**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 tool that helps you see what’s really happening on a network. Think of it like a microscope for network traffic—it lets you capture and study the data that travels between computers, servers, and devices.

**Usage:**

1. To Watch Network Traffic in Real-Time

* You can see every packet (tiny piece of data) going in and out of your network.
* It shows details like where it came from, where it’s going, and what protocol it uses.

1. To Understand Network Protocols

* Wireshark can “translate” thousands of different protocols (like HTTP, DNS, or TCP) into a readable form, so you don’t have to decode them yourself.

1. To Fix Network Problems

* If your internet feels slow or connections keep dropping, Wireshark can help find the cause—like packet loss, delays, or misconfigured devices.

1. To Keep an Eye on Performance

* You can check how much bandwidth is being used and whether the network is overloaded.

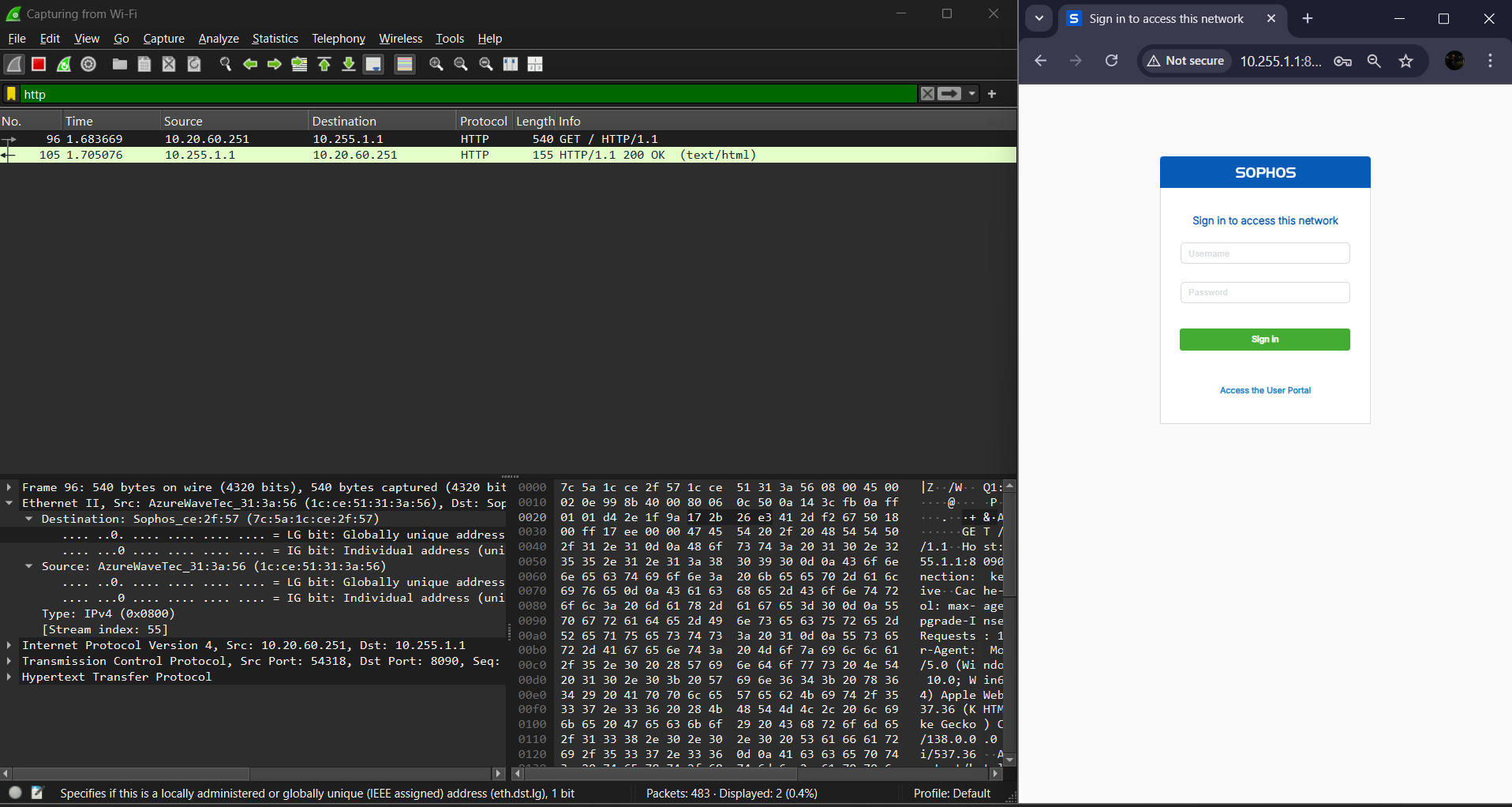
1. To Filter and Focus

* Wireshark lets you filter out unnecessary information and look only at the data that matters to you.

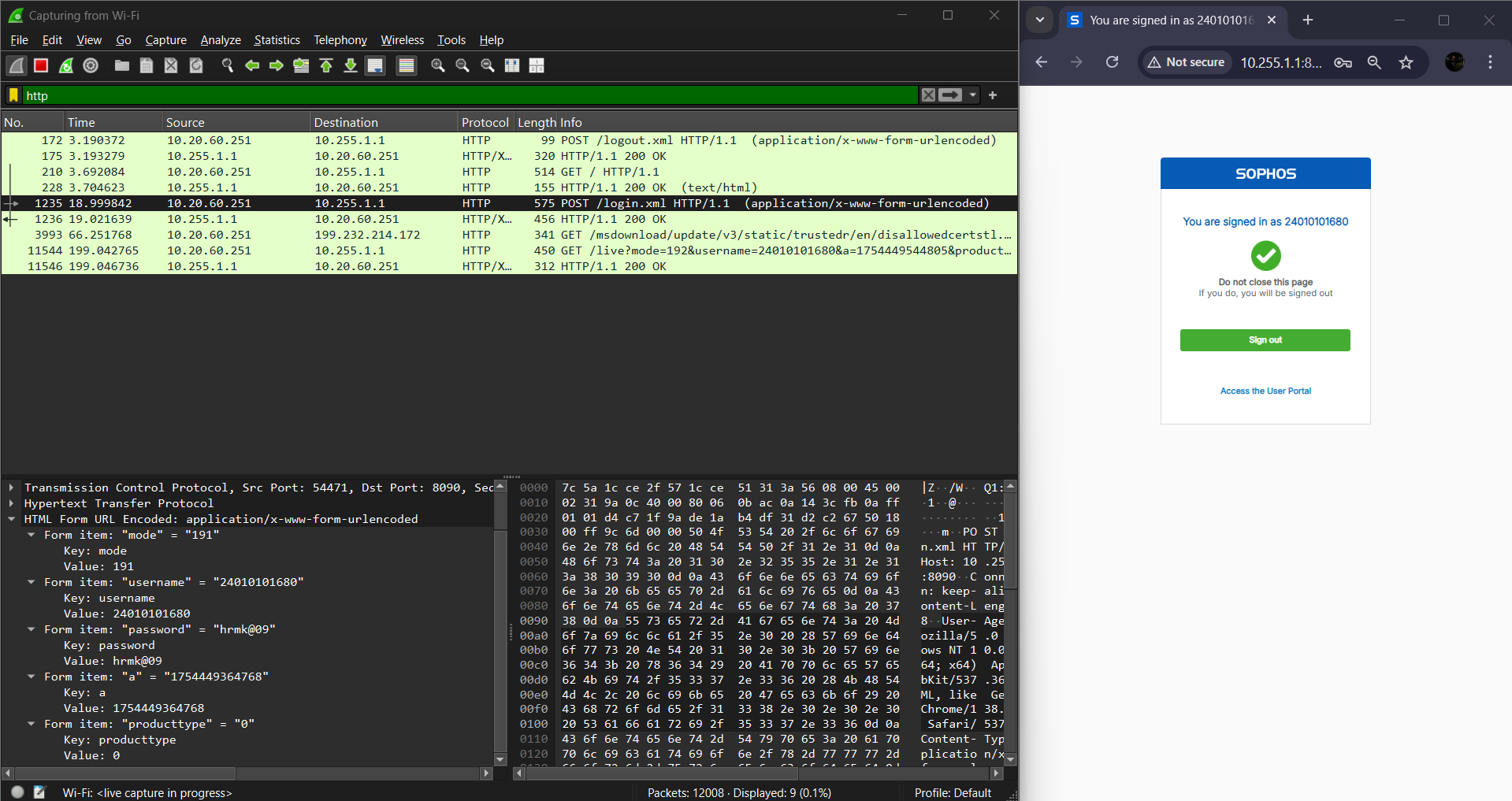
1. To Save and Share Results

* You can save what you capture and share it with your team for further investigation.

