



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.

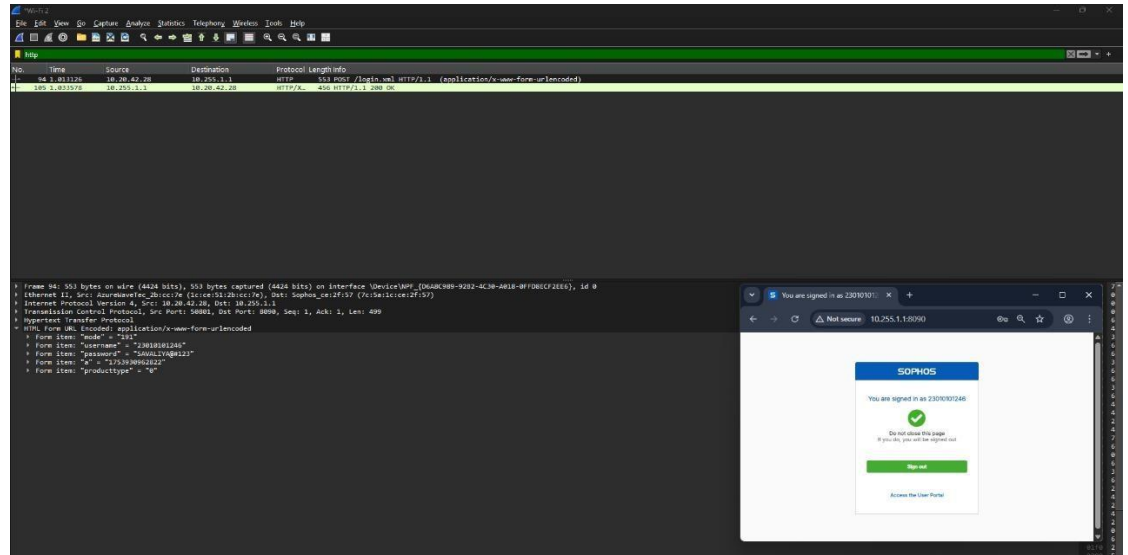
Wireshark is a tool that helps you see what's really happening on a network. Think of it like a microscope for network traffic—it lets you capture and study the data that travels between computers, servers, and devices.

Usage:

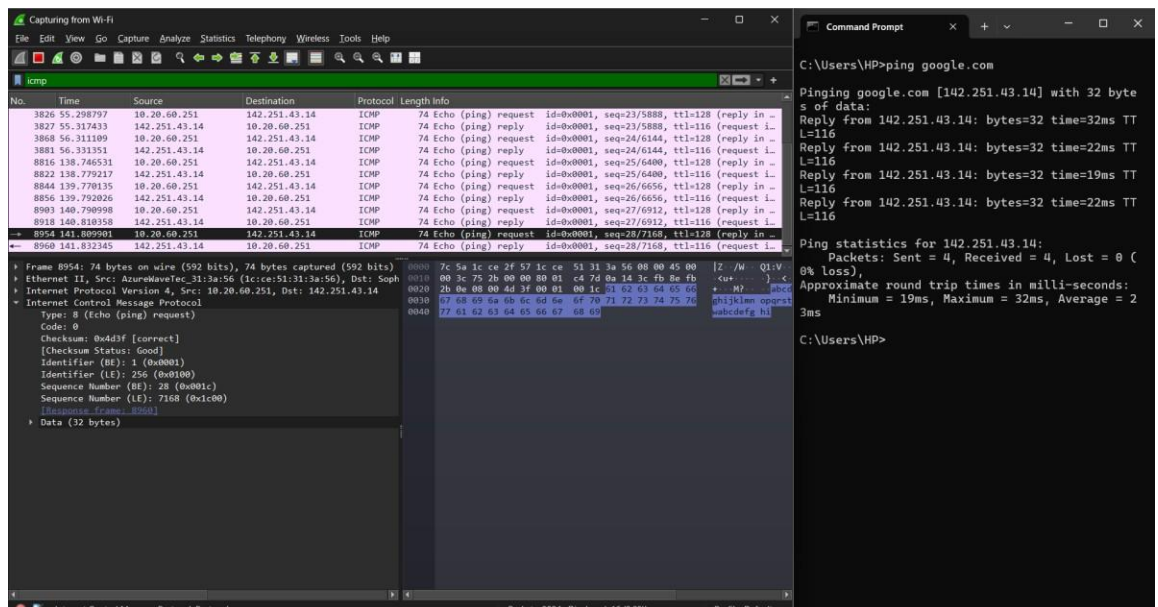
1. To Watch Network Traffic in Real-Time
 - You can see every packet (tiny piece of data) going in and out of your network.
 - It shows details like where it came from, where it's going, and what protocol it uses.
2. To Understand Network Protocols
 - Wireshark can “translate” thousands of different protocols (like HTTP, DNS, or TCP) into a readable form, so you don't have to decode them yourself.
3. 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.
4. To Keep an Eye on Performance
 - You can check how much bandwidth is being used and whether the network is overloaded.
5. To Filter and Focus
 - Wireshark lets you filter out unnecessary information and look only at the data that matters to you.
6. To Save and Share Results
 - You can save what you capture and share it with your team for further investigation.

