

CS331: Data Communications and Computer Networks

Wireshark Lab

Packet Capture and Display Filtering

SHOUG FAWAZ ABDULLAH ALOMRAN

Instructor: Ms.Nada ALALYANI

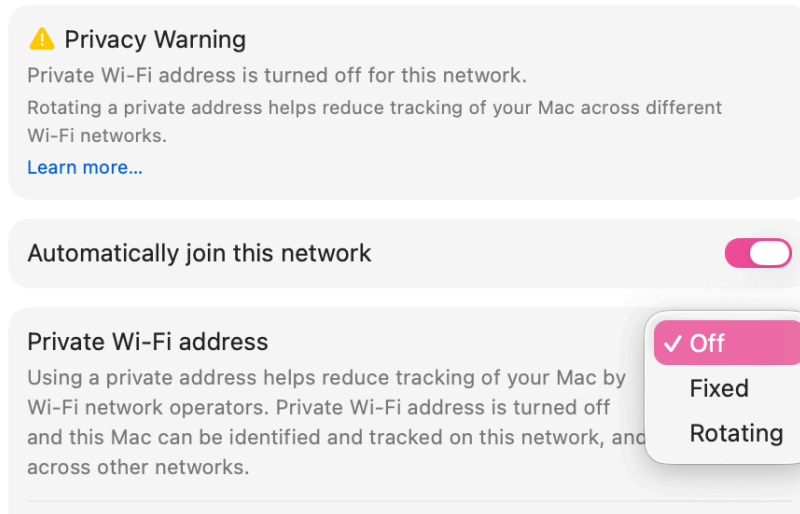
Part 1: Lab Setup	3
Step 1: Finding the IP and MAC address	3
Step 2: Starting Wireshark	3
Steps 3–4: Capturing packets	4
Step 5-12: Filtering	4
Part 2: Packet Filtering Practice	5
Q1. IP address of Google.com.sa: 142.250.203.3	5
Q2. Time for the first Echo packet: 121.913 ms	6
Q3. Active interface:	6
Q4. Filter: icmp and ip.src == 172.217.17.35	7
Q5. Filter: icmp	7
Q6. ICMP packets filtered:	7
Q7. Packets with my IP as source:	7
Q8. Packets with Google's IP as source:	7
Q9. Frame source and destination addresses:	9
Q11. Type field value:	9
Q12. Source and destination IP addresses:	9
Q13. Time for the Echo response:	9

Part 1: Lab Setup

Note: This lab was performed on macOS (MacBook Air M2). macOS equivalents were used for the Windows commands: `ifconfig en0` instead of `ipconfig /all`, and `ping -c 4` instead of `ping -4`.

Step 1: Finding the IP and MAC address

The private Wi-Fi Address was turned off so the real hardware MAC address is shown.

