CS 315 : Computer Networks Lab
Assignment - 12
Wireshark Lab: 802.11 WiFi & TLS

Ayush Mallick
CS22BT008

Part-0

```
cs101@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.240.118.82  netmask 255.255.248.0  broadcast 10.240.119.255
        inet6 fe80::4fe5:4e7c:b1be:5233  prefixlen 64  scopeid 0x20<link>
        ether 7c:57:58:c4:ff:fb  txqueuelen 1000  (Ethernet)
        RX packets 229883  bytes 185566001 (185.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 83843  bytes 13193787 (13.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x80900000-80920000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8770  bytes 1004581 (1.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8770  bytes 1004581 (1.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Part-1

1.1

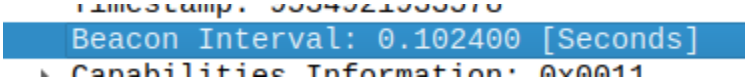
‘*30 Munroe St*’, ‘*linksys12*’

wlan.fc.type_subtype == 0x08

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li\001\004[Malformed Packet]
11	0.393174	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
13	0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID=linksys12
15	0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12
17	0.699847	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
18	0.802226	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID=linksys12
22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
23	1.113691	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=,nksys
24	1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
32	1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
33	1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
34	1.420565	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12
35	1.519009	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2870, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
36	1.621422	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2871, FN=0, Flags=........C, BI=100, SSID=30 Munroe St

1.2

For both access points, the value of the ‘beacon interval’ field is *100*, which is equivalent to *102.4* milliseconds, or *0.1024* seconds.



1.3

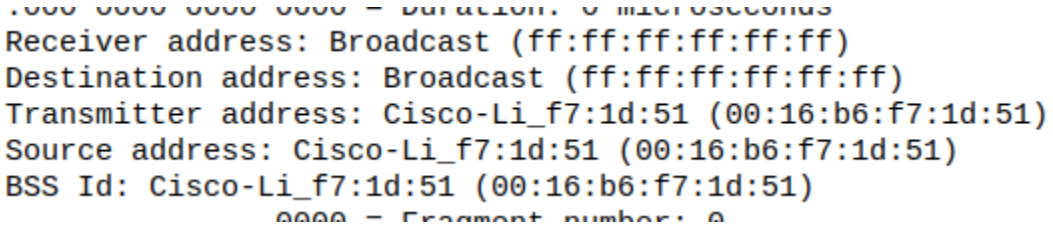
Source address : *00:16:b6:f7:1d:51*