Date: / /

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

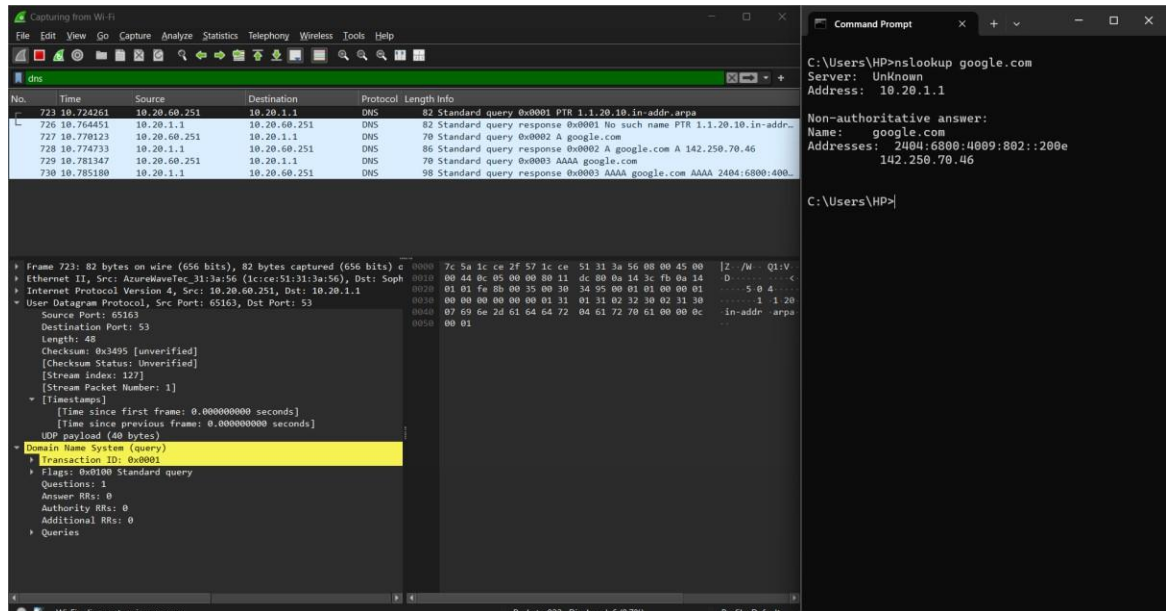


1.1 Analysis of HTTP with login Sophos



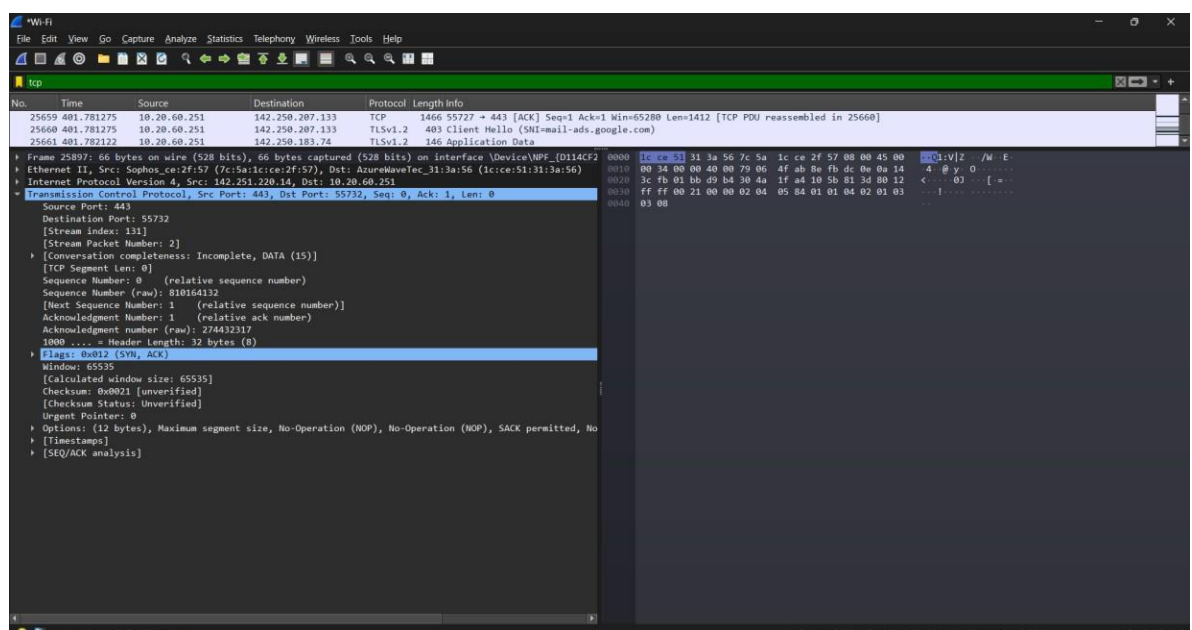
1.2 Analysis of ICMP

Date: / /



The image shows two side-by-side windows. On the left is Wireshark, capturing traffic on the Wi-Fi interface. The packet list shows several DNS messages. Packet 723 is a standard query from 10.20.60.251 to 10.20.1.1. Packet 726 is a standard query response from 10.20.60.251 to 10.20.1.1. Packet 727 is a standard query from 10.20.60.251 to 10.20.1.1. Packet 728 is a standard query response from 10.20.60.251 to 10.20.1.1. Packet 729 is a standard query from 10.20.60.251 to 10.20.1.1. Packet 730 is a standard query response from 10.20.60.251 to 10.20.1.1. The packet details pane for packet 723 shows the domain name system (query) with transaction ID 0x0001. On the right is a Command Prompt window showing the command 'nslookup google.com' and its output: 'Server: Unknown', 'Address: 10.20.1.1', 'Non-authoritative answer:', 'Name: google.com', 'Addresses: 2404:6800:4009:802::200e, 142.250.70.46'.

