

(1) Analyse TCP packets using the pcap file attached.demo file.pcapng  
Download demo file.pcapng

(2) Develop your own sniffer using PCAP API and filter out TCP packets.Sniff  
-1.c.txt Download Sniff -1.c.txt

(3) Make at report for TCL pcap sniff analysis

#### A) To Analyze TCP packets using the pcap file attached.

A TCP protocol works as a transport layer in the OSI model; it works as transport. For example, we have a car that works as data transfer; the data from one place to another, and the TCP works the same. The item of the application layer transfers from destination and source by transport protocol; also, it is a connection protocol, which means before the transfer of data, it will establish some connection between source and destination.

Before understanding the Pcap(Picture Capture ) file, lets understand what a wire shark is. A wire shark is a packet sniffing tool that captures and sees the packet in the network between sender and receiver by sniffing, which protocol is used, its length, and what type of message is sent.

SEED [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities WireShark Jan 20 12:10 [SEED Labs] demo file.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-01-11 10:2...	192.168.43.121	192.168.43.1	DNS	78	Standard query 0x4ef6 A capi.grammarly.com
2	2024-01-11 10:2...	192.168.43.121	192.168.43.1	DNS	78	Standard query 0xf0b4 AAAA capi.grammarly.com
3	2024-01-11 10:2...	192.168.43.1	192.168.43.121	DNS	343	Standard query response 0x4ef6 A capi.grammarly.com A 54.205...
4	2024-01-11 10:2...	192.168.43.1	192.168.43.121	DNS	156	Standard query response 0xf0b4 AAAA capi.grammarly.com SOA ns...
5	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	66	22715 → 443 [SYN] Seq=1324022242 Win=64240 Len=0 MSS=1460 WS=...
6	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	66	443 → 22715 [SYN, ACK] Seq=215212137 Ack=1324022243 Win=26883...
7	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	54	22715 → 443 [ACK] Seq=1324022243 Ack=215212138 Win=131072 Len...
8	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	371	Client Hello
9	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Server Hello
10	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	1354	443 → 22715 [ACK] Seq=215213438 Ack=1324022560 Win=28160 Len=...
11	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	54	22715 → 443 [ACK] Seq=1324022560 Ack=215214738 Win=131072 Len=...
12	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	1354	443 → 22715 [ACK] Seq=215214738 Ack=1324022560 Win=28160 Len=...
13	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF-{83C0C01B-9E7F-44E4-A948-33DB64C7F42B}, id 0

Ethernet II, Src: HonHaiPr\_9a:49:b5 (54:35:30:9a:49:b5), Dst: 3e:f6:32:93:9c:27 (3e:f6:32:93:9c:27)

Internet Protocol Version 4, Src: 192.168.43.121, Dst: 192.168.43.1

User Datagram Protocol, Src Port: 49216, Dst Port: 53

Domain Name System (query)

0000 3e f6 32 93 9c 27 54 35 30 9a 49 b5 08 00 45 00 > 2...T5 0 I...E.

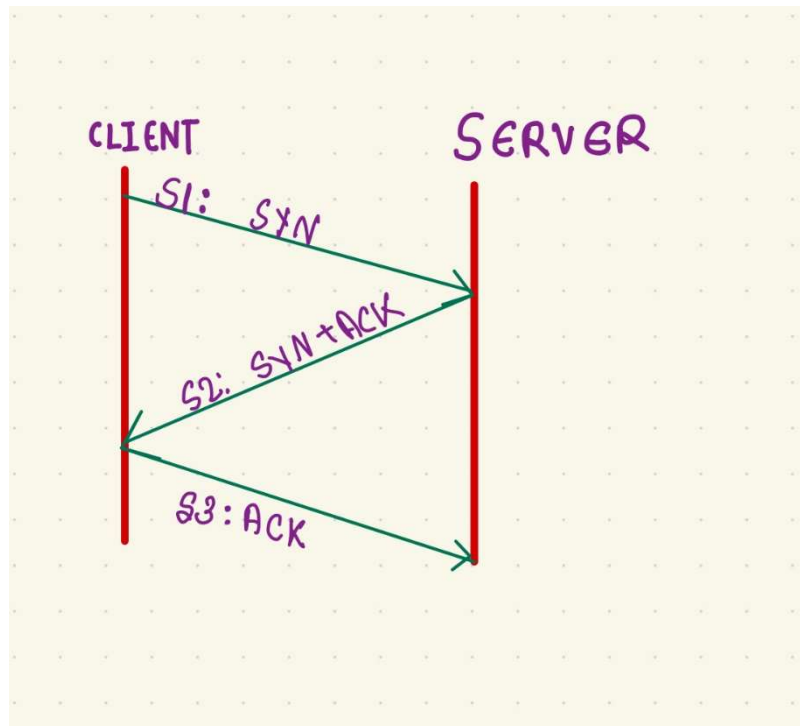
0010 00 40 ed 40 00 00 80 11 75 a1 c0 a8 2b 79 c0 a8 @ @... u...+y..

