COMP416: Computer Networks

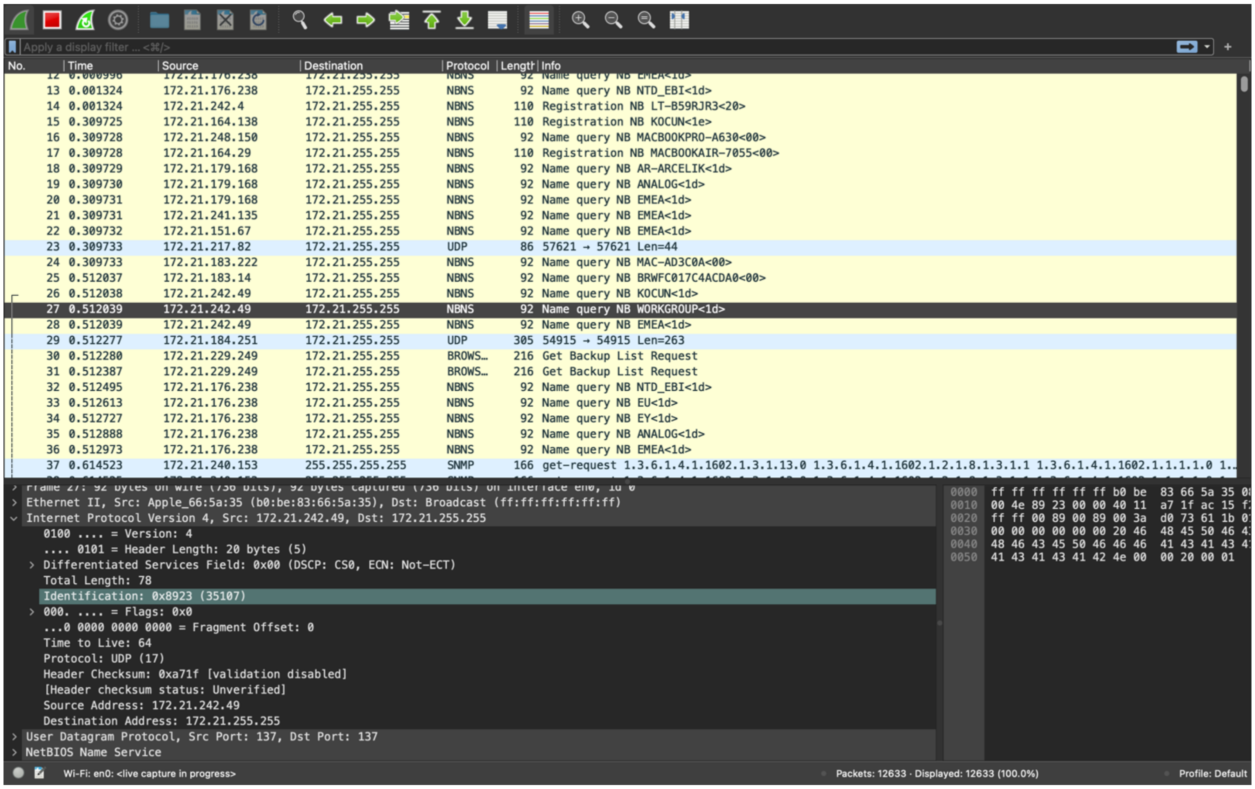
Project 2

Transport Layer Protocols’ Experiments with Wireshark

Emir Fatih AYYILDIZ   71527

Part 1.1

Last 2 digits of my id is 27.



```
No.   Time      Source          Destination      Protocol Length Info
   12 0.000996  172.21.176.238  172.21.255.255   NBNS      92 Name query NB EMEA<1d>
   13 0.001324  172.21.176.238  172.21.255.255   NBNS      92 Name query NB NTD_EBI<1d>
   14 0.001324  172.21.242.4    172.21.255.255   NBNS     110 Registration NB LT-B59RJR3<20>
   15 0.309725  172.21.164.138  172.21.255.255   NBNS     110 Registration NB KOCUN<1e>
   16 0.309728  172.21.248.150  172.21.255.255   NBNS      92 Name query NB MACBOOKPRO-A630<00>
   17 0.309728  172.21.164.29   172.21.255.255   NBNS     110 Registration NB MACBOOKAIR-7055<00>
   18 0.309729  172.21.179.168  172.21.255.255   NBNS      92 Name query NB AR-ARCELIK<1d>
   19 0.309730  172.21.179.168  172.21.255.255   NBNS      92 Name query NB ANALOG<1d>
   20 0.309731  172.21.179.168  172.21.255.255   NBNS      92 Name query NB EMEA<1d>
   21 0.309731  172.21.241.135  172.21.255.255   NBNS      92 Name query NB EMEA<1d>
   22 0.309732  172.21.151.67   172.21.255.255   NBNS      92 Name query NB EMEA<1d>
   23 0.309733  172.21.217.82   172.21.255.255   UDP       86 57621 → 57621 Len=44
   24 0.309733  172.21.183.222  172.21.255.255   NBNS      92 Name query NB MAC-AD3C0A<00>
   25 0.512037  172.21.183.14   172.21.255.255   NBNS      92 Name query NB BRWFC017C4ACDA0<00>
   26 0.512038  172.21.242.49   172.21.255.255   NBNS      92 Name query NB KOCUN<1d>
   27 0.512039  172.21.242.49   172.21.255.255   NBNS      92 Name query NB WORKGROUP<1d>
   28 0.512039  172.21.242.49   172.21.255.255   NBNS      92 Name query NB EMEA<1d>
   29 0.512277  172.21.184.251  172.21.255.255   UDP      305 54915 → 54915 Len=263
   30 0.512280  172.21.229.249  172.21.255.255   BROWS…   216 Get Backup List Request
   31 0.512387  172.21.229.249  172.21.255.255   BROWS…   216 Get Backup List Request
   32 0.512495  172.21.176.238  172.21.255.255   NBNS      92 Name query NB NTD_EBI<1d>
   33 0.512613  172.21.176.238  172.21.255.255   NBNS      92 Name query NB EU<1d>
   34 0.512727  172.21.176.238  172.21.255.255   NBNS      92 Name query NB EY<1d>
   35 0.512888  172.21.176.238  172.21.255.255   NBNS      92 Name query NB ANALOG<1d>
   36 0.512973  172.21.176.238  172.21.255.255   NBNS      92 Name query NB EMEA<1d>
   37 0.614523  172.21.240.153  255.255.255.255  SNMP     166 get-request 1.3.6.1.4.1.1602.1.3.1.13.0 1.3.6.1.4.1.1602.1.2.1.8.1.3.1.1 1.3.6.1.4.1.1602.1.1.1.1.0 1…
```

