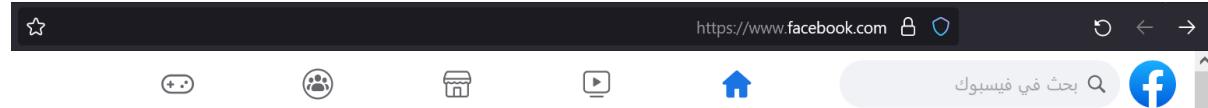


PROJECT

1 . Visit a login page in any trusted website and use Wireshark to : (2 Marks)
Show the data associated with each OSI layer in details.



Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

All interfaces shown ▾

WiFi

Ethernet 4

Adapter for loopback traffic capture

Local Area Connection* 10

Local Area Connection* 9

Local Area Connection* 8

Local Area Connection* 2

Local Area Connection* 1

Local Area Connection

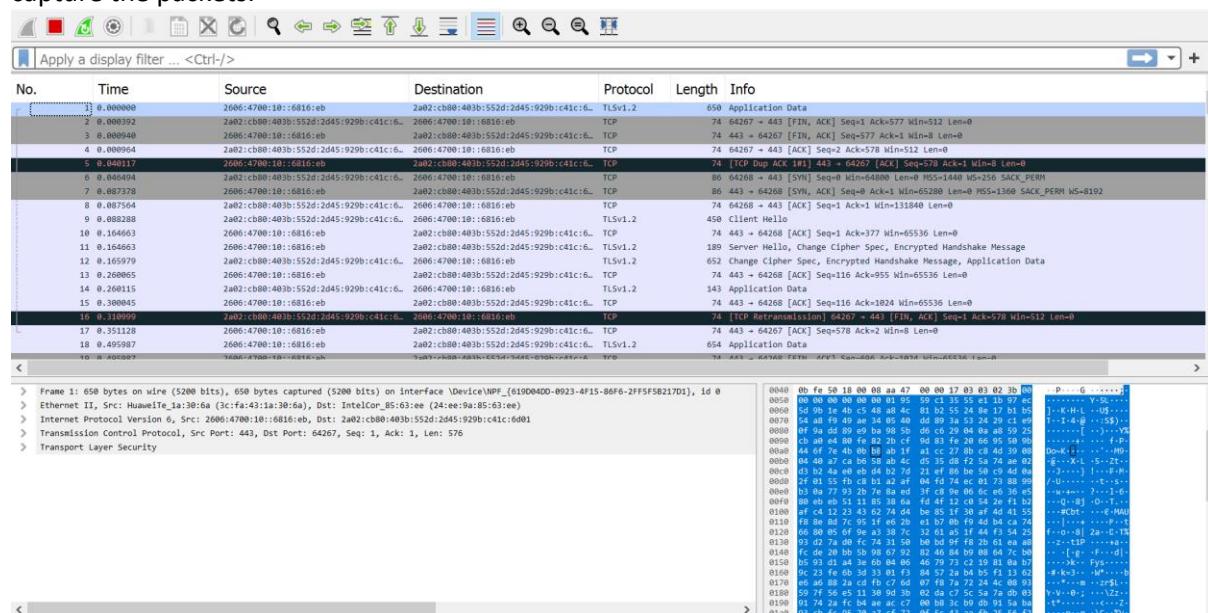
Ethernet

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.3 (v4.0.3-0-gc552f74cdc23). You receive automatic updates.

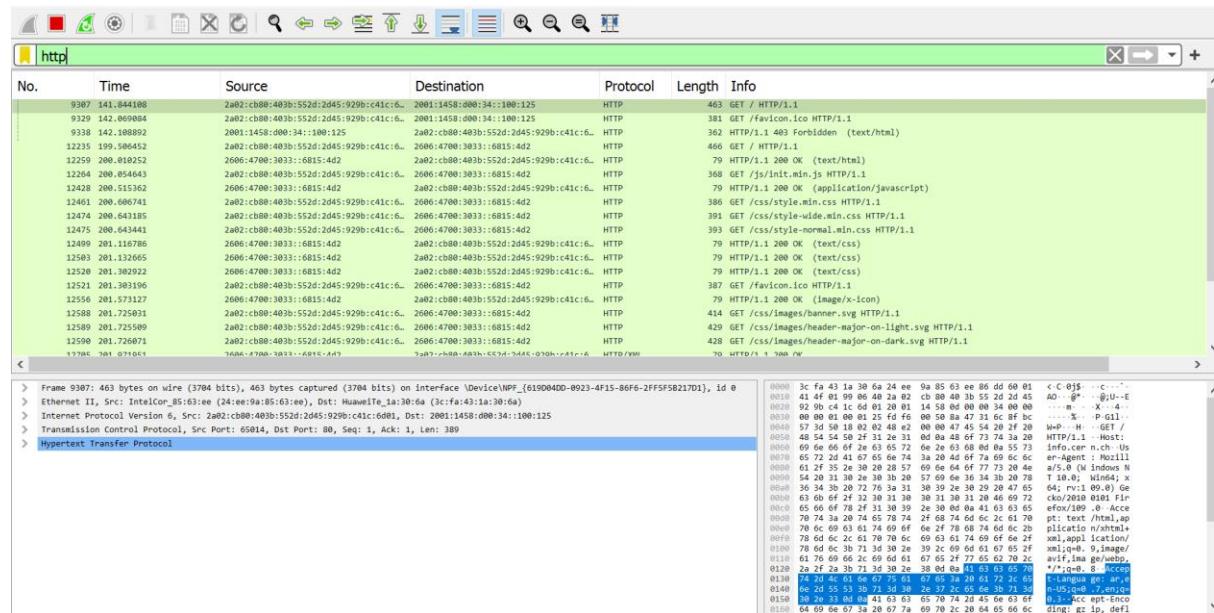
After selecting wifi there are packets captured:
capture the packets:



The screenshot shows the Wireshark interface with the "WiFi" interface selected. A list of captured frames is displayed, starting with frame 1, which is an Application Data frame from source 2a02:cbb0:403b:552d:2d45:929b:c41c:6 to destination TLSv1.2. The packet details, bytes, and hex panes are visible at the bottom, showing the raw network data.

