

CS 315: Computer Networks Lab

Spring 2024-25, IIT Dharwad

Assignment-12

Wireshark Lab: 802.11 WiFi & TLS

April 7, 2025

Chidurala Tejaswini

(220010012 / CS22BT012)

Part 0: Paste a screenshot of your system IP address, using ipconfig (on Windows) or ifconfig (on Mac and Linux), and fill out [this Google form](#) to submit the details of your system. The same system must be used to attempt all exercises of this lab.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.240.118.97 netmask 255.255.248.0 broadcast 10.240.119.255
        inet6 fe80::1d6b:1bfb:2bd6:ef0d prefixlen 64 scopeid 0x20<link>
          ether e0:73:e7:0a:99:9a txqueuelen 1000 (Ethernet)
            RX packets 186173 bytes 143688016 (143.6 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 55113 bytes 7668580 (7.6 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 4723 bytes 521713 (521.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4723 bytes 521713 (521.7 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Introduction

In this lab, we'll investigate the 802.11 wireless network protocol. In all of the Wireshark labs thus far, we've captured frames on a wired Ethernet connection. Here, since 802.11 is a wireless link-layer protocol, we'll be capturing frames "in the air." Unfortunately, some device drivers for wireless 802.11 NICs still don't provide the hooks to capture/copy received 802.11 frames for use in Wireshark. Thus, in this lab, we'll provide a trace of captured 802.11 frames for you to analyze and assume in the questions below that you are using this trace.

Getting Started

Download the file `WiFi_Trace.pcap` from the [link](#). This trace was collected using AirPcap and Wireshark running on a computer in the home network of one of the authors, consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. The author is fortunate to have other access points in neighbouring houses available as well. In this trace file, we'll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we'll see a lot of frames that we're not interested in

for this lab, such as beacon frames advertised by a neighbour's AP also operating on channel 6. The recorded wireless host activities in the trace file are as follows:

- At the start of the trace, the host is already connected to the *30 Munroe St access point (AP)*.
- At t = 24.82, the host sends an HTTP request to <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>, with the destination IP address 128.119.245.12.
- At t = 32.82, the host makes another HTTP request to <http://www.cs.umass.edu>, which resolves to 128.119.240.19.
- At t = 49.58, the host disconnects from the *30 Munroe St AP* and attempts to connect to *linksys_ses_24086*, a secured access point. However, the connection attempt is unsuccessful.
- At t = 63.0, after failing to associate with *linksys_ses_24086*, the host reconnects to the *30 Munroe St AP*.

Part-1: Beacon Frames

Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you'll want to look at the details of the “IEEE 802.11” frame and subfields in the middle Wireshark window.

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1	Cisco-Li_f7:1d:51	Broadcast	0.000000	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	Cisco-Li_f7:1d:51	Broadcast	0.085474	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	Cisco-Li_f7:1d:51	Broadcast	0.187919	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	Cisco-Li_f7:1d:51	Broadcast	0.290284	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	LinksysG_67:22:94	Broadcast	0.294432	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=16:001@004@1M

> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
 > Radiotap Header v6, Length 24
 > 802.11 radio information
 > IEEE 802.11 Beacon frame, Flags:C
 > IEEE 802.11 Wireless Management
 > Fixed parameters (12 bytes)
 > Tagged parameters (119 bytes)
 - Tag: SSID parameter set: 30 Munroe St
 Tag Number: SSID parameter set (0)
 Tag length: 12
 SSID: 30 Munroe St

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
13	Cisco-Li_f7:1d:51	Broadcast	0.495032	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	LinksysG_67:22:94	Broadcast	0.499197	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=linksys12
15	Cisco-Li_f7:1d:51	Broadcast	0.597382	802.11	183	Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	LinksysG_67:22:94	Broadcast	0.601687	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
17	Cisco-Li_f7:1d:51	Broadcast	0.699847	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
 > Radiotap Header v6, Length 24
 > 802.11 radio information
 > IEEE 802.11 Beacon frame, Flags:C
 > IEEE 802.11 Wireless Management
 > Fixed parameters (12 bytes)
 > Tagged parameters (26 bytes)
 - Tag: SSID parameter set: linksys12
 Tag Number: SSID parameter set (0)
 Tag length: 9
 SSID: linksys12

The SSIDs of the two access points that are issuing most of the beacon frames in this trace are:

Access Point	SSID
Munroe ST	30 Munroe St
link_ses_24086	linksys12

2. What are the ‘beacon interval’ field values in the *linksys_ses_24086* access point and the *30 Munroe St.* access point?

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
13	Cisco-Li_f7:1d:51	Broadcast	0.495032	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	LinksysG_67:22:94	Broadcast	0.499197	802.11	90	Beacon frame, SN=3071, FN=0, Flags=.....C, BI=100, SSID=linksys12
15	Cisco-Li_f7:1d:51	Broadcast	0.597382	802.11	183	Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	LinksysG_67:22:94	Broadcast	0.601687	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
17	Cisco-Li_f7:1d:51	Broadcast	0.699647	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:

> IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

> Timestamp: 0x34921933578

> Beacon Interval: 0.162490 [Seconds]

> Capabilities Information: 0x0011

> Tagged parameters (26 bytes)

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1	Cisco-Li_f7:1d:51	Broadcast	0.000000	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	Cisco-Li_f7:1d:51	Broadcast	0.085474	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	Cisco-Li_f7:1d:51	Broadcast	0.187919	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	Cisco-Li_f7:1d:51	Broadcast	0.290284	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	LinksysG_67:22:94	Broadcast	0.294432	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=linksys12

> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:

> IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

> Timestamp: 174319001986

> Beacon Interval: 0.102400 [Seconds]

> Capabilities Information: 0x0601

> Tagged parameters (119 bytes)

The ‘beacon interval’ field values in the *linksys_ses_24086* access point and the *30 Munroe St.* access point are 0.102400 seconds.

3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St?*

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1	Cisco-Li_f7:1d:51	Broadcast	0.000000	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	Cisco-Li_f7:1d:51	Broadcast	0.085474	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	Cisco-Li_f7:1d:51	Broadcast	0.187919	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	Cisco-Li_f7:1d:51	Broadcast	0.290284	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	LinksysG_67:22:94	Broadcast	0.294432	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=linksys12

Source MAC address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St?*

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1	Cisco-Li_f7:1d:51	Broadcast	0.000000	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	Cisco-Li_f7:1d:51	Broadcast	0.085474	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	Cisco-Li_f7:1d:51	Broadcast	0.187919	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	Cisco-Li_f7:1d:51	Broadcast	0.290284	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	Linksvsg 67:22:94	Broadcast	0.294432	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=110\001\004(Malformed)

Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
 Radiotap Header v6, Length 24
 802.11 radio information
 IEEE 802.11 Beacon frame, Flags:C
 Type/Subtype: Beacon frame (0x0008)
 Frame Control Field: 0x0000
 .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: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
 Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

Destination MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
 → indicating a **broadcast** beacon frame

5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1	Cisco-Li_f7:1d:51	Broadcast	0.000000	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	Cisco-Li_f7:1d:51	Broadcast	0.085474	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	Cisco-Li_f7:1d:51	Broadcast	0.187919	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	Cisco-Li_f7:1d:51	Broadcast	0.290284	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	Linksvsg 67:22:94	Broadcast	0.294432	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=110\001\004(Malformed)

Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
 Radiotap Header v6, Length 24
 802.11 radio information
 IEEE 802.11 Beacon frame, Flags:C
 Type/Subtype: Beacon frame (0x0008)
 Frame Control Field: 0x0000
 .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: 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)
- **BSS ID** will often be the same as the Source MAC for APs.

6. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1	Cisco-Li_f7:1d:51	Broadcast	0.000000	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	Cisco-Li_f7:1d:51	Broadcast	0.085474	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	Cisco-Li_f7:1d:51	Broadcast	0.187919	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	Cisco-Li_f7:1d:51	Broadcast	0.290284	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	Linksvsg 67:22:94	Broadcast	0.294432	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=110\001\004(Malformed)

Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
 Radiotap Header v6, Length 24
 802.11 radio information
 IEEE 802.11 Beacon frame, Flags:C
 IEEE 802.11 Wireless Management
 Fixed parameters (12 bytes)
 Tagged parameters (119 bytes)
 Tag: SSID parameter set: 30 Munroe St
 - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 Tag Number: Supported Rates (1)
 Tag length: 4
 Supported Rates: 1(B) (0xB2)
 Supported Rates: 2(B) (0xB4)
 Supported Rates: 5.5(B) (0xB8)
 Supported Rates: 11(B) (0x96)

Supported Data rates are

- 1 (B), 2 (B), 5.5 (B), 11(B) [Mbits/sec]

The (B) indicates **basic rates** that must be supported by all devices in the network.

wlan.fc.type_subtype == 0x08						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1	Cisco-L1_f7:1d:51	Broadcast	0.000000	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	Cisco-L1_f7:1d:51	Broadcast	0.085474	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	Cisco-L1_f7:1d:51	Broadcast	0.187919	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	Cisco-L1_f7:1d:51	Broadcast	0.290284	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	LinksysG 67:22:94	Broadcast	0.294432	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=1\001\004&[Malformed]

Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
 Radiotap Header v0, Length 24
 802.11 radio information
 IEEE 802.11 Beacon frame, Flags:

- IEEE 802.11 Wireless Management
 - Fixed parameters (12 bytes)
 - Tagged parameters (119 bytes)
 - Tag: SSID Information: 30 Munroe St
 - Tag: Extended Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 - Tag: DS Parameter set: Current Channel: 6
 - Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
 - Tag: Country Information: Country Code US, Environment Indoor
 - Tag: EDCA Parameter Set
 - Tag: ERP Information
 - Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 Tag Number: Extended Supported Rates (50)
 Tag length: 8
 Extended Supported Rates: 6(B) (0x0c)
 Extended Supported Rates: 9 (0x12)
 Extended Supported Rates: 12(B) (0x08)
 Extended Supported Rates: 18 (0x24)
 Extended Supported Rates: 24(B) (0xb0)
 Extended Supported Rates: 36 (0x48)
 Extended Supported Rates: 48 (0x60)
 Extended Supported Rates: 54 (0x6c)

Extended Supported Rates are

- 6 (B) , 9, 12(B), 18, 24(B), 36, 48, 54 [Mbit/sec]

Part-2: Data Transfer

Since the trace starts with the host already associated with the AP, let's first look at data transfer over an 802.11 association before looking at AP association/disassociation. Recall that in this trace, at $t = 24.82$, the host makes an HTTP request to <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>. The IP address of gaia.cs.umass.edu is 128.119.245.12. Then, at $t=32.82$, the host makes an HTTP request to <http://www.cs.umass.edu>.

1. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads `alice.txt`). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address?

tcp.flags.syn == 1 && ip.dst == 128.119.245.12						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
474	192.168.1.109	128.119.245.12	24.811093	TCP	110	2538 .. 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
 Radiotap Header v0, Length 24
 802.11 radio information
 IEEE 802.11 QoS Data, Flags:

Type/Subtype: QoS Data (0x0028)
 Frame Control Field: 0x8001
 .000 0000 0010 1100 = Duration: 44 microseconds
 Receiver address: Cisco-L1_f7:1d:51 (00:16:b6:f7:1d:51)
 Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
 Destination address: Cisco-L1_f4:eb:a8 (00:16:b6:f4:eb:a8)
 Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
 BSS Id: Cisco-L1_f7:1d:51 (00:16:b6:f7:1d:51)
 STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

Frame containing the SYN TCP segment for this first TCP session (that downloads `alice.txt`):

- Frame Number: 474

Three MAC Address Fields in the 802.11 Frame:

1. Receiver Address (Access Point): `00:16:b6:f7:1d:51`

2. Transmitter Address (Wireless Host): **00:13:02:d1:b6:4f**
3. Destination Address (First-Hop Router): **00:16:b6:f4:eb:a8**
4. (Also shown: Source Address = same as Transmitter)

The MAC address corresponding to:

- **Wireless Host MAC:** **00:13:02:d1:b6:4f** (Transmitter)
- **Access Point MAC:** **00:16:b6:f7:1d:51** (Receiver)
- **First-Hop Router MAC:** **00:16:b6:f4:eb:a8** (Destination)

IP Address Information:

- **Source IP (Wireless Host):** **192.168.1.109**
- **Destination IP (Server):** **128.119.245.12**
- 2. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which of these are the MAC addresses corresponding to the host sending SYNACK, destination and BSS? What is the IP address of the server sending the TCP SYNACK?

tcp.flags.syn == 1 && tcp.flags.ack == 1 && ip.src == 128.119.245.12						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
476	128.119.245.12	192.168.1.109	24.827751	TCP	110	80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)						
Radiotap Header v0, Length 24						
802.11 radio information						
- IEEE 802.11 QoS Data, Flags: .mP..F.C						
Type/Subtype: QoS Data (0x0028)						
Frame Control Field: 0x8832						
Duration/ID: 11560 (reserved)						
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)						
Transmitter address: Cisco-L1_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-L1_f4:eb:a8 (00:16:b6:f4:eb:a8)						
BSS ID: Cisco-L1_f7:1d:51 (00:16:b6:f7:1d:51)						
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)						

Frame containing the SYNACK TCP segment:

Frame Number containing the SYNACK segment for this TCP session: 476

The three MAC address fields in the 802.11 frame are:

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

The MAC address corresponding to:

- **Host sending SYNACK (Server-side MAC):** **00:16:b6:f4:eb:a8** (Source Address)
- **Destination (Wireless host/client MAC):** **91:2a:b0:49:b6:4f** (Receiver Address)
- **BSS (Basic Service Set) / (Access Point MAC):** **00:16:b6:f7:1d:51** (Transmitter Address)

IP address of the server sending the TCP SYNACK:

- **Source IP Address: 128.119.245.12**

Part-3: Association/Disassociation

In the text, a host must first *associate* with an access point before sending data. Association in 802.11 is performed using the ASSOCIATE REQUEST frame (sent from the host to AP, with a frame type 0 and subtype 0) and the ASSOCIATE RESPONSE frame (sent by the AP to a host with a frame type 0 and subtype of 1, in response to a received ASSOCIATE REQUEST).

