D:\7h SEMESTER - SUBJECTS\ECD403 - Computer Networks\Assignment - 4\wireshark-report.md

Continuous Assessment 4

Student Information

- Serial No.: 31
- Name: Chotaliya Zeel Vijaybhai
- Admin No: 21JE0269

Network Analysis Results

Q1: What is your IP address and port number?

- IP Address: 172.22.50.138
- Port Number: 50267

Q2: What is "www.wikipedia.org" ip address and port number?

- IP Address: 103.102.166.224
- Port Number: 443

Q3: What is the raw sequence number of the first SYN packet sent from you to wikipedia's server?

- Raw Sequence Number: 3542999398

Q4: What is the raw sequence number of the first SYN-ACK packet sent from wikipedia's server to you?

- Raw Sequence Number: 2994873772

Q5: What was the window size shared by client to server in first SYN packet?

- Window Size: 64240

Q6: What was the window size shared by server to client in next SYN-ACK packet?

- Window Size: 42340

Q7: What was the time difference between sending a SYN packet and receiving SYN-ACK?

- Time Difference: 2.622631 - 2.531029 = 0.091602

Q8: What was the 'time to live' value in network header?

- TTL Value: 50

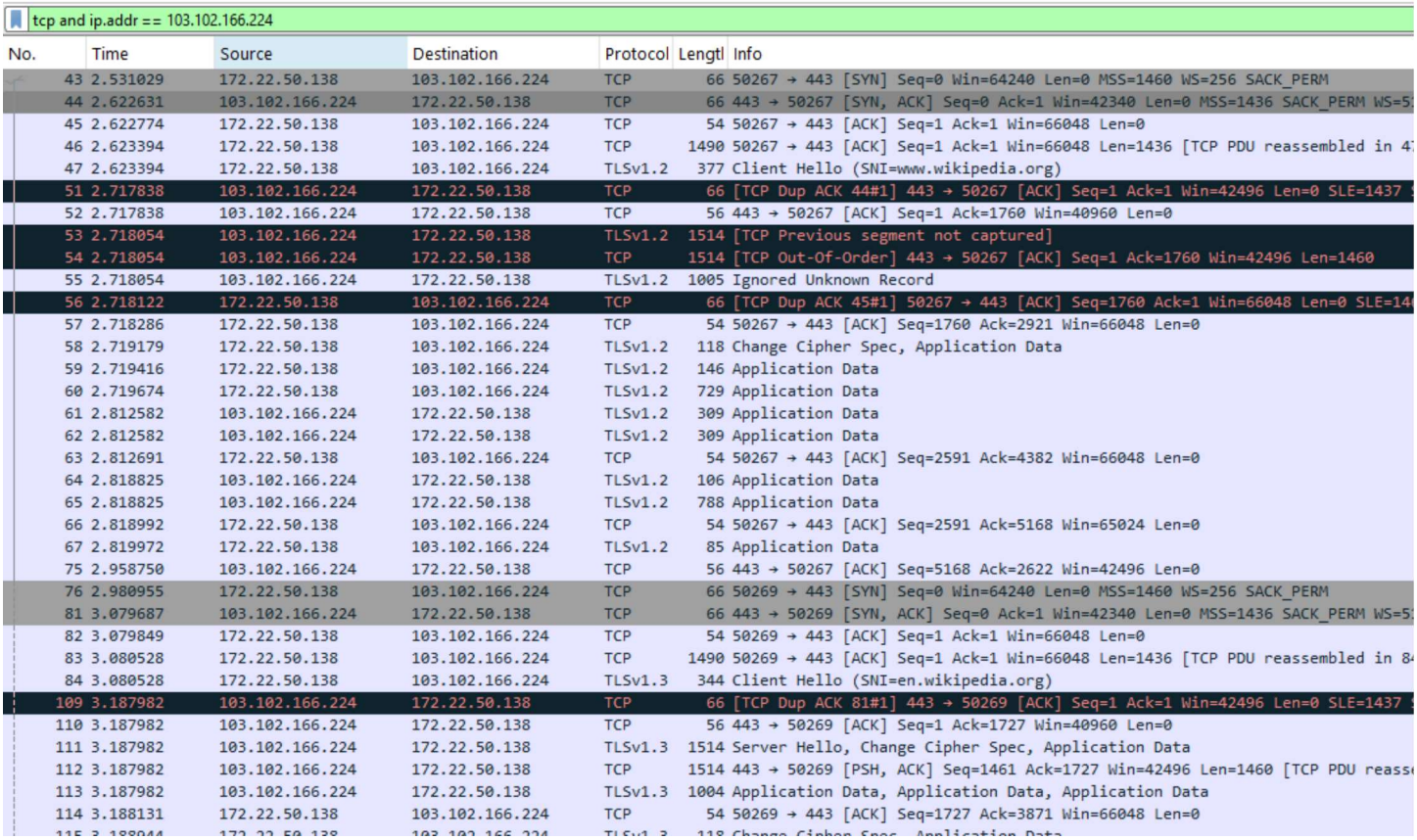
Q9: What was the ipv4 header length?

