

Practical no: 3

Name: Saloni Vishwakarma

Batch-Roll no: C1-13

Subject: Computer Security Lab

Date of execution: 7 October 2023

Aim: Packet sniffing using Wireshark

Task 1: Capturing and Analyzing Network Traffic

Objective: Capture and analyze network traffic to identify specific packets and their contents.

Instructions:

1. Install Wireshark on your computer.
2. Start capturing network traffic on a selected network interface.
3. Capture traffic for a specific duration (e.g., 2 minutes).
4. Stop the capture and save it as a Wireshark capture file (PCAP).
5. Analyze the captured packets to identify specific protocols, source/destination IP addresses, and port numbers.

Task 2: Identifying Suspicious Activity

Objective: Use Wireshark to identify and investigate suspicious network activity.

Instructions:

1. Capture network traffic on a specific interface.
2. Look for any unusual or suspicious network activity, such as unexpected connections or traffic patterns.
3. Analyze the suspicious packets to determine their nature and potential threat.
4. Document your findings and any actions taken to address the issue.

Task 3: Analyzing DNS Traffic

Objective: Capture and analyze DNS (Domain Name System) traffic to understand domain resolutions.

Instructions:

1. Start capturing network traffic on a selected interface.
2. Perform various DNS queries on your computer (e.g., visiting websites).

3. Stop the capture and save it as a PCAP file.
4. Analyze the DNS traffic to identify domain resolutions, IP addresses, and response times.

Task 4: Identifying Malware Communications

Objective: Use Wireshark to identify network communications associated with malware.

Instructions:

1. Set up a controlled environment with a virtual machine.
2. Infect the virtual machine with malware (ensure it is safely isolated).
3. Capture network traffic from the infected virtual machine.
4. Analyze the traffic to identify any suspicious or malicious communications.
5. Document the findings and potential indicators of compromise.

Task 5: Monitoring HTTP Traffic

Objective: Capture and analyze HTTP (Hypertext Transfer Protocol) traffic to understand web browsing behavior.

Instructions:

1. Start capturing network traffic on a selected interface.
2. Open a web browser and visit several websites.
3. Stop the capture and save it as a PCAP file.
4. Analyze the HTTP traffic to identify visited URLs, request methods (GET, POST), and response codes.

Task 6: Analyzing Email Communication

- Task: Capture email communication (SMTP and POP/IMAP) using Wireshark between an email client (e.g., Outlook) and a mail server (e.g., smtp.example.com). Identify the email protocols used and examine the email headers.

Task 7: Detecting ARP Spoofing

- Task: Capture ARP traffic on your local network and detect any signs of ARP spoofing (e.g., ARP requests for IP addresses that don't match the expected mappings).

- Answer: Look for ARP requests and responses in the captured traffic. Pay attention to any ARP requests that don't align with the known IP-to-MAC address mappings in your network.

Task 8: Analyzing VoIP Traffic

- Task: Capture VoIP (Voice over IP) traffic using Wireshark from a VoIP application (e.g., Skype) and analyze the packets. Identify the protocols used and understand how voice communication is transmitted over the network.

TASK 1:

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 60, Time 51650.1168, Source 172.16.146.107, Destination 224.0.0.252, Protocol ARP, Length 60). The bottom pane shows the raw packet data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-------------|------------------------|-----------------|----------|--------|---|
| 51637 | 1168.557290 | 172.16.146.90 | 172.16.147.255 | NBNS | 92 | Name query NB VSL-DESK<00> |
| 51638 | 1168.659326 | 172.16.147.107 | 224.0.0.252 | LLMNR | 75 | Standard query 0x660f ANY LAPTOP-TVLKUCSQ |
| 51639 | 1168.659326 | fe80::f8c1:f95b:8ff... | ff02::1:3 | LLMNR | 95 | Standard query 0x660f ANY LAPTOP-TVLKUCSQ |
| 51640 | 1168.659326 | 172.16.147.107 | 224.0.0.251 | MDNS | 110 | Standard query response 0x0000 AAAA fe80::f8c1:f95b:8ff0:a217 A 172.16.147.107 |
| 51641 | 1168.659326 | fe80::f8c1:f95b:8ff... | ff02::fb | MDNS | 130 | Standard query response 0x0000 AAAA fe80::f8c1:f95b:8ff0:a217 A 172.16.147.107 |
| 51642 | 1168.659326 | 172.16.147.107 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 ANY LAPTOP-TVLKUCSQ.local, "QM" question |
| 51643 | 1168.659326 | fe80::f8c1:f95b:8ff... | ff02::fb | MDNS | 101 | Standard query 0x0000 PTR LAPTOP-TVLKUCSQ.local, "QM" question |
| 51644 | 1168.870247 | fe80::47a4:8cbb:125... | ff02::fb | MDNS | 102 | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question |
| 51645 | 1168.870247 | 172.16.147.95 | 224.0.0.251 | MDNS | 82 | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question |
| 51646 | 1168.870247 | 172.16.146.31 | 224.0.0.252 | LLMNR | 69 | Standard query 0x6d84 A DEV255C16 |
| 51647 | 1168.870247 | 172.16.146.31 | 224.0.0.252 | LLMNR | 69 | Standard query 0x67a7 AAAA DEV255C16 |
| 51648 | 1168.870247 | fe80::bd42:2baa:4f9... | ff02::1:3 | LLMNR | 89 | Standard query 0x6d84 A DEV255C16 |
| 51649 | 1168.870247 | fe80::bd42:2baa:4f9... | ff02::1:3 | LLMNR | 89 | Standard query 0x67a7 AAAA DEV255C16 |
| 51650 | 1168.870247 | D-LinkIn_ea:64:11 | Broadcast | ARP | 60 | Who has 172.16.146.102? Tell 172.16.146.1 |
| 51651 | 1168.964786 | 172.16.147.8 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 51652 | 1168.964786 | 172.16.146.187 | 224.0.0.251 | MDNS | 74 | Standard query 0x0000 AAAA TNPADMIN.local, "QM" question |
| 51653 | 1168.964786 | fe80::a42b:c0d:a2d2... | ff02::fb | MDNS | 94 | Standard query 0x0000 AAAA TNPADMIN.local, "QM" question |
| 51654 | 1168.964786 | fe80::a42b:c0d:a2d2... | ff02::fb | MDNS | 94 | Standard query 0x0000 A TNPADMIN.local, "QM" question |
| 51655 | 1168.964786 | 172.16.146.187 | 224.0.0.251 | MDNS | 74 | Standard query 0x0000 A TNPADMIN.local, "QM" question |
| 51656 | 1169.075011 | 172.16.147.114 | 224.0.0.251 | MDNS | 210 | Standard query 0x0000 ANY ("nm":"POCO M2 Pro","as":["8194"],"ip":"2")._mi-connect._udp.local, "QU" question ANY Android.local, "QU" question... |
| 51657 | 1169.075011 | 172.16.146.90 | 224.0.0.252 | LLMNR | 75 | Standard query 0x5ca7 A DESKTOP-CLB3SAM |
| 51658 | 1169.075011 | fe80::e99e:3959:854... | ff02::1:3 | LLMNR | 95 | Standard query 0x5ca7 A DESKTOP-CLB3SAM |
| 51659 | 1169.075011 | fe80::e99e:3959:854... | ff02::1:3 | LLMNR | 86 | Standard query 0xb7da A ECHORK |
| 51660 | 1169.075011 | fe80::e99e:3959:854... | ff02::fb | MDNS | 101 | Standard query 0x0000 A DESKTOP-CLB3SAM.local, "QM" question |
| 51661 | 1169.075011 | 172.16.146.90 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 A DESKTOP-CLB3SAM.local, "QM" question |
| 51662 | 1169.075011 | 172.16.146.90 | 224.0.0.252 | LLMNR | 66 | Standard query 0xb7da A ECHORK |
| 51663 | 1169.075011 | fe80::e99e:3959:854... | ff02::fb | MDNS | 92 | Standard query 0x0000 A ECHORK.local, "QM" question |
| 51664 | 1169.075011 | 172.16.146.90 | 224.0.0.252 | LLMNR | 64 | Standard query 0x3a7a A VCNJ |
| 51665 | 1169.075011 | fe80::a42b:c0d:a2d2... | ff02::1:3 | LLMNR | 84 | Standard query 0x3a7a A VCNJ |

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF{70D8FC68-D4D4-4A2...}

> Ethernet II, Src: IntelCor_20:fc:9c (2c:33:58:20:fc:9c), Dst: D-LinkIn_ea:64:11 (60:63:4c:ea:64:11)