1. **What two actions are taken (i.e., frames are sent) by the host in the trace just after $t=49$, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?**

frame.time_relative>49						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1733	192.168.1.109	192.168.1.1	49.583615	DHCP	390 /	DHCP Release - Transaction ID 0xea5a526
1734	IntelCor_d1:b6:...	IntelCor_d1:b6:...	49.583771	802.11	38	Acknowledgement, Flags=.....C
1735	IntelCor_d1:b6:...	Cisco-Li_f7:1d:...	49.609617	802.11	54	Deauthentication, SN=1685, FN=0, Flags=.....C
1736	IntelCor_d1:b6:...	IntelCor_d1:b6:...	49.609770	802.11	38	Acknowledgement, Flags=.....C
1737	IntelCor_d1:b6:...	Broadcast	49.614478	802.11	99	Probe Request, SN=1666, FN=0, Flags=.....C, SSID=linksy_SE
1738	Cisco-Li_f5:ba:...	Cisco-Li_f5:ba:...	49.615869	802.11	38	Acknowledgement, Flags=.....C
1739	Cisco-Li_f5:ba:...	Cisco-Li_f5:ba:...	49.617713	802.11	38	Acknowledgement, Flags=.....C

Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Radiotap Header v0, Length 24
802.11 radio information
- IEEE 802.11 Deauthentication, Flags:C
 Type/Subtype: Deauthentication (0x000c)
 Frame Control Field: 0xc000
 .000 0000 0010 1100 = Duration: 44 microseconds
 Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
 Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
 Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
 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)
 0000 = Fragment number: 0
 0110 0100 0101 = Sequence number: 1605
 Frame check sequence: 0x3b4a8b9c [unverified]
 [FCS Status: Unverified]

After $t = 49$, the following actions are taken to end the association with the 30 Munroe St:

- At $t = 49.583615$, DHCP Release is done. The host is releasing its IP address back to the DHCP server, and is exiting the network.
- At $t = 49.609617$, Deauthentication is done, to terminate a Wi-Fi connection.

One would expect a DISASSOCIATION request, but that is not observed here.

2. **Examine the trace file and look for AUTHENTICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the *linksy_ses_24086* AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around $t=49$?**

frame.time_relative>49 and wlan.fc.type == 0 && wlan.fc.subtype == 11 && wlan.da == 00:18:39:f5:ba:bb						
Time	No.	Source	Destination	Protocol	Length	Info
49.638857	1740	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
49.639700	1741	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
49.640702	1742	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
49.642315	1744	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
49.645319	1746	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
49.649705	1749	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
53.785833	1821	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
53.787070	1822	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
57.889232	1921	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
57.890325	1922	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
57.891321	1923	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
57.896970	1924	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
62.171951	2122	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
62.172946	2123	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
62.174070	2124	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C

A total of 15 AUTHENTICATION messages are sent from the wireless host to the *linksys_ses_24086* AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49.

3. Does the host want the authentication to require a key or be open?

frame.time_relative>49 and frame.time_relative<50 and wlan.fc.type == 0 && wlan.fc.subtype == 11 && wlan.sa == 00:18:39:f5:ba:bb						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
1740	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	49.638857	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	49.639700	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	49.640702	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	49.642315	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	49.645319	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	49.649705	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C

> Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Authentication, Flags:
> IEEE 802.11 Wireless Management
- Fixed parameters (6 bytes)
Authentication Algorithm: Open System (0)

- Based on the **Authentication Algorithm** field in the AUTHENTICATION frames,
- The value is **0**, which corresponds to **Open System authentication** (i.e., **no shared key required**).
- So, the **host wants the authentication to be Open**.

4. Do you see a reply AUTHENTICATION from the *linksys_ses_24086* AP in the trace?

frame.time_relative>49 and frame.time_relative<50 and wlan.fc.type == 0 && wlan.fc.subtype == 11 && wlan.sa == 00:18:39:f5:ba:bb						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info

A reply AUTHENTICATION means the access point is acknowledging the host's request to authenticate. In this trace, no authentication reply is observed from the AP (**00:18:39:f5:ba:bb**), indicating the authentication attempt failed and the host did not successfully connect to this AP.

5. Now let's consider what happens as the host gives up trying to associate with the *linksys_ses_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENTICATION frames sent from the host to an AP and vice versa. At what times is there an AUTHENTICATION frame from the host to *30 Munroe St.* AP, and when is there a reply AUTHENTICATION sent from that AP to the host reply? (Note that you can use the filter expression “`wlan.fc.subtype == 11 && wlan.fc.type == 0 && wlan.addr == 00:13:02:d1:b6:4f`” to display only the AUTHENTICATION frames in this trace for this wireless host.)

wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == 00:16:b6:f7:1d:51						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
2156	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	63.168087	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	63.169071	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	63.169707	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R...C
2164	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	63.170692	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

- At times 63.168087 seconds and 63.169707 seconds , there is an AUTHENTICATION frame from the host to the AP.
- At times 63.169071 seconds and 63.170692 seconds , there is an AUTHENTICATION reply

6. An ASSOCIATE REQUEST from the host to AP and a corresponding ASSOCIATE RESPONSE frame from AP to the host is used for the host to be associated with an AP. At what time is there an ASSOCIATE REQUEST from the host to *30 Munroe St* AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression “`wlan.fc.subtype < 2 && wlan.fc.type == 0 && wlan.addr == 00:13:02:d1:b6:4f`” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

wlan.fc.subtype < 2 && wlan.fc.type == 0 && wlan.addr == 00:16:b6:f7:1d:51						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
2162	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	63.169910	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	63.192101	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

- An ASSOCIATION REQUEST (i.e., the ASSOCIATE REQUEST) is sent from host to the *30 Munroe St* AP at time t = 63.169910 seconds.
- An ASSOCIATION RESPONSE (i.e., the ASSOCIATE REPLY) is sent from that AP to the host at time t = 63.192101 seconds.

7. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameter fields of the 802.11 wireless LAN management frame.

To determine what transmission rates the host and the access point (AP) are willing to use, we examine the **Supported Rates** and **Extended Supported Rates** fields in **802.11 management frames** (typically in **Probe Request/Response** or **Association Request/Response** frames).