- IPv4 Header Length: 20 bytes

Q10: What is the difference between raw sequence number and relative sequence number in wireshark?

- Raw sequence numbers are the actual huge numbers TCP uses that start from some random Initial Sequence Number (ISN). These numbers are confusing to work with since they're so large - like when I was analyzing packets, I'd see numbers like 3,542,167,832.
- Relative sequence numbers are way easier to understand because Wireshark automatically converts them to start from 0. It basically subtracts the ISN from all the numbers so we can easily track how much data is moving.
- Example:
    - When I captured a TCP stream:
    - Raw number started at: 2,947,253,187 (wireshark showed this as 0)
    - After sending 100 bytes:
    - Raw became: 2,947,253,287
    - Relative showed: 100
- So when I'm counting bytes transferred, relative numbers make it super simple since I can just subtract them directly. Though we can switch between both views in Wireshark settings if needed.

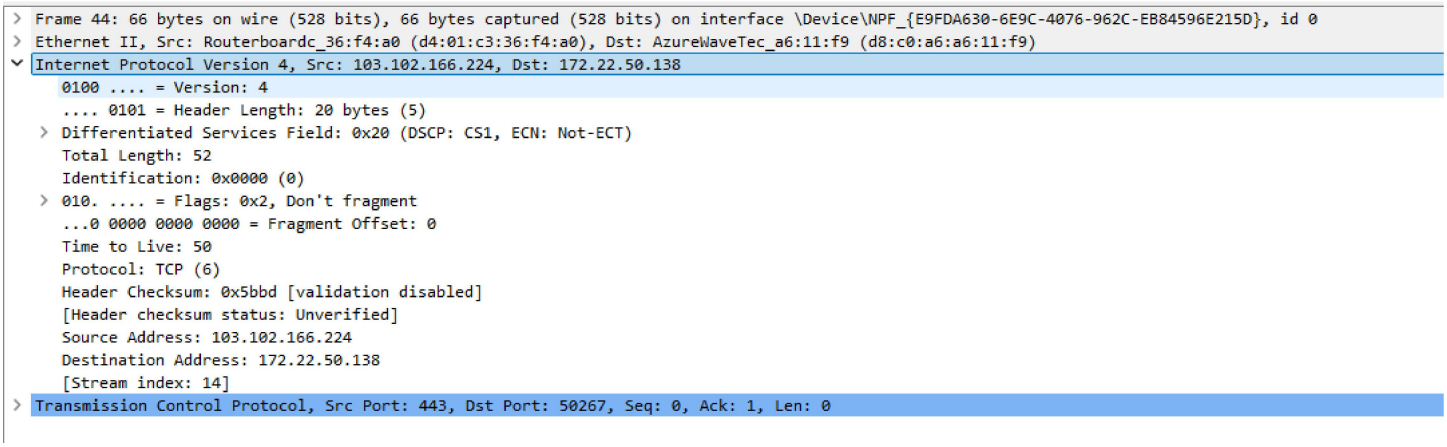
Screenshot 1: TCP Handshake (SYN, SYN-ACK, ACK)