> Internet Protocol Version 4, Src: 172.16.146.197, Dst: 216.58.203.40

> Transmission Control Protocol, Src Port: 3014, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000 60 63 4c ea 64 11 2c 33 58 20 fc 9c 00 00 45 00 "cl.d",3 XE
0010 00 29 90 e0 40 00 00 06 00 00 ac 10 92 c5 d8 3a):@.....:
0020 cb 28 00 c6 01 b0 4d af eb dd ad 13 ed 05 50 10 (....W.....P
0030 02 01 e2 54 00 00 00T....

wireshark_Wi-Fi32M2C2.pcapng | Packets: 51704 · Displayed: 51704 (100.0%) | Profile: Default

TASK 2:

The screenshot shows the Wireshark network protocol analyzer. The main packet list on the left displays several packets, with packet 46569 selected. The packet details pane on the right shows the structure of this packet, which is a Transmission Control Protocol (TCP) segment. The 'Flags' field is expanded, showing 'RST' (Reset) and 'ACK' (Acknowledgment). The 'Sequence Number' is 2053, and the 'Acknowledgment Number' is 4877. The 'Window' size is 0. The packet is from source 172.16.146.197 to destination 172.16.146.197. The packet bytes pane at the bottom shows the raw data of the packet.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>-F

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-------------|------------------------|-------------|----------|--------|---|
| 46555 | 1072.587454 | fe80::bd42:2baa:4f9... | ff02::fb | MDNS | 95 | Standard query 0x0000 A DEV255C16.local, "QM" question |
| 46556 | 1072.587454 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46557 | 1072.587454 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46558 | 1072.587454 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46559 | 1072.587454 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46560 | 1072.587454 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46561 | 1072.587454 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46562 | 1072.587454 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46563 | 1072.607016 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46564 | 1072.607016 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46565 | 1072.646021 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46566 | 1072.646021 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46567 | 1072.646021 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46568 | 1072.646021 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46569 | 1072.646021 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46570 | 1072.646021 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46571 | 1072.710506 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46572 | 1072.710506 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46573 | 1072.710506 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46574 | 1072.710506 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46575 | 1072.710506 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46576 | 1072.922831 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46577 | 1072.922831 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46578 | 1072.922831 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46579 | 1072.922831 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46580 | 1072.922831 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46581 | 1073.017002 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46582 | 1073.120390 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |
| 46583 | 1073.120390 | 172.16.146.31 | 224.0.0.251 | MDNS | 75 | Standard query 0x0000 AAAA DEV255C16.local, "QM" question |

Wireshark - Packet 46569 - Wi-Fi

> Frame 46569: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{7008FC60-D4D4-4A24-B1C8-70D45477480}, id 0

> Ethernet II, Src: IntelCor_20:fc:9c (2c:33:58:20:fc:9c), Dst: D-LinkIn_ea:64:11 (60:63:4c:ea:64:11)

> Internet Protocol Version 4, Src: 172.16.146.197, Dst: 20.198.119.84

> Transmission Control Protocol, Src Port: 3176, Dst Port: 443, Seq: 2053, Ack: 4877, Len: 0

Source Port: 3176

Destination Port: 443

[Stream index: 186]

[Conversation completeness: Complete, WITH_DATA (63)]

[TCP Segment Len: 0]

Sequence Number: 2053 (relative sequence number)

Sequence Number (raw): 1903806959

[Next Sequence Number: 2053 (relative sequence number)]

Acknowledgment Number: 4877 (relative ack number)

Acknowledgment number (raw): 1532635946

0101 = Header Length: 20 bytes (5)

> Flags: 0x014 (RST, ACK)

Window: 0

[Calculated window size: 0]

[Window size scaling factor: 256]

Checksum: 0xcbb8 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

Show packet bytes

Close Help

Profile: Default

TASK 3:

The screenshot shows the Wireshark network protocol analyzer. The main packet list on the left displays several packets, with packet 44407 selected. The packet details pane on the right shows the structure of this packet, which is a Domain Name System (DNS) response. The 'Flags' field is expanded, showing 'Standard query response, No error'. The 'Transaction ID' is 0x009f1. The 'Request ID' is 44406. The 'Time' is 0.001579000 seconds. The packet bytes pane at the bottom shows the raw data of the packet.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>-F