Host's Supported Rates

wlan.fc.subtype < 2 && wlan.fc.type == 0 && wlan.addr == 00:16:b6:f7:1d:51

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

> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
> Radiotap Header V0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Request, Flags:C
> IEEE 802.11 Wireless Management
> Fixed parameters (4 bytes)
> Tagged parameters (33 bytes)
> Tag: SSID parameter set: 30 Munroe St
> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
> Tag: QoS Capability
> Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]

Rates advertised in request

From the 802.11 frame (e.g., Probe Request or Association Request):

- **Supported Rates:**
1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, Mbps
- **Extended Supported Rates:**
24(B), 36, 48, 54 Mbps

The (B) indicates **basic rates** that must be supported by all devices in the network.

wlan.fc.subtype < 2 && wlan.fc.type == 0 && wlan.addr == 00:16:b6:f7:1d:51

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

> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Radiotap Header V0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Response, Flags:C
> IEEE 802.11 Wireless Management
> Fixed parameters (6 bytes)
> Tagged parameters (36 bytes)
> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
> Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
> Tag: EDCA Parameter Set

Rates advertised in response

Access Point's (AP's) Supported Rates

From the AP's Probe Response or Association Response:

- **Supported Rates:**
1(B), 2(B), 5.5(B), 11(B), Mbps
- **Extended Supported Rates:**
6(B), 9, 12(B), 18, 24(B), 36, 48, 54 Mbps

Note: The AP also supports the same total set of rates but distributes them slightly differently between **Supported** and **Extended Supported Rates** fields.

Part-4: Other Frame types

Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.

1. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

wlan.fc.type_subtype == 0x04						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
50	IntelCor_1f:57:13	Broadcast	2.297613	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
87	IntelCor_1f:57:13	Broadcast	4.298449	802.11	78	Probe Request, SN=598, FN=0, Flags=.....C, SSID=phoiphas
117	IntelCor_1f:57:13	Broadcast	6.299705	802.11	79	Probe Request, SN=620, FN=0, Flags=.....C, SSID=concourse
118	IntelCor_1f:57:13	Broadcast	6.300439	802.11	70	Probe Request, SN=621, FN=0, Flags=.....C, SSID=wildcard (Broadcast)

> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
 > Radiotap Header w0, Length 24
 > 802.11 radio information
 - IEEE 802.11 Probe Request, Flags:

Type/Subtype: Probe Request (0x0004)
 > Frame Control Field: 0x4000
 .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)

First PROBE REQUEST Frame (at t = 2.297613):

- Source / Sender MAC address:** **00:12:f0:1f:57:13** (wireless host)
- Receiver MAC address:** **ff:ff:ff:ff:ff:ff** (broadcast address)
- BSS ID MAC address:** **ff:ff:ff:ff:ff:ff** (broadcast address)

wlan.fc.type_subtype == 0x05						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
27	Cisco-Li_f7:1d:51	Intelcor_d1:b6:4f	1.212185	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
51	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	2.300697	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	2.302191	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
53	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	2.304063	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St

> Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
 > Radiotap Header w0, Length 24
 > 802.11 radio information
 - IEEE 802.11 Probe Response, Flags:

Type/Subtype: Probe Response (0x0005)
 > Frame Control Field: 0x5000
 .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)

Corresponding PROBE RESPONSE Frame (at t = 2.300697):

- Source / Sender MAC address:** **00:16:b6:f7:1d:51** (Access Point)
- Receiver MAC address:** **00:12:f0:1f:57:13** (wireless host)
- BSS ID MAC address:** **00:16:b6:f7:1d:51** (same as AP MAC address)

Purpose of Probe Request & Response Frames

- Probe Request (Type/Subtype: 0x04)**
 - Purpose:** Sent by a client (station) to discover nearby Wi-Fi networks.
 - Use Case:** Especially useful when the SSID is hidden or when actively scanning.
- Probe Response (Type/Subtype: 0x05)**
 - Purpose:** Sent by an Access Point (AP) in reply to a Probe Request.
 - Includes:** SSID, supported data rates, capabilities, etc.

TLS

Introduction

In this lab, we'll investigate Transport Layer Security (known as TLS) and aspects of the authentication, data integrity, and confidentiality services provided by TLS. TLS is the successor to the now-deprecated Secure Sockets Layer (SSL).

We'll investigate TLS by analyzing a Wireshark packet trace captured during the retrieval of a web page via HTTPS - a secure version of HTTP, which implements TLS on top of HTTP. We'll look at TLS's client-server handshaking protocol in some detail since that's where most of the interesting action happens. You may use online resources for learning more about TLS [here](#), [here](#), and [here](#); and, of course, in [RFC 5246](#).

Capturing packets in a TLS session

The first step in this lab is to capture the packets in a TLS session. To do this, you should start Wireshark and begin packet capture, retrieve the homepage from <https://www.cics.umass.edu> using the browser of your choice, and then stop Wireshark packet capture. The ‘s’ after ‘http’ will cause the **Hypertext Transfer Protocol Secure (HTTPS)** – an extension of HTTP – to be used to securely retrieve the homepage from www.cics.umass.edu. Here, “securely” means that the www.cics.umass.edu server will be authenticated by your web browser, that the transmission of your client HTTP GET request and the server’s reply will be encrypted, and the integrity of all message content will be cryptographically verified. Of course, the authentication, integrity and encryption of a computer science department’s web page may not be as critical as that for Internet commerce and banking sites, but the same TLS protocol and TLS messages are used in all cases.

Part-5: A first look at the captured trace

Let's first set Wireshark's display so that only the packets to and from www.cics.umass.edu, are displayed.

It's important to keep in mind that an Ethernet frame (containing an IP datagram containing a TCP segment) may contain one or more TLS records. (This is very different from HTTP, for which each frame contains either one complete HTTP message or a portion of an HTTP message.) Also, a TLS record may not completely fit into an Ethernet frame, in which case multiple frames will be needed to carry the record.

We've said earlier that HTTPS implements TLS running “over” TCP. That means that a TCP connection must first be established between your browser and the web server for www.cics.umass.edu before TLS and HTTP messages can be exchanged, just as we saw with the vanilla (non-TLS) HTTP protocol.

Answer the following questions:

1. What is the IP address of the domain www.cics.umass.edu?

IP Address of the domain www.cics.umass.edu is

http.host == "www.cics.umass.edu" tls.handshake.extensions_server_name == "www.cics.umass.edu"						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
2565	10.240.118.97	34.227.156.202	9.048973013	TLSV1...	1969	Client Hello
2568	10.240.118.97	34.227.156.202	9.050069502	TLSV1...	1969	Client Hello
2571	10.240.118.97	34.227.156.202	9.064200403	TLSV1...	1969	Client Hello

Destination IP: 34.227.156.202

This is the IP address your system resolves for www.cics.umass.edu in the trace.