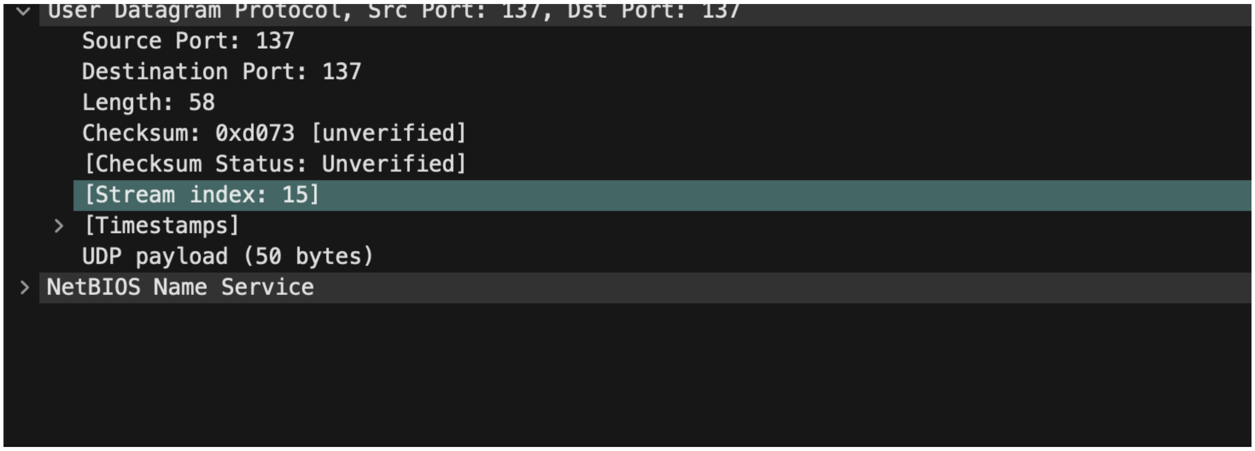
```
> Frame 27: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface en0, id 0
> Ethernet II, Src: Apple_66:5a:35 (b0:be:83:66:5a:35), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 172.21.242.49, Dst: 172.21.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 78
    Identification: 0x8923 (35107)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xa71f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.21.242.49
    Destination Address: 172.21.255.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff b0 be  83 66 5a 35 08
0010  00 4e 89 23 00 00 40 11  a7 1f ac 15 f2
0020  ff ff 00 89 00 89 00 3a  d0 73 61 1b 01
0030  00 00 00 00 00 00 20 46  48 45 50 46 43
0040  48 46 43 45 50 46 46 46  41 43 41 43 43
0050  41 43 41 43 41 42 4e 00  00 20 00 01
```

Wi-Fi: en0: <live capture in progress>   Packets: 12633 · Displayed: 12633 (100.0%)   Profile: Default

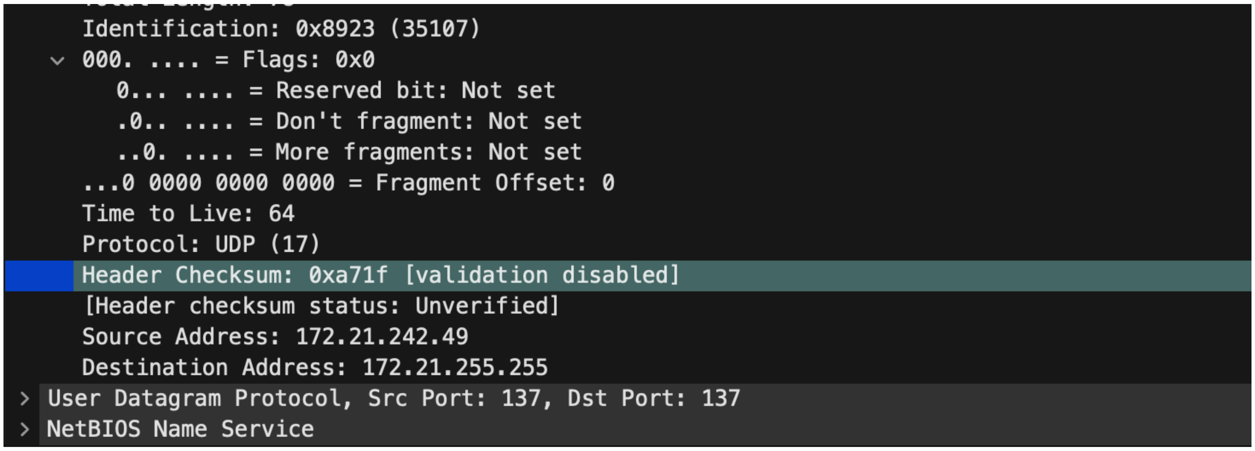
1)- Under the IPV4 segment, it shows that time to live (TTL) is 64. TTL defines the lifespan or number of hops it can make in network. If TTL becomes 0, it is dropped. So, it doesn’t take space forever in the network.

2)- Stream index shows the order that UDP packets are captured. My segments stream index is 15



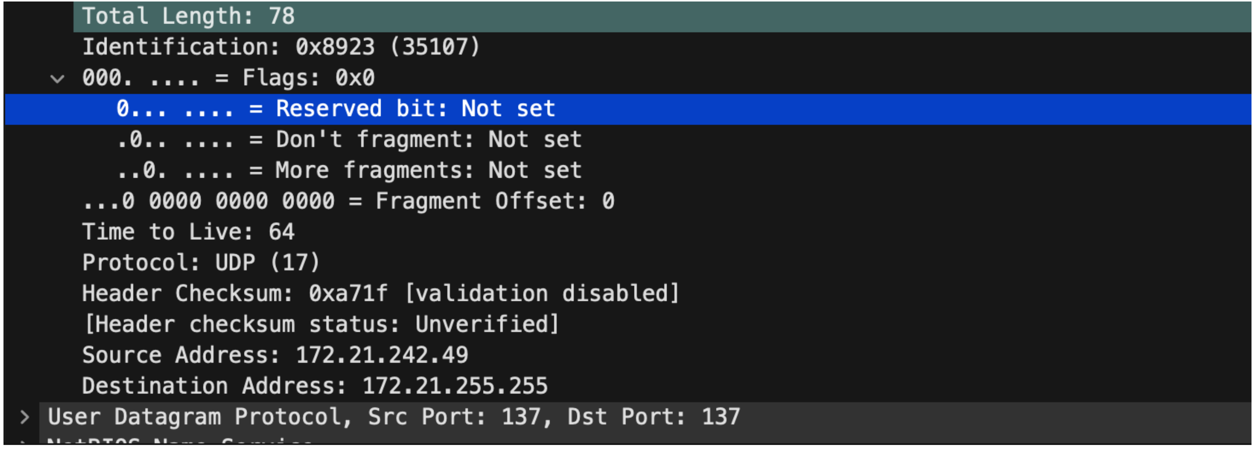
```
∨ User Datagram Protocol, Src Port: 137, Dst Port: 137
     Source Port: 137
     Destination Port: 137
     Length: 58
     Checksum: 0xd073 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 15]
  >  [Timestamps]
     UDP payload (50 bytes)
> NetBIOS Name Service
```

3)- Checksum is used for determining if the message has been corrupted or not. If the value observed is different, the message may be corrupted. TCP also uses checksum to ensure message is not corrupted but also it protects against misrouting because TCP header contains ip addresses of src and dst. My checksum is disabled.