0020 2b 01 c0 40 00 35 00 2c 56 5e 4e f6 01 00 00 01 +- @ 5, vAN... ..

0030 00 00 00 00 00 04 63 61 70 69 09 67 72 61 6d .....c api gram

0040 6d 61 72 6c 79 03 63 6f 6d 00 00 01 00 01 marly.co m.....

In this window we have seen at top we will be able to see the type, source, destination, length and information of packets that are being transferred. After going to the first TCP packet we have seen multiple things such as Internet Protocol, Ethernet, frame number and details of its TCP protocol.



In the TCP protocol, the initial connection establishment involves three steps, as illustrated in the diagram above. Additionally, we are examining this process in Wireshark, with the corresponding image provided below.

### S1: SYN: Initiating Connection

The client triggers the connection initiation process by dispatching a SYN packet, signifying its desire to establish a connection. The TCP segment length of 0 suggests that this pertains to the preliminary handshake stage, with no data exchange occurring at this point.

In attached we can see that **the SYN is set but ACK is not set** that means first step for connection establishment is done.

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-01-11 10:2...	192.168.43.121	192.168.43.1	DNS	78	Standard query 0x4ef6 A capi.grammarly.com
2	2024-01-11 10:2...	192.168.43.121	192.168.43.1	DNS	78	Standard query 0xf0b4 AAAA capi.grammarly.com
3	2024-01-11 10:2...	192.168.43.1	192.168.43.121	DNS	343	Standard query response 0x4ef6 A capi.grammarly.com A 54.205...
4	2024-01-11 10:2...	192.168.43.1	192.168.43.121	DNS	156	Standard query response 0xf0b4 AAAA capi.grammarly.com SOA ns...
5	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	66	22715 → 443 [SYN] Seq=1324022242 Win=64240 Len=0 MSS=1460 WS=...
6	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	66	443 → 22715 [SYN, ACK] Seq=215212137 Ack=1324022243 Win=26883...
7	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	54	22715 → 443 [ACK] Seq=1324022243 Ack=215212138 Win=131072 Len...
8	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	371	Client Hello
9	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Server Hello
10	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	1354	443 → 22715 [ACK] Seq=215213438 Ack=1324022560 Win=28160 Len=...
11	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	54	22715 → 443 [ACK] Seq=1324022560 Ack=215214738 Win=131072 Len...
12	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	1354	443 → 22715 [ACK] Seq=215214738 Ack=1324022560 Win=28160 Len=...
13	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]

▶ Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{83C0C01B-9E7F-44E4-A948-33DB64C7F42B}, id 0  
 ▶ Ethernet II, Src: HonHaiPr\_9a:49:b5 (54:35:30:9a:49:b5), Dst: 3e:f6:32:93:9c:27 (3e:f6:32:93:9c:27)  
 ▶ Internet Protocol Version 4, Src: 192.168.43.121, Dst: 54.205.188.156  
 ▶ Transmission Control Protocol, Src Port: 22715, Dst Port: 443, Seq: 1324022242, Len: 0

Source Port: 22715  
 Destination Port: 443  
 [Stream index: 0]  
 [TCP Segment Len: 0]  
 Sequence number: 1324022242  
 [Next sequence number: 1324022243]  
 Acknowledgment number: 0  
 Acknowledgment number (raw): 0  
 1000 .... = Header Length: 32 bytes (8)  
 ▶ Flags: 0x002 (SYN)