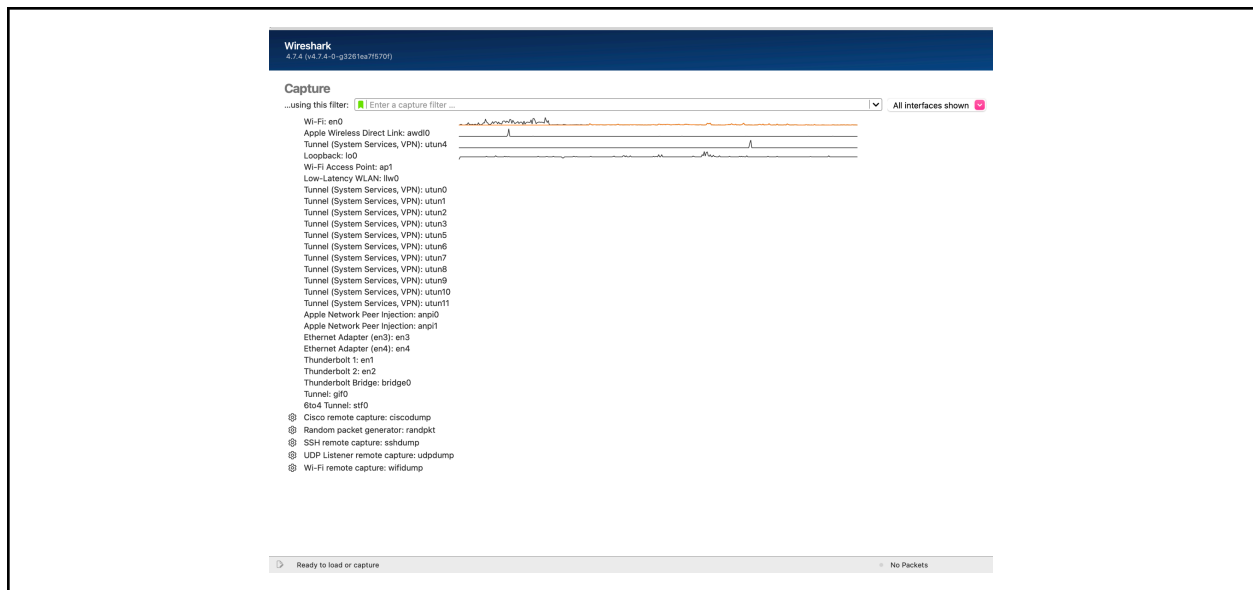


Command used: `ifconfig en0`

```
[shougalomran@Mac ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=6460<TS04,TS06,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
    ether a8:8f:d9:4f:26:6f
    inet6 fe80::188b:dacc:bfea:b9c6%en0 prefixlen 64 secured scopeid 0xb
    inet 192.168.1.229 netmask 0xffffffff broadcast 192.168.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
shougalomran@Mac ~ %
```

Step 2: Starting Wireshark

The active interface Wi-Fi: en0 was selected for capturing.



Steps 3–4: Capturing packets

While capturing, www.psu.edu.sa was opened in the browser and an HTTP request was sent to neverssl.com, then the capture was stopped.

```

curl (20) failed to connect to www.psu.edu.sa: port
[shougalomran@Mac ~ % curl -I http://neverssl.com
HTTP/1.1 200 OK
Date: Sun, 18 Oct 2026 10:50:19 GMT
Server: Apache/2.4.68 ()
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Wed, 29 Jun 2022 00:23:33 GMT
ETag: "f79-5e28b29d38e93"
Accept-Ranges: bytes
Content-Length: 3961
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8

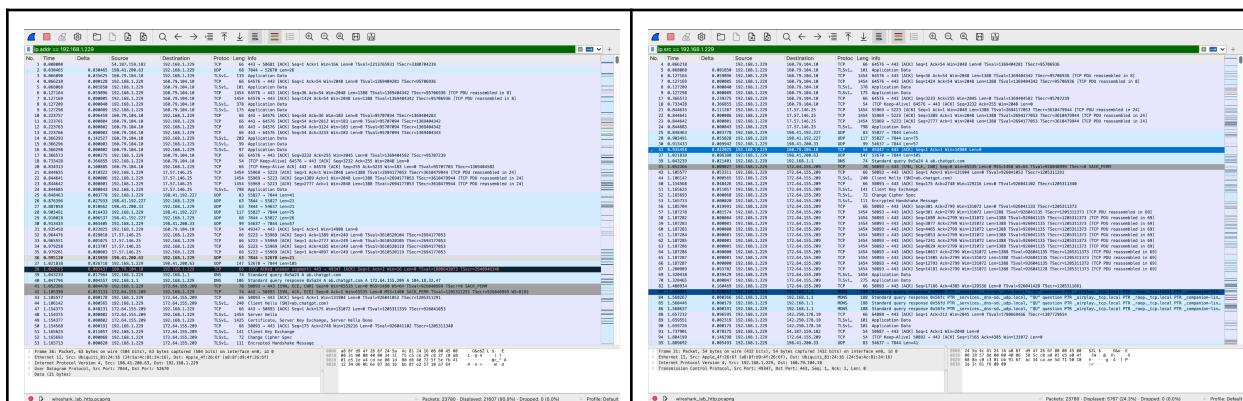
```

No.	Time	Delta	Source	Destination	Protoc	Leng	Info
2...	199.445292		192.168.1.229	34.223.124.45	HTTP	142	HEAD / HTTP/1.1
2...	199.813242	0.367950	34.223.124.45	192.168.1.229	HTTP	366	HTTP/1.1 200 OK