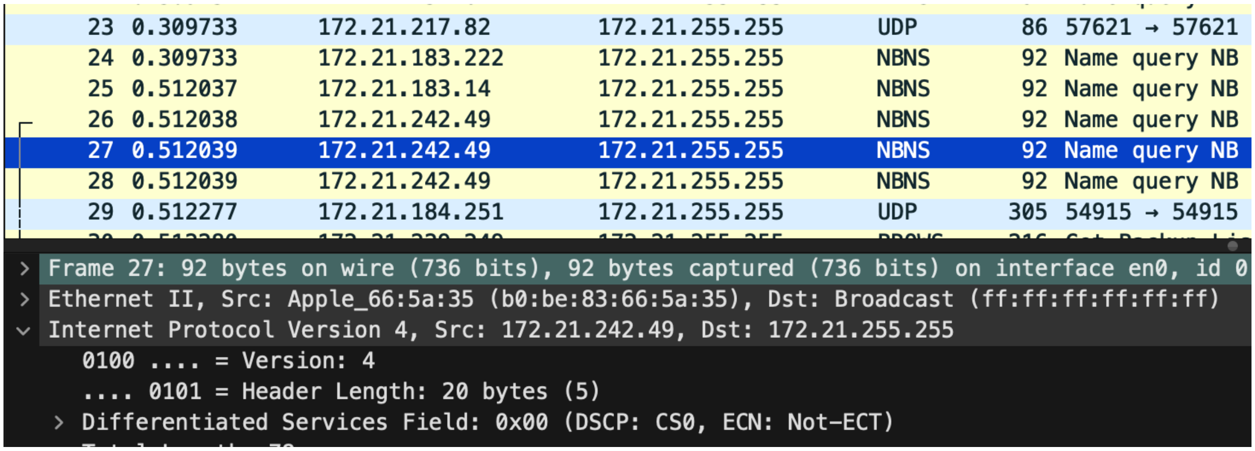
```
     Total Length: 78
     Identification: 0x8923 (35107)
  ∨  000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: UDP (17)
     Header Checksum: 0xa71f [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 172.21.242.49
     Destination Address: 172.21.255.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

4)- Reserved bit flag allows enhancements made on IP protocol on future uses. My reserved bit flag is not set yet.



```
     Total Length: 78
     Identification: 0x8923 (35107)
  ∨  000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: UDP (17)
     Header Checksum: 0xa71f [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 172.21.242.49
     Destination Address: 172.21.255.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