000. .... = Reserved: Not set  
 ...0 .... = Nonce: Not set  
 ....0 .... = Congestion Window Reduced (CWR): Not set  
 ....0 .... = ECN-Echo: Not set  
 ....0 .... = Urgent: Not set  
 ....0 .... = Acknowledgment: Not set  
 ....0 .... = Push: Not set  
 ....0 .... = Reset: Not set  
 ▶ ....1 .... = Syn: Set  
 0 = Fin: Not set

0000 3e f6 32 93 9c 27 54 35 30 9a 49 b5 08 00 45 00 >...T5 0-I...E-  
 0010 00 34 4b 91 40 00 80 06 cf a7 c0 a8 2b 79 36 cd -4K@... ..+y6-  
 0020 bc 9c 58 bb 01 bb 4e ea f9 e2 00 00 00 00 80 02 --X...N.....  
 0030 fa f0 f1 50 00 00 02 04 05 b4 01 03 03 08 01 01 .P.....

## S2: SYN-ACK: Acknowledging Connection Request

The server acknowledges the client's SYN packet by responding with a SYN-ACK packet, signifying the acknowledgment of synchronization. The flags in the packet indicate that both SYN and ACK are set, confirming the successful establishment of the connection.

Also, in below snap shot we can see that **SYN and ACK both flags are set** that means step 2 of connection establishment.

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-01-11 10:2...	192.168.43.121	192.168.43.1	DNS	78	Standard query 0x4ef6 A capi.grammarly.com
2	2024-01-11 10:2...	192.168.43.121	192.168.43.1	DNS	78	Standard query 0xf0b4 AAAA capi.grammarly.com
3	2024-01-11 10:2...	192.168.43.1	192.168.43.121	DNS	343	Standard query response 0x4ef6 A capi.grammarly.com A 54.205...
4	2024-01-11 10:2...	192.168.43.1	192.168.43.121	DNS	156	Standard query response 0xf0b4 AAAA capi.grammarly.com SOA ns...
5	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	66	22715 → 443 [SYN] Seq=1324022242 Win=64240 Len=0 MSS=1460 WS=...
6	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	66	443 → 22715 [SYN, ACK] Seq=215212137 Ack=1324022243 Win=26883...
7	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	54	22715 → 443 [ACK] Seq=1324022243 Ack=215212138 Win=131072 Len...
8	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	371	Client Hello
9	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Server Hello
10	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	1354	443 → 22715 [ACK] Seq=215213438 Ack=1324022560 Win=28160 Len=...
11	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TCP	54	22715 → 443 [ACK] Seq=1324022560 Ack=215214738 Win=131072 Len...
12	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TCP	1354	443 → 22715 [ACK] Seq=215214738 Ack=1324022560 Win=28160 Len=...
13	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]

▶ Internet Protocol Version 4, Src: 54.205.188.156, Dst: 192.168.43.121  
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 22715, Seq: 215212137, Ack: 1324022243, Len: 0

Source Port: 443  
 Destination Port: 22715  
 [Stream index: 0]  
 [TCP Segment Len: 0]  
 Sequence number: 215212137  
 [Next sequence number: 215212138]  
 Acknowledgment number: 1324022243  
 1000 .... = Header Length: 32 bytes (8)  
 ▶ Flags: 0x012 (SYN, ACK)

