

Networks Laboratory - Assignment 2

Muhammed Jaseem Pallikkal
B190703CS
CSE-B

1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.57	192.168.1.1	DNS	89	Standard query 0xd454 AAAA minerva.nitc.ac.in OPT
2	0.003578	192.168.1.1	192.168.1.57	DNS	89	Standard query response 0xd454 AAAA minerva.nitc.ac.in OPT
3	0.004482	192.168.1.57	103.160.223.7	TCP	74	37708 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3711029860 TSecr=0 WS=128
4	0.009063	103.160.223.7	192.168.1.57	TCP	74	443 → 37708 [SYN, ACK] Seq=0 Ack=1 Win=22592 Len=0 MSS=1412 WS=128 SACK_PERM=1 TSval=2267551918 TSecr=3711029860
5	0.009327	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3711029865 TSecr=2267551918
6	0.009774	192.168.1.57	103.160.223.7	TLSv1.2	464	Client Hello
7	0.023079	103.160.223.7	192.168.1.57	TCP	66	443 → 37708 [ACK] Seq=1 Ack=399 Win=22912 Len=0 TSval=2267551922 TSecr=3711029866
8	0.725350	103.160.223.7	192.168.1.57	TLSv1.2	1464	Server Hello
9	0.725951	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=399 Ack=1399 Win=64128 Len=0 TSval=3711030582 TSecr=2267552493
10	0.726762	103.160.223.7	192.168.1.57	TCP	1464	443 → 37708 [PSH, ACK] Seq=1399 Ack=399 Win=22912 Len=1398 TSval=2267552493 TSecr=3711029866 [TCP segment of a reassembled PDU]
11	0.727208	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=399 Ack=2797 Win=64128 Len=0 TSval=3711030583 TSecr=2267552493
12	0.728477	103.160.223.7	192.168.1.57	TCP	1366	443 → 37708 [PSH, ACK] Seq=2797 Ack=399 Win=22912 Len=1300 TSval=2267552493 TSecr=3711029866 [TCP segment of a reassembled PDU]
13	0.728554	103.160.223.7	192.168.1.57	TLSv1.2	442	Certificate, Server Key Exchange, Server Hello Done
14	0.728554	103.160.223.7	192.168.1.57	TCP	442	[TCP Retransmission] 443 → 37708 [PSH, ACK] Seq=4097 Ack=399 Win=22912 Len=376 TSval=2267552504 TSecr=3711029866
15	0.728554	103.160.223.7	192.168.1.57	TCP	442	[TCP Retransmission] 443 → 37708 [PSH, ACK] Seq=4097 Ack=399 Win=22912 Len=376 TSval=2267552514 TSecr=3711029866
16	0.728816	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=399 Ack=4097 Win=64128 Len=0 TSval=3711030585 TSecr=2267552493
17	0.728923	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=399 Ack=4473 Win=63872 Len=0 TSval=3711030585 TSecr=2267552494
18	0.729094	103.160.223.7	192.168.1.57	TCP	20	[TCP Dup ACK 17x1] 37708 → 443 [ACK] Seq=399 Ack=4473 Win=63872 Len=0 TSval=3711030585 TSecr=2267552494
19	0.729061	192.168.1.57	103.160.223.7	TCP	78	[TCP Dup ACK 17x2] 37708 → 443 [ACK] Seq=399 Ack=4473 Win=63872 Len=0 TSval=3711030585 TSecr=2267552504 SLE=4097 SRE=4473
20	0.730907	192.168.1.57	103.160.223.7	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
21	0.742940	103.160.223.7	192.168.1.57	TCP	66	443 → 37708 [ACK] Seq=4473 Ack=492 Win=23040 Len=0 TSval=2267552644 TSecr=3711030587
22	1.015143	103.160.223.7	192.168.1.57	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
23	1.015616	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=492 Ack=4524 Win=64128 Len=0 TSval=3711030872 TSecr=2267552924
24	1.016125	192.168.1.57	103.160.223.7	TLSv1.2	309	Application Data
25	1.024556	103.160.223.7	192.168.1.57	TCP	66	443 → 37708 [ACK] Seq=4524 Ack=735 Win=23296 Len=0 TSval=2267552928 TSecr=3711030872
26	1.302282	103.160.223.7	192.168.1.57	TCP	1464	443 → 37708 [PSH, ACK] Seq=4524 Ack=735 Win=23296 Len=1398 TSval=2267553211 TSecr=3711030872 [TCP segment of a reassembled PDU]
27	1.302856	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=5922 Win=64128 Len=0 TSval=3711031159 TSecr=2267553211

