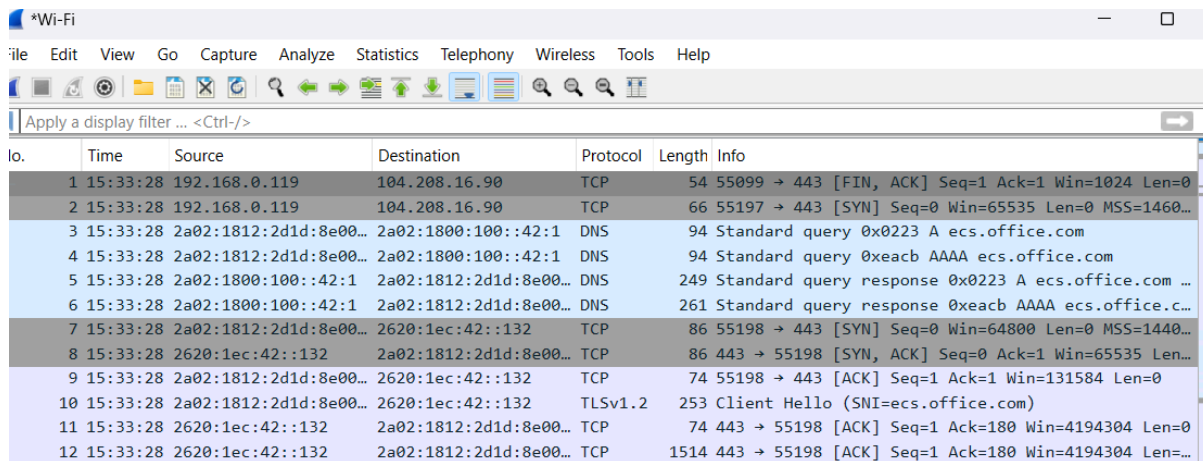


Wireshark 1

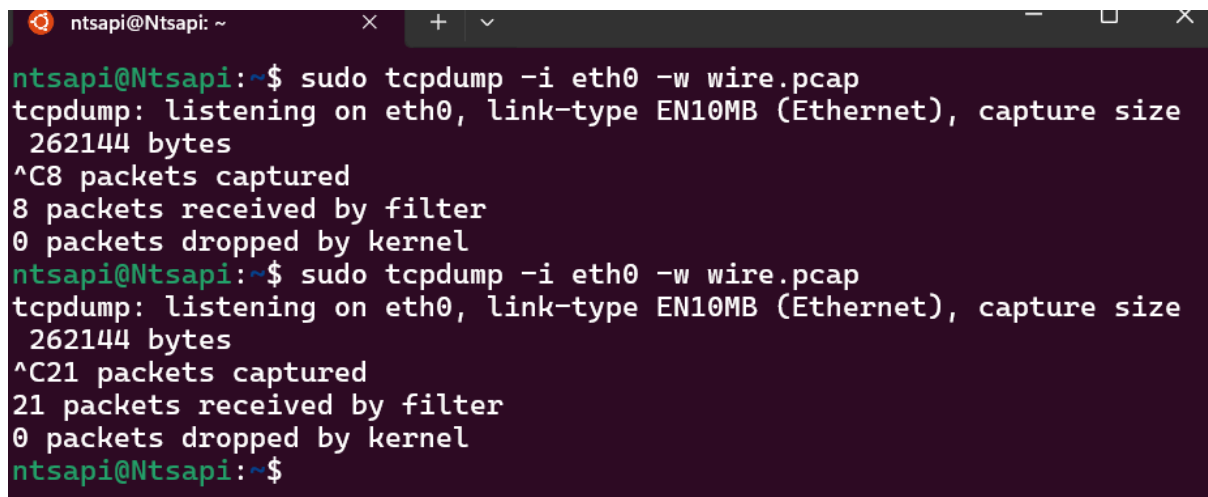
2. Capture Network Traffic:

- Use Wireshark to capture network traffic on your computer. You can capture traffic from your Wi-Fi or Ethernet connection.