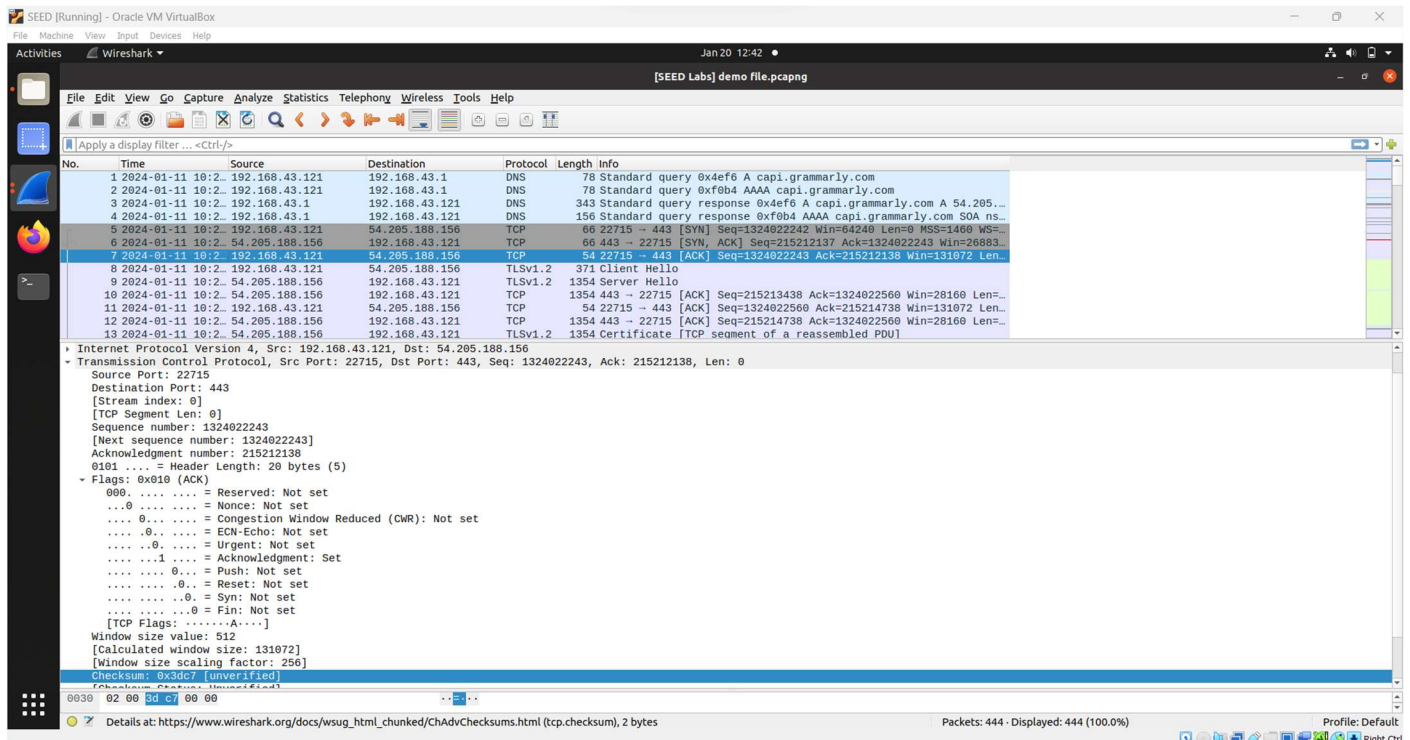
000. .... = Reserved: Not set  
 ...0 .... = Nonce: Not set  
 ....0 .... = Congestion Window Reduced (CWR): Not set  
 ....0 .... = ECN-Echo: Not set  
 ....0 .... = Urgent: Not set  
 ....1 .... = Acknowledgment: Set  
 ....0 .... = Push: Not set  
 ....0 .... = Reset: Not set  
 ▶ ....1 .... = Syn: Set  
 0 = Fin: Not set  
 [TCP Flags: .....A..S]  
 Window size value: 26883  
 [Calculated window size: 26883]  
 Checksum: 0x9690 [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0

0000 54 35 30 9a 49 b5 3e f6 32 93 9c 27 08 00 45 00 T50-I-> 2...E-

## S3: ACK: Completing Connection Establishment

The client, upon receiving the SYN-ACK packet from the server, responds with a TCP packet containing the ACK flag set. This ACK packet serves as confirmation to the server that the client has received the acknowledgment, and both ends are now synchronized. The TCP segment length remains at 0, indicating that this is an acknowledgment without any data exchange at this stage.

Also in snapshot attached below **SYN flag is not set while ACK flag is set**



The three-way handshake is like a conversation between a client and a server when they want to connect. First, the client starts the conversation by asking to connect. Then, the server responds, saying it's ready to connect. Finally, the client confirms that it got the message from the server. This whole process ensures that the client and server are on the same page and ready to share information in a reliable and coordinated way before any actual data is sent between them.

