

Exercise 11

ICMP – Wireshark

Command used: ping 8.8.8.8

Request:

Wireshark - Packet 845 - Wi-Fi: en0

> Frame 845: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Apple_33:6e:eb (bc:d0:74:33:6e:eb), Dst: SagemcomBros_81:9d:c0 (ec:be:dd:81:9d:c0)
Internet Protocol Version 4, Src: 192.168.1.34, Dst: 8.8.8.8
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSGP: CS0, ECN: Not-ECT)
Total Length: 98
Identification: 0x7a29 (31273)
> 000. = Flags: 0x0
..0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x2ea6 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.34
Destination Address: 8.8.8.8
Internet Control Message Protocol

0000 ec be dd 81 9d c0 bc d0 74 33 6e eb 08 00 45 00 ..t3n... E:
0010 00 54 00 00 00 00 75 01 73 cf 08 08 08 08 c0 a8 ..I...U: \$-P...
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..0.....
0030 0c 36 08 00 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 17.....
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 18.....
0060 36 37 67 19#%&(!)*+,- ./012345

No.: 845 - Time: 72.654693 - Source: 192.168.1.34 - Destination: 8.8.8.8 - Protocol: ICMP - Length: 98 - Info: Echo (ping) request id=0xd108, seq=1/256, ttl=64 (reply in 846)

Show packet bytes

Help Close

Reply:

Wireshark - Packet 846 - Wi-Fi: en0

> Frame 846: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: SagemcomBros_81:9d:c0 (ec:be:dd:81:9d:c0), Dst: Apple_33:6e:eb (bc:d0:74:33:6e:eb)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.34
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSGP: CS0, ECN: Not-ECT)
Total Length: 98
Identification: 0x0000 (0)
> 000. = Flags: 0x0
..0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 117
Protocol: ICMP (1)
Header Checksum: 0x73cf [validation disabled]
[Header checksum status: Unverified]
Source Address: 8.8.8.8
Destination Address: 192.168.1.34
Internet Control Message Protocol

0000 bc d0 74 33 6e eb ec be dd 81 9d c0 08 00 45 00 ..t3n...E:
0010 00 54 00 00 00 00 75 01 73 cf 08 08 08 08 c0 a8 ..I...U: \$-P...
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..0.....
0030 0c 36 08 00 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 17.....
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 18.....
0060 36 37 67 19#%&(!)*+,- ./012345

No.: 846 - Time: 72.860799 - Source: 8.8.8.8 - Destination: 192.168.1.34 - Protocol: ICMP - Length: 98 - Info: Echo (ping) reply id=0xd108, seq=1/256, ttl=117 (request in 845)

Show packet bytes

Help Close

Observations:

1. The Version field gives the version of the Internet Protocol used. In this case, it's 4, therefore it's an IPv4 packet.
2. TTL gives the maximum number of hops that the packet can travel before being discarded. In this case, it is 64 for the request and 117 for the reply
3. The 'Protocol: ICMP (1)' field identifies the protocol encapsulated in the IP packet's payload. In this case the value is 1, therefore the payload contains an ICMP packet.

Exercise 13

TCP – Wireshark

The screenshot shows a Wireshark window with the following details:

Packet 778 - Wireshark - Packet 778 - Wi-Fi: en0

Frame 778: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0

Ethernet II, Src: Apple_33:6e:eb (bc:db:74:33:6e:eb), Dst: SagemcomBrosa_81:9d:c0 (ec:be:dd:81:9d:c0)

Internet Protocol Version 4, Src: 192.168.1.34, Dst: 13.249.9.100

[Transmission Control Protocol, Src Port: 51481, Dst Port: 443, Seq: 65, Ack: 57, Len: 0]

Source Port: 51481
Destination Port: 443
[Stream index: 7]
> [Conversation completeness: Incomplete (12)]
[TCP Segment Len: 0]
Sequence Number: 65 (relative sequence number)
Sequence Number (raw): 3476866629
[Next Sequence Number: 66 (relative sequence number)]
Acknowledgment Number: 57 (relative ack number)
Acknowledgment number (raw): 3765483234
1000 = Header Length: 32 bytes (8)
> Flags: 0x010 (ACK)
Window: 2047
[Calculated window size: 2047]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xc723 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
> [Timestamps]
> [SEQ/ACK analysis]