2. Does your system set up a TCP connection with the server of www.cics.umass.edu? Provide the packet numbers of the three-way handshake, with the corresponding screenshot.

ip.addr == 34.227.156.202 && tcp						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
2555	10.240.118.97	34.227.156.202	8.893195684	TCP	74	45922 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=3405793
2556	10.240.118.97	34.227.156.202	8.893305903	TCP	74	45938 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=3405793
2557	10.240.118.97	34.227.156.202	8.893367646	TCP	74	45950 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=3405793
2563	34.227.156.202	10.240.118.97	9.047535048	TCP	74	443 -> 45922 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TS
2564	10.240.118.97	34.227.156.202	9.047588911	TCP	66	45922 -> 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=3405793272 TSecr=99347
2565	10.240.118.97	34.227.156.202	9.048973013	TLSV1...	1969	Client Hello

Three-Way Handshake Packet Numbers (from the screenshot):

TCP Stream (Client Port: 45922)

1. **Packet 2555:** 45922 → 443 [SYN]
Client initiates the connection to the server.
2. **Packet 2563:** 443 → 45922 [SYN, ACK]
Server responds with SYN-ACK.
3. **Packet 2564:** 45922 → 443 [ACK]
Client sends ACK to complete the handshake.

The screenshot clearly shows:

- All three packets (2555, 2563, 2564) in sequence.
- TLS Client Hello follows right after, in **Packet 2565**.

Summary:

- Yes, the TCP connection is successfully established.
 - Three-way handshake packets: 2555 (SYN), 2563 (SYN-ACK), 2564 (ACK).
3. Is the TCP connection set up before or after the first TLS message is sent from the client to the server?

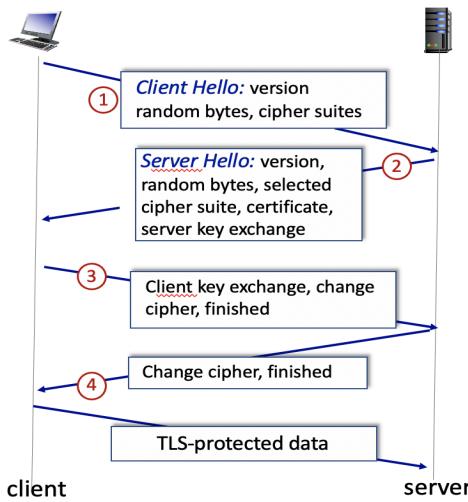


Figure 2: TLS handshake

- Yes — TLS runs over TCP.
- The **TCP connection is set up before** the first TLS message (Client Hello) is sent from the client to the server.
- As shown in **Figure 2: TLS handshake**, the TLS handshake begins **after** the three-way TCP handshake is completed. This ensures a reliable transport layer connection is in place before exchanging any TLS-specific messages

4. What TLS version is used by the www.cics.umass.edu server?

No.	Source	Destination	Time	Protocol	Length	User Datagram Info
2576	34.227.156.202	10.240.118.97	9.295499219	TLSV1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2581	34.227.156.202	10.240.118.97	9.298311900	TLSV1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2587	34.227.156.202	10.240.118.97	9.326014025	TLSV1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done

Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 74
 - Handshake Protocol: Server Hello
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 - TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

Version: TLS 1.2

Thus, the TLS version used by www.cics.umass.edu is TLS 1.2.

5. List the various TLS messages between the client and the server?

tls.handshake.type && ip.addr==34.227.156.202						
No.	Source	Destination	Time	Protocol	Length	User Datagram Info
2565	10.240.118.97	34.227.156.202	9.048973013	TLSv1.2	1969	Client Hello
2568	10.240.118.97	34.227.156.202	9.050069502	TLSv1.2	1969	Client Hello
2571	10.240.118.97	34.227.156.202	9.064200403	TLSv1.2	1969	Client Hello
2576	34.227.156.202	10.240.118.97	9.295499219	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2580	10.240.118.97	34.227.156.202	9.297943783	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2581	34.227.156.202	10.240.118.97	9.298311900	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2583	10.240.118.97	34.227.156.202	9.300114216	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2587	34.227.156.202	10.240.118.97	9.326014025	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2589	10.240.118.97	34.227.156.202	9.327971881	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2592	34.227.156.202	10.240.118.97	9.542846224	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2598	34.227.156.202	10.240.118.97	9.546159382	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2603	34.227.156.202	10.240.118.97	9.588116378	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

Based on the screenshot, the TLS handshake between the client (10.240.118.97) and the server (34.227.156.202) includes the following TLS messages: These packets represent the full TLS handshake exchange for setting up a secure connection using **TLS 1.2**.

The various TLS messages between the client and the server are

1. Client Hello:

- Sent by the client to initiate the TLS handshake.
- Contains supported cipher suites, TLS version, random data, and other information.

2. Server Hello:

- Sent by the server in response to the Client Hello.
- Includes the selected cipher suite, session ID, and server random data.

3. Certificate:

- Sent by the server.
- Contains the server's certificate for authentication.

4. Server Key Exchange:

- Sent by the server if required by the chosen cipher suite.
- Includes key exchange parameters.

5. Server Hello Done:

- Indicates that the server has finished its part of the handshake.

6. Client Key Exchange:

- Sent by the client.
- Contains key exchange information (e.g., pre-master secret).

7. Change Cipher Spec:

- Sent by both client and server to indicate that subsequent messages will be encrypted using the negotiated cipher suite.

8. Encrypted Handshake Message:

- Sent by both client and server.
- Confirms that encryption and keys are correctly set up.

9. New Session Ticket (Optional):

- Sent by the server to provide a session ticket for resuming sessions

6. In the Client Hello message, what are the two versions of the TLS, and are they different and why?

No.	Source	Destination	Time	Protocol	Length	User Datagram Info
2565	10.240.118.97	34.227.156.202	9.048973013	TLSv1.2	1969	Client Hello
2568	10.240.118.97	34.227.156.202	9.050069502	TLSv1.2	1969	Client Hello
2571	10.240.118.97	34.227.156.202	9.064200403	TLSv1.2	1969	Client Hello
2576	34.227.156.202	10.240.118.97	9.295499219	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2580	10.240.118.97	34.227.156.202	9.297943783	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2581	34.227.156.202	10.240.118.97	9.298311900	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 1898
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 1894
Version: TLS 1.2 (0x0303)
Random: 09044429e21e88413af0f288bc95e79e9fd134503b52a5e39da364239c3a126
Session ID Length: 32
Session ID: 636dbd1abca62a3ddd8e70f9a63c13a232033787b305ab8f1cb01437c3fe006
Cipher Suites Length: 34
Cipher Suites (17 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 1787
Extension: server_name (len=23)
Extension: extended_master_secret (len=0)
Extension: renegotiation_info (len=1)
Extension: supported_groups (len=16)
Extension: ec_point_formats (len=2)
Extension: session_ticket (len=0)
Extension: application_layer_protocol_negotiation (len=14)
Extension: status_request (len=5)
Extension: delegated_credentials (len=10)
Extension: signed_certificate_timestamp (len=0)
Extension: key_share (len=1327)
Extension: supported_versions (len=5)
Type: supported_versions (43)
Length: 5
Supported Versions length: 4
Supported Version: TLS 1.3 (0x0304)
Supported Version: TLS 1.2 (0x0303)

In the Client Hello:

- **Version field:** TLS 1.2 (0x0303)
- **Supported Versions extension:** TLS 1.3(0x0304)

Yes, they are different. The reason the client advertises both versions is to ensure that it can communicate with a wider variety of servers. If the server supports TLS 1.3, it will typically select that version; otherwise, the connection will fall back to TLS 1.2. This negotiation helps maintain both security and interoperability during the TLS handshake.