As you can see now with shark:

It start works:



First we have the physical layer (data transmitted into bits):



Second we have the Data Link Layer which represent with Ethernet as protocol:

As you can see we have the mac address of source and destination :



Third we have the Network Layer where we have the IP here we have version 4 also you can see our ip source and destination :

> Frame 21: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{61900400-0923-4F15-86F6-2FF5F5B217D1}, id 0

> Ethernet II, Src: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a), Dst: IntelCor_B5:63:ee (24:ee:9a:85:63:ee)

> Internet Protocol Version 4, Src: 23.182.0.171, Dst: 192.168.0.107

 Internet Protocol Version 4, Src: 23.182.0.171, Dst: 192.168.0.107

 Total Length: 88

 Identification: 0x2ee1 (12001)

 Flags: 0x02, Don't fragment

 Fragment Offset: 0

 Time to Live: 108

 Protocol: TCP (6)

 Header Checksum: 0xfe9a [validation disabled]

 [Header checksum status: Unverified]

 Source Address: 23.182.0.171

 Destination Address: 192.168.0.107

> Transmission Control Protocol, Src Port: 443, Dst Port: 55175, Seq: 1, Ack: 60, Len: 48

> Frame 21: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{61900400-0923-4F15-86F6-2FF5F5B217D1}, id 0

> Ethernet II, Src: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a), Dst: IntelCor_B5:63:ee (24:ee:9a:85:63:ee)

> Internet Protocol Version 4, Src: 23.182.0.171, Dst: 192.168.0.107

 Internet Protocol Version 4, Src: 23.182.0.171, Dst: 192.168.0.107

 Total Length: 88

 Identification: 0x2ee1 (12001)

 Flags: 0x02, Don't fragment

 Fragment Offset: 0

 Time to Live: 108

 Protocol: TCP (6)

 Header Checksum: 0xfe9a [validation disabled]

 [Header checksum status: Unverified]

 Source Address: 23.182.0.171

 Destination Address: 192.168.0.107

> Transmission Control Protocol, Src Port: 443, Dst Port: 55175, Seq: 1, Ack: 60, Len: 48

> Transmission Control Protocol, Src Port: 443, Dst Port: 55175, Seq: 1, Ack: 60, Len: 48

Source Port: 443

Destination Port: 55175

[Stream index: 3]

[Conversation completeness: Incomplete (12)]

[TCP Segment Len: 48]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1081696725

[Next Sequence Number: 49 (relative sequence number)]

Acknowledgment Number: 60 (relative ack number)

Acknowledgment number (raw): 231108555

Flags: 0x18 (PSH, ACK)

Window: 2047

[Calculated window size: 2047]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xaaf7f1 [unverified]

Fourth it's the UDP and TCP layer so it's the Transport layer and here you see the 443 ports and dest 55175 :

> Frame 21: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{61900400-0923-4F15-86F6-2FF5F5B217D1}, id 0

> Ethernet II, Src: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a), Dst: IntelCor_B5:63:ee (24:ee:9a:85:63:ee)

> Internet Protocol Version 4, Src: 23.182.0.171, Dst: 192.168.0.107

> Transmission Control Protocol, Src Port: 443, Dst Port: 55175, Seq: 1, Ack: 60, Len: 48

> Transport Layer Security

 TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

 Content Type: Application Data (23)

 Version: TLS 1.2 (0x0303)

 Length: 43

 Encrypted Application Data: 000000000000002be78a08563100646bb67c351e5eb2013afb6a9249ca5d2ee71000b687d..

 [Application Data Protocol: Hypertext Transfer Protocol]

You can see the application is: HTTP and the encrypted for security.

do the same task but with http page (not encrypted) and show the differences between layers.

Here the website for http only

First the https was operates at the Application Layer, whereas HTTPS operates at Transport Layer

No.	Time	Source	Destination	Protocol	Length	Info
46	9.525477	fe80::411:4f37:bd1f...	ff02::fb	MDNS	197	Standard query response 0x0000 PTR Home iPhone._rdlin
47	11.284639	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64596 → 80 [ACK] Seq=1 Ack=1 Win=253
48	11.600364	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64596 [ACK] Seq=1 Ack=2 Win
49	11.625206	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64595 → 80 [ACK] Seq=1 Ack=1 Win=253
50	11.918909	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64597 → 80 [ACK] Seq=1 Ack=1 Win=253
51	11.919170	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64595 [ACK] Seq=1 Ack=2 Win
52	12.204250	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64597 [ACK] Seq=1 Ack=2 Win
53	13.107630	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
54	13.110054	fe80::8ec:32bb:668d...	ff02::fb	MDNS	199	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
55	14.133162	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM"

```

> Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{619D0
> Ethernet II, Src: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a), Dst: IntelCor_85:63:ee (24:ee:9a:85:63:ee)
> Internet Protocol Version 4, Src: 44.238.29.244, Dst: 192.168.8.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 64597, Seq: 1, Ack: 2, Len: 0
    0000 24 ee 9a 85 63 ee 3c fa
    0010 00 34 7c 28 40 00 5b 06
    0020 08 6b 00 50 fc 55 a2 81
    0030 02 02 82 ce 00 00 01 01
    0040 f7 18

```

Also we can see here at the transport layer that the port for http(80) in https was(443)

No.	Time	Source	Destination	Protocol	Length	Info
46	9.525477	fe80::411:4f37:bd1f...	ff02::fb	MDNS	197	Standard query response 0x0000 PTR Home iPhone._rdlin
47	11.284639	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64596 → 80 [ACK] Seq=1 Ack=1 Win=253
48	11.600364	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64596 [ACK] Seq=1 Ack=2 Win
49	11.625206	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64595 → 80 [ACK] Seq=1 Ack=1 Win=253
50	11.918909	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64597 → 80 [ACK] Seq=1 Ack=1 Win=253
51	11.919170	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64595 [ACK] Seq=1 Ack=2 Win
52	12.204250	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64597 [ACK] Seq=1 Ack=2 Win
53	13.107630	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
54	13.110054	fe80::8ec:32bb:668d...	ff02::fb	MDNS	199	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
55	14.133162	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM"

```

> Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{619D0
> Ethernet II, Src: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a), Dst: IntelCor_85:63:ee (24:ee:9a:85:63:ee)
> Internet Protocol Version 4, Src: 44.238.29.244, Dst: 192.168.8.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 64597, Seq: 1, Ack: 2, Len: 0
    Source Port: 80
    Destination Port: 64597
    [Stream index: 4]
    [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 0]
    Sequence Number: 1      (relative sequence number)
    Sequence Number (raw): 2726404069
    0000 24 ee 9a 85 63 ee 3c fa
    0010 00 34 7c 28 40 00 5b 06
    0020 08 6b 00 50 fc 55 a2 81
    0030 02 02 82 ce 00 00 01 01
    0040 f7 18

```

Here we have the network layer for http it operates with TCP/IP not like https operates with TLS