> Frame 219: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E610F281-1F54-4390-B1CC-80BA387EF4F8}, id 0
> Ethernet II, Src: CloudNet_80:4d:a3 (90:0f:0c:80:4d:a3), Dst: HuaweiTe_c3:64:c7 (08:c0:21:c3:64:c7)
> Internet Protocol Version 4, Src: 192.168.1.57, Dst: 103.160.223.7
> Transmission Control Protocol, Src Port: 37708, Dst Port: 443, Seq: 735, Ack: 143907, Len: 0

0000 08 c0 21 c3 64 c7 90 0f 0c 80 4d a3 08 00 45 00 ...I..d...M...E-
0010 00 34 b4 3e 40 00 40 06 7d fc c0 a8 01 39 67 a0 ...4->@: }....9g.
0020 df 07 93 4c 01 bb df 50 84 aa 7c 78 b7 ca 80 11 ...L...P...|x....
0030 06 fc 49 a5 00 00 01 01 08 0a dd 31 da e0 87 281....(
0040 21 10I..

Beginning of the transfer of packets

No.	Time	Source	Destination	Protocol	Length	Info
196	2.167722	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=128950 Win=197120 Len=0 TSval=3711032024 TSecr=2267554063
197	2.167952	103.160.223.7	192.168.1.57	TCP	1460	443 → 37708 [PSH, ACK] Seq=128950 Ack=735 Win=23296 Len=1394 TSval=2267554063 TSecr=3711031755 [TCP segment of a reassembled P...
198	2.168139	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=130344 Win=200064 Len=0 TSval=3711032024 TSecr=2267554063
199	2.168682	103.160.223.7	192.168.1.57	TCP	1466	443 → 37708 [ACK] Seq=130344 Ack=735 Win=23296 Len=1400 TSval=2267554063 TSecr=3711031755 [TCP segment of a reassembled PDU]
200	2.168910	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=131744 Win=202880 Len=0 TSval=3711032025 TSecr=2267554063
201	2.169142	103.160.223.7	192.168.1.57	TCP	1466	443 → 37708 [ACK] Seq=131744 Ack=735 Win=23296 Len=1400 TSval=2267554063 TSecr=3711031755 [TCP segment of a reassembled PDU]
202	2.169333	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=133144 Win=205824 Len=0 TSval=3711032026 TSecr=2267554063
203	2.169713	103.160.223.7	192.168.1.57	TCP	1466	443 → 37708 [ACK] Seq=133144 Ack=735 Win=23296 Len=1400 TSval=2267554063 TSecr=3711031755 [TCP segment of a reassembled PDU]
204	2.169970	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=134544 Win=208640 Len=0 TSval=3711032026 TSecr=2267554063
205	2.170681	103.160.223.7	192.168.1.57	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
206	2.170908	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=135944 Win=211584 Len=0 TSval=3711032027 TSecr=2267554063
207	2.171344	103.160.223.7	192.168.1.57	TCP	1456	443 → 37708 [PSH, ACK] Seq=135944 Ack=735 Win=23296 Len=1390 TSval=2267554063 TSecr=3711031755 [TCP segment of a reassembled P...
208	2.171344	103.160.223.7	192.168.1.57	TCP	1464	443 → 37708 [PSH, ACK] Seq=137334 Ack=735 Win=23296 Len=1398 TSval=2267554063 TSecr=3711031755 [TCP segment of a reassembled P...
209	2.171628	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=137334 Win=214528 Len=0 TSval=3711032028 TSecr=2267554063
210	2.171691	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=138732 Win=217344 Len=0 TSval=3711032028 TSecr=2267554063
211	2.171914	103.160.223.7	192.168.1.57	TCP	1464	443 → 37708 [PSH, ACK] Seq=138732 Ack=735 Win=23296 Len=1398 TSval=2267554064 TSecr=3711031755 [TCP segment of a reassembled P...
212	2.172075	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=140130 Win=220288 Len=0 TSval=3711032028 TSecr=2267554064
213	2.173806	103.160.223.7	192.168.1.57	TCP	1464	443 → 37708 [PSH, ACK] Seq=140130 Ack=735 Win=23296 Len=1398 TSval=2267554064 TSecr=3711031755 [TCP segment of a reassembled P...
214	2.174141	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=141528 Win=223232 Len=0 TSval=3711032030 TSecr=2267554064
215	2.174385	103.160.223.7	192.168.1.57	TCP	1464	443 → 37708 [PSH, ACK] Seq=141528 Ack=735 Win=23296 Len=1398 TSval=2267554064 TSecr=3711031755 [TCP segment of a reassembled P...
216	2.174517	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=142926 Win=226048 Len=0 TSval=3711032031 TSecr=2267554064
217	2.174902	103.160.223.7	192.168.1.57	TLSv1.2	1047	Application Data
218	2.175085	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=735 Ack=143907 Win=228864 Len=0 TSval=3711032031 TSecr=2267554064
219	2.175960	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [FIN, ACK] Seq=735 Ack=143907 Win=228864 Len=0 TSval=3711032032 TSecr=2267554064
220	2.183577	103.160.223.7	192.168.1.57	TCP	66	443 → 37708 [ACK] Seq=143907 Ack=736 Win=23296 Len=0 TSval=2267554088 TSecr=3711032032
221	2.479808	103.160.223.7	192.168.1.57	TCP	66	443 → 37708 [FIN, ACK] Seq=143907 Ack=736 Win=23296 Len=0 TSval=2267554373 TSecr=3711032032
222	2.480117	192.168.1.57	103.160.223.7	TCP	66	37708 → 443 [ACK] Seq=736 Ack=143908 Win=228864 Len=0 TSval=3711032336 TSecr=2267554373