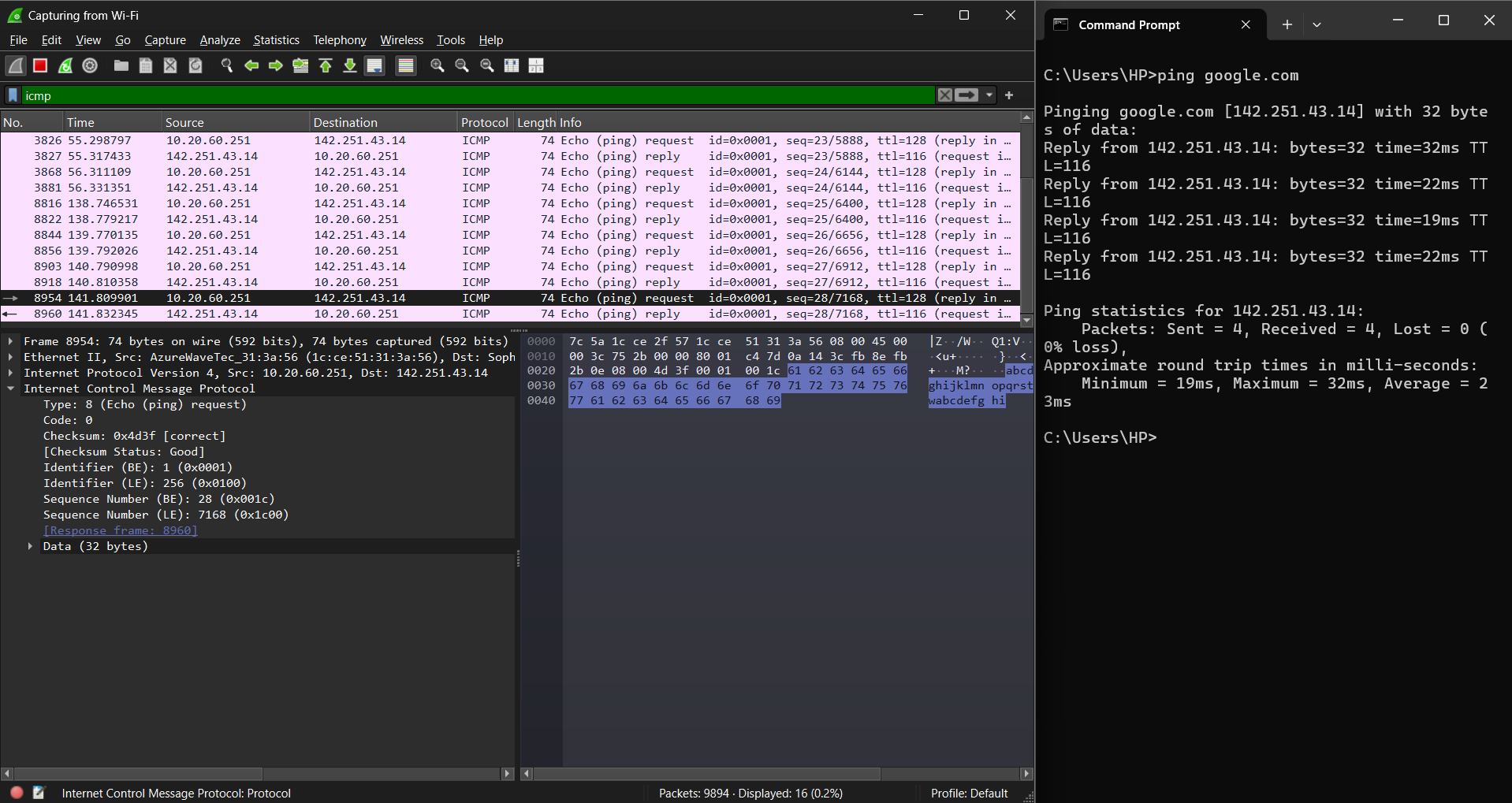
1. **Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)**