1.4

Destination address : *ff:ff:ff:ff:ff:ff*

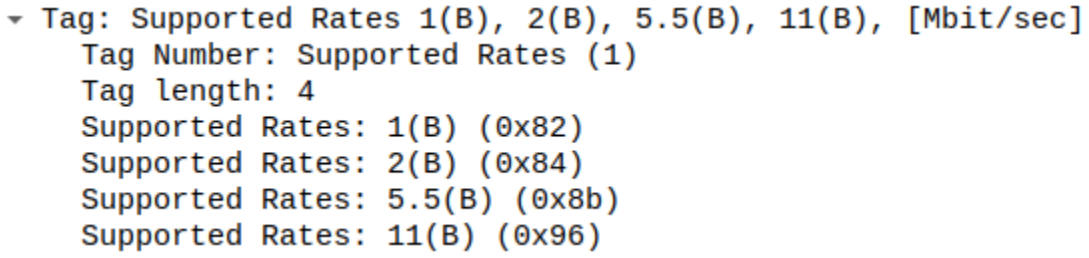
1.5

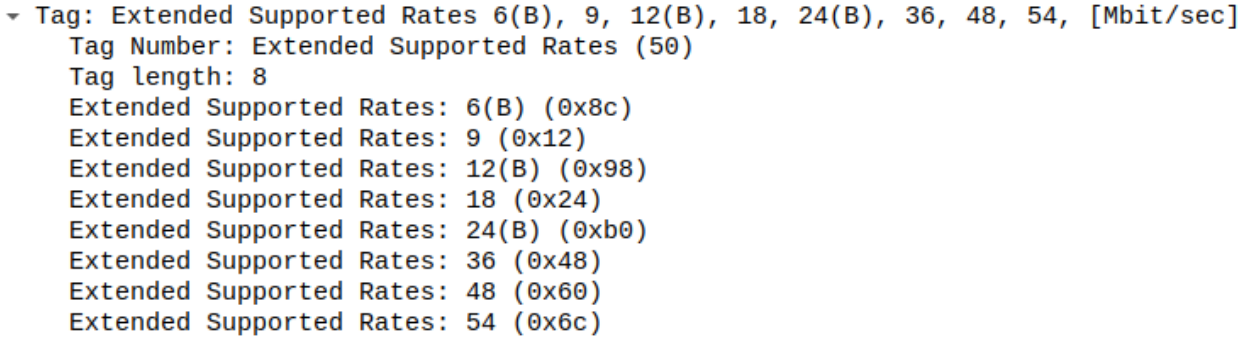
BSS ID : *00:16:b6:f7:1d:51*



1.6

Supported rates : *1 Mbps*, *2 Mbps*, *5.5 Mbps*, *11 Mbps*
Extended supported rates : *6 Mbps*, *9 Mbps*, *12 Mbps*, *18 Mbps*, *24 Mbps*, *36 Mbps*, *48 Mbps*, *54 Mbps*





Part-2

2.1

Receiver address : *00:16:b6:f7:1d:51*
Transmitter address : *00:13:02:d1:b6:4f*
Destination address : *00:16:b6:f4:eb:a8*

```
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
               0000 = Fragment number: 0
```

The transmitter address, *00:13:02:d1:b6:4f*, corresponds to the wireless host.
The receiver address, *00:16:b6:f7:1d:51*, corresponds to the access point.
The destination address, *00:16:b6:f4:eb:a8*, corresponds to the first-hop router.

Source address : *192.168.1.109*
Destination address : *128.119.245.12*

```
[Header checksum status: Unverified]
Source Address: 192.168.1.109
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port
```

2.2

Receiver address : *91:2a:b0:49:b6:4f*
Transmitter address : *00:16:b6:f7:1d:51*
Source address : *00:16:b6:f4:eb:a8*

```
Duration/ID: 11500 (reserved)
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
               0000 = Fragment number: 0
```

The source address, *00:16:b6:f4:eb:a8*, corresponds to the host server.
The receiver address, *91:2a:b0:49:b6:4f*, corresponds to the destination.
The transmitter address, *00:16:b6:f7:1d:51*, corresponds to the access point.

Source address : *128.119.245.12*

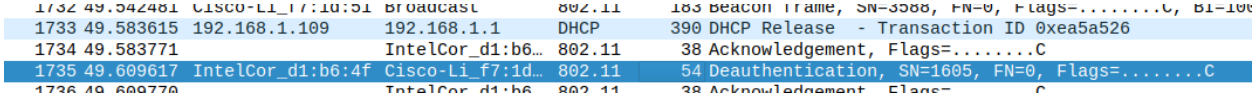
```
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.1.109
```

Part-3

3.1

Frame number *1733*, *DHCP Release message* (IP-layer)
Frame number *1735*, *Deauthentication* (802.11-layer)

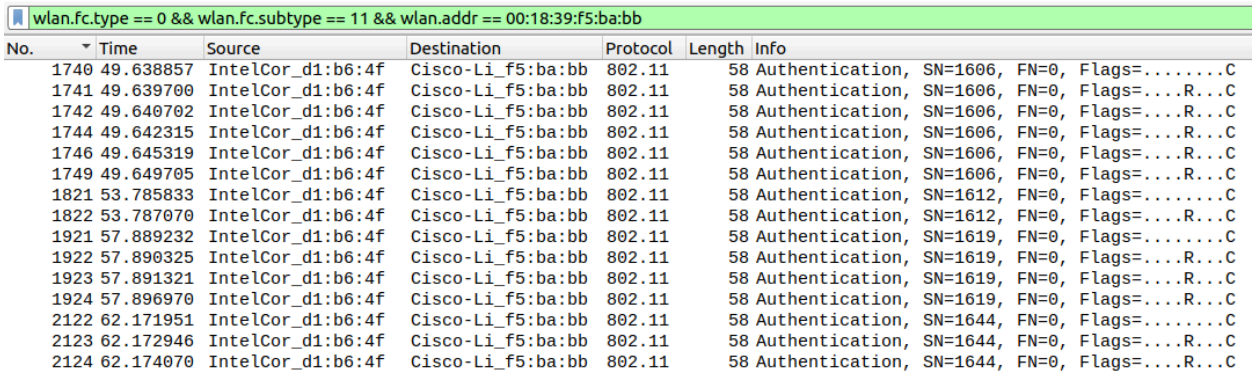
Expected but missing : *Disassociation* frame



1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6…	802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d…	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770		IntelCor_d1:b6	802.11	38	Acknowledgement, Flags= C

3.2

15 Authentication frames