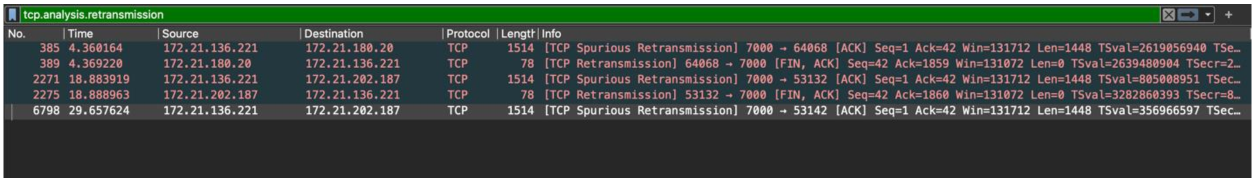
5)- length field tells about the IP packets length. It is used to ensure the calculated length is same as this length. In my case, its length is 92.



```
 23 0.309733   172.21.217.82    172.21.255.255   UDP    86  57621 → 57621
 24 0.309733   172.21.183.222   172.21.255.255   NBNS   92  Name query NB
 25 0.512037   172.21.183.14    172.21.255.255   NBNS   92  Name query NB
 26 0.512038   172.21.242.49    172.21.255.255   NBNS   92  Name query NB
 27 0.512039   172.21.242.49    172.21.255.255   NBNS   92  Name query NB
 28 0.512039   172.21.242.49    172.21.255.255   NBNS   92  Name query NB
 29 0.512277   172.21.184.251   172.21.255.255   UDP   305  54915 → 54915

> Frame 27: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface en0, id 0
> Ethernet II, Src: Apple_66:5a:35 (b0:be:83:66:5a:35), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 172.21.242.49, Dst: 172.21.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

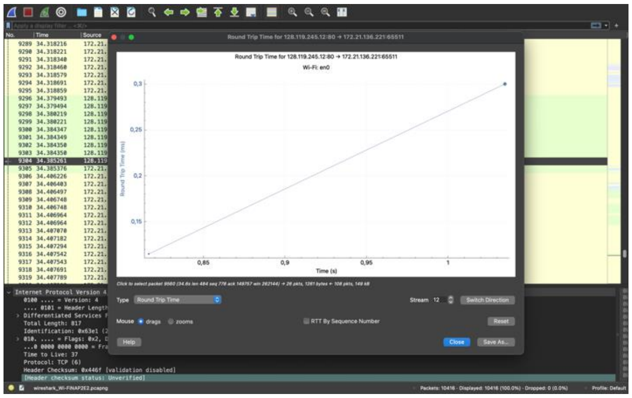
Part 1.2

1)- By entering “tcp.analysis.retransmission” into the filter, I can display all retransmissions. These retransmissions are caused by segment losses. To recover these packets, retransmission occurs.



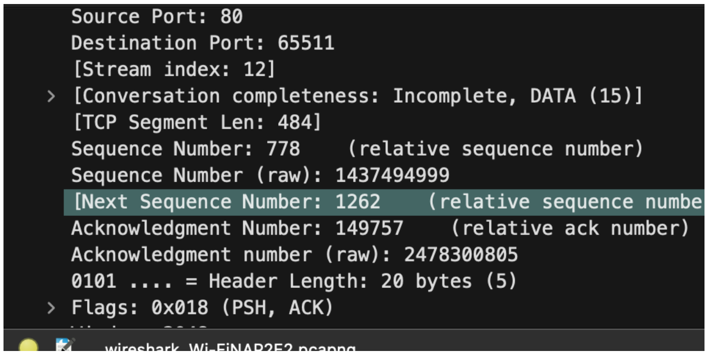
```
tcp.analysis.retransmission
No.   Time       Source           Destination      Protocol Length Info
  385 4.360164   172.21.136.221   172.21.180.20    TCP      1514 [TCP Spurious Retransmission] 7000 → 64068 [ACK] Seq=1 Ack=42 Win=131712 Len=1448 TSval=2619056940 TSe…
  389 4.369220   172.21.180.20    172.21.136.221   TCP        78 [TCP Retransmission] 64068 → 7000 [FIN, ACK] Seq=42 Ack=1859 Win=131072 Len=0 TSval=2639480904 TSecr=2…
 2271 18.883919  172.21.136.221   172.21.202.187   TCP      1514 [TCP Spurious Retransmission] 7000 → 53132 [ACK] Seq=1 Ack=42 Win=131712 Len=1448 TSval=805008951 TSec…
 2275 18.888963  172.21.202.187   172.21.136.221   TCP        78 [TCP Retransmission] 53132 → 7000 [FIN, ACK] Seq=42 Ack=1860 Win=131072 Len=0 TSval=3282860393 TSecr=8…
 6798 29.657624  172.21.136.221   172.21.202.187   TCP      1514 [TCP Spurious Retransmission] 7000 → 53142 [ACK] Seq=1 Ack=42 Win=131712 Len=1448 TSval=356966597 TSec…
```

2)- the statistics menu has an option to display a graph of a tcp connection. We can see that rtt is 0.3 from the graph. There are variations in rtt because the RTT starts at 0.1 milliseconds and increases to 0.3 milliseconds.



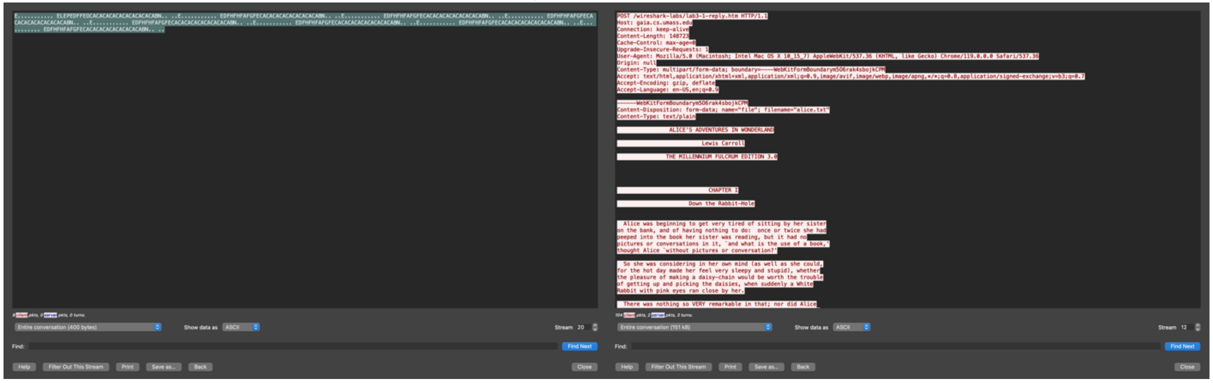
```
No.  Time       Source
9289 34.318216  172.21.
9290 34.318221  172.21.
9291 34.318340  172.21.
9292 34.318460  172.21.
9293 34.318579  172.21.
9294 34.318691  172.21.
9295 34.318859  172.21.
9296 34.379493  128.119
9297 34.379494  128.119
9298 34.380219  128.119
9299 34.380221  128.119
9300 34.384347  128.119
9301 34.384349  128.119
9302 34.384350  128.119
9303 34.384350  128.119
9304 34.385261  128.119
9305 34.385376  172.21.
9306 34.406226  172.21.
9307 34.406403  172.21.
9308 34.406497  172.21.
9309 34.406740  172.21.
9310 34.406748  172.21.
9311 34.406964  172.21.
9312 34.406964  172.21.
9313 34.407070  172.21.
9314 34.407182  172.21.
9315 34.407294  172.21.
9316 34.407542  172.21.
9317 34.407543  172.21.
9318 34.407691  172.21.
9319 34.407789  172.21.

v Internet Protocol Version 4
    0100 .... = Version: 4
    .... 0101 = Header Length
  > Differentiated Services F
    Total Length: 817
    Identification: 0x63e1 (2
  > 010. .... = Flags: 0x2, D
    ...0 0000 0000 0000 = Fra
    Time to Live: 37
    Protocol: TCP (6)
    Header Checksum: 0x446f [validation disabled]
    [Header checksum status: Unverified]

wireshark_Wi-FiNAP2E2.pcapng    Packets: 10416 · Displayed: 10416 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

3)- TCP includes sequence and acknowledge numbers and various flags however udp does not contain this information. They are used to make sure the message is transmitted successfully.



```
    Source Port: 80
    Destination Port: 65511
    [Stream index: 12]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 484]
    Sequence Number: 778    (relative sequence number)
    Sequence Number (raw): 1437494999
    [Next Sequence Number: 1262    (relative sequence numbe
    Acknowledgment Number: 149757    (relative ack number)
    Acknowledgment number (raw): 2478300805
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

4)- by right clicking and selecting follow, I opened segments for udp and tcp. The first one is udp and contains hexadecimal notations. The second one is tcp and contains more information about the data, to make sure its reliability.



```
E.......... ELEPEDFFEOCACACACACACACACACABN.. ..E.......... EDFHFHFAFGFECACACACACACACACACABN.. ..E.......... EDFHFHFAFGFECACACACACACACACACABN.. ..E.......... EDFHFHFAFGFECA
CACACACACACACABN.. ..E.......... EDFHFHFAFGFECACACACACACACACACABN.. ..E.......... EDFHFHFAFGFECACACACACACACACACABN.. ..E.......... EDFHFHFAFGFECACACACACACACACACABN.. ..E...
........ EDFHFHFAFGFECACACACACACACACACABN.. ..
```

8 client pkts, 0 server pkts, 0 turns.

Entire conversation (400 bytes) — Show data as: ASCII — Stream: 20

Find:

```
POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Content-Length: 148723
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarym5O6rak4sbojkCPM
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

------WebKitFormBoundarym5O6rak4sbojkCPM
Content-Disposition: form-data; name="file"; filename="alice.txt"
Content-Type: text/plain

                ALICE'S ADVENTURES IN WONDERLAND

                          Lewis Carroll

               THE MILLENNIUM FULCRUM EDITION 3.0




                            CHAPTER I

                      Down the Rabbit-Hole


  Alice was beginning to get very tired of sitting by her sister
on the bank, and of having nothing to do:  once or twice she had
peeped into the book her sister was reading, but it had no
pictures or conversations in it, `and what is the use of a book,'
thought Alice `without pictures or conversation?'