No.	Time	Source	Destination	Protocol	Length	Info
46	9.525477	fe80::411:4f37:bd1f...	ff02::fb	MDNS	197	Standard query response 0x0000 PTR Home iPhone._rdlin
47	11.284639	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64596 → 80 [ACK] Seq=1 Ack=1 Win=253
48	11.600364	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64596 [ACK] Seq=1 Ack=2 Win
49	11.625206	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64595 → 80 [ACK] Seq=1 Ack=1 Win=253
50	11.918909	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64597 → 80 [ACK] Seq=1 Ack=1 Win=253
51	11.919170	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64595 [ACK] Seq=1 Ack=2 Win
52	12.204250	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64597 [ACK] Seq=1 Ack=2 Win
53	13.107630	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
54	13.110054	fe80::8ec:32bb:668d...	ff02::fb	MDNS	199	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
55	14.133162	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM"

```

> Ethernet II, Src: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a), Dst: IntelCor_85:63:ee (24:ee:9a:85:63:ee)
> Internet Protocol Version 4, Src: 44.238.29.244, Dst: 192.168.8.107
    0100 ... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DS24: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x7c28 (31784)
    > 010. .... = Flags: 0x2, Don't fragment
    .... 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 91
    Protocol: TCP (6)
    0000 24 ee 9a 85 63 ee 3c fa
    0010 00 34 7c 28 40 00 5b 06
    0020 08 6b 00 50 fc 55 a2 81
    0030 02 02 82 ce 00 00 01 01
    0040 f7 18

```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
46	9.525477	fe80::411:4f37:bd1f...	ff02::fb	MDNS	197	Standard query response 0x0000 PTR Home iPhone._rdlin
47	11.284639	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64596 → 80 [ACK] Seq=1 Ack=1 Win=253
48	11.600364	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64596 [ACK] Seq=1 Ack=2 Win
49	11.625206	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64595 → 80 [ACK] Seq=1 Ack=1 Win=253
50	11.918999	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64597 → 80 [ACK] Seq=1 Ack=1 Win=257
51	11.919170	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64595 [ACK] Seq=1 Ack=2 Win
52	12.204250	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64597 [ACK] Seq=1 Ack=2 Win
53	13.107630	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
54	13.110054	fe80::8ec:32bb:668d...	ff02::fb	MDNS	199	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
55	14.133162	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM"

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x7c28 (31784)
 > 010. = Flags: 0x2, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 91
 Protocol: TCP (6)
 Header Checksum: 0x8fa6 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 44.238.29.244
 Destination Address: 192.168.8.107

Frame (frame) 66 bytes

Packets: 73811 · Displayed: 73811 (100.0%) · Profile: Default

And here we can see the data link layer and the physical layer:

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
46	9.525477	fe80::411:4f37:bd1f...	ff02::fb	MDNS	197	Standard query response 0x0000 PTR Home iPhone._rdlin
47	11.284639	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64596 → 80 [ACK] Seq=1 Ack=1 Win=253
48	11.600364	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64596 [ACK] Seq=1 Ack=2 Win
49	11.625206	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64595 → 80 [ACK] Seq=1 Ack=1 Win=253
50	11.918999	192.168.8.107	44.238.29.244	TCP	55	[TCP Keep-Alive] 64597 → 80 [ACK] Seq=1 Ack=1 Win=257
51	11.919170	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64595 [ACK] Seq=1 Ack=2 Win
52	12.204250	44.238.29.244	192.168.8.107	TCP	66	[TCP Keep-Alive ACK] 80 → 64597 [ACK] Seq=1 Ack=2 Win
53	13.107630	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
54	13.110054	fe80::8ec:32bb:668d...	ff02::fb	MDNS	199	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
55	14.133162	192.168.8.106	224.0.0.251	MDNS	179	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM"

[Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp]
 [Coloring Rule Name: HTTP]
 [Coloring Rule String: http || tcp.port == 80 || http2]
 ▾ Ethernet II, Src: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a), Dst: IntelCor_85:63
 ▾ Destination: IntelCor_85:63:ee (24:ee:9a:85:63:ee)
 Address: IntelCor_85:63:ee (24:ee:9a:85:63:ee)
0. = LG bit: Globally unique address (factor
0. = IG bit: Individual address (unicast)
 ▾ Source: HuaweiTe_1a:30:6a (3c:fa:43:1a:30:6a)

0000 24 ee 9a 85 63 ee 3c fa 43 1a 30 6a 08 00 4!
 0010 00 34 7c 28 40 00 5b 06 8f a6 2c ee 1d f4 c0
 0020 08 6b 00 50 fc 55 a2 81 9f e5 94 35 f7 18 80
 0030 02 02 82 ce 00 00 01 01 05 0a 94 35 f7 17 94
 0040 f7 18

2. Establish a handshake session with any trusted website and show the following :

1 . What is the IP address of the website >>use nslookup in command terminal .

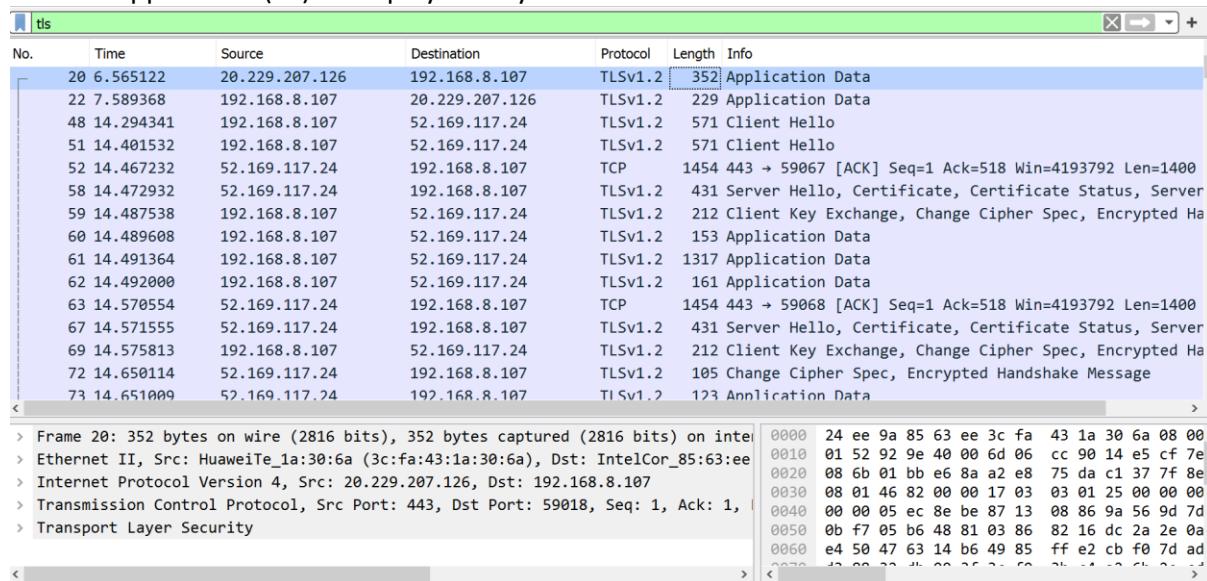
```
C:\Users\shama>nslookup www.instagram.com
Server: UnKnown
Address: fe80::3efa:43ff:fe1a:306a

Non-authoritative answer:
Name: z-p42-instagram.c10r.instagram.com
Addresses: 2a03:2880:f242:e0:face:b00c:0:4420
          157.240.195.174
Aliases: www.instagram.com
geo-p42.instagram.com

C:\Users\shama>
```