Step 5-12: Filtering

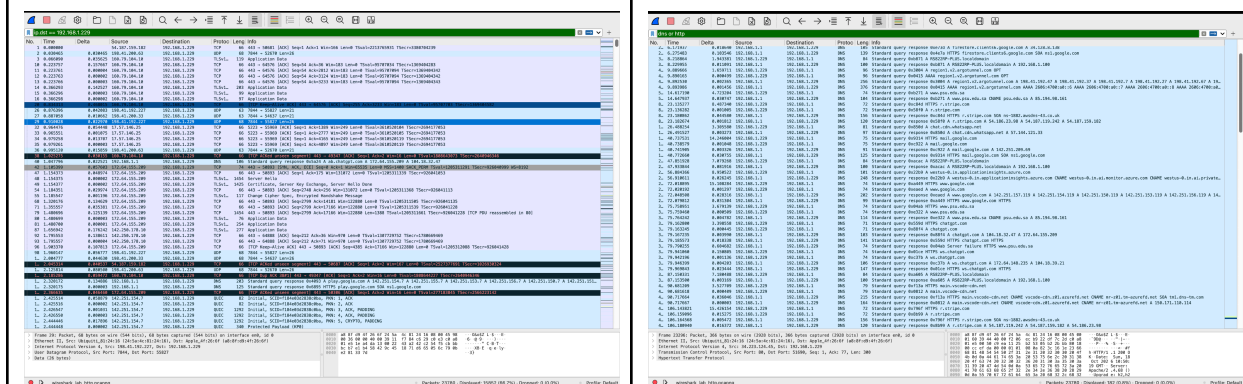
Note: www.psu.edu.sa only accepts HTTPS (port 80 is closed), so its traffic appears as encrypted TLS rather than HTTP. A plain HTTP request was sent to <http://neverssl.com> to

demonstrate the http filter. The result shows the HEAD request from my machine and the HTTP/1.1 200 OK response.



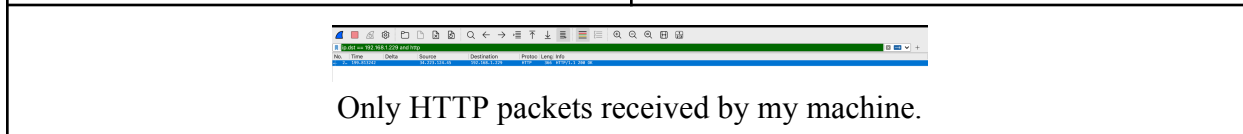
All packets to or from my machine.

Only packets sent by my machine.



Only packets received by my machine.

All DNS and HTTP packets.



Only HTTP packets received by my machine.

Part 2: Packet Filtering Practice

Q1. IP address of Google.com.sa: 142.250.203.3

```
shougalomran@Mac ~ % nslookup google.com.sa 8.8.8.8
Server:           8.8.8.8
Address:          8.8.8.8#53

Non-authoritative answer:
Name:   google.com.sa
Address: 142.250.203.3
```

```
[shougalomran@Mac ~ % ping -c 4 google.com.sa
PING google.com.sa (172.217.17.35): 56 data bytes
64 bytes from 172.217.17.35: icmp_seq=0 ttl=114 time=121.913 ms
64 bytes from 172.217.17.35: icmp_seq=1 ttl=114 time=91.989 ms
64 bytes from 172.217.17.35: icmp_seq=2 ttl=114 time=92.667 ms
64 bytes from 172.217.17.35: icmp_seq=3 ttl=114 time=106.484 ms

--- google.com.sa ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 91.989/103.263/121.913/12.223 ms
shougalomran@Mac ~ %
```

Note: nslookup via 8.8.8.8 returned 142.250.203.3, while the ping resolved google.com.sa through the local DNS server (192.168.1.1) to 172.217.17.35. Google uses many server IPs, so different DNS resolvers can return different addresses. The captured ICMP packets use 172.217.17.35.

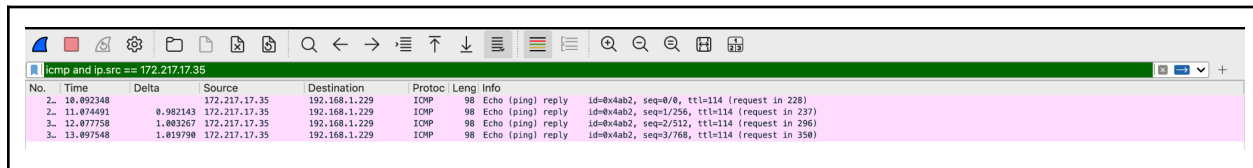
<

Q2. Time for the first Echo packet: 121.913 ms

Q3. Active interface:

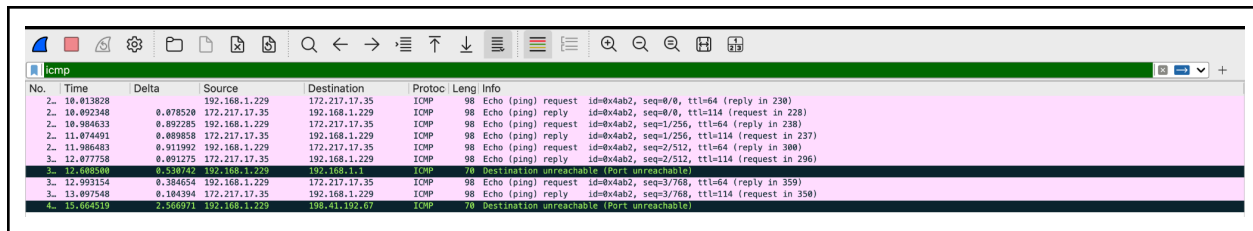
MAC address	a8:8f:d9:4f:26:6f
IP address	192.168.1.229

Q4. Filter: **icmp and ip.src == 172.217.17.35**



No.	Time	Delta	Source	Destination	Protoc	Leng	Info
2.	10.092348		172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=0/0, ttl=114 (request in 228)
2.	11.074491	0.982143	172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=1/256, ttl=114 (request in 237)
3.	12.077758	1.003267	172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=2/512, ttl=114 (request in 296)
3.	13.097548	1.019798	172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=3/768, ttl=114 (request in 350)

Q5. Filter: **icmp**



No.	Time	Delta	Source	Destination	Protoc	Leng	Info
2.	10.013828		192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=0/0, ttl=64 (reply in 230)
2.	10.092348	0.079520	172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=0/0, ttl=114 (request in 228)
2.	10.984633	0.892585	192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=1/256, ttl=64 (reply in 230)
2.	11.074491	0.089858	172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=1/256, ttl=114 (request in 237)
2.	11.986483	0.911992	192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=2/512, ttl=64 (reply in 300)
3.	12.077758	0.091275	172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=2/512, ttl=114 (request in 296)
3.	12.688500	0.610742	192.168.1.229	192.168.1.1	ICMP	70	Destination unreachable (Port unreachable)
3.	12.993154	0.304654	192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=3/768, ttl=64 (reply in 359)
3.	13.097548	0.104394	172.217.17.35	192.168.1.229	ICMP	98	Echo (ping) reply id=0x4ab2, seq=3/768, ttl=114 (request in 350)
4.	13.604519	0.506971	192.168.1.229	192.41.152.67	ICMP	70	Destination unreachable (Port unreachable)

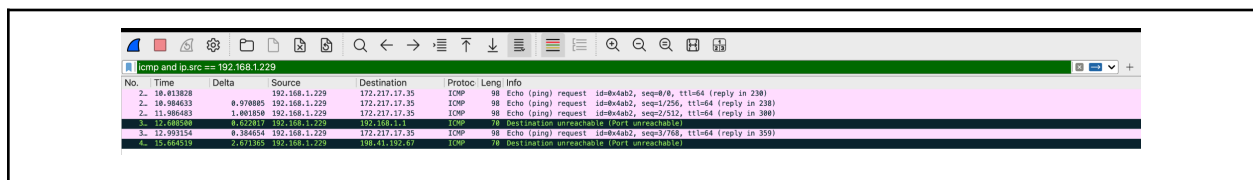
Q6. ICMP packets filtered:

10 (8 ping packets: 4 Echo requests + 4 Echo replies, plus 2 Destination Unreachable messages from other background traffic)

Q7. Packets with my IP as source:

6 (4 Echo requests + 2 Destination Unreachable)

Filter used: **icmp and ip.src == 192.168.1.229**



No.	Time	Delta	Source	Destination	Protoc	Leng	Info
2.	10.013828		192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=0/0, ttl=64 (reply in 230)
2.	10.984633	0.970885	192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=1/256, ttl=64 (reply in 230)
2.	11.986483	1.001850	192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=2/512, ttl=64 (reply in 300)
3.	12.688500	0.699518	192.168.1.229	192.41.152.67	ICMP	70	Destination unreachable (Port unreachable)
3.	12.993154	0.304654	192.168.1.229	172.217.17.35	ICMP	98	Echo (ping) request id=0x4ab2, seq=3/768, ttl=64 (reply in 359)
4.	13.604519	0.610742	192.168.1.229	192.41.152.67	ICMP	70	Destination unreachable (Port unreachable)

Q8. Packets with Google's IP as source:

4 (the Echo replies)