  So she was considering in her own mind (as well as she could,
for the hot day made her feel very sleepy and stupid), whether
the pleasure of making a daisy-chain would be worth the trouble
of getting up and picking the daisies, when suddenly a White
Rabbit with pink eyes ran close by her.

  There was nothing so VERY remarkable in that; nor did Alice
```

104 client pkts, 2 server pkts, 3 turns.

Entire conversation (151 kB) — Show data as: ASCII — Stream: 12

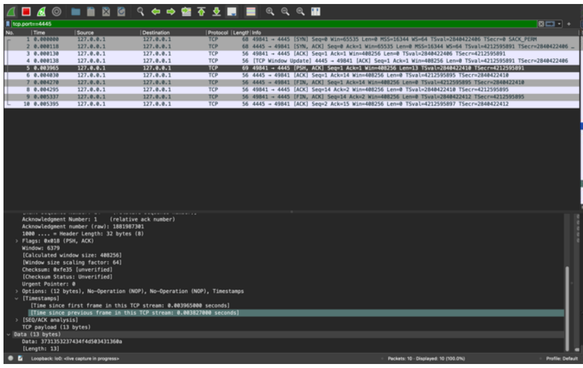
Find:

Part2.1

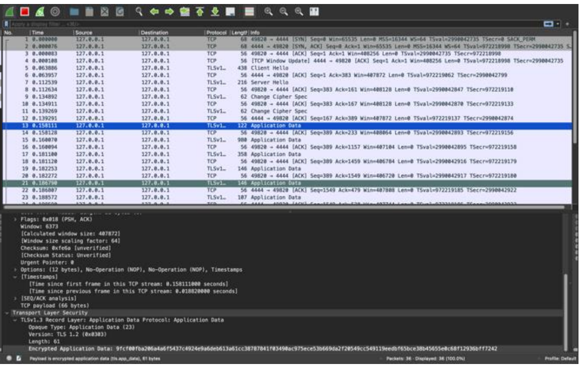
1)- for unsecure connection, only tcp is used. For secure connection, tcp and tls were used. Important messages were sent with tls.

2)- for unsecure connections, data can be seen as hexadecimal characters. These can be converted to text very easily. In my case, I converted the hexadecimal characters to text and saw 71527COMP416. In secure connection, data is in tlsv1.3 protocol. In application data, you can see encrypted data. unless you have the key, you cant see data.

3)- in unsecure connection, data is hexadecimal caharacters. In secure connection, data is encrypted.

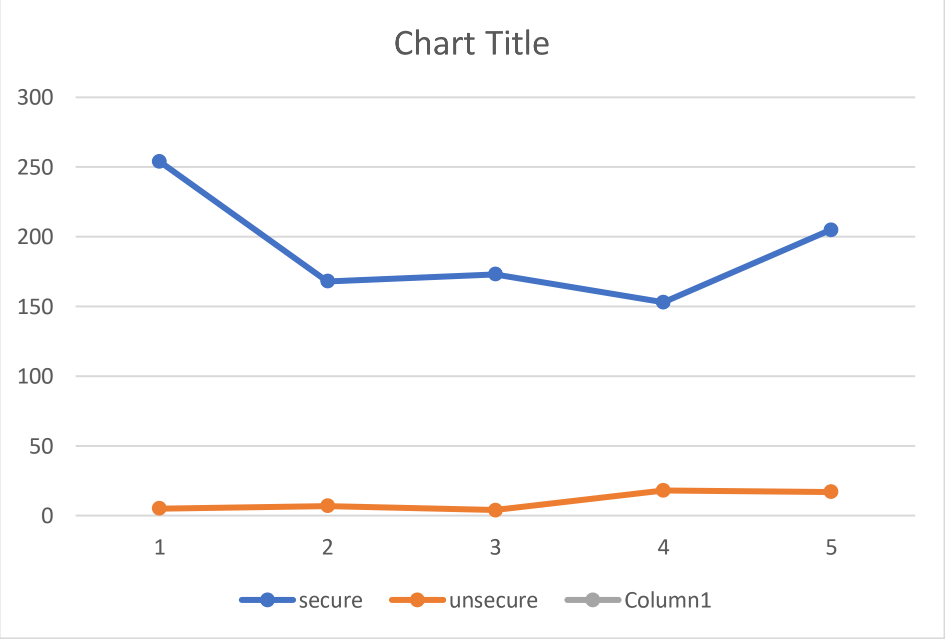


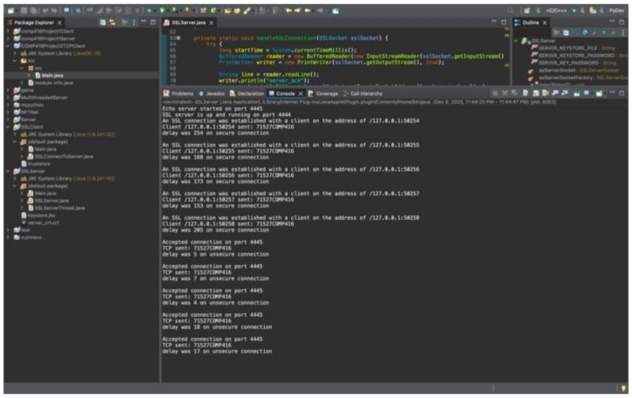
```
tcp.port==4445
No.  Time      Source     Destination  Protocol Length Info
  1 0.000000  127.0.0.1  127.0.0.1    TCP      68 49841 → 4445 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=2840422406 TSecr=0 SACK_PERM
  2 0.000118  127.0.0.1  127.0.0.1    TCP      68 4445 → 49841 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=4212595891 TSecr=2840422406 …
  3 0.000130  127.0.0.1  127.0.0.1    TCP      56 49841 → 4445 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2840422406 TSecr=4212595891
  4 0.000138  127.0.0.1  127.0.0.1    TCP      56 [TCP Window Update] 4445 → 49841 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=4212595891 TSecr=2840422406
  5 0.003965  127.0.0.1  127.0.0.1    TCP      69 49841 → 4445 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=13 TSval=2840422410 TSecr=4212595891
  6 0.004030  127.0.0.1  127.0.0.1    TCP      56 4445 → 49841 [ACK] Seq=1 Ack=14 Win=408256 Len=0 TSval=4212595895 TSecr=2840422410
  7 0.004270  127.0.0.1  127.0.0.1    TCP      56 4445 → 49841 [FIN, ACK] Seq=1 Ack=14 Win=408256 Len=0 TSval=4212595895 TSecr=2840422410
  8 0.004295  127.0.0.1  127.0.0.1    TCP      56 49841 → 4445 [ACK] Seq=14 Ack=2 Win=408256 Len=0 TSval=2840422410 TSecr=4212595895
  9 0.005337  127.0.0.1  127.0.0.1    TCP      56 49841 → 4445 [FIN, ACK] Seq=14 Ack=2 Win=408256 Len=0 TSval=2840422412 TSecr=4212595895
 10 0.005395  127.0.0.1  127.0.0.1    TCP      56 4445 → 49841 [ACK] Seq=2 Ack=15 Win=408256 Len=0 TSval=4212595897 TSecr=2840422412