Hex View:

0000	ec be dd 81 9d c0 bc d0	74 33 6e eb 08 00 A5 00 t3n E
0010	00 34 00 00 48 00 40 06	61 9d c0 a8 01 22 0d f9	:4-@-@-a-..
0020	09 64 c9 19 81 bb cf 3c	c6 45 df e5 53 48 08 18	:d-...<`E-SJ
0030	07 0f c7 28 00 00 01 81	08 8a a5 2b 54 46 25 54	:#-....+TF%T
0040	1c 26		-8-

Text View:

No.: 778 - Time: 70.881587 - Source: 192.168.1.34 - Destination: 13.249.9.100 - Protocol: TCP - Length: 66 - Info: 51481 > 443 [ACK] Seq=65 Ack=57 Win=2047 Len=0 TStamp=2771080262 TSecr=626269222

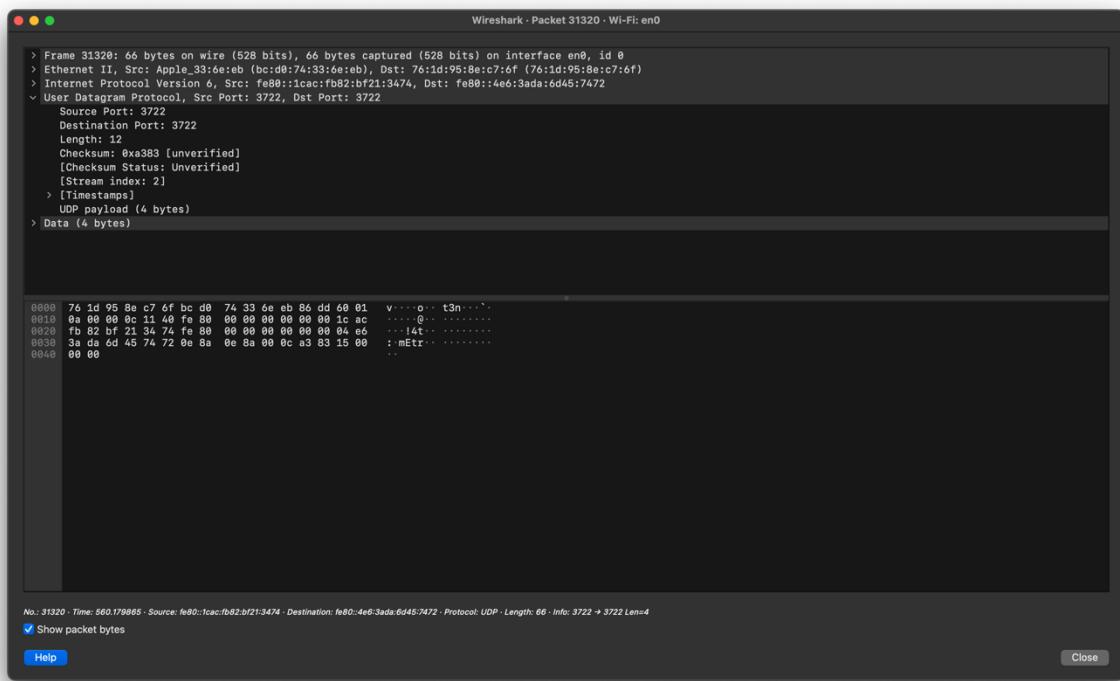
Show packet bytes

Help Close

Observations:

1. Destination port is 443, which corresponds to HTTPS
2. The sequence number of first octet in the segment (in this case, it is 3476866629) indicates that the first byte of data in this segment is the 2476866629th byte of the data stream (because 3476866629 - 10000000000 = 2476866629).
3. The relative sequence number (in this case, 65) is a number used by wireshark for easier interpretation.
4. Acknowledgment Number (3765483824) indicates that the sender has received all bytes up to this number minus one.
5. Header length = 32 bytes (8 * 4 = 32 bytes, as the header length field is in 4-byte words).

UDP – Wireshark



Observations:

1. The source port is equal to the destination port (3722)
2. The checksum value is 0xa383, but it's marked as unverified, therefore it hasn't been verified by the receiving system