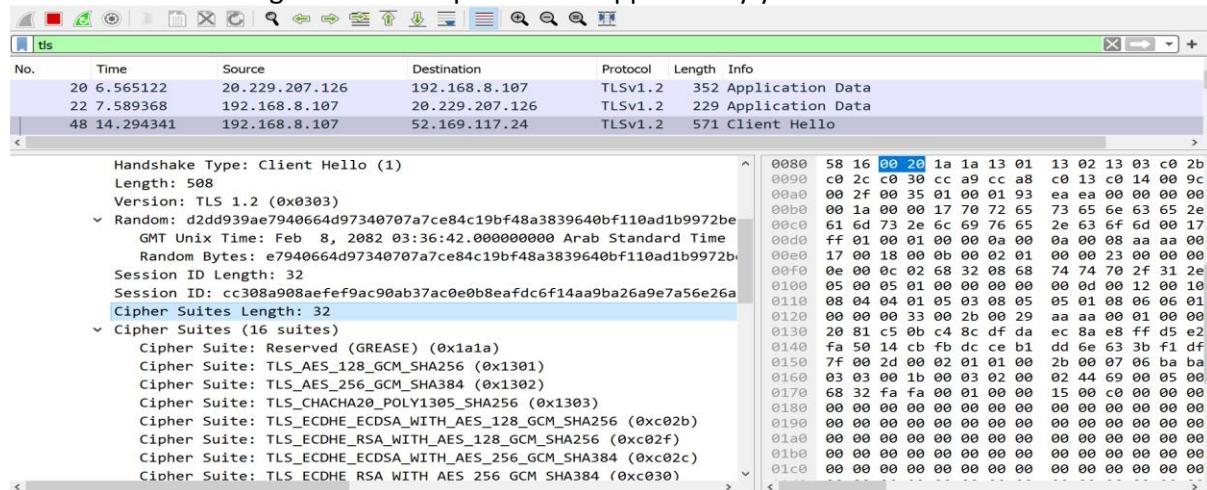
Then from Wireshark, inspect the following:

First we applied the (tls) to display the layers



This Wireshark screenshot shows a TLS handshake between two hosts. The timeline pane displays 73 frames, with frames 20, 22, and 48 highlighted. Frame 20 shows the initial Application Data (Client Hello). Frame 22 shows the second Application Data (Server Hello). Frame 48 shows the Client Hello message. The details pane shows the raw hex and ASCII data for these frames, including the TLS handshake messages.

2. Client Hello message and show cipher suite supported by your browser



This Wireshark screenshot focuses on the Client Hello message (Frame 48). It shows the detailed structure of the Client Hello, including the Handshake Type, Length, Version (TLS 1.2), Random bytes, Session ID, and a list of supported Cipher Suites. The Cipher Suites section is expanded, showing 16 individual cipher suites with their names and identifiers.

3. What is the compression method?

Algorithms used to compress stored files.

The screenshot shows a Wireshark capture titled "tls". The packet list pane shows three captured frames:

- Frame 20: 6.565122, Source 20.229.207.126, Destination 192.168.8.107, Protocol TLSv1.2, Length 352 Application Data
- Frame 22: 7.589368, Source 192.168.8.107, Destination 20.229.207.126, Protocol TLSv1.2, Length 229 Application Data
- Frame 48: 14.294341, Source 192.168.8.107, Destination 52.169.117.24, Protocol TLSv1.2, Length 571 Client Hello

The details pane displays the Client Hello message from frame 48. It includes sections for cipher suites, compression methods, and extensions. The "Compression Methods" section shows a length of 1, indicating a single method: null (0). The "Extensions" section lists various TLS extensions with their lengths and types.

No.	Time	Source	Destination	Protocol	Length	Info
20	6.565122	20.229.207.126	192.168.8.107	TLSv1.2	352	Application Data
22	7.589368	192.168.8.107	20.229.207.126	TLSv1.2	229	Application Data
48	14.294341	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello

4. What is the session ID?

Unique number from the website to the user in the duration of the visit.

The screenshot shows a Wireshark capture titled "tls". The packet list pane shows the same three frames as the previous screenshot.

The details pane displays the Client Hello message from frame 48. A specific field, "Session ID", is highlighted in blue. The value of the Session ID is cc308a908aeef9ac90ab37ac0e0b8eafdc6f14aa9ba26a9e7a56e26a. This value is also copied to the clipboard, indicated by the "C" icon in the toolbar.

The "Cipher Suites" section of the details pane is expanded, showing a list of supported cipher suites.

No.	Time	Source	Destination	Protocol	Length	Info
20	6.565122	20.229.207.126	192.168.8.107	TLSv1.2	352	Application Data
22	7.589368	192.168.8.107	20.229.207.126	TLSv1.2	229	Application Data
48	14.294341	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello

5.What is Random number?

Small utility that creates a pcap trace file full of random packets.