Filter used: **icmp and ip.src == 172.217.17.35**

Using the first Echo request (frame 228):

```
> Frame 228: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Apple_4f:26:6f (a8:8f:d9:4f:26:6f), Dst: Ubiquiti_81:24:16 (24:5a:4c:81:24:16)
> Internet Protocol Version 4, Src: 192.168.1.229, Dst: 172.217.17.35
> Internet Control Message Protocol

0000 24 5a 4c 81 24 16 a8 8f d9 4f 26 6f 08 00 45 00 52L-$---06o-5-
0010 00 54 c3 98 00 00 40 01 36 87 c0 a8 01 e5 ac d9 -T---@ 6---
0020 11 23 08 00 f6 7d 4a b2 00 00 d4 a8 22 00 05 -#---}]-j---
0030 b8 d0 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ------!""#$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ------&'()*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 6'()*+,-./012345
0060 36 37 67
```

No.: 228 - Time: 10.013820 - Delta: - Source: 192.168.1.229 - Destination: 172.217.17.35 - Protocol: ICMP - Length: 98 - Info: Echo (ping) request id=0x4ab2, seq=0/0, ttl=64 (reply in 230)

☐ Find in Packet ☒ Show packet bytes ☐ Layout: Vertical (Stacked) ☒

```
> Frame 228: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Apple_4f:26:6f (a8:8f:d9:4f:26:6f), Dst: Ubiquiti_81:24:16 (24:5a:4c:81:24:16)
> Destination: Ubiquiti_81:24:16 (24:5a:4c:81:24:16)
> Source: Apple_4f:26:6f (a8:8f:d9:4f:26:6f)
Type: IPv4 (0x0800)
[Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.1.229, Dst: 172.217.17.35
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0xc398 (50072)
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x3687 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.229
Destination Address: 172.217.17.35
[Stream index: 23]
- Internet Control Message Protocol

0000 24 5a 4c 81 24 16 a8 8f d9 4f 26 6f 08 00 45 00 52L-$---06o-5-
0010 00 54 c3 98 00 00 40 01 36 87 c0 a8 01 e5 ac d9 -T---@ 6---
0020 11 23 08 00 f6 7d 4a b2 00 00 d4 a8 22 00 05 -#---}]-j---
0030 b8 d0 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ------!""#$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ------&'()*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 6'()*+,-./012345
0060 36 37 67
```

Using the first Echo request (frame 230):

```
> Frame 230: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
- Ethernet II, Src: Ubiquiti_81:24:16 (24:5a:4c:81:24:16), Dst: Apple_4f:26:6f (a8:8f:d9:4f:26:6f)
> Destination: Apple_4f:26:6f (a8:8f:d9:4f:26:6f)
> Source: Ubiquiti_81:24:16 (24:5a:4c:81:24:16)
Type: IPv4 (0x0800)
[Stream index: 0]
- Internet Protocol Version 4, Src: 172.217.17.35, Dst: 192.168.1.229
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x0000 (0)
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 114
Protocol: ICMP (1)
Header Checksum: 0xc81f [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.217.17.35
Destination Address: 192.168.1.229
[Stream index: 23]
- Internet Control Message Protocol

0000 a8 8f d9 4f 26 6f 24 5a 4c 81 24 16 08 00 45 00 --06o$Z L-$---E-
0010 00 54 00 00 00 00 72 01 c8 1f ac d9 11 23 c0 a8 -T---@- ---#-
0020 01 e5 00 00 fe 7d 4a b2 00 00 6a d4 a8 22 00 05 -#---}]-j---
0030 b8 d0 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ------!""#$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ------&'()*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 6'()*+,-./012345
0060 36 37 67
```

Q9. Frame source and destination addresses:

Source MAC: a8:8f:d9:4f:26:6f (my Mac)

Destination MAC: 24:58:4c:81:24:16 (Ubiquiti router)

Q10. Is the destination MAC the address of Google.com.sa?

No. It is the MAC address of the default gateway (my router, 192.168.1.1). MAC addresses are only used for delivery within the local network, hop by hop. Since Google is on a different network, the frame is sent to the router, which forwards the packet toward Google. The IP addresses stay the same end to end, but the MAC addresses change at every hop.

Q11. Type field value:

0x0800, which means the Ethernet frame carries an IPv4 packet.

Q12. Source and destination IP addresses:

Source: 192.168.1.229, Destination: 172.217.17.35

Q13. Time for the Echo response:

Echo request (frame 228): 10.013828 s

Echo reply (frame 230): 10.092348 s

$10.092348 - 10.013828 = 0.078520 \text{ s} = 78.52 \text{ ms}$

It is lower than the 121.913 ms in Q2. Wireshark timestamps packets at the network interface, so it measures only the network round-trip time. The ping command measures in the application, so its time also includes operating-system processing delay, which is usually largest for the first packet.