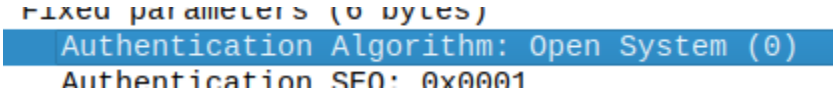


wlan.fc.type == 0 && wlan.fc.subtype == 11 && wlan.addr == 00:18:39:f5:ba:bb

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C

3.3

Open authentication



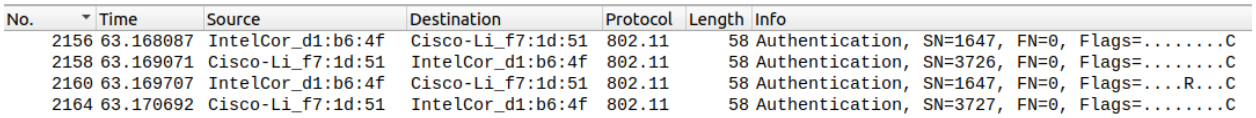
Fixed parameters (6 bytes)
Authentication Algorithm: Open System (0)
Authentication SEQ: 0x0001

3.4

No

3.5

Authentication frames were sent from the host to 30 Munroe St. access point, at frames *2156* (*63.168087*) and *2160* (*63.169707*), whose replies were sent at frames *2158* (*63.169071*) and *2164* (*63.170692*) respectively.



No.	Time	Source	Destination	Protocol	Length	Info
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

3.6

Association request was sent at frame number *2162* (*63.169910*), and association response was received at frame number *2166* (*63.192101*)

No.	Time	Source	Destination	Protocol	Length	Info
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=........C

3.7

Supported rates : *1 Mbps*, *2 Mbps*, *5.5 Mbps*, *11 Mbps*, *6 Mbps*, *9 Mbps*, *12 Mbps*, *18 Mbps*

Extended supported rates : *24 Mbps*, *36 Mbps*, *48 Mbps*, *54 Mbps*

```
▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
    Supported Rates: 6(B) (0x8c)
    Supported Rates: 9 (0x12)
    Supported Rates: 12(B) (0x98)
    Supported Rates: 18 (0x24)
  ▾ Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 24(B) (0xb0)
      Extended Supported Rates: 36 (0x48)
      Extended Supported Rates: 48 (0x60)
      Extended Supported Rates: 54 (0x6c)
```

Part-4

4.1

Probe Request

Source address : *00:12:f0:1f:57:13*
Receiver address : *ff:ff:ff:ff:ff:ff*
BSS id : *ff:ff:ff:ff:ff:ff*

```
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
               0000 = Fragment number: 0
```

Probe Response

Source address : *00:16:b6:f7:1d:51*
Receiver address : *00:12:f0:1f:57:13*
BSS id : *00:16:b6:f7:1d:51*

```
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
               0000 = Fragment number: 0
```

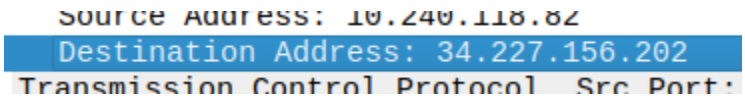
Probe requests are sent by a wireless client (host) actively scanning for available WiFi networks, to discover nearby access points.