No.	Time	Source	Destination	Protocol	Length	Info
20	6.565122	20.229.207.126	192.168.8.107	TLSv1.2	352	Application Data
22	7.589368	192.168.8.107	20.229.207.126	TLSv1.2	229	Application Data
48	14.294341	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello

Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: d2dd939ae7940664d97340707a7ce84c19bf48a3839640bf110ad1b9972be
GMT Unix Time: Feb 8, 2082 03:36:42.000000000 Arab Standard Time
Random Bytes: e7940664d97340707a7ce84c19bf48a3839640bf110ad1b9972be
Session ID Length: 32
Session ID: cc308a908aefef9ac90ab37ac0e0b8eafdc6f14aa9ba26a9e7a56e26a
Cipher Suites Length: 32
Cipher Suites (16 suites)
Cipher Suite: Reserved (GREASE) (0x1a1a)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_ECDHE_ECDSA WITH AES 128 GCM SHA256 (0xc02b)

0040 03 d2 dd 93 9a e7 94 06 64 d9 73 40 70 7a
0050 4c 19 bf 48 a3 83 96 40 bf 11 0a d1 b9 97
0060 ac 20 cc 30 8a 90 8a ef ef 9a c9 0a b3 7a
0070 b8 ea fd c6 f1 4a a9 ba 26 a9 e7 a5 6e 26
0080 58 16 00 20 1a 1a 13 01 13 02 13 03 c0 2b
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c
00a0 00 2f 00 35 01 00 01 93 ea ea 00 00 00 00
00b0 00 1a 00 00 17 70 72 65 73 65 6e 63 65 2e
00c0 61 6d 73 2e 6c 69 76 65 2e 63 6f 6d 00 17
00d0 ff 01 00 01 00 00 0a 00 0a 00 08 aa aa 00
00e0 17 00 18 00 0b 00 02 01 00 00 23 00 00 00
00f0 0e 00 02 68 32 08 68 74 74 70 2f 31 2e
0100 05 00 05 01 00 00 00 00 00 0d 00 12 00 10
0110 08 04 04 01 05 03 08 05 05 01 08 06 06 01
0120 00 00 00 33 00 2b 00 29 aa aa 00 01 00 00
0130 20 81 c5 0b c4 8c df da ec 8a e8 ff d5 e2
0140 fa 50 14 cb fb dc ce b1 dd 6e 63 3b f1 df
0150 ff 00 2d 00 02 01 01 00 2b 00 07 06 ba ba
0160 03 03 00 1b 00 03 02 00 02 44 69 00 05 00
0170 68 32 fa fa 00 01 00 00 15 00 c0 00 00 00
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

6.Inspect Server Hello, what did the server choose in cipher suite .

No.	Time	Source	Destination	Protocol	Length	Info
20	6.565122	20.229.207.126	192.168.8.107	TLSv1.2	352	Application Data
22	7.589368	192.168.8.107	20.229.207.126	TLSv1.2	229	Application Data
48	14.294341	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
51	14.401532	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
52	14.467232	52.169.117.24	192.168.8.107	TCP	1454	443 → 59067 [ACK] Seq=1 Ack=518 Win=4193792 Len=1400
58	14.472932	52.169.117.24	192.168.8.107	TLSv1.2	431	Server Hello, Certificate, Certificate Status, Server
59	14.487538	192.168.8.107	52.169.117.24	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60	14.489608	192.168.8.107	52.169.117.24	TLSv1.2	153	Application Data
61	14.491364	192.168.8.107	52.169.117.24	TLSv1.2	1317	Application Data
62	14.492000	192.168.8.107	52.169.117.24	TLSv1.2	161	Application Data

Version: TLS 1.2 (0x0303)
Random: 63e18010d3b65e9b0f4ea7b87e7fc91c94afe95a5d2fea80a4825dafa77c1
GMT Unix Time: Feb 7, 2023 01:32:48.000000000 Arab Standard Time
Random Bytes: d3b65e9b0f4ea7b87e7fc91c94afe95a5d2fea80a4825dafa77c1
Session ID Length: 32
Session ID: b31e00092d32b8e0bea16906e8609b6ee4f6e771570863a25b1aaec8
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Compression Method: null (0)
Extensions Length: 22
Extension: status_request (len=0)
Extension: application_layer_protocol_negotiation (len=5)

0040 15 70 86 3a 25 b1 aa ec 87 ae ed 51 c0 30
0050 16 00 05 00 00 00 10 00 05 00 03 02 68 32
0060 00 00 ff 01 00 01 00 00 00 0e a8 00 0e a5
0070 a8 30 82 08 a4 30 82 06 8c a0 03 02 01 02
0080 33 00 4b 66 86 48 d3 6f b4 f7 1c 37 7f 00
0090 4b 6e 86 30 0d 06 09 2a 86 48 86 f7 0d 01
00a0 05 00 30 59 31 0b 30 09 06 03 55 04 06 13
00b0 53 31 1e 30 1c 06 03 55 04 0a 13 15 4d 69
00c0 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74
00d0 6e 31 2a 30 28 06 03 55 04 03 13 21 4d 69
00e0 6f 73 6f 66 74 20 41 7a 75 72 65 20 54 4c
00f0 49 73 73 75 69 6e 67 20 43 41 20 30 36 30

Frame (431 bytes) Reassembled TCP (5977 bytes)

Protocol: TLS

Key exchange: ECDHE

Authentication: RSA

Encrypted: AES 128 GCM

Hash: SHA256

7. Is the session ID the same from Server Hello? What does this refer to?

The ID of a session the client wishes to use for this connection. In the first Client

Hello of the exchange, the session ID is empty for client here or with different number which mean new session

No.	Time	Source	Destination	Protocol	Length	Info
20	6.565122	20.229.207.126	192.168.8.107	TLSv1.2	352	Application Data
22	7.589368	192.168.8.107	20.229.207.126	TLSv1.2	229	Application Data
48	14.294341	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
51	14.401532	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
52	14.467232	52.169.117.24	192.168.8.107	TCP	1454	443 → 59067 [ACK] Seq=1 Ack=518 Win=4193792 Len=1400
58	14.472932	52.169.117.24	192.168.8.107	TLSv1.2	431	Server Hello, Certificate, Certificate Status, Server
59	14.487538	192.168.8.107	52.169.117.24	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60	14.489608	192.168.8.107	52.169.117.24	TLSv1.2	153	Application Data
61	14.491364	192.168.8.107	52.169.117.24	TLSv1.2	1317	Application Data
62	14.492000	192.168.8.107	52.169.117.24	TLSv1.2	161	Application Data

```

    Random: d2dd939ae7940664d97340707a7ce84c19bf48a3839640bf110ad1b9972be ^
      GMT Unix Time: Feb 8, 2082 03:36:42.000000000 Arab Standard Time
      Random Bytes: e7940664d97340707a7ce84c19bf48a3839640bf110ad1b9972be
Session ID Length: 32
Session ID: cc308a908aefef9ac90ab37ac0e0b8eafdc6f14aa9ba26a9e7a56e26a
Cipher Suites Length: 32
  Cipher Suites (16 suites)
    Cipher Suite: Reserved (GREASE) (0x1a1a)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
  
```

and for server it's also different because for user it's new session but not recovering a previous session to be the same number.

