

CS3093D: NETWORKS LABORATORY

ASSIGNMENT 2



Hadif Yassin Hameed

B190513CS

1. DNS Resolution:

- a. Type A DNS query sent from source 192.168.0.178 to destination 102.168.0.1 for minerva.nitc.ac.in

```
▶ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c), Dst: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b)
▶ Internet Protocol Version 4, Src: 192.168.0.178, Dst: 192.168.0.1
▶ User Datagram Protocol, Src Port: 52587, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x62f2
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ minerva.nitc.ac.in: type A, class IN
    [Response In: 3]
```

- b. Standard DNS type A query response of 103.160.223.7 received from source 192.168.0.1 to destination 192.168.0.178

```
▶ Ethernet II, Src: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b), Dst: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c)
▶ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.178
▶ User Datagram Protocol, Src Port: 53, Dst Port: 52587
▼ Domain Name System (response)
  Transaction ID: 0x62f2
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ minerva.nitc.ac.in: type A, class IN
  ▼ Answers
    ▶ minerva.nitc.ac.in: type A, class IN, addr 103.160.223.7
    [Request In: 1]
    [Time: 0.002609833 seconds]
```

TCP handshake:

- a. TCP SYN packet sent from 192.168.0.178 to 103.160.223.7 to synchronize sequence numbers and initiate TCP connection

```

▶ Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c), Dst: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b)
▶ Internet Protocol Version 4, Src: 192.168.0.178, Dst: 103.160.223.7
▼ Transmission Control Protocol, Src Port: 33854, Dst Port: 443, Seq: 0, Len: 0
  -Source Port: 33854
  -Destination Port: 443
  -[Stream index: 0]
  -[Conversation completeness: Complete, WITH_DATA (31)]
  -[TCP Segment Len: 0]
  -Sequence Number: 0 (relative sequence number)
  -Sequence Number (raw): 4245264762
  -[Next Sequence Number: 1 (relative sequence number)]
  -Acknowledgment Number: 0
  -Acknowledgment number (raw): 0
  -1010 .... = Header Length: 40 bytes (10)
  ▶ Flags: 0x002 (SYN)
  -Window: 64240
  -[Calculated window size: 64240]
  -Checksum: 0x63ed [unverified]
  -[Checksum Status: Unverified]
  -Urgent Pointer: 0
  ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▶ [Timestamps]

```

b. TCP SYN+ACK response sent from 103.160.223.7 to 192.168.0.178 to acknowledge connection request.

```

▶ Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b), Dst: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c)
▶ Internet Protocol Version 4, Src: 103.160.223.7, Dst: 192.168.0.178
▼ Transmission Control Protocol, Src Port: 443, Dst Port: 33854, Seq: 0, Ack: 1, Len: 0
  -Source Port: 443
  -Destination Port: 33854
  -[Stream index: 0]
  -[Conversation completeness: Complete, WITH_DATA (31)]
  -[TCP Segment Len: 0]
  -Sequence Number: 0 (relative sequence number)
  -Sequence Number (raw): 1190386205
  -[Next Sequence Number: 1 (relative sequence number)]
  -Acknowledgment Number: 1 (relative ack number)
  -Acknowledgment number (raw): 4245264763
  -1010 .... = Header Length: 40 bytes (10)
  ▶ Flags: 0x012 (SYN, ACK)
  -Window: 65160
  -[Calculated window size: 65160]
  -Checksum: 0xd469 [unverified]
  -[Checksum Status: Unverified]
  -Urgent Pointer: 0
  ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▶ [Timestamps]

```

c. TCP ACK packet sent from 192.168.0.178 to 103.160.223.7 to complete the

3-way TCP handshake and start the TCP session

```
▶ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c), Dst: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b)
▶ Internet Protocol Version 4, Src: 192.168.0.178, Dst: 103.160.223.7
▼ Transmission Control Protocol, Src Port: 33854, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  -Source Port: 33854
  -Destination Port: 443
  -[Stream index: 0]
  -[Conversation completeness: Complete, WITH_DATA (31)]
  -[TCP Segment Len: 0]
  -Sequence Number: 1 (relative sequence number)
  -Sequence Number (raw): 4245264763
  -[Next Sequence Number: 1 (relative sequence number)]
  -Acknowledgment Number: 1 (relative ack number)
  -Acknowledgment number (raw): 1190386206
  -1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x010 (ACK)
  -Window: 502
  -[Calculated window size: 64256]
  -[Window size scaling factor: 128]
  -Checksum: 0xfe9c [unverified]
  -[Checksum Status: Unverified]
  -Urgent Pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
```