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-------------|----------------|----------------|----------|--------|--|
| 42949 | 1089.037969 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 42950 | 1089.040467 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 43720 | 1024.292763 | 172.16.146.197 | 172.16.146.197 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 43721 | 1024.292958 | 172.16.146.197 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 43722 | 1024.294220 | 172.16.146.197 | 172.16.146.197 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 43723 | 1024.294543 | 172.16.146.197 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 43724 | 1024.315860 | 172.16.146.197 | 172.16.146.197 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 43725 | 1024.315860 | 172.16.146.197 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 43726 | 1024.315860 | 172.16.146.197 | 172.16.146.197 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 43731 | 1024.378975 | 172.16.146.197 | 172.16.146.197 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44406 | 1039.092043 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44407 | 1039.093622 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 44442 | 1039.387561 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44443 | 1039.389414 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 44491 | 1040.093973 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44496 | 1040.163315 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 44497 | 1040.179089 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44540 | 1041.052660 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44774 | 1046.710279 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44775 | 1046.710540 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 44777 | 1046.735465 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 44778 | 1046.736439 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 45085 | 1050.724157 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 45086 | 1050.724157 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 45087 | 1050.807646 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 45677 | 1056.982225 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 46468 | 1069.163237 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |
| 46469 | 1069.182126 | 172.16.177.5 | 172.16.146.197 | DNS | 227 | Standard query response 0x777c A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961... |
| 46796 | 1076.409613 | 172.16.146.197 | 172.16.177.5 | DNS | 83 | Standard query 0x777c A www.msftconnecttest.com |

Wireshark - Packet 44407 - Wi-Fi

> Frame 44407: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface \Device\NPF_{7008FC60-D4D4-4A24-B1C8-70D45477480}, id 0

> Ethernet II, Src: D-LinkIn_ea:64:11 (60:63:4c:ea:64:11), Dst: IntelCor_20:fc:9c (2c:33:58:20:fc:9c)

> Internet Protocol Version 4, Src: 172.16.177.5, Dst: 172.16.146.197

> User Datagram Protocol, Src Port: 53, Dst Port: 60240

> Domain Name System (response)

Transaction ID: 0x009f1

> Flags: 0x0100 Standard query response, No error

Questions: 1

Answer RRs: 5

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

[Request ID: 44406]

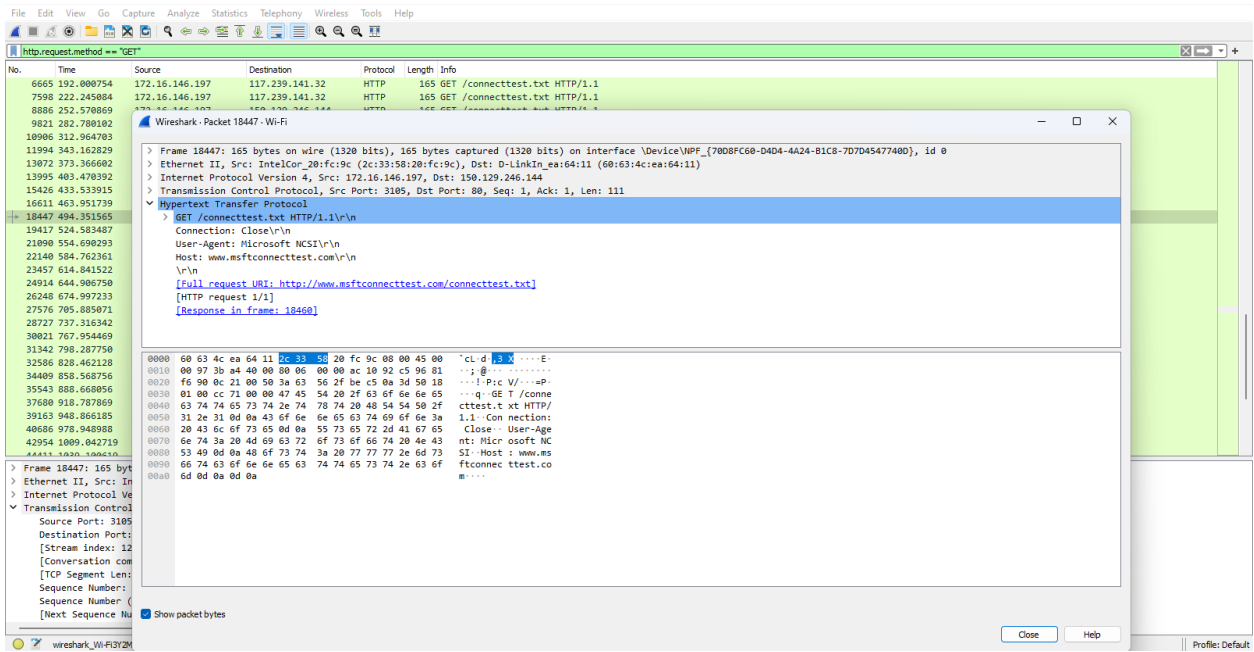
[Time: 0.001579000 seconds]