7. Which field in the Client Hello message has the value of the domain? Is it encrypted or in plaintext?

Time	No.	Source	Destination	Protocol	Length	Info
9.048973013	2565	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.050069502	2568	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)

Extension: server_name (len=23) name=www.cics.umass.edu
Type: server_name (0)
Length: 23
Server Name Indication extension
Server Name list length: 21
Server Name Type: host_name (0)
Server Name length: 18
Server Name: www.cics.umass.edu

00b0	00	35	01	00	06	fb	00	00	00	17	00	15
00c0	77	77	2e	63	69	63	73	2e	75	6d	61	73
00d0	75	00	17	00	00	ff	01	00	01	00	00	0a
00e0	11	ec	00	1d	00	17	00	18	00	19	01	00
00f0	00	02	01	00	00	23	00	00	00	10	00	0e
0100	32	08	68	74	74	70	2f	31	2e	31	00	05
0110	00	00	00	00	22	00	0a	00	08	04	03	05
0120	03	00	12	00	00	33	05	2f	05	2d	11	
0130	74	40	74	43	31	54	a4	95	2b	fb	3e	35

Field: **Server Name Indication (SNI)** under **Extension: server_name** Shows **www.cics.umass.edu**

It is **plaintext**, not encrypted (used to let the server know which certificate to send) even though it's part of the TLS handshake. This means anyone capturing the traffic (e.g., via Wireshark) can see which domain the client is trying to reach.

8. Traverse through the ‘Extension:’ parameters of the Client Hello message and provide the field name that contains the version of the HTTP, and what is the HTTP version?

ts.handshake.type && ip.addr==34.227.156.202						
Time	No.	Source	Destination	Protocol	Length	Info
9.048973013	2565	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.050069502	2568	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)

<ul style="list-style-type: none"> ✓ Extension: application_layer_protocol_negotiation (len=14) <ul style="list-style-type: none"> Type: application_layer_protocol_negotiation (16) Length: 14 ALPN Extension Length: 12 ✗ ALPN Protocol ALPN string length: 2 ALPN Next Protocol: h2 ALPN string length: 8 ALPN Next Protocol: http/1.1 	<pre>0100 32 08 68 74 74 70 2f 31 2e 31 00 0 0110 00 00 00 00 22 00 0a 00 08 04 03 0 0120 03 00 12 00 00 00 33 05 2f 05 2d 1 0130 74 40 74 43 31 54 a4 95 2b fb 3e 3 0140 0e 35 61 9c f7 f4 3d 0e c8 bf a8 1 0150 15 f9 bd 97 e6 14 fc 65 a9 cd 99 6 0160 29 b3 88 d9 61 7e 0c ab 98 10 a2 9 0170 01 02 32 11 88 2c 34 24 c9 1f ea 4 0180 2a 75 7d 0c c2 3f f4 38 84 e5 26 1 0190 e9 c1 2d eb b1 f8 72 2c 97 98 77 b</pre>
---	--

In the Client Hello message,

- Field: **ALPN Next Protocol** under **Extension: application_layer_protocol_negotiation(ALPN)**
- So the HTTP version is: "**HTTP/2 (h2) and HTTP/1.1 (http/1.1)**"

9. List all the cipher suites the client offers the server to choose from for further communication.

The cipher suites offered by the client to the server in the Client Hello message are as follows:

ts.handshake.type && ip.addr==34.227.156.202						
Time	No.	Source	Destination	Protocol	Length	Info
9.048973013	2565	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.050069502	2568	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)

<ul style="list-style-type: none"> ✓ Cipher Suites (17 suites) <ul style="list-style-type: none"> Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303) Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa9) Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa8) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x002f) Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) 	<pre>0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 00a0 c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00b0 00 35 01 00 06 fb 00 00 00 17 00 15 00c0 77 77 2e 63 69 63 73 2e 75 6d 61 73 00d0 75 00 17 00 00 ff 01 00 01 00 00 0a 00e0 11 ec 00 1d 00 17 00 18 00 19 01 06 00f0 00 02 01 00 00 23 00 00 00 10 00 06 0100 32 08 68 74 74 70 2f 31 2e 31 00 05 0110 00 00 00 00 22 00 00 00 08 04 03 05 0120 03 00 12 00 00 00 33 05 2f 05 2d 11 0130 74 40 74 43 31 54 a4 95 2b fb 3e 35 0140 0e 35 61 9c f7 f4 3d 0e c8 bf a8 11 0150 15 f9 bd 97 e6 14 fc 65 a9 cd 99 6c 0160 29 b3 88 d9 61 7e 0c ab 98 10 a2 95 0170 01 02 32 11 88 2c 34 24 c9 1f ea 47 0180 2a 75 7d 0c c2 3f f4 38 84 e5 26 16 0190 e9 c1 2d eb b1 f8 72 2c 97 98 77 b5 01a0 b9 82 c8 48 92 ea b9 a2 9b a5 a4 b5 01b0 fd a4 10 09 c7 a7 d7 b7 46 6f f4 51 01c0 62 60 32 ec 5e be 49 28 5c ca a1 45</pre>
---	--

Cipher Suites (17 suites)

1. Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
2. Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
3. Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
4. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
5. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
6. Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa9)
7. Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa8)
8. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
9. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
10. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
11. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
12. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
13. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
14. Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
15. Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
16. Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
17. Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

These cipher suites represent the encryption algorithms and key exchange methods supported by the client, allowing the server to select one for secure communication based on mutual compatibility.

Now, analyse the corresponding Server Hello message and answer the following questions.

10. Which TLS version has the server agreed on to set the TLS handshake?

The Wireshark capture shows three entries for the Server Hello message (Protocol: TLSv1.2) from source 34.227.156.202 to destination 10.240.118.97. The third entry is selected, revealing its details:

Time	No.	Source	Destination	Protocol	Length	Info
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.298311900	2581	34.227.156.202	10.240.118.97	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.326014025	2587	34.227.156.202	10.240.118.97	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done

Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 74

Hex dump of the selected message:
0040 5f 69 16 03 03 00 4a 02 00 00 46 03 03 77 16 f2 _i.....J...F
0050 da 85 5c 5f f5 39 9c cf e3 72 d7 a3 ec d4 4e 3d ..._9...r...
0060 a8 ad da a6 73 6a 0a 3f b4 30 18 75 03 00 c0 2f ...sj..? 0...
0070 00 00 1e 00 00 00 ff 01 00 01 00 00 0b 00 04#....
0080 03 00 01 02 00 23 00 00 00 10 00 05 00 03 02 68#....
0090 32 16 03 03 12 cb 0b 00 12 c7 00 12 c4 00 06 e8 2.....

From the provided Wireshark capture, the server has agreed to use TLS 1.2 for the TLS handshake. This is evident in the Server Hello message, where the "Version" field specifies TLS 1.2 (0x0303).