## B) Develop your own sniffer using PCAP API and filter out TCP packets.

```
#include <stdlib.h>
#include <stdio.h>
#include <pcap.h>
void got_packet(u_char *args, const struct pcap_pkthdr *header, const u_char *packet)
{
    printf("Got a new packet\n");
}
int main()
{
    pcap_t *handle;
    char errbuf[PCAP_ERRBUF_SIZE];
    struct bpf_program fp;
    char filter_exp[] = "tcp";
    bpf_u_int32 net;
```

$$\}$$



































**C) Make at report for TCL pcap sniff analysis using the questionnaire.**



1. For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.

The image displays a Wireshark packet capture analysis of a TLS handshake. The top pane shows a list of packets, with packet 8 selected. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
8	2024-01-11 10:11:20.2	192.168.43.121	54.205.188.156	TLSv1.2	371	Client Hello
9	2024-01-11 10:11:20.2	54.205.188.156	192.168.43.121	TLSv1.2	1354	Server Hello
13	2024-01-11 10:11:20.2	54.205.188.156	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]
14	2024-01-11 10:11:20.2	54.205.188.156	192.168.43.121	TLSv1.2	287	Server Key Exchange, Server Hello Done
16	2024-01-11 10:11:20.2	192.168.43.121	54.205.188.156	TLSv1.2	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
18	2024-01-11 10:11:20.2	54.205.188.156	192.168.43.121	TLSv1.2	225	New Session Ticket, Change Cipher Spec, Encrypted Handshake A.
19	2024-01-11 10:11:20.2	192.168.43.121	54.205.188.156	TLSv1.2	981	Application Data
20	2024-01-11 10:11:20.2	54.205.188.156	192.168.43.121	TLSv1.2	1184	Application Data
22	2024-01-11 10:11:20.2	192.168.43.121	54.205.188.156	TLSv1.2	825	Application Data
23	2024-01-11 10:11:20.2	54.205.188.156	192.168.43.121	TLSv1.2	382	Application Data
36	2024-01-11 10:11:20.2	192.168.43.121	23.211.135.143	TLSv1.2	235	Client Hello
38	2024-01-11 10:11:20.2	23.211.135.143	192.168.43.121	TLSv1.2	1354	Server Hello
39	2024-01-11 10:11:20.2	23.211.135.143	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]

**Packet 8 Details:**

- Ethernet II, Src: RealtekPciB0:49:05 (54:35:30:04:49:05), Dst: 3e:f6:32:93:9c:27 (3e:f6:32:93:9c:27)**
- Internet Protocol Version 4, Src: 192.168.43.121, Dst: 54.205.188.156**
- Transmission Control Protocol, Src Port: 22715, Dst Port: 443, Seq: 1324822243, Ack: 215212138, Len: 317**
  - Source Port: 22715
  - Destination Port: 443
  - Stream index: 0
  - [TCP Segment Len: 317]
  - Sequence number: 1324822243
  - [Next sequence number: 1324822560]
  - Acknowledgment number: 215212138
  - 0101 .... = Header Length: 20 bytes (5)
  - Flags: 0x018 (PSH, ACK)
  - Window size value: 512
  - [Calculated window size: 131072]
  - [Window size scaling factor: 256]
  - Checksum: 0xf531 [unverified]
  - [Checksum Status: Unverified]
  - Urgent pointer: 0
- TLSv1.2 Record Layer: Handshake Protocol: Client Hello**
  - Content Type: Handshake (22)

**Raw Data:**

```

0000  02 00 f5 31 00 00 00 03 03 01 20 01 00 01 34 03  ...1...R...4...
0008  03 05 40 09 32 09 03 00 0c 0f 50 f6 f1 52 12 e4  ...2...R...
0016  bf be 11 92 35 90 7f 91 ee e3 6b c2 8c e4 30 bd  ...3...k...0...
  
