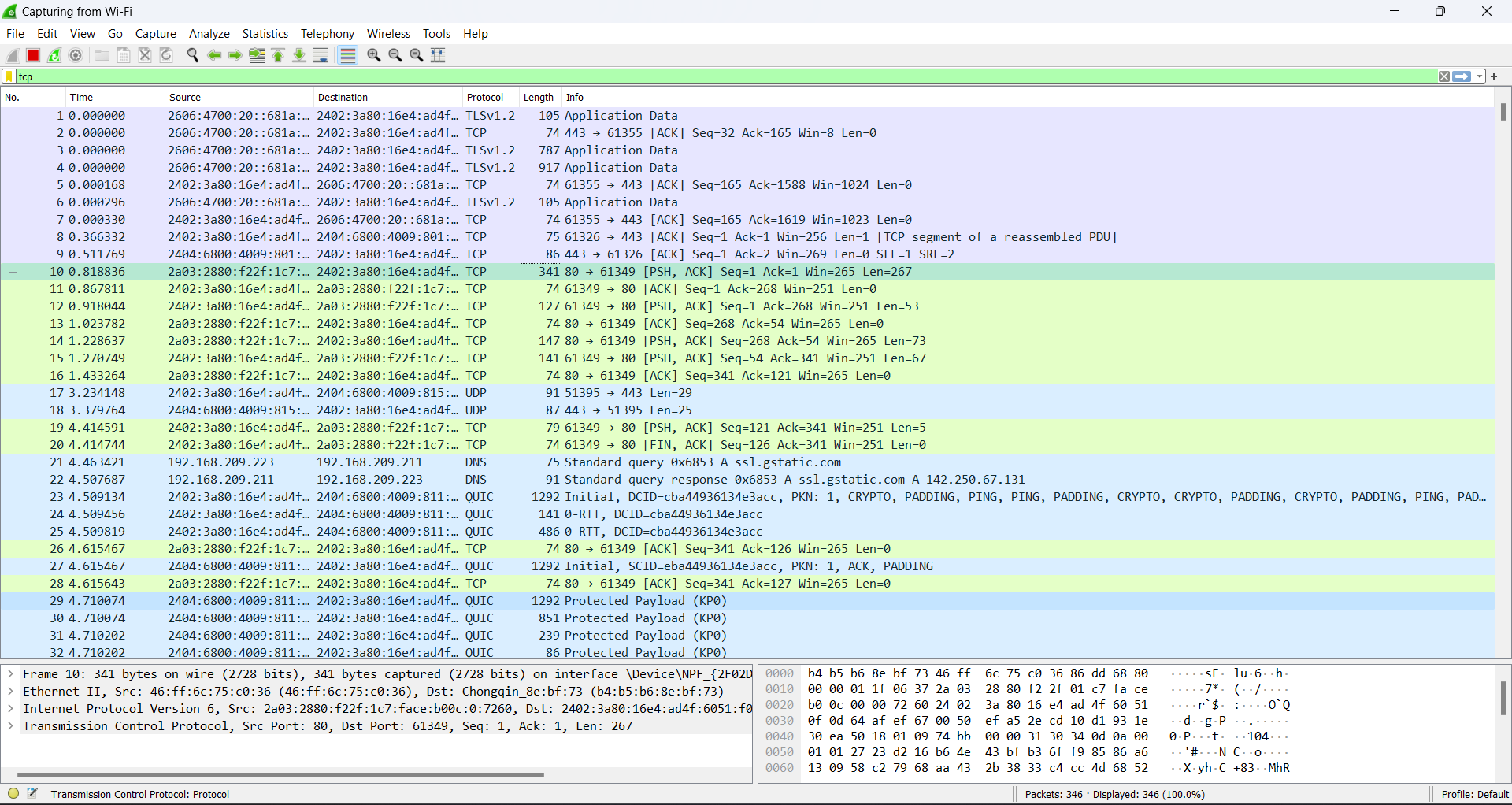
Wireshark is a powerful tool for security professionals. It can be used to detect security breaches, unauthorized access, and malicious activities. Security analysts use Wireshark to inspect network traffic for signs of attacks, such as malware infections, intrusion attempts, or data exfiltration.