Version: TLS 1.2 (0x0303)

11. Which cipher suite has the server agreed on for further communication?

ts.handshake.type && ip.addr==34.227.156.202					
Time	No.	Source	Destination	Protocol	Length Info
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969 Client Hello (SNI=www.cics.umass.edu)
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.297943783	2580	10.240.118.97	34.227.156.202	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
a.708211000	2581	34.227.156.202	10.240.118.97	TLSv1.2	5208 Server Hello, Certificate, Server Key Exchange, Server Hello Done

▾ Handshake Protocol: Server Hello
 Handshake Type: Server Hello (2)
 Length: 70
 Version: TLS 1.2 (0x0303)
 Random: 7716f2da855c5fff5399ccfe372d7a3ecd44e3da8addaa6736a0a3fb430187503
 Session ID Length: 0
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite agreed by the server for further communication is :
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Analyse the Certificate, Server Key Exchange, Server Hello Done packet to answer the following questions.

12. What is the size (in bytes) of the Certificate, Server Key Exchange, Server Hello Done messages?

Message	Size of Record Layer (in Bytes)	Size of Handshake Protocol Message(in Bytes)
Certificate	4816 bytes	4811 bytes
Server Key Exchange	338 bytes	333 bytes
Server Hello Done	9 bytes	4 bytes

ts.handshake.type && ip.addr==34.227.156.202					
Time	No.	Source	Destination	Protocol	Length Info
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969 Client Hello (SNI=www.cics.umass.edu)
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.297943783	2580	10.240.118.97	34.227.156.202	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
a.708211000	2581	34.227.156.202	10.240.118.97	TLSv1.2	5208 Server Hello, Certificate, Server Key Exchange, Server Hello Done

▾ Frame 2576: 5308 bytes on wire (42464 bits), 5308 bytes captured (42464 bits) on interface eno1, id 0
 ▾ Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: HP_9a:99:9a (e0:73:e7:0a:99:9a)
 ▾ Internet Protocol Version 4, Src: 34.227.156.202, Dst: 10.240.118.97
 ▾ Transmission Control Protocol, Src Port: 443, Dst Port: 45922, Seq: 1, Ack: 1904, Len: 5242
 ▾ Transport Layer Security
 ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 ▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
 ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

Terminal
 Record Layer (tls.record), 4,816 bytes
 Packets: 7162 · Displayed: 12 (0.2%) · Profile:

```

> Frame 2576: 5308 bytes on wire (42464 bits), 5308 bytes captured (42464 bits) on interface eno1, id 0
> Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: HP_0a:99:9a (e0:73:e7:0a:99:9a)
> Internet Protocol Version 4, Src: 34.227.156.202, Dst: 10.240.118.97
> Transmission Control Protocol, Src Port: 443, Dst Port: 45922, Seq: 1, Ack: 1904, Len: 5242
  ▾ Transport Layer Security
    > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    > TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4811
      ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4807
        Certificates Length: 4804
        Certificates (4804 bytes)
    > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
      ▾ Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 329
        ▶ EC Diffie-Hellman Server Params
    > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)

  Handshake protocol message (tls.handshake), 4811 bytes

```

Packets: 7162 · Displayed: 12 (0.2%)

ts.handshake.type && ip.addr==34.227.156.202					
Time	No.	Source	Destination	Protocol	Length Info
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969 Client Hello (SNI=www.cics.umass.edu)
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.297943783	2580	10.240.118.97	34.227.156.202	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9.298110000	2581	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done

```

> Frame 2576: 5308 bytes on wire (42464 bits), 5308 bytes captured (42464 bits) on interface eno1, id 0
> Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: HP_0a:99:9a (e0:73:e7:0a:99:9a)
> Internet Protocol Version 4, Src: 34.227.156.202, Dst: 10.240.118.97
> Transmission Control Protocol, Src Port: 443, Dst Port: 45922, Seq: 1, Ack: 1904, Len: 5242
  ▾ Transport Layer Security
    > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    > TLSv1.2 Record Layer: Handshake Protocol: Certificate
    > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

  Record Layer (tls.record), 338 bytes

```

Packets: 7162 · Displayed: 12 (0.2%)

```

  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 333
    ▾ Handshake Protocol: Server Key Exchange
      Handshake Type: Server Key Exchange (12)
      Length: 329
      ▶ EC Diffie-Hellman Server Params
  ▾ 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
      Handshake Type: Server Hello Done (14)
      Length: 0

  Handshake protocol message (tls.handshake), 333 bytes

```

ts.handshake.type && ip.addr==34.227.156.202

Time	No.	Source	Destination	Protocol	Length	Info
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.297943783	2580	10.240.118.97	34.227.156.202	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9.298311000	2581	34.227.156.202	10.240.118.97	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done

> Frame 2576: 5308 bytes on wire (42464 bits), 5308 bytes captured (42464 bits) on interface eno1, id 0
> Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: HP_0a:99:9a (e0:73:e7:0a:99:9a)
> Internet Protocol Version 4, Src: 34.227.156.202, Dst: 10.240.118.97
> Transmission Control Protocol, Src Port: 443, Dst Port: 45922, Seq: 1, Ack: 1904, Len: 5242
`- Transport Layer Security
 > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 > TLSv1.2 Record Layer: Handshake Protocol: Certificate
 > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 > **TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done**

Record Layer (tls.record), 9 bytes

Packets: 7162 - Displayed: 12 (0.2%) Profil

```

▼ 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
  Handshake Type: Server Hello Done (14)
  Length: 0
Handshake protocol message (tls.handshake), 4 bytes

```

13. Which certificate is agreed upon by the server?

ts.handshake.type && ip.addr==34.227.156.202

Time	No.	Source	Destination	Protocol	Length	Info
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969	Client Hello (SNI=www.cics.umass.edu)
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.297943783	2580	10.240.118.97	34.227.156.202	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9.298311000	2581	34.227.156.202	10.240.118.97	TLSv1.2	5308	Server Hello, Certificate, Server Key Exchange, Server Hello Done

> Certificates (4804 bytes)
 Certificate Length: 1768
 Certificate [...] 308206e43082054ca003020102021100b3ead3c417ed80a3b46b499d0259537c300d06092a864886f70d01010c05003044310b30090603550406130255331123010
 > signedCertificate
 > version: v3 (2)
 > serialNumber: 0x00b3ead3c417ed80a3b46b499d0259537c
 > signature (sha384WithRSAEncryption)
 > Algorithm Id: 1.2.840.113549.1.1.12 (sha384WithRSAEncryption)
 > issuer: rdnSequence (0)
 > rdnSequence: 3 items (id-at-commonName=InCommon RSA Server CA 2,id-at-organizationName=Internet2,id-at-countryName=US)
 > RDNSequence item: 1 item (id-at-countryName=US)
 > RDNSequence item: 1 item (id-at-organizationName=Internet2)
 > RDNSequence item: 1 item (id-at-commonName=InCommon RSA Server CA 2)
 > subject: rdnSequence (0)
 > rdnSequence: 4 items (id-at-commonName=www.cics.umass.edu,id-at-organizationName=University of Massachusetts Amherst,id-at-stateOrProvinceName=Massachusetts)
 > RDNSequence item: 1 item (id-at-countryName=US)
 > RDNSequence item: 1 item (id-at-stateOrProvinceName=Massachusetts)
 > RDNSequence item: 1 item (id-at-organizationName=University of Massachusetts Amherst)
 > RDNSequence item: 1 item (id-at-commonName=www.cics.umass.edu)
 > subjectPublicKeyInfo
 > extensions: 10 items
 > algorithmIdentifier (sha384WithRSAEncryption)

The certificate agreed upon by the server is the end-entity certificate presented in the Handshake Protocol: Certificate message (Frame 2793). Its key details are:

- Certificate Length: 1768 bytes.
- Version: v3 (2).
- Serial Number: 0x00b3ead3c417ed80a3b46b499d0259537c.