TLSv1.2 handshake:

a. Client Hello sent from 192.168.0.178 to 103.160.223.7

```
▶ Frame 8: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c), Dst: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b)
▶ Internet Protocol Version 4, Src: 192.168.0.178, Dst: 103.160.223.7
▶ Transmission Control Protocol, Src Port: 33854, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    -Content Type: Handshake (22)
    -Version: TLS 1.0 (0x0301)
    -Length: 512
    ▶ Handshake Protocol: Client Hello
```

b. Server Hello sent from 103.160.223.7 to 192.168.0.178

```
▶ Frame 10: 4162 bytes on wire (33296 bits), 4162 bytes captured (33296 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b), Dst: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c)
▶ Internet Protocol Version 4, Src: 103.160.223.7, Dst: 192.168.0.178
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 33854, Seq: 1, Ack: 518, Len: 4096
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 93
    ▶ Handshake Protocol: Server Hello
```

c. Certificate, server encrypted key, Server Hello Done sent from 103.160.223.7 to 192.168.0.178

```
▶ Frame 12: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b), Dst: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c)
▶ Internet Protocol Version 4, Src: 103.160.223.7, Dst: 192.168.0.178
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 33854, Seq: 4097, Ack: 518, Len: 372
▶ [2 Reassembled TCP Segments (4056 bytes): #10(3998), #12(58)]
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 4051
    ▶ Handshake Protocol: Certificate
  ▼ Transport Layer Security
    ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      - Content Type: Handshake (22)
      - Version: TLS 1.2 (0x0303)
      - Length: 300
      ▶ Handshake Protocol: Server Key Exchange
    ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      - Content Type: Handshake (22)
      - Version: TLS 1.2 (0x0303)
      - Length: 4
      ▶ Handshake Protocol: Server Hello Done
```

d. Client encrypted key, change cipher spec, encrypted handshake message sent from 192.168.0.178 to 103.160.223.7

```
▶ Frame 14: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c), Dst: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b)
▶ Internet Protocol Version 4, Src: 192.168.0.178, Dst: 103.160.223.7
▶ Transmission Control Protocol, Src Port: 33854, Dst Port: 443, Seq: 518, Ack: 4469, Len: 93
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 37
    ▶ Handshake Protocol: Client Key Exchange
  ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    - Content Type: Change Cipher Spec (20)
    - Version: TLS 1.2 (0x0303)
    - Length: 1
    - Change Cipher Spec Message
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 40
    - Handshake Protocol: Encrypted Handshake Message
```

e. Change cipher spec, encrypted handshake message sent from 103.160.223.7 to 192.168.0.178 signifying completion of TLS handshake

```
▶ Frame 15: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b), Dst: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c)
▶ Internet Protocol Version 4, Src: 103.160.223.7, Dst: 192.168.0.178
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 33854, Seq: 4469, Ack: 611, Len: 51
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    - Content Type: Change Cipher Spec (20)
    - Version: TLS 1.2 (0x0303)
    - Length: 1
    - Change Cipher Spec Message
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 40
    - Handshake Protocol: Encrypted Handshake Message
```

Data Transfer:

Data is transferred over the following frames using TCP and TLS v1.2 protocols

- ▶ Frame 22: 2946 bytes on wire (23568 bits), 2946 bytes captured (23568 bits) on interface wlp63s0, id 0
- ▶ Ethernet II, Src: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b), Dst: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c)
- ▶ Internet Protocol Version 4, Src: 103.160.223.7, Dst: 192.168.0.178
- ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 33854, Seq: 18920, Ack: 842, Len: 2880
- ▶ [3 Reassembled TCP Segments (16413 bytes): #18(1440), #20(12960), #22(2013)]
- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 16408
 - Encrypted Application Data: c8ec5c8ff3d7b5cfd7c0a15cdef38362e612b446c6762acd30d79ddc53a5997068ecbfe...
 - [Application Data Protocol: http-over-tls]
- ▶ Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp63s0, id 0
- ▶ Ethernet II, Src: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c), Dst: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b)
- ▶ Internet Protocol Version 4, Src: 192.168.0.178, Dst: 103.160.223.7
- ▼ Transmission Control Protocol, Src Port: 33854, Dst Port: 443, Seq: 842, Ack: 21800, Len: 0
 - Source Port: 33854
 - Destination Port: 443
 - [Stream index: 0]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 0]
 - Sequence Number: 842 (relative sequence number)
 - Sequence Number (raw): 4245265604
 - [Next Sequence Number: 842 (relative sequence number)]
 - Acknowledgment Number: 21800 (relative ack number)
 - Acknowledgment number (raw): 1190408005
 - 1000 = Header Length: 32 bytes (8)
 - ▶ Flags: 0x010 (ACK)
 - Window: 477
 - [Calculated window size: 61056]
 - [Window size scaling factor: 128]
 - Checksum: 0x9cbb [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - ▶ [Timestamps]
 - ▶ [SEQ/ACK analysis]

FIN:

FIN+ACK packets sent in both directions to mark end of TCP session

```
▶ Frame 58: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c), Dst: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b)
▶ Internet Protocol Version 4, Src: 192.168.0.178, Dst: 103.160.223.7
▼ Transmission Control Protocol, Src Port: 33854, Dst Port: 443, Seq: 842, Ack: 143903, Len: 0
```

```
  -Source Port: 33854
  -Destination Port: 443
  -[Stream index: 0]
  -[Conversation completeness: Complete, WITH_DATA (31)]
  -[TCP Segment Len: 0]
  -Sequence Number: 842      (relative sequence number)
  -Sequence Number (raw): 4245265604
  -[Next Sequence Number: 843      (relative sequence number)]
  -Acknowledgment Number: 143903      (relative ack number)
  -Acknowledgment number (raw): 1190530108
  -1000 .... = Header Length: 32 bytes (8)
▶ Flags: 0x011 (FIN, ACK)
  -Window: 1787
  -[Calculated window size: 228736]
  -[Window size scaling factor: 128]
  -Checksum: 0xa508 [unverified]
  -[Checksum Status: Unverified]
  -Urgent Pointer: 0
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶ [Timestamps]
```

```
▶ Frame 59: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp63s0, id 0
▶ Ethernet II, Src: D-LinkIn_70:ce:5b (78:98:e8:70:ce:5b), Dst: IntelCor_d8:be:7c (34:f6:4b:d8:be:7c)
▶ Internet Protocol Version 4, Src: 103.160.223.7, Dst: 192.168.0.178
▼ Transmission Control Protocol, Src Port: 443, Dst Port: 33854, Seq: 143903, Ack: 843, Len: 0
```

```
  -Source Port: 443
  -Destination Port: 33854
  -[Stream index: 0]
  -[Conversation completeness: Complete, WITH_DATA (31)]
  -[TCP Segment Len: 0]
  -Sequence Number: 143903      (relative sequence number)
  -Sequence Number (raw): 1190530108
  -[Next Sequence Number: 143904      (relative sequence number)]
  -Acknowledgment Number: 843      (relative ack number)
  -Acknowledgment number (raw): 4245265605
  -1000 .... = Header Length: 32 bytes (8)
▶ Flags: 0x011 (FIN, ACK)
  -Window: 505
  -[Calculated window size: 64640]
  -[Window size scaling factor: 128]
  -Checksum: 0xa8d1 [unverified]
  -[Checksum Status: Unverified]
  -Urgent Pointer: 0
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶ [Timestamps]
▶ [SEQ/ACK analysis]
```


2. a. Source IP address: 192.168.44.53
Destination IP address: 192.168.44.1
- b. Application Layer Protocol: HTTP
- c. magic: 179048ba09bf3146
username: vasudevanar
password: vasu

3. Packet 27

443								59138							
3056868986															
1084580465															
20 bytes	000000	0	1	0	0	0	1	60							
0x5442								0							
Options															
Data															

Packet 32

59139								443							
1660956066															
3861199010															
20 bytes	000000	0	1	0	1	0	0	0							
0xfaec								0							
Options															
Data															