No.	Time	Source	Destination	Protocol	Length	Info
1	15:33:28	192.168.0.119	104.208.16.90	TCP	54	55099 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
2	15:33:28	192.168.0.119	104.208.16.90	TCP	66	55197 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460...
3	15:33:28	2a02:1812:2d1d:8e00...	2a02:1800:100::42:1	DNS	94	Standard query 0x0223 A ecs.office.com
4	15:33:28	2a02:1812:2d1d:8e00...	2a02:1800:100::42:1	DNS	94	Standard query 0xeacb AAAA ecs.office.com
5	15:33:28	2a02:1800:100::42:1	2a02:1812:2d1d:8e00...	DNS	249	Standard query response 0x0223 A ecs.office.com ...
6	15:33:28	2a02:1800:100::42:1	2a02:1812:2d1d:8e00...	DNS	261	Standard query response 0xeacb AAAA ecs.office.c...
7	15:33:28	2a02:1812:2d1d:8e00...	2620:1ec:42::132	TCP	86	55198 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440...
8	15:33:28	2620:1ec:42::132	2a02:1812:2d1d:8e00...	TCP	86	443 → 55198 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=...
9	15:33:28	2a02:1812:2d1d:8e00...	2620:1ec:42::132	TCP	74	55198 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
10	15:33:28	2a02:1812:2d1d:8e00...	2620:1ec:42::132	TLSv1.2	253	Client Hello (SNI=ecs.office.com)
11	15:33:28	2620:1ec:42::132	2a02:1812:2d1d:8e00...	TCP	74	443 → 55198 [ACK] Seq=1 Ack=180 Win=4194304 Len=0
12	15:33:28	2620:1ec:42::132	2a02:1812:2d1d:8e00...	TCP	1514	443 → 55198 [ACK] Seq=1 Ack=180 Win=4194304 Len=...

- Use tcpdump to capture traffic as well and save the captured file for further analysis.



```
ntsapi@Ntsapi: ~  
ntsapi@Ntsapi:~$ sudo tcpdump -i eth0 -w wire.pcap  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size  
262144 bytes  
^C8 packets captured  
8 packets received by filter  
0 packets dropped by kernel  
ntsapi@Ntsapi:~$ sudo tcpdump -i eth0 -w wire.pcap  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size  
262144 bytes  
^C21 packets captured  
21 packets received by filter  
0 packets dropped by kernel  
ntsapi@Ntsapi:~$
```

- ### 4. Answer the following questions based on your analysis: Question
- Identify the protocols operating at the Network layer (Layer 3) in the captured packets.
 - ARP Request: The first packet is an ARP request from a TP-Link device trying to resolve the MAC address for the IP address 192.168.68.91. This is a fundamental part of IPv4 networking for address resolution.
 - ICMPv6 Router Advertisement: The second packet is an ICMPv6 Router Advertisement from the same TP-Link device, informing all IPv6-capable devices on the network about routing information. This is essential for IPv6 network configuration and communication.

These packets illustrate the use of ARP in IPv4 networks for MAC address resolution and ICMPv6 Router Advertisements in IPv6 networks for router discovery and network configuration.

The screenshot shows a Wireshark packet capture window titled '*Wi-Fi'. The filter bar is set to 'ipv6 or arp or icmp'. The packet list shows several ARP and ICMPv6 packets. The packet details pane is empty.

No.	Time	Source	Destination	Protocol	Length	Info
1239	15:38:48	82:0c:7f:8a:79:97	Broadcast	ARP	42	Who has 192.168.68.1? Tell 192.168.68.64
1246	15:38:49	Apple_dd:64:18	Broadcast	ARP	42	Who has 192.168.68.1? Tell 192.168.68.71
1258	15:38:49	82:0c:7f:8a:79:97	Broadcast	ARP	42	Who has 192.168.68.71? Tell 192.168.68.64
1259	15:38:49	TPLink_66:33:a4	Broadcast	ARP	60	Who has 192.168.68.66? Tell 192.168.68.1
1294	15:38:51	TPLink_66:33:a4	Broadcast	ARP	60	Who has 192.168.68.97? Tell 192.168.68.1
1305	15:38:51	82:0c:7f:8a:79:97	Broadcast	ARP	42	Who has 192.168.68.1? Tell 192.168.68.64
1306	15:38:52	TPLink_66:33:a4	Broadcast	ARP	60	Who has 192.168.68.60? Tell 192.168.68.1
1315	15:38:52	Apple_dd:64:18	Broadcast	ARP	42	Who has 192.168.68.1? Tell 192.168.68.71
1331	15:38:53	TPLink_66:33:a4	Broadcast	ARP	60	Who has 192.168.68.91? Tell 192.168.68.1
841	15:38:37	fe80::abf7:1961:855...	ff02::1:2	DHCPv6	138	Solicit XID: 0x51fe83 CID: 0004931bc3da936f9e85f...
170	15:38:26	192.168.68.76	195.130.131.2	ICMP	320	Destination unreachable (Port unreachable)
909	15:38:39	192.168.68.76	195.130.131.2	ICMP	325	Destination unreachable (Port unreachable)
270	15:38:29	fe80::5ee9:31ff:fe6...	ff02::1	ICMPv6	78	Router Advertisement from 5c:e9:31:66:33:a4
271	15:38:29	fe80::db0d:8daf:f17...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
272	15:38:29	fe80::abf7:1961:855...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
277	15:38:29	fe80::abf7:1961:855...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
306	15:38:30	fe80::db0d:8daf:f17...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
883	15:38:39	fe80::5ee9:31ff:fe6...	ff02::1	ICMPv6	78	Router Advertisement from 5c:e9:31:66:33:a4
884	15:38:39	fe80::db0d:8daf:f17...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2

- Find and describe a packet at the Transport layer (Layer - Identify the source and destination ports.