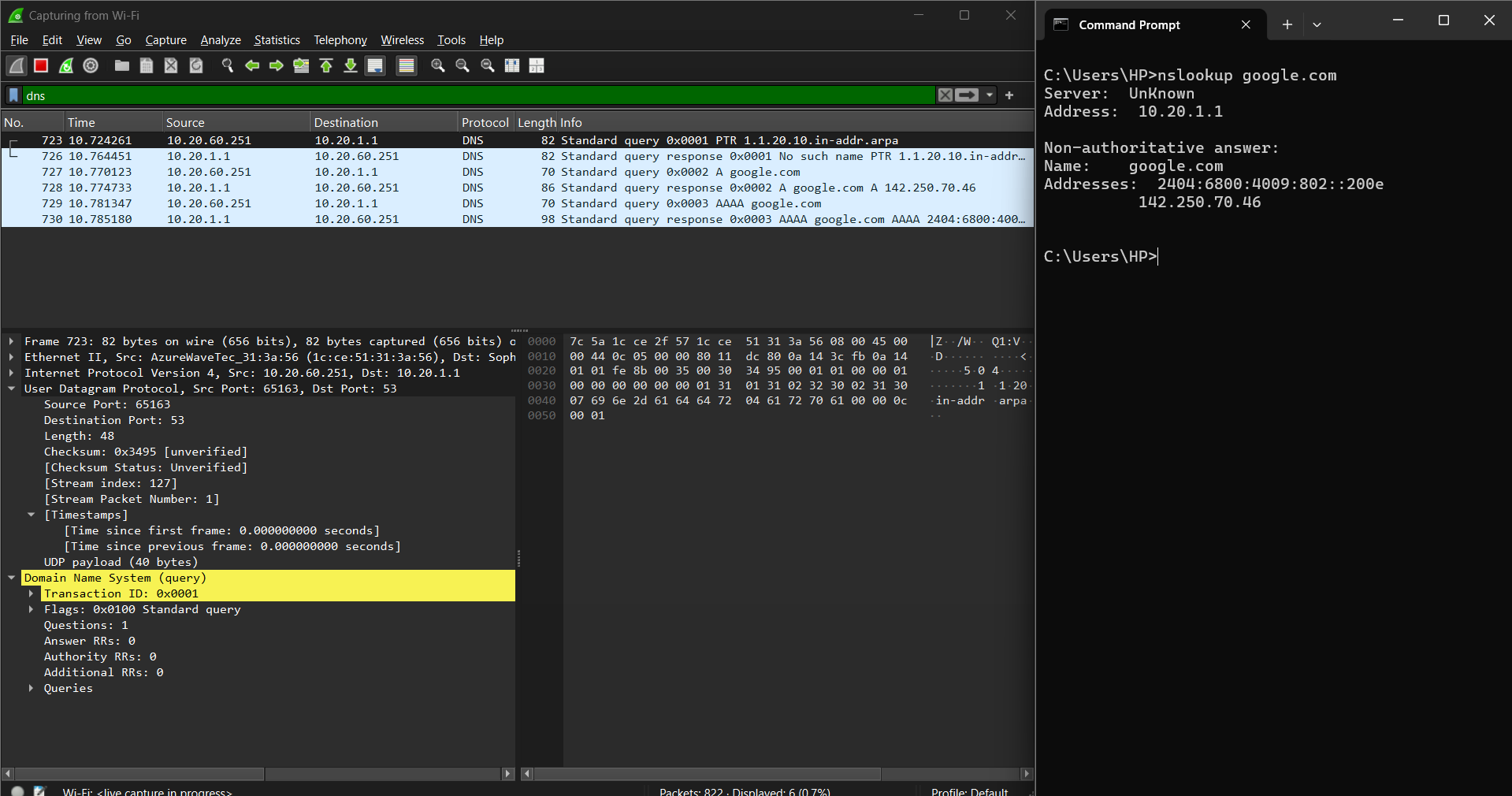
* 1. *Analysis of HTTP without login Sophos*