No.	Time	Source	Destination	Protocol	Length	Info
20	6.565122	20.229.207.126	192.168.8.107	TLSv1.2	352	Application Data
22	7.589368	192.168.8.107	20.229.207.126	TLSv1.2	229	Application Data
48	14.294341	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
51	14.401532	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
52	14.467232	52.169.117.24	192.168.8.107	TCP	1454	443 → 59067 [ACK] Seq=1 Ack=518 Win=4193792 Len=1400
58	14.472932	52.169.117.24	192.168.8.107	TLSv1.2	431	Server Hello, Certificate, Certificate Status, Server
59	14.487538	192.168.8.107	52.169.117.24	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60	14.489608	192.168.8.107	52.169.117.24	TLSv1.2	153	Application Data
61	14.491364	192.168.8.107	52.169.117.24	TLSv1.2	1317	Application Data
62	14.492000	192.168.8.107	52.169.117.24	TLSv1.2	161	Application Data

```

Version: TLS 1.2 (0x0303)
Random: 63e18010d3b65e9b0f4ea7b87e7fc91c94afe95a5d2fea80a4825dafa77c1
  GMT Unix Time: Feb 7, 2023 01:32:48.000000000 Arab Standard Time
  Random Bytes: d3b65e9b0f4ea7b87e7fc91c94afe95a5d2fea80a4825dafa77c1
Session ID Length: 32
Session ID: b31e00092d32b8e0bea16906e8609b6ee4f6e77150863a25b1aaec8
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Compression Method: null (0)
Extensions Length: 22
  Extension: status_request (len=0)
  Extension: application_layer_protocol_negotiation (len=5)
  
```

Frame (431 bytes) Reassembled TCP (5977 bytes)

8. Is the Random number the same from Server Hello? Why?

number is different and why it must be different because later will use this number to generate the key for encryption, by this we approve the message is refresh and the attacker cannot take it and prevent replay attack.

No.	Time	Source	Destination	Protocol	Length	Info
20	6.565122	20.229.207.126	192.168.8.107	TLSv1.2	352	Application Data
22	7.589368	192.168.8.107	20.229.207.126	TLSv1.2	229	Application Data
48	14.294341	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
51	14.401532	192.168.8.107	52.169.117.24	TLSv1.2	571	Client Hello
52	14.467232	52.169.117.24	192.168.8.107	TCP	1454	443 → 59067 [ACK] Seq=1 Ack=518 Win=4193792 Len=1400
58	14.472932	52.169.117.24	192.168.8.107	TLSv1.2	431	Server Hello, Certificate, Certificate Status, Server
59	14.487538	192.168.8.107	52.169.117.24	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60	14.489608	192.168.8.107	52.169.117.24	TLSv1.2	153	Application Data
61	14.491364	192.168.8.107	52.169.117.24	TLSv1.2	1317	Application Data
62	14.492000	192.168.8.107	52.169.117.24	TLSv1.2	161	Application Data

```

Version: TLS 1.2 (0x0303)
Random: 63e18010d3b65e9b0f4ea7b87e7fc91c94afe95a5d2fea80a4825dafa77c1
  GMT Unix Time: Feb 7, 2023 01:32:48.000000000 Arab Standard Time
  Random Bytes: d3b65e9b0f4ea7b87e7fc91c94afe95a5d2fea80a4825dafa77c1
Session ID Length: 32
Session ID: b31e00092d32b8e0bea16906e8609b6ee4f6e77150863a25b1aaec8
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Compression Method: null (0)
Extensions Length: 22
  Extension: status_request (len=0)
  Extension: application_layer_protocol_negotiation (len=5)
  
```

Frame (431 bytes) Reassembled TCP (5977 bytes)

9. Is there a certificate packet between KKU and your browser? Why ?

Yes, to approve the identity of the user that visit the site
Also, to let the user felt safe while visiting the website

No.	Time	Source	Destination	Protocol	Length	Info
< 20. 6. 561461	20. 6. 561461	20. 6. 561461	100. 102. 0. 107	TLSv1.2	451	Client Hello
10 0.181461	2a02:cb80:403b:552d...	2606:4700:10::6816:...	TLSv1.2	451	Client Hello	Version: TLS 1.2 (0x0303) Length: 5972
12 0.280314	2606:4700:10::6816:...	2a02:cb80:403b:552d...	TLSv1.2	189	Server Hello, Change Cipher Spec, Encrypted Handshake	Handshake Protocol: Server Hello
13 0.286413	2a02:cb80:403b:552d...	2606:4700:10::6816:...	TLSv1.2	654	Change Cipher Spec, Encrypted Handshake Message, Application Data	Handshake Protocol: Certificate
15 0.415050	2a02:cb80:403b:552d...	2606:4700:10::6816:...	TLSv1.2	963	Application Data	Handshake Type: Certificate (11) Length: 3752 Certificates Length: 3749 > Certificates (3749 bytes)
						0060 00 00 ff 01 00 01 00 0b 00 0e a8 00 0e a5 0070 a8 30 82 08 a4 30 82 06 8c a0 03 02 01 02 0080 33 00 4b 6e 86 48 d3 6f b4 f7 1c 37 7f 00 0090 4b 6e 86 30 0d 06 09 2a 86 48 86 f7 0d 01 00a0 05 00 30 59 31 0b 30 09 06 03 55 04 06 13 00b0 53 31 1e 30 1c 06 03 55 04 0a 13 15 4d 69 00c0 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 00d0 6e 31 2a 30 28 06 03 55 04 03 13 21 4d 69 00e0 6f 73 6f 66 74 20 41 7a 75 72 65 20 54 4c 00f0 49 73 73 75 69 6e 67 28 43 41 20 30 36 30 0100 0d 32 32 30 39 30 32 31 33 30 38 32 32 5a 0110 32 33 30 38 32 38 31 33 30 38 32 32 5a 30 0120 0b 30 09 06 03 55 04 06 13 02 55 53 31 0b 0130 06 03 55 04 08 13 02 57 41 31 10 30 0e 06 0140 04 07 13 07 52 65 64 6d 6f 6e 64 31 1e 30 0150 03 55 04 0a 13 15 4d 69 63 72 6f 73 6f 66 0160 43 6f 72 70 6f 72 61 74 69 6f 6e 31 1b 30 0170 03 55 04 03 13 12 70 72 65 73 65 6e 63 65 0180 6b 79 70 65 2e 63 6f 6d 30 82 01 22 30 0d 0190 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 01a0 30 82 01 0a 02 82 01 01 00 e1 99 35 a2 4d 01b0 4d 56 98 d9 59 81 f6 73 7a d8 bc c2 e2 24 01c0 df e2 a6 28 9a 99 7b 35 12 3c 1d 70 07 8f
						Frame (431 bytes) Reassembled TCP (5977 bytes)