Probe responses are sent by an access point (AP) in reply to a probe request. It contains information about the access point and lets the client know it's available to connect.

Part-5

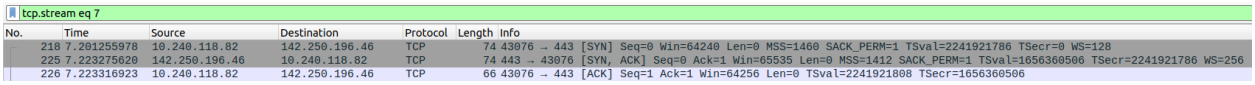
5.1

Domain IP address : *34.227.156.202*



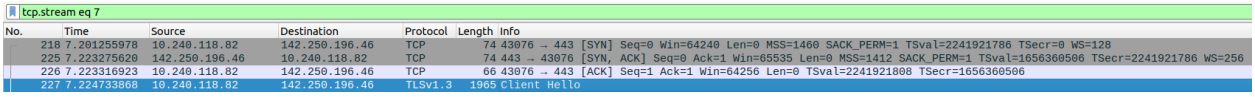
5.2

Yes, the three-way handshake is set up, as seen in frames *218*, *225*, *226*.



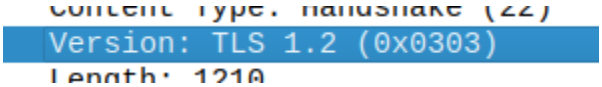
5.3

TCP connection is set up before the first TLS message is sent.



5.4

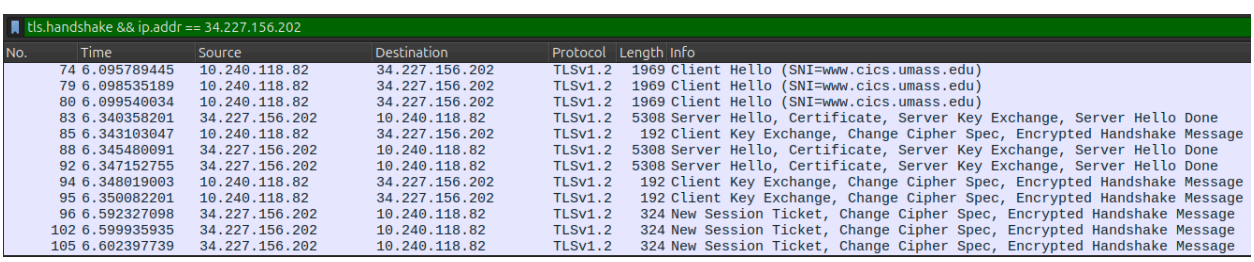
Version : *TLS 1.2*



5.5

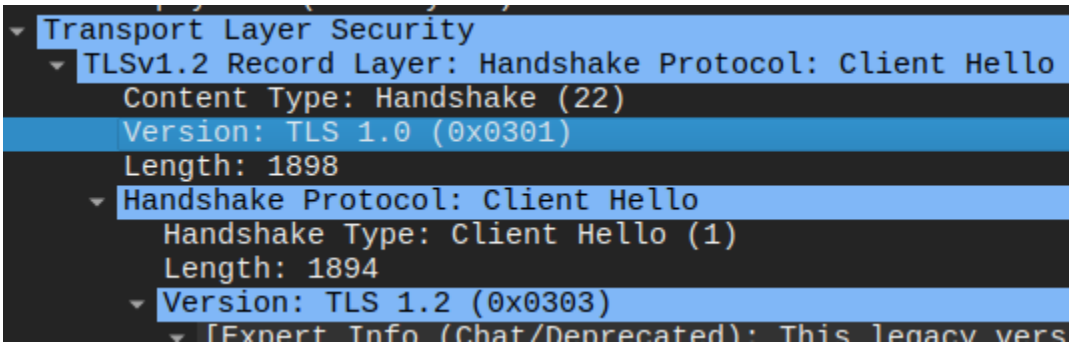
TLS messages between server and client :

Client Hello
Server Hello
Certificate
Server Key Exchange
Server Hello Done