**

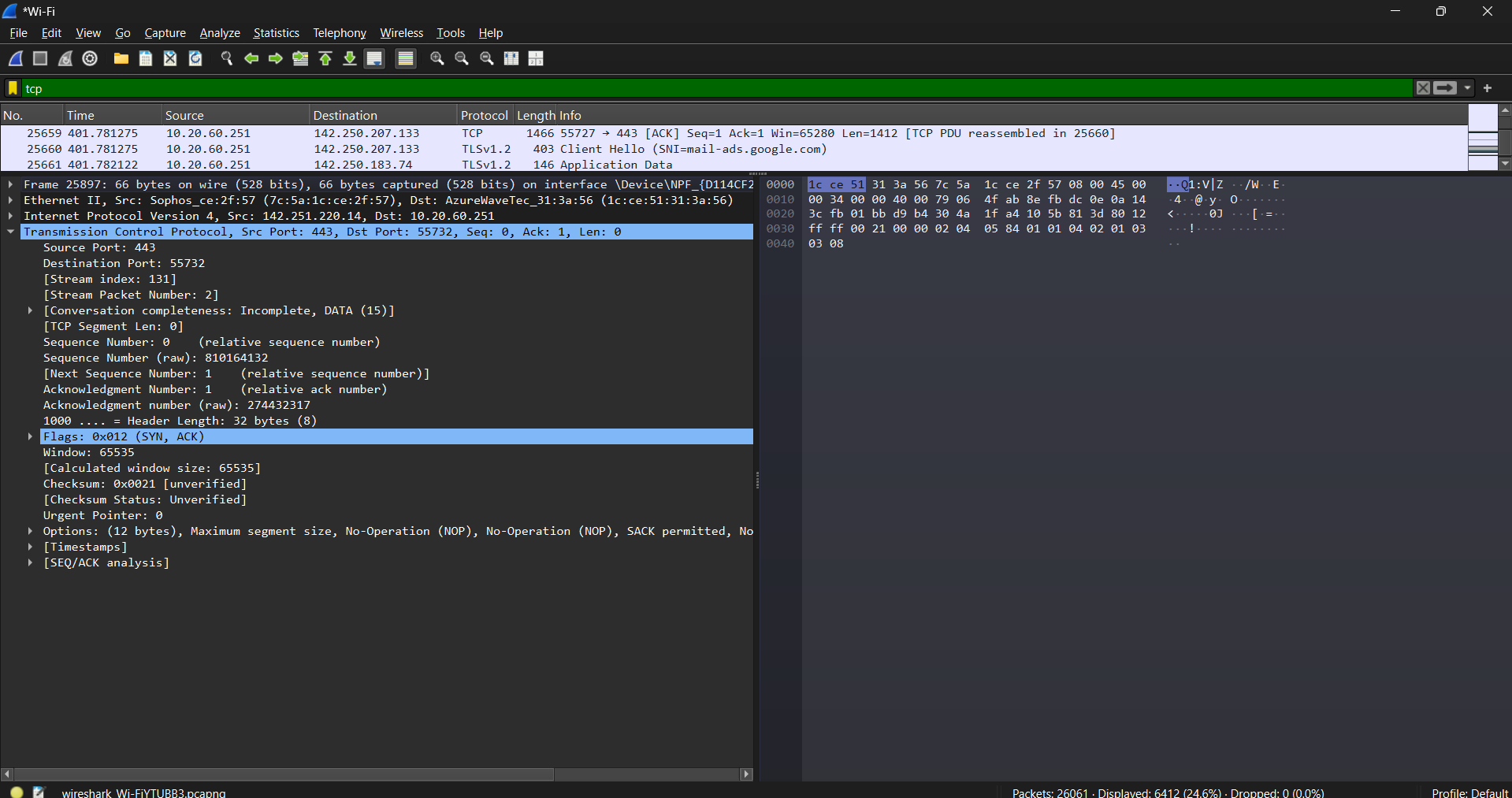
* 1. *Analysis of HTTP with login Sophos*

