

Question 1

TCP Header

Source Port		destination Port	
Sequence number			
Data Offset	Reserved	Flags	Window
Checksum		Urgent Pointer	
Data			

```
▼ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 104.47.28.22
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1492
    Identification: 0xafbf (44991)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xff73 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.3
    Destination: 104.47.28.22
  > Transmission Control Protocol, Src Port: 56117, Dst Port: 443, Seq: 3236, Ack: 11517, Len: 1452
```

TCP Packet Captured with header above

Source Ip Address: 192.168.1.3 the address of the host that sent the packet.

Destination Ip Address: 104.47.28.22 the address of the receiver.

Version 4 is the ip protocol version.

Header length is the length of the header 20 out of 60 max bytes. Total length is the total length of the packet including the header of 20 bytes. Identification describes the packet, flag controls the fragmentation and it doesn't fragment here. The fragment offset describes if the packet is too big to take apart and put together here it's not.

Time to live describes the length of time it has to send and discards if longer than the TTL. TTL is 128

Protocol is the type the packet is and this is a TCP.

Header checksum checks the headers checksum and its unverified.

Question 2

UDP Pseudo Header

32-bit source IP Address		
32-bit destination IP Address		
zero	8-bit protocol (17)	16-bit UDP length
16-bit source port number		16-bit destination port number
16-bit UDP length		16-bit UDP checksum
Data		

```
▼ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 74.125.193.101
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0x0ab1 (2737)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x2271 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.3
    Destination: 74.125.193.101
  > User Datagram Protocol, Src Port: 50896, Dst Port: 443
  > Data (33 bytes)
```

UDP Packet Captured with header above

Source Ip Address: 192.168.1.3 the address of the host that sent the packet.

Destination Ip Address: 74.125.193.101 the address of the receiver.

Version 4 is the ip protocol version.

Header length is the length of the header 20 out of 60 max bytes. Total length is the total length of the packet including the header of 20 bytes.

Identification describes the packet, flag controls the fragmentation and it doesn't fragment here. The fragment offset describes if the packet is too big to take apart and put together here it's not.

Time to live describes the length of time it has to send and discards if longer than the TTL. In this case 128

Protocol is the type the packet is and this is a UDP.

Header checksum checks the headers checksum and its unverified.

Question 3

16456 88.866241	192.168.1.3	74.125.193.101	UDP	75 50896 → 443 Len=33
16455 88.866133	74.125.193.101	192.168.1.3	UDP	106 443 → 50896 Len=64
16454 88.866133	74.125.193.101	192.168.1.3	UDP	74 443 → 50896 Len=32
16453 88.865463	192.168.1.3	74.125.193.101	UDP	75 50896 → 443 Len=33
16452 88.865345	74.125.193.101	192.168.1.3	UDP	424 443 → 50896 Len=382
16451 88.864505	74.125.193.101	192.168.1.3	UDP	123 443 → 50896 Len=81
16450 88.806896	74.125.193.101	192.168.1.3	UDP	67 443 → 50896 Len=25
16449 88.798900	192.168.1.3	74.125.193.101	UDP	636 50896 → 443 Len=594
16448 88.798790	192.168.1.3	74.125.193.101	UDP	1392 50896 → 443 Len=1350
11858 74.753246	192.168.1.3	74.125.193.101	UDP	75 50896 → 443 Len=33
11857 74.753119	74.125.193.101	192.168.1.3	UDP	139 443 → 50896 Len=97
11856 74.753119	74.125.193.101	192.168.1.3	UDP	74 443 → 50896 Len=32
11855 74.752394	192.168.1.3	74.125.193.101	UDP	75 50896 → 443 Len=33
11854 74.752262	74.125.193.101	192.168.1.3	UDP	423 443 → 50896 Len=381
11853 74.751390	74.125.193.101	192.168.1.3	UDP	123 443 → 50896 Len=81
11852 74.689070	74.125.193.101	192.168.1.3	UDP	67 443 → 50896 Len=25
11851 74.681020	192.168.1.3	74.125.193.101	UDP	582 50896 → 443 Len=540