tcp and ip.addr == 103.102.166.224

No.	Time	Source	Destination	Protocol	Lengtl	Info
43	2.531029	172.22.50.138	103.102.166.224	TCP	66	50267 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
44	2.622631	103.102.166.224	172.22.50.138	TCP	66	443 → 50267 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1436 SACK_PERM WS=5
45	2.622774	172.22.50.138	103.102.166.224	TCP	54	50267 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
46	2.623394	172.22.50.138	103.102.166.224	TCP	1490	50267 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=1436 [TCP PDU reassembled in 4
47	2.623394	172.22.50.138	103.102.166.224	TLSv1.2	377	Client Hello (SNI=www.wikipedia.org)
51	2.717838	103.102.166.224	172.22.50.138	TCP	66	[TCP Dup ACK 44#1] 443 → 50267 [ACK] Seq=1 Ack=1 Win=42496 Len=0 SLE=1437
52	2.717838	103.102.166.224	172.22.50.138	TCP	56	443 → 50267 [ACK] Seq=1 Ack=1760 Win=40960 Len=0
53	2.718054	103.102.166.224	172.22.50.138	TLSv1.2	1514	[TCP Previous segment not captured]
54	2.718054	103.102.166.224	172.22.50.138	TCP	1514	[TCP Out-Of-Order] 443 → 50267 [ACK] Seq=1 Ack=1760 Win=42496 Len=1460
55	2.718054	103.102.166.224	172.22.50.138	TLSv1.2	1005	Ignored Unknown Record
56	2.718122	172.22.50.138	103.102.166.224	TCP	66	[TCP Dup ACK 45#1] 50267 → 443 [ACK] Seq=1760 Ack=1 Win=66048 Len=0 SLE=14
57	2.718286	172.22.50.138	103.102.166.224	TCP	54	50267 → 443 [ACK] Seq=1760 Ack=2921 Win=66048 Len=0
58	2.719179	172.22.50.138	103.102.166.224	TLSv1.2	118	Change Cipher Spec, Application Data
59	2.719416	172.22.50.138	103.102.166.224	TLSv1.2	146	Application Data
60	2.719674	172.22.50.138	103.102.166.224	TLSv1.2	729	Application Data
61	2.812582	103.102.166.224	172.22.50.138	TLSv1.2	309	Application Data
62	2.812582	103.102.166.224	172.22.50.138	TLSv1.2	309	Application Data
63	2.812691	172.22.50.138	103.102.166.224	TCP	54	50267 → 443 [ACK] Seq=2591 Ack=4382 Win=66048 Len=0
64	2.818825	103.102.166.224	172.22.50.138	TLSv1.2	106	Application Data
65	2.818825	103.102.166.224	172.22.50.138	TLSv1.2	788	Application Data
66	2.818992	172.22.50.138	103.102.166.224	TCP	54	50267 → 443 [ACK] Seq=2591 Ack=5168 Win=65024 Len=0
67	2.819972	172.22.50.138	103.102.166.224	TLSv1.2	85	Application Data
75	2.958750	103.102.166.224	172.22.50.138	TCP	56	443 → 50267 [ACK] Seq=5168 Ack=2622 Win=42496 Len=0
76	2.980955	172.22.50.138	103.102.166.224	TCP	66	50269 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
81	3.079687	103.102.166.224	172.22.50.138	TCP	66	443 → 50269 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1436 SACK_PERM WS=5
82	3.079849	172.22.50.138	103.102.166.224	TCP	54	50269 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
83	3.080528	172.22.50.138	103.102.166.224	TCP	1490	50269 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=1436 [TCP PDU reassembled in 8
84	3.080528	172.22.50.138	103.102.166.224	TLSv1.3	344	Client Hello (SNI=en.wikipedia.org)
109	3.187982	103.102.166.224	172.22.50.138	TCP	66	[TCP Dup ACK 81#1] 443 → 50269 [ACK] Seq=1 Ack=1 Win=42496 Len=0 SLE=1437
110	3.187982	103.102.166.224	172.22.50.138	TCP	56	443 → 50269 [ACK] Seq=1 Ack=1727 Win=40960 Len=0
111	3.187982	103.102.166.224	172.22.50.138	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
112	3.187982	103.102.166.224	172.22.50.138	TCP	1514	443 → 50269 [PSH, ACK] Seq=1461 Ack=1727 Win=42496 Len=1460 [TCP PDU reass
113	3.187982	103.102.166.224	172.22.50.138	TLSv1.3	1004	Application Data, Application Data, Application Data
114	3.188131	172.22.50.138	103.102.166.224	TCP	54	50269 → 443 [ACK] Seq=1727 Ack=3871 Win=66048 Len=0

Screenshot 2: IPv4 Details



```
> Frame 44: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E9FDA630-6E9C-4076-962C-EB84596E215D}, id 0
> Ethernet II, Src: Routerboardc_36:f4:a0 (d4:01:c3:36:f4:a0), Dst: AzureWaveTec_a6:11:f9 (d8:c0:a6:a6:11:f9)
v Internet Protocol Version 4, Src: 103.102.166.224, Dst: 172.22.50.138
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 50
    Protocol: TCP (6)
    Header Checksum: 0x5bbd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 103.102.166.224
    Destination Address: 172.22.50.138
    [Stream index: 14]
> Transmission Control Protocol, Src Port: 443, Dst Port: 50267, Seq: 0, Ack: 1, Len: 0
```

Screenshot 3: TCP Details