The screenshot shows a Wireshark packet capture window titled '*Wi-Fi'. The filter bar is set to 'tcp'. The packet list shows three TCP packets. The packet details pane shows the details of the first packet (No. 815).

No.	Time	Source	Destination	Protocol	Length	Info
815	15:38:37	192.168.68.76	20.56.187.20	TCP	1494	65150 → 443 [ACK] Seq=4628 Ack=8141 Win=263424 L...
817	15:38:37	195.130.131.2	192.168.68.76	TCP	54	53 → 65155 [FIN, ACK] Seq=132 Ack=37 Win=29312 L...
818	15:38:37	192.168.68.76	195.130.131.2	TCP	54	65155 → 53 [ACK] Seq=37 Ack=133 Win=262656 Len=0

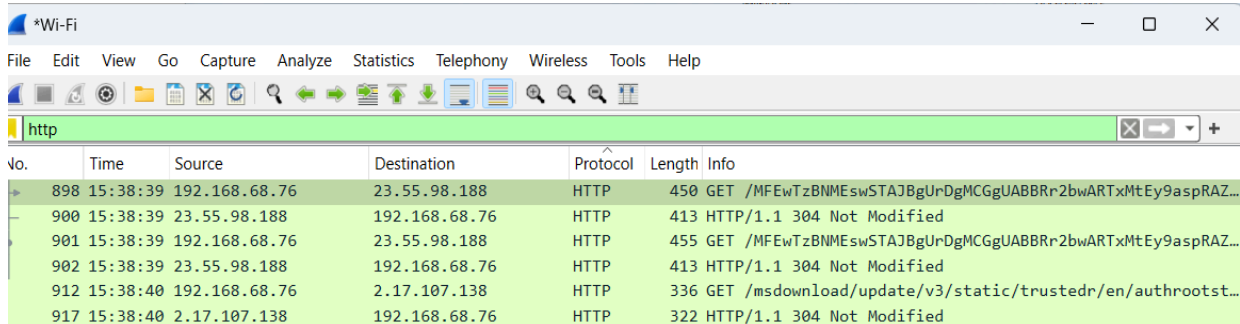
Packet details for No. 815:

- Frame 815: 1494 bytes on wire (11952 bits), 1494 byte captured (11952 bits) on interface 0
- Ethernet II, Src: CloudNetwork_d6:28:cf (74:97:79:d6:28:cf), Dst: 08:00:00:00:00:00
- Internet Protocol Version 4, Src: 192.168.68.76, Dst: 20.56.187.20
- Transmission Control Protocol, Src Port: 65150, Dst Port: 443
 - Source Port: 65150
 - Destination Port: 443
 - [Stream index: 26]
 - [Conversation completeness: Incomplete, DATA (15)]
 - [TCP Segment Len: 1440]

The captured packet details an acknowledgment (ACK) segment in a TCP connection. Here are the specifics related to the ports:

- Source Port: 64237
 - This is the ephemeral port on the local device with the IP address 192.168.68.76. Ephemeral ports are typically used for the client side of a TCP/IP connection and are assigned dynamically from a predefined range.

- Destination Port: 443
 - This is the well-known port used for HTTPS (HTTP Secure) on the remote server with the IP address 107.23.86.112. Port 443 is standard for secure web traffic, indicating that the communication is encrypted using TLS/SSL.
- Locate a packet at the Application layer (Layer 7). - Identify the application protocol being used.



No.	Time	Source	Destination	Protocol	Length	Info
898	15:38:39	192.168.68.76	23.55.98.188	HTTP	450	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRn2bwARTxMtEy9aspRAZ...
900	15:38:39	23.55.98.188	192.168.68.76	HTTP	413	HTTP/1.1 304 Not Modified
901	15:38:39	192.168.68.76	23.55.98.188	HTTP	455	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRn2bwARTxMtEy9aspRAZ...
902	15:38:39	23.55.98.188	192.168.68.76	HTTP	413	HTTP/1.1 304 Not Modified
912	15:38:40	192.168.68.76	2.17.107.138	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab
917	15:38:40	2.17.107.138	192.168.68.76	HTTP	322	HTTP/1.1 304 Not Modified

The captured packet represents an HTTP GET request made by a device with the IP address 192.168.68.76 to a server with the IP address 2.17.107.138. The request is specifically for a file named `authrootstl.cab` located at the path `/msdownload/update/v3/static/trustedr/en/`. The file appears to be part of a Microsoft download, possibly related to updates or trusted root certificates, as indicated by the URL path and file name. The HTTP version used for the request is 1.1, and the total size of the packet is 336 bytes. The timestamp for this packet is 15:38:40.

5)

Identify if there are differences in findings between tcpdump and wireshark captures.

- Tcpdump is better suited for quick captures, scripting, and environments without a GUI.
- Wireshark excels in detailed analysis, troubleshooting, and educational purposes due to its rich feature set and user-friendly interface.