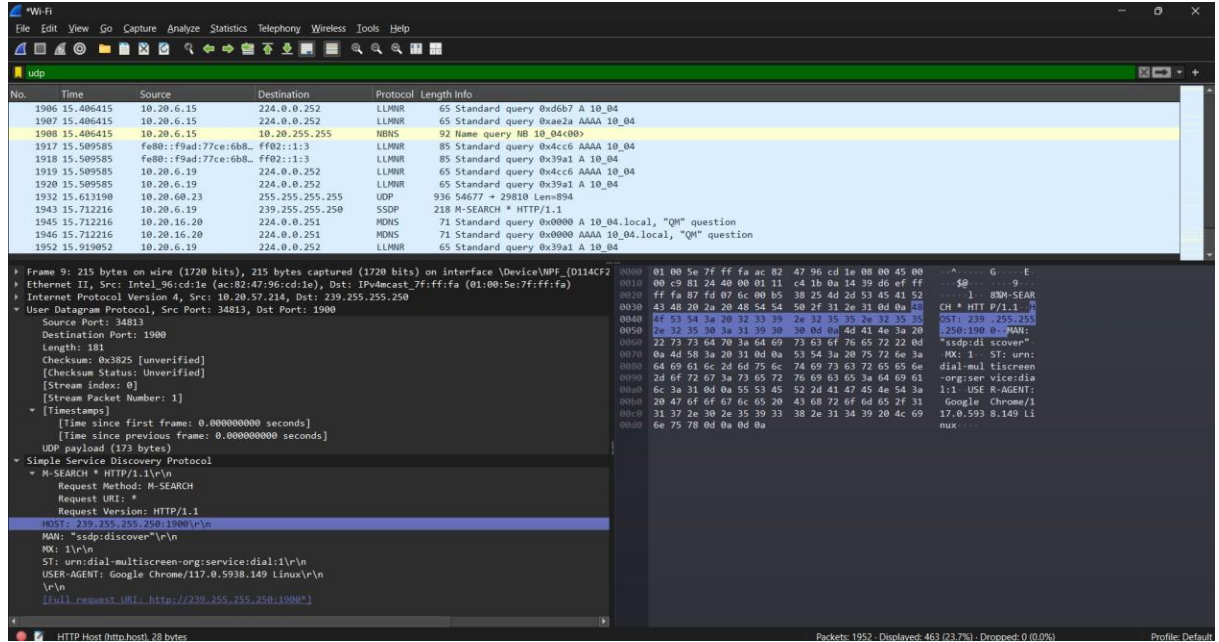
1.3 Analysis of DNS



The image shows a Wireshark window capturing traffic on the Wi-Fi interface. The packet list shows several TCP messages. Packet 25659 is a TCP segment from 10.20.60.251 to 142.250.207.133. Packet 25660 is a TCP segment from 10.20.60.251 to 142.250.207.133. Packet 25661 is a TCP segment from 10.20.60.251 to 142.250.183.74. The packet details pane for packet 25659 shows the Transmission Control Protocol (TCP) with source port 443, destination port 55732, sequence number 810164132, and acknowledgment number 274432317. The packet length is 0 bytes.

1.4 Analysis of TCP

Date: / /



Wireshark Packet Capture Analysis:

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1906	15.406415	10.20.6.15	224.0.0.252	LLMNR	65	Standard query 0xd6b7 A 10_04
1907	15.406415	10.20.6.15	224.0.0.252	LLMNR	65	Standard query 0xae2a AAAA 10_04
1908	15.406415	10.20.6.15	10.20.255.255	NBNS	92	Name query hb 10_04(00)
1917	15.509585	fe80::f9ad:77ce:6b8... ff02::1:3	ff02::1:3	LLMNR	85	Standard query 0x4cc6 AAAA 10_04
1918	15.509585	fe80::f9ad:77ce:6b8... ff02::1:3	ff02::1:3	LLMNR	85	Standard query 0x39a1 A 10_04
1919	15.509585	10.20.6.19	224.0.0.252	LLMNR	65	Standard query 0x4cc6 AAAA 10_04
1920	15.509585	10.20.6.19	224.0.0.252	LLMNR	65	Standard query 0x39a1 A 10_04
1932	15.613190	10.20.60.23	255.255.255.255	UDP	936	54677 → 29810 Len=894
1943	15.712216	10.20.6.19	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
1945	15.712216	10.20.16.20	224.0.0.251	MDNS	71	Standard query 0x0000 A 10_04.local, "Q"
1946	15.712216	10.20.16.20	224.0.0.251	MDNS	71	Standard query 0x0000 AAAA 10_04.local, "Q"
1952	15.919852	10.20.6.19	224.0.0.252	LLMNR	65	Standard query 0x39a1 A 10_04

Packet Details:

- Frame 9: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface \Device\NPF... (0114CF2)