Client Key Exchange
Change Cipher Spec
Encrypted Handshake Message
New Session Ticket



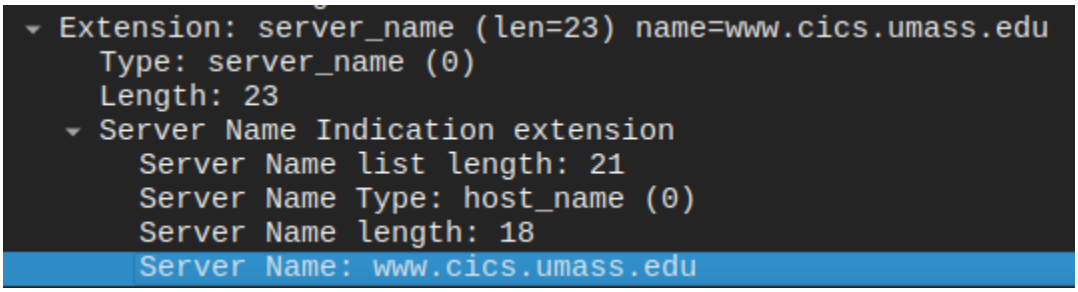
5.6

The two different versions of TLS mentioned are *TLS 1.0* and *TLS 1.2*. They differ because the main field indicates the minimum version supported, and the extension displays all supported versions.



5.7

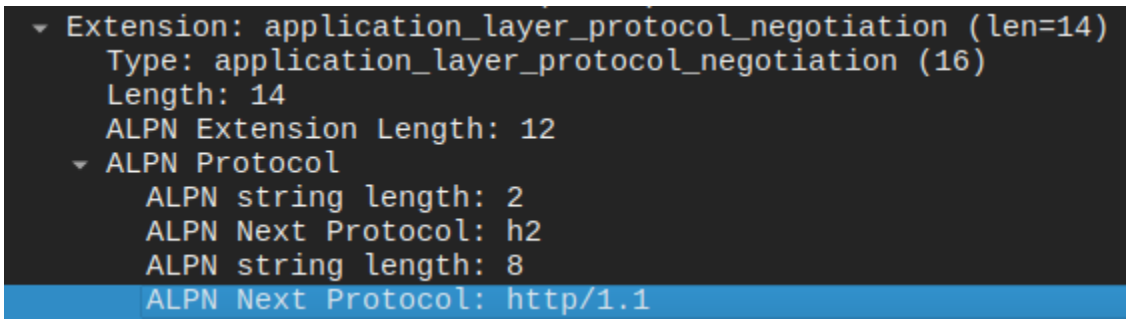
The name of the domain is mentioned under the *Extension: server_name* field.



This is not encrypted, because the server needs to know which domain to serve.

5.8

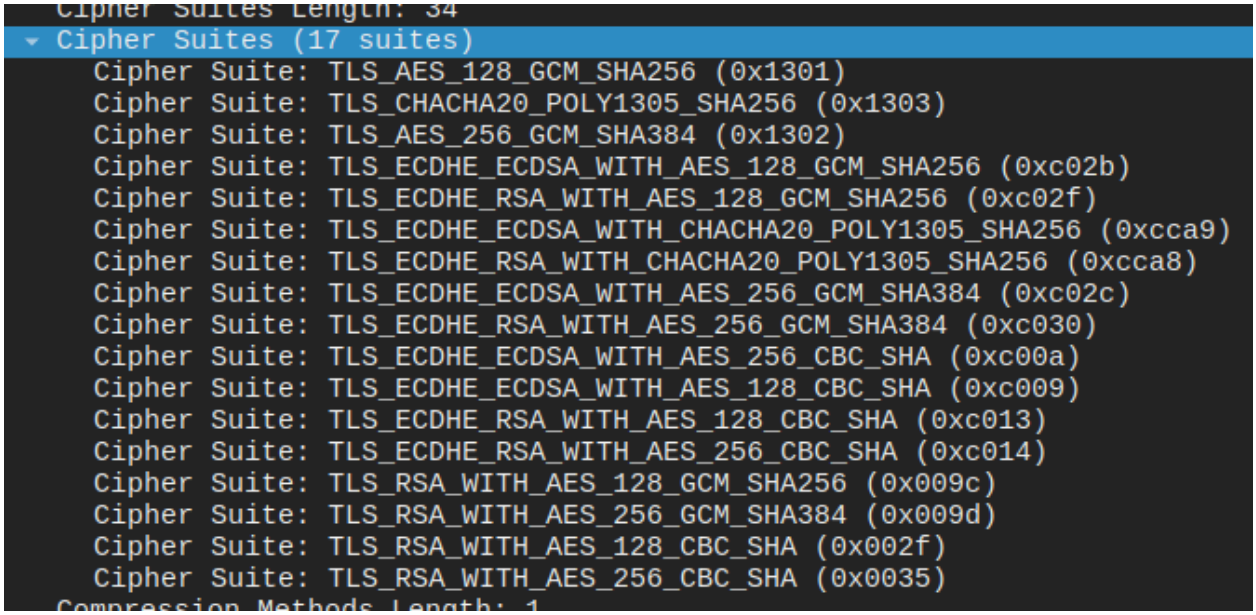
The HTTP version is indicated by the *ALPN Next Protocol* field under *Extension: application_layer_protocol_negotiation*, which is *http/1.1*.