**Network Performance Analysis**

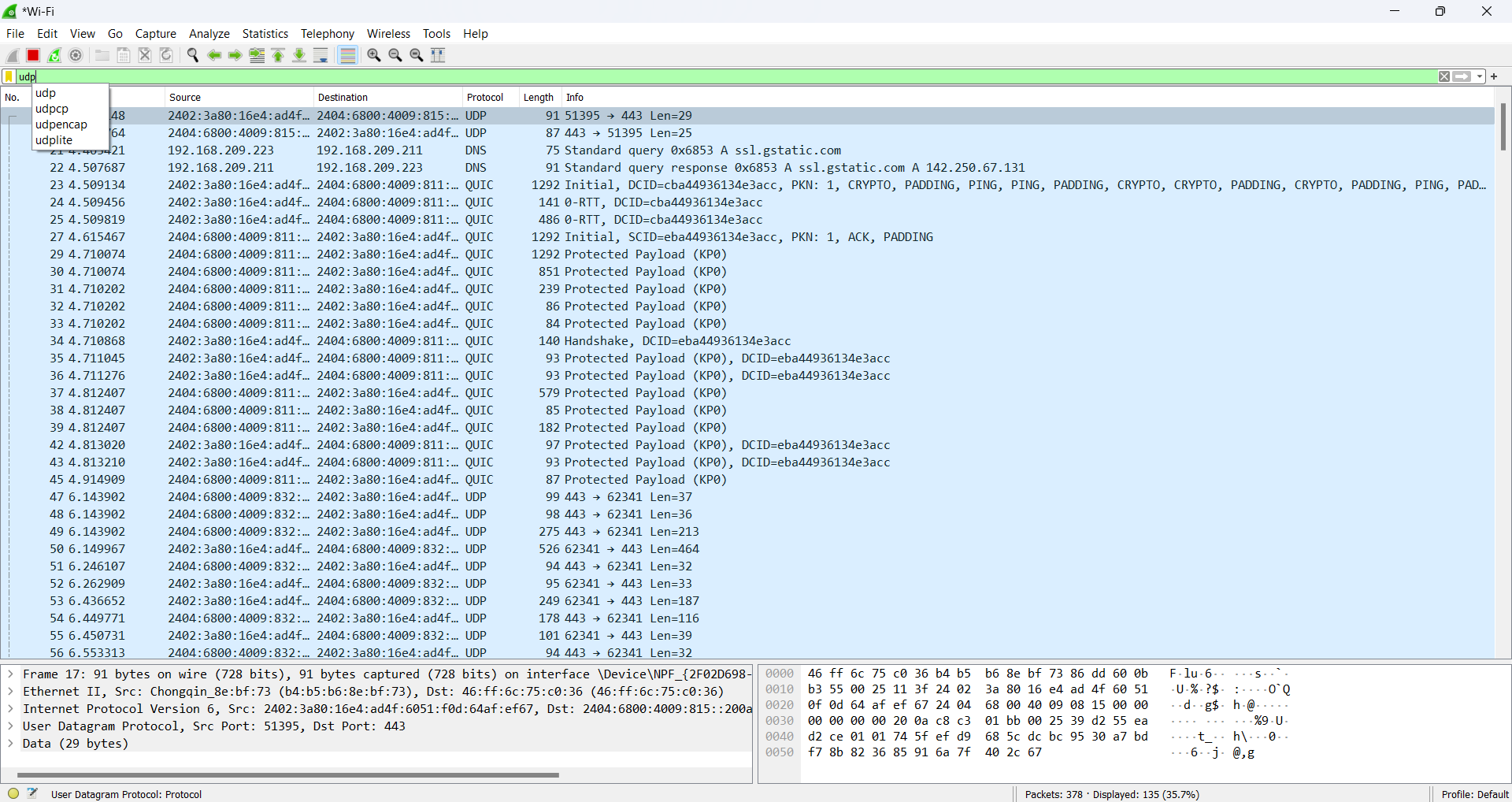
Wireshark helps in analyzing network performance by providing insights into data transfer rates, response times, and bottlenecks. By studying the captured packets, network administrators can optimize the network infrastructure for better performance.

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

* **TCP:**



* **UDP:**



* **IP:**