> Frame 219: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E610F281-1F54-4390-B1CC-80BA387EF4F8}, id 0
> Ethernet II, Src: CloudNet_80:4d:a3 (90:0f:0c:80:4d:a3), Dst: HuaweiTe_c3:64:c7 (08:c0:21:c3:64:c7)
> Internet Protocol Version 4, Src: 192.168.1.57, Dst: 103.160.223.7
> Transmission Control Protocol, Src Port: 37708, Dst Port: 443, Seq: 735, Ack: 143907, Len: 0

0000 08 c0 21 c3 64 c7 90 0f 0c 80 4d a3 08 00 45 00 ...I..d...M...E-
0010 00 34 b4 3e 40 00 40 06 7d fc c0 a8 01 39 67 a0 ...4->@: }....9g.
0020 df 07 93 4c 01 bb df 50 84 aa 7c 78 b7 ca 80 11 ...L...P...|x....
0030 06 fc 49 a5 00 00 01 01 08 0a dd 31 da e0 87 281....(
0040 21 10I..

End of transfer of packets

- Initially, in frames 1 and 2, we are doing a DNS lookup of minerva.nitc.ac.in to find its IP address.
- IP address of minerva.nitc.ac.in is 103.160.223.7 and the port used is 443
- IP address of the laptop is 192.168.1.57 and the port used is 37708
- Most of the frames are using TCP protocol which indicates that the data is transmitted using TCP protocol.
- Transport Layer Security (TLSv1.2) protocol is used to encrypt data sent through the internet.
- Then in frames 3 and 4, the SYN flag is set which synchronises the sequence numbers and indicates that the connection is initiated.
- In frame 6 we see the client sending hello and in frame 8, we can see the server sending hello. This is known as TLS handshake and is what starts a communication session between the client and the server.
- In frames 219 and 221, the FIN flag is set which indicates that the connection is being terminated.

2. a. Source: 192.168.44.53
Destination: 192.168.44.1
- b. HTTP
- c. Username: vasudevanar
Password: vasu

3. **Packet Number: 27**

Source Port: 443
 Destination Port: 59138
 Sequence Number: 3056868986
 Acknowledgement Number: 1084580465
 Data Offset: 20
 Reserved: 0
 URG: 0
 ACK: 1
 PSH: 0
 RST: 0
 SYN: 0
 FIN: 1
 Window Size: 60
 Checksum: 0x5442
 Urgent Pointer: 0

Packet Number: 32

Source Port: 59139

Destination Port: 443

Sequence Number: 1660956066

Acknowledgement Number: 3861199010

Data Offset: 20

Reserved: 000

URG: 0

ACK: 1

PSH: 0

RST: 1

SYN: 0

FIN: 0

Window Size: 0

Checksum: 0xfaec

Urgent Pointer: 0