10. Inspect Change cipher spec, do you see the contents of the message? If not, why ?
No , because the message is encrypted

No.	Time	Source	Destination	Protocol	Length	Info
< 10 0.181461	2a02:cb80:403b:552d...	2606:4700:10::6816:...	TLSv1.2	451	Client Hello	
12 0.280314	2606:4700:10::6816:...	2a02:cb80:403b:552d...	TLSv1.2	189	Server Hello, Change Cipher Spec, Encrypted Handshake	Handshake Protocol: Server Hello
13 0.286413	2a02:cb80:403b:552d...	2606:4700:10::6816:...	TLSv1.2	654	Change Cipher Spec, Encrypted Handshake Message, Application Data	Handshake Protocol: Certificate
15 0.415050	2a02:cb80:403b:552d...	2606:4700:10::6816:...	TLSv1.2	963	Application Data	Handshake Type: Certificate (11) Length: 3752 Certificates Length: 3749 > Certificates (3749 bytes)
						0000 3c fa 43 1a 30 6a 24 ee 9a 85 63 ee 86 dd 0010 48 68 02 58 06 40 2a 02 cb 80 40 3b 55 2d 0020 6f 30 1c 58 87 c8 26 06 47 00 00 10 00 00 0030 00 00 68 16 01 eb d5 26 01 bb ad b6 fd af 0040 45 93 50 18 01 03 f1 38 00 00 14 03 03 00 0050 16 03 03 00 28 00 00 00 00 00 00 00 00 00 d5 0060 c4 23 90 1d 00 6b de 8f 46 33 1a f2 46 7c 0070 52 99 18 f4 a7 17 cf 6c f2 11 b5 cb 9f 17 0080 02 0c 00 00 00 00 00 00 00 01 85 dd 52 8b 0090 b0 6c 4d 8d 7a fe a7 a3 77 ca ae 0b 19 54 00a0 05 ab f5 58 34 d2 a0 8e 39 4b 16 63 a1 60 00b0 11 67 d6 1c c6 f9 eb 14 b9 54 5a 63 49 68 00c0 ee ff df 62 79 1a 23 d1 c8 cf 3b 0c e2 85 00d0 d0 cc 67 42 83 11 77 40 46 0d b3 11 6b 13 00e0 e5 84 b1 e2 37 c0 a3 3c bf ce b8 2d 69 00f0 b5 a5 c5 59 57 ac bb b3 39 dc c1 a3 33 98 0100 8a 13 28 3f b8 73 58 77 29 8f b0 8c 76 04 0110 ed 8a 5c e5 4e 06 c9 5e 6c ae 84 2c d2 0d 0120 fa 86 a7 d7 b1 0b 3e cd 89 72 4d cb 65 70 0130 91 4b 86 fe 8c fd 9f eb c4 7c 93 8f f6 49 0140 b5 f0 52 9c 6c 44 b9 76 86 1b a2 77 d4 25
						Frame (431 bytes) Reassembled TCP (5977 bytes)

11. Open any other website (https) and show the certificate of the website and explain its contents captured by Wireshark (BLACKBOARD)

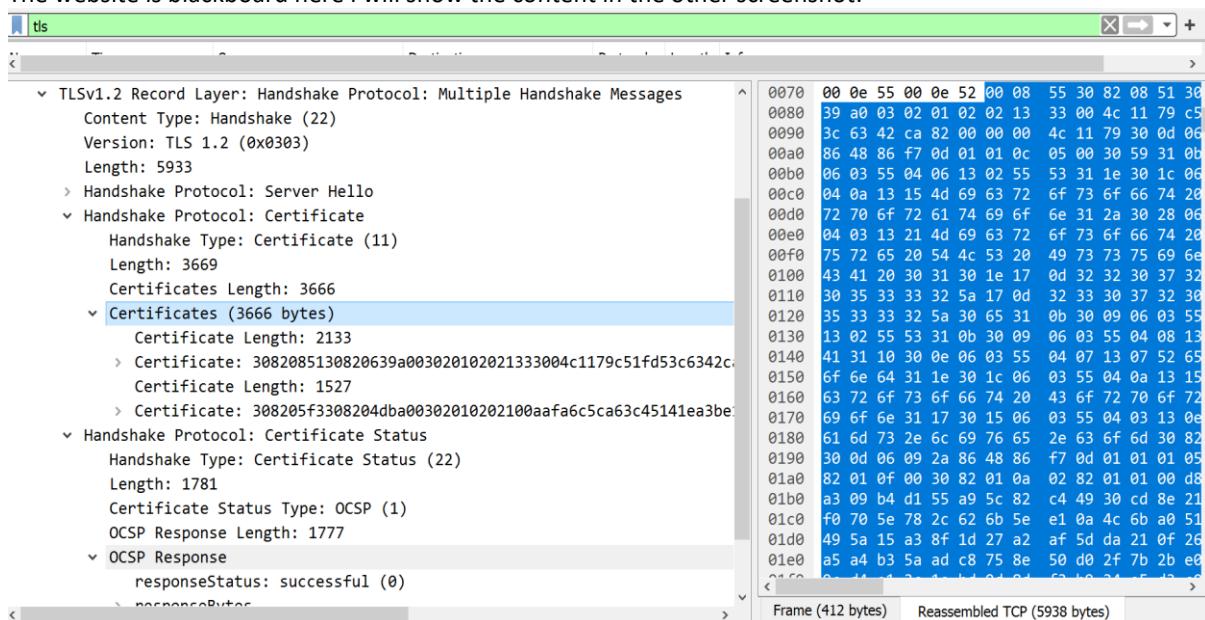
```
Command Prompt
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\shama>nslookup myso.kku.edu.sa
Server: Unknown
Address: fe80::3efa:43ff:fe1a:306a

Non-authoritative answer:
Name: myso.kku.edu.sa
Address: 212.26.68.247

C:\Users\shama>
```

The website is blackboard here I will show the content in the other screenshot:



3 . Building a simple Firewall on the client machine :