    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1881987301
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 6379
    [Calculated window size: 408256]
    [Window size scaling factor: 64]
    Checksum: 0xfe35 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 0.003965000 seconds]
      [Time since previous frame in this TCP stream: 0.003827000 seconds]
  > [SEQ/ACK analysis]
    TCP payload (13 bytes)
⌄ Data (13 bytes)
    Data: 3731353237434f4d503431360a
    [Length: 13]

Loopback: lo0: <live capture in progress>          Packets: 10 · Displayed: 10 (100.0%)          Profile: Default
```



```
Apply a display filter … <⌘/>
No.  Time      Source     Destination  Protocol Length Info
  1 0.000000  127.0.0.1  127.0.0.1    TCP       68 49820 → 4444 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=2990042735 TSecr=0 SACK_PERM
  2 0.000076  127.0.0.1  127.0.0.1    TCP       68 4444 → 49820 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=972218998 TSecr=2990042735 S…
  3 0.000083  127.0.0.1  127.0.0.1    TCP       56 49820 → 4444 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2990042735 TSecr=972218998
  4 0.000108  127.0.0.1  127.0.0.1    TCP       56 [TCP Window Update] 4444 → 49820 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=972218998 TSecr=2990042735
  5 0.063886  127.0.0.1  127.0.0.1    TLSv1…   438 Client Hello
  6 0.063957  127.0.0.1  127.0.0.1    TCP       56 4444 → 49820 [ACK] Seq=1 Ack=383 Win=407872 Len=0 TSval=972219062 TSecr=2990042799
  7 0.112539  127.0.0.1  127.0.0.1    TLSv1…   216 Server Hello
  8 0.112634  127.0.0.1  127.0.0.1    TCP       56 49820 → 4444 [ACK] Seq=383 Ack=161 Win=408128 Len=0 TSval=2990042847 TSecr=972219110
  9 0.134892  127.0.0.1  127.0.0.1    TLSv1…    62 Change Cipher Spec
 10 0.134911  127.0.0.1  127.0.0.1    TCP       56 49820 → 4444 [ACK] Seq=383 Ack=167 Win=408128 Len=0 TSval=2990042870 TSecr=972219133
 11 0.139269  127.0.0.1  127.0.0.1    TLSv1…    62 Change Cipher Spec
 12 0.139291  127.0.0.1  127.0.0.1    TCP       56 4444 → 49820 [ACK] Seq=167 Ack=389 Win=407872 Len=0 TSval=972219137 TSecr=2990042874
 13 0.158111  127.0.0.1  127.0.0.1    TLSv1…   122 Application Data
 14 0.158128  127.0.0.1  127.0.0.1    TCP       56 49820 → 4444 [ACK] Seq=389 Ack=233 Win=408064 Len=0 TSval=2990042893 TSecr=972219156
 15 0.160070  127.0.0.1  127.0.0.1    TLSv1…   980 Application Data
 16 0.160094  127.0.0.1  127.0.0.1    TCP       56 49820 → 4444 [ACK] Seq=389 Ack=1157 Win=407104 Len=0 TSval=2990042895 TSecr=972219158
 17 0.181100  127.0.0.1  127.0.0.1    TLSv1…   358 Application Data
 18 0.181120  127.0.0.1  127.0.0.1    TCP       56 49820 → 4444 [ACK] Seq=389 Ack=1459 Win=406784 Len=0 TSval=2990042916 TSecr=972219179
 19 0.182253  127.0.0.1  127.0.0.1    TLSv1…   146 Application Data
 20 0.182272  127.0.0.1  127.0.0.1    TCP       56 49820 → 4444 [ACK] Seq=389 Ack=1549 Win=406720 Len=0 TSval=2990042917 TSecr=972219180
 21 0.186790  127.0.0.1  127.0.0.1    TLSv1…   146 Application Data
 22 0.186807  127.0.0.1  127.0.0.1    TCP       56 4444 → 49820 [ACK] Seq=1549 Ack=479 Win=407808 Len=0 TSval=972219185 TSecr=2990042922
 23 0.188572  127.0.0.1  127.0.0.1    TLSv1…   107 Application Data

  > Flags: 0x018 (PSH, ACK)
    Window: 6373
    [Calculated window size: 407872]
    [Window size scaling factor: 64]
    Checksum: 0xfe6a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 0.158111000 seconds]
      [Time since previous frame in this TCP stream: 0.018820000 seconds]
  > [SEQ/ACK analysis]
    TCP payload (66 bytes)
⌄ Transport Layer Security
  ⌄ TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 61
      Encrypted Application Data: 9fcf00fba206a4a6f5437c4924e9a6deb613a61cc38787841f03490ac975ece53b669da2f20549cc549119eedbf65bce38b45655e0c68f12936bff7242

Payload is encrypted application data (tls.app_data), 61 bytes          Packets: 36 · Displayed: 36 (100.0%)          Profile: Default
```

4)- from the results I obtained from tests below we can see secure connection takes way more time than unsecure connection. This is because it takes time to decrypt and make a secure connection. Unsecure connection takes less time to transmit data because it doesn't waste time on making client hello and server hello messages. It doesn't transmit keys and doesn't decrypt data.





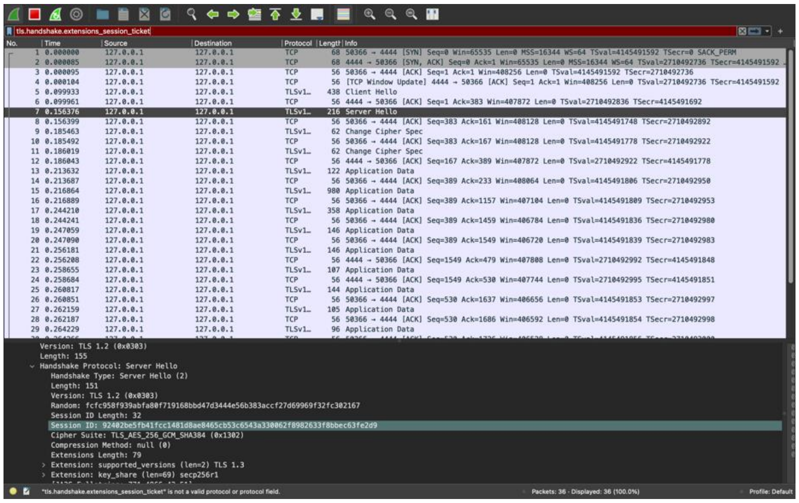
```java
private static void handleSSLConnection(SSLSocket sslSocket) {
    try {
        long startTime = System.currentTimeMillis();
        BufferedReader reader = new BufferedReader(new InputStreamReader(sslSocket.getInputStream()
        PrintWriter writer = new PrintWriter(sslSocket.getOutputStream(), true);