Show packet bytes

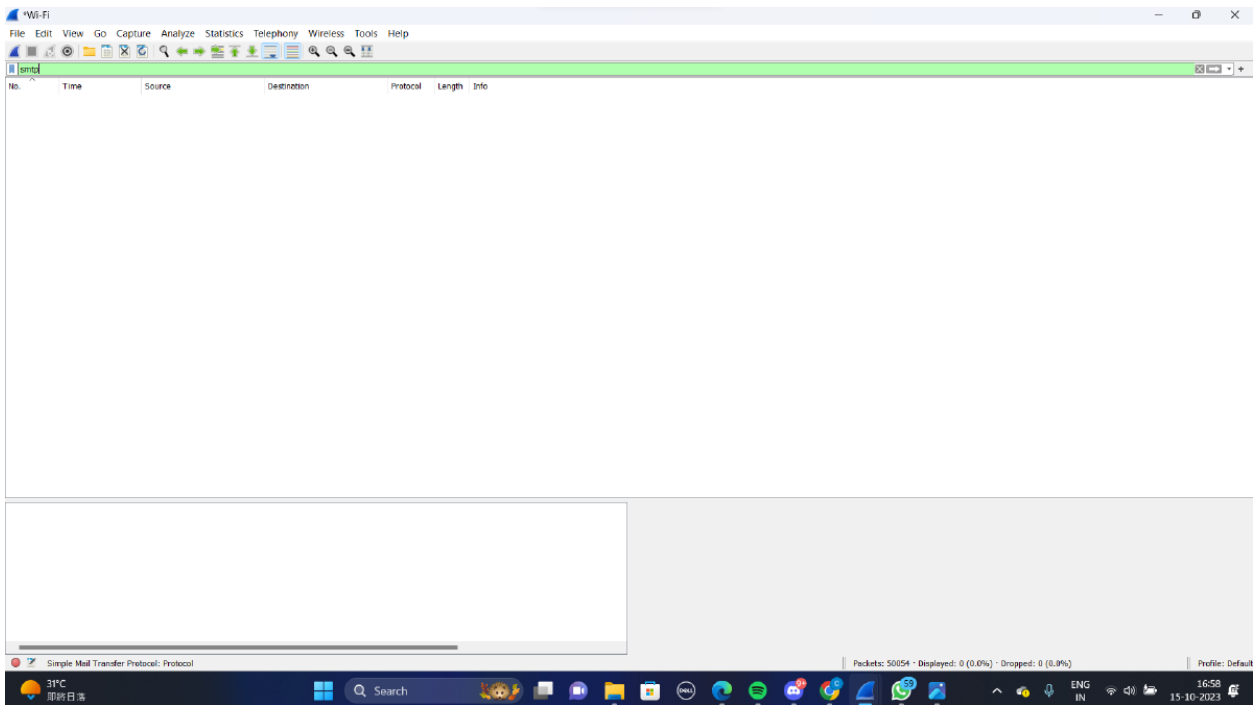
Close Help

Profile: Default

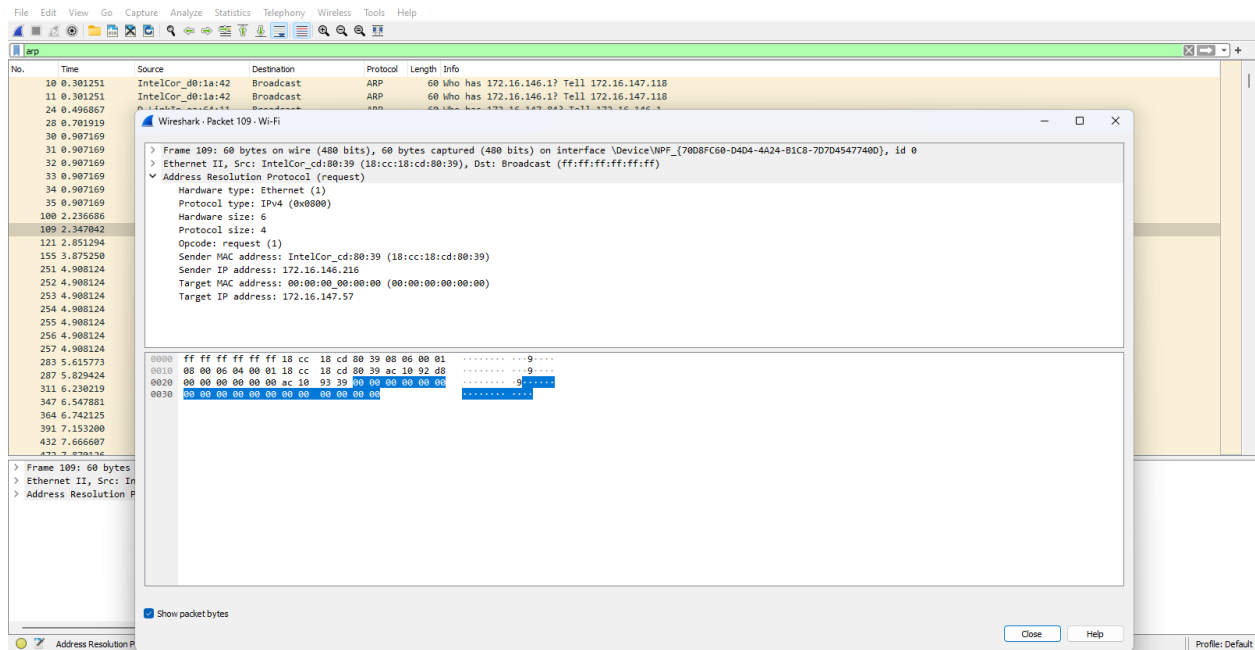
TASK 5:



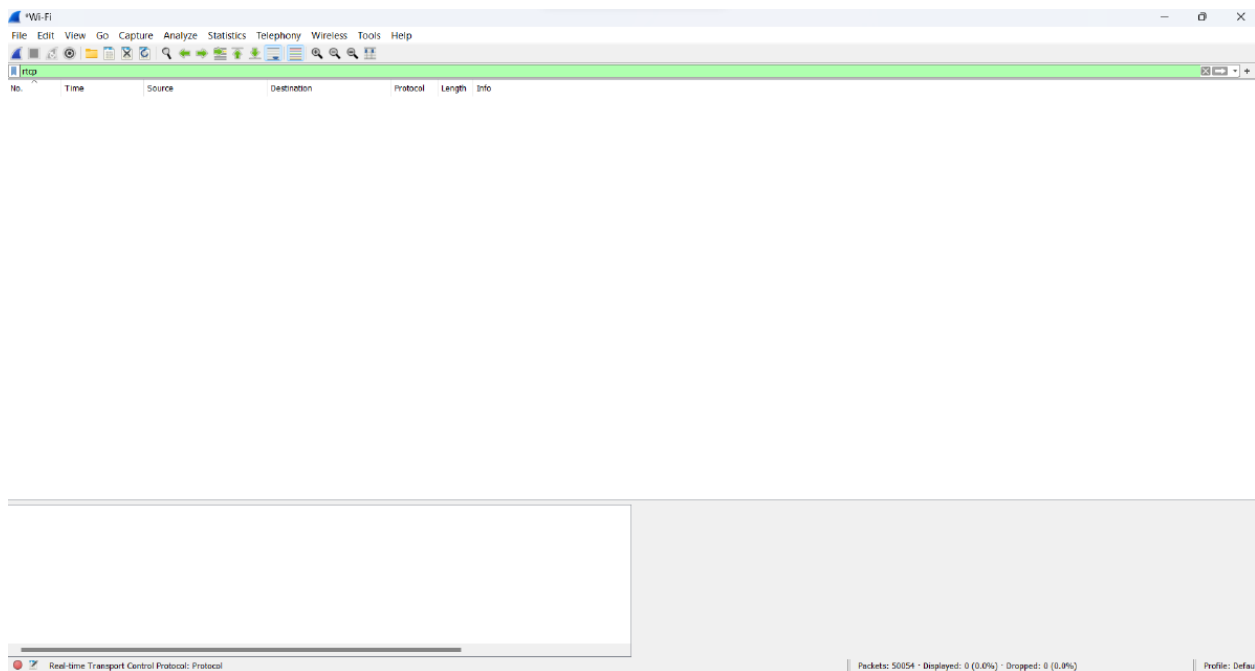
TASK 6:



TASK 7:



TASK 8:



Conclusion: Through this practical ,we implemented various ways of packet sniffing using Wireshark.