5.9

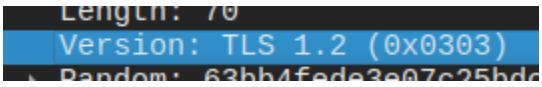
Cipher suited offered by client :

TLS_AES_128_GCM_SHA256 (0x1301)
TLS_CHACHA20_POLY1305_SHA256 (0x1303)
TLS_AES_256_GCM_SHA384 (0x1302)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)



5.10

Version : *TLS 1.2*

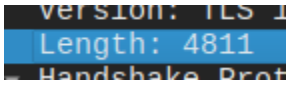


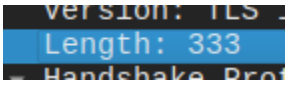
5.11

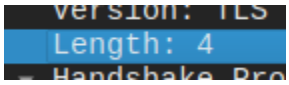
Cipher suite : *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)*

5.12

Size of Certificate message : *4811 bytes*
Size of Server Key Exchange message : *333 bytes*
Size of Server Hello Done message : *4 bytes*

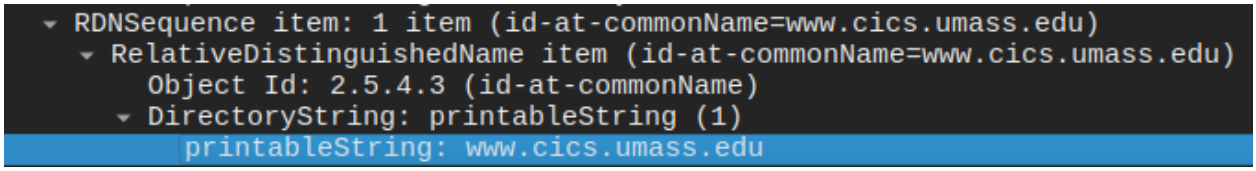






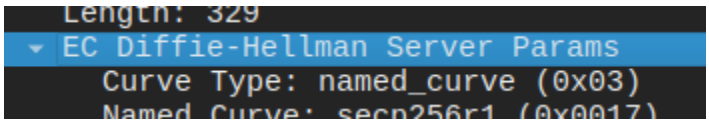
5.13

Certificate name : *www.cics.umass.edu*



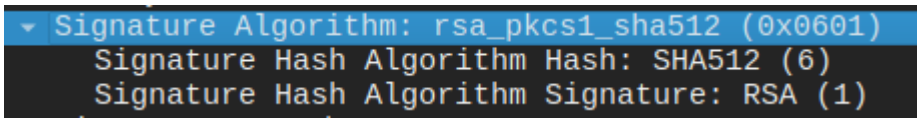
5.14

Handshake protocol : *EC Diffie-Hellman Server Params*



5.15

Signature algorithm : *rsa_pkcs1_sha512 (0x0601)*



5.16

Yes, the client agrees on the same handshake protocol.