- Ethernet II, Src: Intel_96cd1e (ac:82:47:96:cd:1e), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 10.20.57.214, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 34813, Dst Port: 1900
 - Source Port: 34813
 - Destination Port: 1900
 - Length: 181
 - Checksum: 0x3825 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 0]
 - [Stream Packet Number: 1]
 - [Timestamps]
 - [Time since first frame: 0.000000000 seconds]
 - [Time since previous frame: 0.000000000 seconds]
 - UDP payload (173 bytes)
 - Simple Service Discovery Protocol
 - Request Method: M-SEARCH
 - Request URI: *
 - Request Version: HTTP/1.1
 - MX: 1 239.255.255.250:1900\r\n
 - MAN: ssdp:discover\r\n
 - MX: 1\r\n
 - ST: urn:dial-multiscreen-org:service:dial:1\r\n
 - USER-AGENT: Google Chrome/117.0.5938.149 Linux\r\n
 - \r\n
 - [raw request URI: http://239.255.255.250:1900]

Packet Bytes:

```

0000  01 00 5e 7f ff fa ac 82 47 96 cd 1e 08 00 45 00  ...$E...9...
0010  00 c9 81 24 40 00 01 11 c4 1b 0a 14 39 d6 ef ff  ...1...8M-SEAR
0020  ff fa 87 fd 07 6c 00 85 38 25 44 2d 53 45 41 52  ...Ch * HIT P/1.1
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a ff  ...OST: 239.255.255
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  ...255:1900:1900
0050  2e 32 35 30 3a 31 39 30 30 04 0a 40 41 4e 3a 20  ...ssdp:discover"
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  ...MX: 1 ST: urn:
0070  0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  ...dial-multiscreen
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  ...-org:service:dial
0090  2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  ...1:1 USE R-AGENT:
00a0  6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4a 54 3a  ...Google Chrome/1
00b0  20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 31  ...17.0.5938.149 Li
00c0  31 37 2e 30 2e 35 39 33 38 2e 31 34 39 20 4c 69  ...nux
00d0  6e 75 78 0d 0a 0d 0a
  
```

1.5 Analysis of UDP