        String line = reader.readLine();
        writer.println("server_ack");
```

```
<terminated> SSLServer [Java Application] /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/java (Dec 6, 2023, 11:44:23 PM – 11:44:47 PM) [pid: 9263]
Echo server started on port 4445
SSL server is up and running on port 4444
An SSL connection was established with a client on the address of /127.0.0.1:50254
Client /127.0.0.1:50254 sent: 71527COMP416
delay was 254 on secure connection

An SSL connection was established with a client on the address of /127.0.0.1:50255
Client /127.0.0.1:50255 sent: 71527COMP416
delay was 168 on secure connection

An SSL connection was established with a client on the address of /127.0.0.1:50256
Client /127.0.0.1:50256 sent: 71527COMP416
delay was 173 on secure connection

An SSL connection was established with a client on the address of /127.0.0.1:50257
Client /127.0.0.1:50257 sent: 71527COMP416
delay was 153 on secure connection

An SSL connection was established with a client on the address of /127.0.0.1:50258
Client /127.0.0.1:50258 sent: 71527COMP416
delay was 205 on secure connection

Accepted connection on port 4445
TCP sent: 71527COMP416
delay was 5 on unsecure connection

Accepted connection on port 4445
TCP sent: 71527COMP416
delay was 7 on unsecure connection

Accepted connection on port 4445
TCP sent: 71527COMP416
delay was 4 on unsecure connection

Accepted connection on port 4445
TCP sent: 71527COMP416
delay was 18 on unsecure connection

Accepted connection on port 4445
TCP sent: 71527COMP416
delay was 17 on unsecure connection
```

Package Explorer
SSLServer.java
Outline
SSLServer
SERVER_KEYSTORE_FILE : String
SERVER_KEYSTORE_PASSWORD : String
SERVER_KEY_PASSWORD : String
sslServerSocket : SSLServerSocket
sslServerSocketFactory : SSLServerSocketFactory
Problems
Javadoc
Declaration
Console
Coverage
Call Hierarchy
PyDev

5)- client hello sends client's supported cryptographic algorithms and other parameters. Server hello is the response for client hello. A certificate is shared at this handshake.

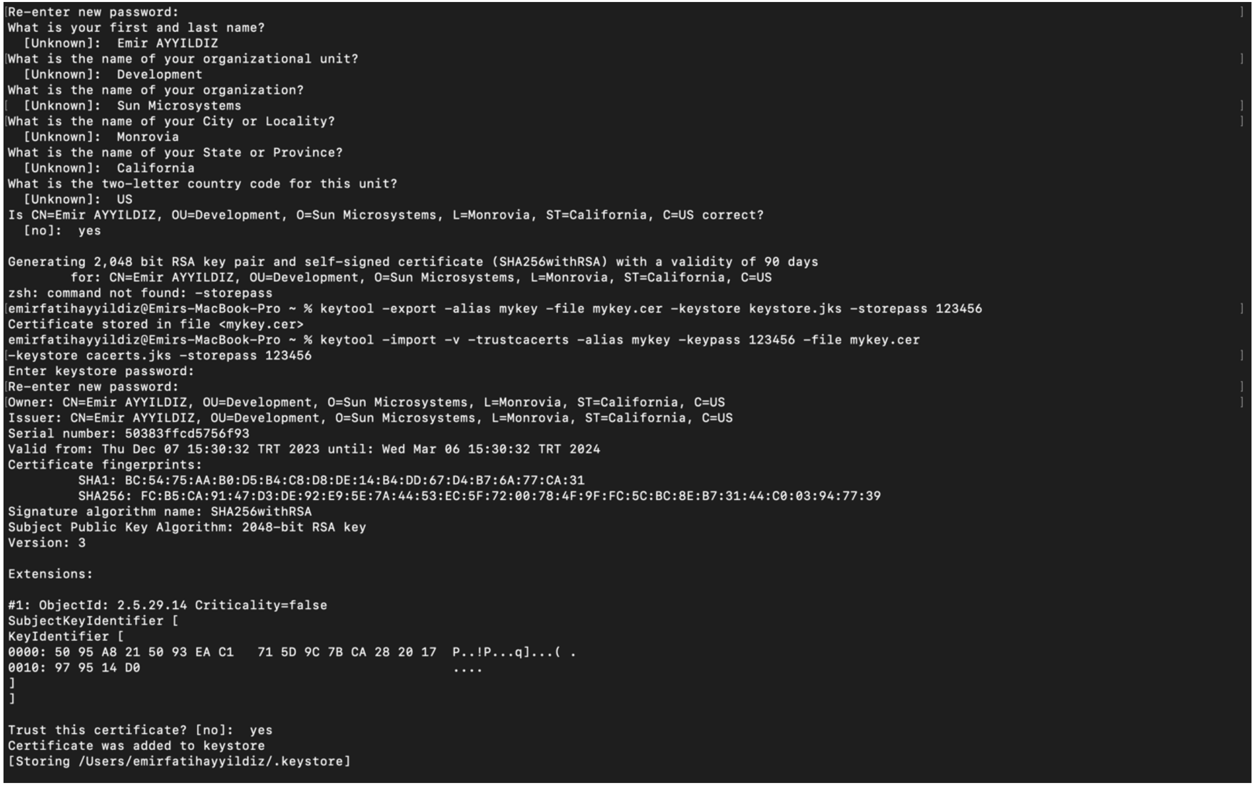
6)- when initial handshake occurs, the session id is saved on both sides. When the connection happens again, server looks for its cache to find the session id. If it finds the session id, the connection resumes. Therefore, they don’t have to handshake in every connection.