> Frame 16456: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{0DE75947-765C-47DD-BFDC-84F2D0D11D64}, id 0
 > Ethernet II, Src: ASUSTek_79:e4:2b (4c:ed:fb:79:e4:2b), Dst: HuaweiTe_25:db:a5 (14:b9:68:25:db:a5)
 > Internet Protocol Version 4, Src: 192.168.1.3, Dst: 74.125.193.101
 > 0100 = Version: 4
 > 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 > Total Length: 61
 > Identification: 0x0ab1 (2737)
 > Flags: 0x4000, Don't fragment
 > Fragment offset: 0
 > Time to live: 128
 > Protocol: UDP (17)
 > Header checksum: 0x2271 [validation disabled]
 > [Header checksum status: Unverified]
 > Source: 192.168.1.3
 > Destination: 74.125.193.101
 > User Datagram Protocol, Src Port: 50896, Dst Port: 443
 > Data (33 bytes)

c0a8 7c45
 0103 7D113
 = C1AB 3787
 4a7d = 8089A
 = 10C28 4bce
 c165 = 85486
 = 1CD8D 6d5b
 0011 = 8C1E1
 = 1CD9E 5c16
 c6d0 = 91DF7
 = 2946E 168e
 01bb = 93485
 = 29629 0069
 0029 = 934EE
 = 29652 f08a
 1ada = A2578
 = 2B12C A2578
 4735 0063
 = 2F861 A25DB
 c4dd = 3BD3E
 = 3BD3E 10100010010111011011
 1110 = 3CE4E 01011101101000100100
 = 3CE4E 5da24
 930a = 46158
 = 46158 c9c8
 c9c8 = 52B20
 = 52B20 ab31
 ab31 = 5D651
 = 5D651 1380
 1380 = 5E9D1
 = 5E9D1 f25e
 f25e = 6DC2F
 = 6DC2F 789f
 789f = 754CE
 = 754CE

Addition of values and 16-bit ones complement Sum.

Question 4

158	0.040104	185.42.206.97	192.168.1.3	TLSv1.2	1506	Application Data [TCP segment of a reassembled PDU]
159	0.040104	185.42.206.97	192.168.1.3	TCP	1506	443 → 65263 [ACK] Seq=181824 Ack=1354 Win=199 Len=1452 [TCP segment of a reassembled PDU]
160	0.040104	185.42.206.97	192.168.1.3	TCP	1506	443 → 65263 [ACK] Seq=183276 Ack=1354 Win=199 Len=1452 [TCP segment of a reassembled PDU]
161	0.040104	185.42.206.97	192.168.1.3	TCP	1506	443 → 65263 [ACK] Seq=184728 Ack=1354 Win=199 Len=1452 [TCP segment of a reassembled PDU]

The packet above uses the TCP. I'm not sure if this is a streaming packet but it came up a lot while I ran a stream on its own.

Question 5

39	0.954610	192.168.1.3	140.82.121.3	TCP	66	49295 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
43	0.986227	140.82.121.3	192.168.1.3	TCP	66	443 → 49295 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 SACK_PERM=1 WS=1024
44	0.986280	192.168.1.3	140.82.121.3	TCP	54	49295 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0

Segment with SYN sent to start a connection with server and the sequence number of it. Tells the server the client is about to communicate with it. Next will be the response from the server and this will be a SYN , ACK. These are the segment that was received and the sequence number.

The last part is the ACK and this establishes that a connection between the client and the server has occurred.

Question 6

431	4.173726	192.168.1.3	140.82.112.25	TCP	54	49462 → 443 [FIN, ACK] Seq=1894 Ack=4276 Win=131328 Len=0
-----	----------	-------------	---------------	-----	----	---

Client sends FIN , ACK to state that the client wants to end the connection with the server

466	4.228570	192.168.1.3	140.82.121.4	TCP	54	49456 → 443 [ACK] Seq=6194 Ack=60270 Win=514 Len=0
469	4.277745	192.168.1.3	140.82.112.25	TCP	54	49462 → 443 [RST, ACK] Seq=1895 Ack=4349 Win=0 Len=0
473	4.282753	140.82.112.25	192.168.1.3	TCP	60	443 → 49462 [FIN, ACK] Seq=4399 Ack=1895 Win=72704 Len=0

The server sends back a ACK and then sends a FIN , ACK to the client to start the close of the connection.

564	4.701916	192.168.1.3	140.82.121.5	TCP	54	49443 → 443 [ACK] Seq=44513 Ack=3103 Win=512 Len=0
-----	----------	-------------	--------------	-----	----	--

The final ACK is sent from the client to the server to make sure the connection has been closed

Bonus Question

What are the gateways in case of Tcp/ip?

(WisdomJobs.com, 2020) states its function is to provide connectivity between network segments and runs on a computer and is a type of software. It provides a translation and allows systems to communicate on a network.

What is a link in the case of Tcp/ip?

(WisdomJobs.com, 2020) states that this is how two devices are communicating together and include protocols and the cables used and its describes the connectivity between the two devices.

Reference

WisdomJobs.com 2020, *TCP/IP INTERVIEW QUESTIONS & ANSWERS*, WisdomJobs.com, viewed 3 November 2020,
< <https://www.wisdomjobs.com/e-university/tcp-ip-interview-questions.html> >