- Signature Algorithm: sha384WithRSAEncryption.
- Issuer: Common Name: InCommon RSA Server CA 2, Organization: Internet, Country: US.
- Validity: Dates specified as notBefore(2024-07-23) and notAfter values(2025-08-23)
- Subject: Common Name: www.cics.umass.edu, Organization: University of Massachusetts Amherst, State: Massachusetts, Country: US.
- Subject Public Key Info:
 - Algorithm: rsaEncryption.
 - Public Key: (hexadecimal representation provided in the capture).

This certificate, along with the intermediate certificates (InCommon RSA Server CA 2 issued by USERTrust RSA Certification Authority, and USERTrust RSA Certification Authority issued by AAA Certificate Services), forms the chain presented by the server for authentication.

The certificate agreed upon by the server is issued to www.cics.umass.edu, and it is signed by **InCommon RSA Server CA 2**, using the **sha384WithRSAEncryption** algorithm.

14. Which handshake protocol is used in the **Server Key Exchange** message?

ts.handshake.type && ip.addr==34.227.156.202					
Time	No.	Source	Destination	Protocol	Length Info
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969 Client Hello (SNI=www.cics.umass.edu)
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.297943783	2580	10.240.118.97	34.227.156.202	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9.298111000	2581	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done

```

> Frame 2576: 5308 bytes on wire (42464 bits), 5308 bytes captured (42464 bits) on interface eno1, id 0
> Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: HP_9a:99:9a (e0:73:e7:0a:99:9a)
> Internet Protocol Version 4, Src: 34.227.156.202, Dst: 10.240.118.97
> Transmission Control Protocol, Src Port: 443, Dst Port: 45922, Seq: 1, Ack: 1904, Len: 5242
└ Transport Layer Security
  └ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    └ TLSv1.2 Record Layer: Handshake Protocol: Certificate
    └ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
      └ Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 329
        └ EC Diffie-Hellman Server Params

```

The handshake protocol used in the Server Key Exchange message is EC Diffie-Hellman Server Params i.e **ECDHE** (Elliptic Curve Diffie-Hellman Ephemeral).

15. Which signature algorithm does the server send to the client?

ts.handshake.type && ip.addr==34.227.156.202					
Time	No.	Source	Destination	Protocol	Length Info
9.064200403	2571	10.240.118.97	34.227.156.202	TLSv1.2	1969 Client Hello (SNI=www.cics.umass.edu)
9.295499219	2576	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done
9.297943783	2580	10.240.118.97	34.227.156.202	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9.298111000	2581	34.227.156.202	10.240.118.97	TLSv1.2	5308 Server Hello, Certificate, Server Key Exchange, Server Hello Done

```

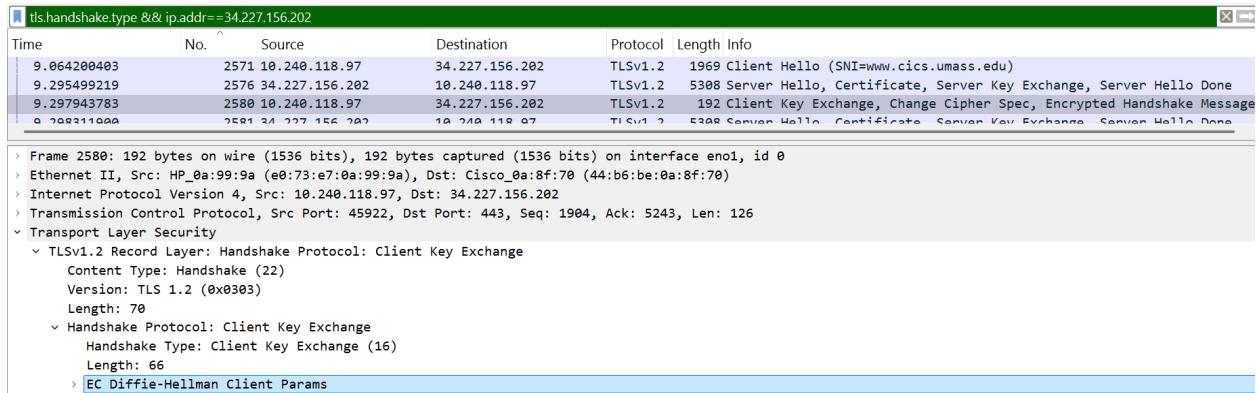
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 333
└ Handshake Protocol: Server Key Exchange
  Handshake Type: Server Key Exchange (12)
  Length: 329
  └ EC Diffie-Hellman Server Params
    Curve Type: named_curve (0x03)
    Named Curve: secp256r1 (0x0017)
    Pubkey Length: 65
    Pubkey: 049742ebf8b546a911a392632bde1e592f7e8499cab5e923989476e76b9ca35b812a41c2b67652f594853dc6609f170ef8b66c1e3e504f39eb9a18180d368f2e76
    └ Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
      Signature Hash Algorithm Hash: SHA512 (6)
      Signature Hash Algorithm Signature: RSA (1)

```

The server sends **rsa_pkcs1_sha512 (0x0601)** as the signature algorithm to the client.

Analyse the Client Key Exchange, Change Cipher Spec, Finished message and answer the following questions.

16. Does the client agree on the same handshake protocol?



A Wireshark screenshot showing a TLS handshake. The timeline shows four frames:

- Frame 9.064200403: Client Hello (SNI=www.cics.umass.edu)
- Frame 9.295499219: Server Hello, Certificate, Server Key Exchange, Server Hello Done
- Frame 9.297943783: Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
- Frame 9.298110000: Server Hello, Certificate, Server Key Exchange, Server Hello Done

The details pane shows the Client Key Exchange message, which includes:

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 70
- Handshake Protocol: Client Key Exchange
- Handshake Type: Client Key Exchange (16)
- Length: 66

The selected message is EC Diffie-Hellman Client Params.

Yes, the client agrees on the **same handshake protocol (ECDHE)** as indicated by the **Client Key Exchange** message and continues with **Change Cipher Spec** and **Finished**, completing the handshake using the agreed **ECDHE protocol**.

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).