```
tls.handshake.extensions_session_ticket
No.  Time      Source     Destination  Protocol Length Info
  1 0.000000  127.0.0.1  127.0.0.1    TCP       68 50366 → 4444 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=4145491592 TSecr=0 SACK_PERM
  2 0.000085  127.0.0.1  127.0.0.1    TCP       68 4444 → 50366 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=2710492736 TSecr=4145491592 …
  3 0.000095  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=4145491592 TSecr=2710492736
  4 0.000104  127.0.0.1  127.0.0.1    TCP       56 [TCP Window Update] 4444 → 50366 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2710492736 TSecr=4145491592
  5 0.099933  127.0.0.1  127.0.0.1    TLSv1…   438 Client Hello
  6 0.099961  127.0.0.1  127.0.0.1    TCP       56 4444 → 50366 [ACK] Seq=1 Ack=383 Win=407872 Len=0 TSval=2710492836 TSecr=4145491692
  7 0.156376  127.0.0.1  127.0.0.1    TLSv1…   216 Server Hello
  8 0.156399  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=383 Ack=161 Win=408128 Len=0 TSval=4145491748 TSecr=2710492892
  9 0.185463  127.0.0.1  127.0.0.1    TLSv1…    62 Change Cipher Spec
 10 0.185492  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=383 Ack=167 Win=408128 Len=0 TSval=4145491778 TSecr=2710492922
 11 0.186019  127.0.0.1  127.0.0.1    TLSv1…    62 Change Cipher Spec
 12 0.186043  127.0.0.1  127.0.0.1    TCP       56 4444 → 50366 [ACK] Seq=167 Ack=389 Win=407872 Len=0 TSval=2710492922 TSecr=4145491778
 13 0.213632  127.0.0.1  127.0.0.1    TLSv1…   122 Application Data
 14 0.213687  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=389 Ack=233 Win=408064 Len=0 TSval=4145491806 TSecr=2710492950
 15 0.216864  127.0.0.1  127.0.0.1    TLSv1…   980 Application Data
 16 0.216889  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=389 Ack=1157 Win=407104 Len=0 TSval=4145491809 TSecr=2710492953
 17 0.244210  127.0.0.1  127.0.0.1    TLSv1…   358 Application Data
 18 0.244241  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=389 Ack=1459 Win=406784 Len=0 TSval=4145491836 TSecr=2710492980
 19 0.247059  127.0.0.1  127.0.0.1    TLSv1…   146 Application Data
 20 0.247090  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=389 Ack=1549 Win=406720 Len=0 TSval=4145491839 TSecr=2710492983
 21 0.256181  127.0.0.1  127.0.0.1    TLSv1…   146 Application Data
 22 0.256208  127.0.0.1  127.0.0.1    TCP       56 4444 → 50366 [ACK] Seq=1549 Ack=479 Win=407808 Len=0 TSval=2710492992 TSecr=4145491848
 23 0.258655  127.0.0.1  127.0.0.1    TLSv1…   107 Application Data
 24 0.258684  127.0.0.1  127.0.0.1    TCP       56 4444 → 50366 [ACK] Seq=1549 Ack=530 Win=407744 Len=0 TSval=2710492995 TSecr=4145491851
 25 0.260817  127.0.0.1  127.0.0.1    TLSv1…   144 Application Data
 26 0.260851  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=530 Ack=1637 Win=406656 Len=0 TSval=4145491853 TSecr=2710492997
 27 0.262159  127.0.0.1  127.0.0.1    TLSv1…   105 Application Data
 28 0.262187  127.0.0.1  127.0.0.1    TCP       56 50366 → 4444 [ACK] Seq=530 Ack=1686 Win=406592 Len=0 TSval=4145491854 TSecr=2710492998
 29 0.264229  127.0.0.1  127.0.0.1    TLSv1…    96 Application Data

    Version: TLS 1.2 (0x0303)
    Length: 155
  ⌄ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 151
      Version: TLS 1.2 (0x0303)
      Random: fcfc958f939abfa80f719168bbd47d3444e56b383accf27d69969f32fc302167
      Session ID Length: 32
      Session ID: 92402be5fb41fcc1481d8ae8465cb53c6543a330062f8982633f8bbec63fe2d9
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Compression Method: null (0)
      Extensions Length: 79
    › Extension: supported_versions (len=2) TLS 1.3
    › Extension: key_share (len=69) secp256r1

"tls.handshake.extensions_session_ticket" is not a valid protocol or protocol field.    Packets: 36 · Displayed: 36 (100.0%)    Profile: Default
```

Part 2.2

Passwords for keystore and trust store = 123456



```
Re-enter new password:
What is your first and last name?
  [Unknown]:  Emir AYYILDIZ
What is the name of your organizational unit?
  [Unknown]:  Development
What is the name of your organization?
  [Unknown]:  Sun Microsystems
What is the name of your City or Locality?
  [Unknown]:  Monrovia
What is the name of your State or Province?
  [Unknown]:  California
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=Emir AYYILDIZ, OU=Development, O=Sun Microsystems, L=Monrovia, ST=California, C=US correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 90 days
        for: CN=Emir AYYILDIZ, OU=Development, O=Sun Microsystems, L=Monrovia, ST=California, C=US
zsh: command not found: -storepass
emirfatihayyildiz@Emirs-MacBook-Pro ~ % keytool -export -alias mykey -file mykey.cer -keystore keystore.jks -storepass 123456
Certificate stored in file <mykey.cer>
emirfatihayyildiz@Emirs-MacBook-Pro ~ % keytool -import -v -trustcacerts -alias mykey -keypass 123456 -file mykey.cer
-keystore cacerts.jks -storepass 123456
Enter keystore password:
Re-enter new password:
Owner: CN=Emir AYYILDIZ, OU=Development, O=Sun Microsystems, L=Monrovia, ST=California, C=US
Issuer: CN=Emir AYYILDIZ, OU=Development, O=Sun Microsystems, L=Monrovia, ST=California, C=US
Serial number: 50383ffcd5756f93
Valid from: Thu Dec 07 15:30:32 TRT 2023 until: Wed Mar 06 15:30:32 TRT 2024
Certificate fingerprints:
         SHA1: BC:54:75:AA:B0:D5:B4:C8:D8:DE:14:B4:DD:67:D4:B7:6A:77:CA:31
         SHA256: FC:B5:CA:91:47:D3:DE:92:E9:5E:7A:44:53:EC:5F:72:00:78:4F:9F:FC:5C:BC:8E:B7:31:44:C0:03:94:77:39
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 50 95 A8 21 50 93 EA C1   71 5D 9C 7B CA 28 20 17  P..!P...q]...( .
0010: 97 95 14 D0                                        ....
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing /Users/emirfatihayyildiz/.keystore]
```