**

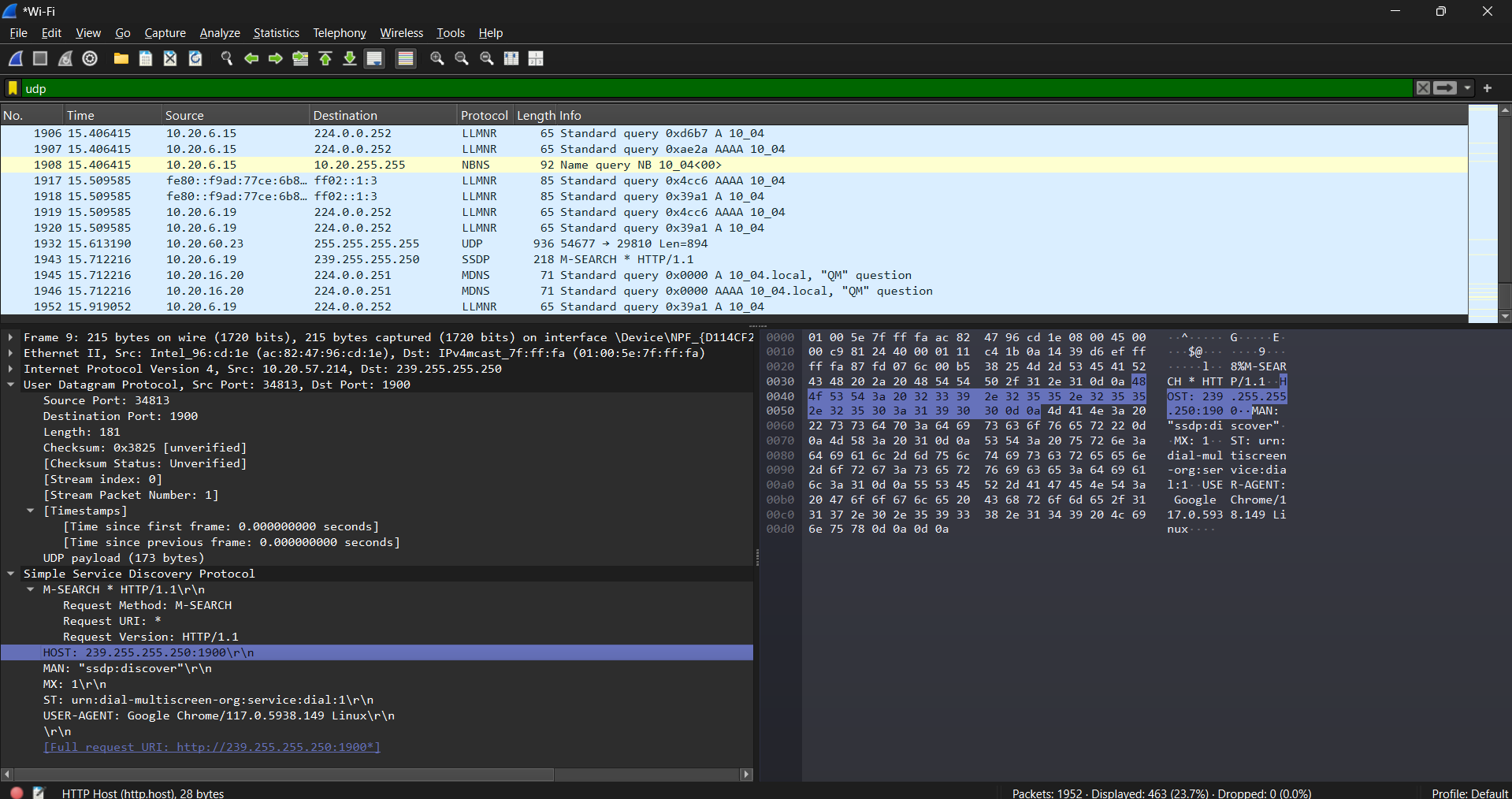
* 1. *Analysis of ICMP*

**

* 1. *Analysis of DNS*

**

* 1. *Analysis of TCP*

**

* 1. *Analysis of UDP*