1-Change the Default Chain Policies to Drop

```
[02/07/23]seed@VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT    tcp  --  anywhere        anywhere         tcp dpt:https
ACCEPT    tcp  --  anywhere        anywhere         tcp dpt:http
ACCEPT    tcp  --  anywhere        anywhere         tcp dpt:https
ACCEPT    tcp  --  anywhere        anywhere         tcp dpt:http

Chain FORWARD (policy DROP)
target     prot opt source          destination
DOCKER-USER  all  --  anywhere      anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere      anywhere
ACCEPT    all  --  anywhere        anywhere        ctstate RELATED,ESTABLISHED
DOCKER    all  --  anywhere        anywhere
ACCEPT    all  --  anywhere        anywhere
ACCEPT    all  --  anywhere        anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT    tcp  --  anywhere        anywhere

Chain DOCKER (1 references)
target     prot opt source          destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source          destination
DOCKER-ISOLATION-STAGE-2  all  --  anywhere      anywhere
RETURN    all  --  anywhere        anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
[02/07/23]seed@VM:~$ RETURN    all  --  anywhere        anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source          destination
DROP     all  --  anywhere        anywhere
RETURN    all  --  anywhere        anywhere

Chain DOCKER-USER (1 references)
target     prot opt source          destination
RETURN    all  --  anywhere        anywhere
[02/07/23]seed@VM:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
[02/07/23]seed@VM:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
[02/07/23]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -j ACCEPT
[02/07/23]seed@VM:~$ sudo iptables -A INPUT -i lo -j ACCEPT
[02/07/23]seed@VM:~$ sudo iptables -P INPUT DROP
[02/07/23]seed@VM:~$ sudo iptables -P OUTPUT DROP
[02/07/23]seed@VM:~$ sudo iptables -P FORWARD DROP
iptables: Bad built-in chain name.
[02/07/23]seed@VM:~$ sudo iptables -P FORWARD DROP
[02/07/23]seed@VM:~$ sudo iptables -F
[02/07/23]seed@VM:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source          destination

Chain FORWARD (policy DROP)
target     prot opt source          destination

Chain OUTPUT (policy DROP)
target     prot opt source          destination
```

Allow forwarding of TCP traffic on IP interface 10.0.1.2 (client) port 80 (HTTP) and port 443 (HTTPS) to go to 192.168.23.10

```
[02/07/23]seed@VM:~$ sudo iptables -A INPUT -s 192.168.23.10 -j ACCEPT  
[02/07/23]seed@VM:~$ sudo iptables -A INPUT -s 10.0.1.2 -j ACCEPT  
[02/07/23]seed@VM:~$ S
```

```
[02/07/23]seed@VM:~$ telnet 10.0.1.2  
Trying 10.0.1.2...  
telnet: Unable to connect to remote host: Connection timed out  
[02/07/23]seed@VM:~$ wget 10.0.1.2  
--2023-02-07 07:51:38-- http://10.0.1.2/  
Connecting to 10.0.1.2:80... failed: Connection timed out.  
Retrying.  
--2023-02-07 07:53:49-- (try: 2) http://10.0.1.2/  
Connecting to 10.0.1.2:80... failed: Connection timed out.  
Retrying.
```

```
--2023-02-07 07:56:01-- (try: 3) http://10.0.1.2/  
Connecting to 10.0.1.2:80... failed: Connection timed out.
```

```
[02/07/23]seed@VM:~$ ssh 10.0.1.2
```

```
ssh: connect to host 10.0.1.2 port 22: Connection timed out
```

```
[02/07/23]seed@VM:~$
```

```
[02/07/23]seed@VM:~$ S
```

```
[02/07/23]seed@VM:~$  
[02/07/23]seed@VM:~$ telnet 192.168.23.10  
Trying 192.168.23.10...  
telnet: Unable to connect to remote host: Connection timed out  
[02/07/23]seed@VM:~$ Wget 192.168.23.10
```

Command 'Wget' not found, did you mean:

```
command 'mget' from snap mget (0.1.2)  
command 'kget' from deb kget (4:19.12.3-0ubuntu1)  
command 'wget' from deb wget (1.20.3-1ubuntu1)  
command 'bget' from deb ax25-tools (0.0.10-rc4-3build1)  
command 'dget' from deb devscripts (2.20.2ubuntu2)  
command 'pget' from deb pbuilder-scripts (22)
```

See 'snap info <snapname>' for additional versions.

```
[02/07/23]seed@VM:~$ wget 192.168.23.10  
--2023-02-07 08:18:17-- http://192.168.23.10/  
Connecting to 192.168.23.10:80... failed: Connection timed out.  
Retrying.
```

```
--2023-02-07 08:20:29-- (try: 2) http://192.168.23.10/  
Connecting to 192.168.23.10:80... failed: Connection timed out.  
--2023-02-07 08:59:32-- (try:19) http://192.168.23.10/  
Connecting to 192.168.23.10:80... failed: Connection timed out.  
Retrying.
```

```
--2023-02-07 09:01:52-- (try:20) http://192.168.23.10/  
Connecting to 192.168.23.10:80... failed: Connection timed out.  
Giving up.
```

```
[02/07/23]seed@VM:~$ ssh 192.168.23.10  
ssh: connect to host 192.168.23.10 port 22: Connection timed out  
[02/07/23]seed@VM:~$
```

3-block a specific ip-address from reaching organization.

```
[02/07/23] seed@VM:~$  
[02/07/23] seed@VM:~$  
[02/07/23] seed@VM:~$  
[02/07/23] seed@VM:~$ sudo iptables -A INPUT -s 10.0.2.15 -j DROP  
[02/07/23] seed@VM:~$
```

4-Allow Incoming HTTP and HTTPS

To allow HTTP Web traffic:

```
[02/07/23] seed@VM:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
[02/07/23] seed@VM:~$
```

To allow HTTPS Internet traffic:

```
[02/07/23] seed@VM:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT  
[02/07/23] seed@VM:~$  
[02/07/23] seed@VM:~$
```

5-Allow outbound DNS.

```
[02/07/23] seed@VM:~$ sudo iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT  
[02/07/23] seed@VM:~$ sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT  
[02/07/23] seed@VM:~$ sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT  
[02/07/23] seed@VM:~$ sudo iptables -A OUTPUT -p udp --dport 53 -j ACCEPT  
[02/07/23] seed@VM:~$
```

DNS connections are made to a remote host on port 53 using the UDP protocol with a fall back to TCP if the answer is too large for a UDP datagram.

DONE

NAMES:

ID

SHAMAM ALKAFRI	441813693
RAZAN AHMAD	441808325
FAYROUZ ASIRI	439803568