```

Frame	Source	Destination	Info/Type
8	192.168.43.121	54.205.188.156	Client Hello
9	54.205.188.156	192.168.43.121	Server Hello
13	54.205.188.156	192.168.43.121	Certificte
14	54.205.188.156	192.168.43.121	Server Hello Done
			Client Key
16	192.168.43.121	54.205.188.156	Exchange
18	54.205.188.156	192.168.43.121	Change Cipher Spec
19	192.168.43.121	54.205.188.156	Application Data
20	54.205.188.156	192.168.43.121	Application Data

- 2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.**

- Content Type: 1 byte
- Version: 2 bytes
- Length: 2 bytes

[SEED Labs] demo file.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: ssl

No.	Time	Source	Destination	Protocol	Length	Info
8	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	371	Client Hello
9	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Server Hello
13	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]
14	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	287	Server Key Exchange, Server Hello Done
16	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
18	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	225	New Session Ticket, Change Cipher Spec, Encrypted Handshake M...
19	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	981	Application Data
20	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1164	Application Data
22	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	825	Application Data
23	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	362	Application Data
36	2024-01-11 10:2...	192.168.43.121	23.211.135.143	TLSv1.2	235	Client Hello
38	2024-01-11 10:2...	23.211.135.143	192.168.43.121	TLSv1.2	1354	Server Hello
39	2024-01-11 10:2...	23.211.135.143	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]

▶ Frame 16: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF\_{83C8C81B-9E7F-44E4-A948-33DB64C7F42B}, id 0  
 ▶ Ethernet II, Src: HonHaiPr\_9a:49:b5 (54:35:30:9a:49:b5), Dst: 3e:f6:32:93:9c:27 (3e:f6:32:93:9c:27)  
 ▶ Internet Protocol Version 4, Src: 192.168.43.121, Dst: 54.205.188.156  
 ▶ Transmission Control Protocol, Src Port: 22715, Dst Port: 443, Seq: 1324022560, Ack: 215217571, Len: 126  
 ▶ Transport Layer Security  
   ▶ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 70  
     ▶ Handshake Protocol: Client Key Exchange  
       Handshake Type: Client Key Exchange (16)  
       Length: 66  
       ▶ EC Diffie-Hellman Client Params  
     ▶ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec  
       Content Type: Change Cipher Spec (20)  
       Version: TLS 1.2 (0x0303)  
       Length: 1  
       Change Cipher Spec Message  
     ▶ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message  
       Content Type: Handshake (22)  
       Version: TLS 1.2 (0x0303)  
       Length: 40  
       Handshake Protocol: Encrypted Handshake Message

0000 28 14 03 03 00 01 01 16 03 03 00 28 00 00 00 00 (.....)(....  
 0090 00 00 00 00 4d 68 17 86 81 94 3e e5 15 31 34 fb ...Mh...>..14..  
 00a0 1f d8 d9 3f 8e 11 7c bf c1 1c 41 ac c5 87 d9 27 ...?..|..A.....

Length of TLS record data (tls.record.length), 2 bytes

Packets: 444 · Displayed: 86 (19.4%)

## ClientHello Record:

3. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

[SEED Labs] demo file.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: ssl

No.	Time	Source	Destination	Protocol	Length	Info
8	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	371	Client Hello
9	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Server Hello
13	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]
14	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	287	Server Key Exchange, Server Hello Done
16	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake M...
18	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	225	New Session Ticket, Change Cipher Spec, Encrypted Handshake M...
19	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	981	Application Data
20	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	1164	Application Data
22	2024-01-11 10:2...	192.168.43.121	54.205.188.156	TLSv1.2	825	Application Data
23	2024-01-11 10:2...	54.205.188.156	192.168.43.121	TLSv1.2	362	Application Data
36	2024-01-11 10:2...	192.168.43.121	23.211.135.143	TLSv1.2	235	Client Hello
38	2024-01-11 10:2...	23.211.135.143	192.168.43.121	TLSv1.2	1354	Server Hello
39	2024-01-11 10:2...	23.211.135.143	192.168.43.121	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]

Internet Protocol Version 4, Src: 192.168.43.121, Dst: 54.205.188.156

Transmission Control Protocol, Src Port: 22715, Dst Port: 443, Seq: 1324922243, Ack: 215212138, Len: 317

Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 312

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 308

Version: TLS 1.2 (0x0303)

Random: 65a00932d9d800dc0fbbf8f15212e4bfbe119235b97f91ee...

GMT Unix Time: Jan 11, 2024 10:28:50.000000000 EST

Random Bytes: d9d800dc0fbbf8f15212e4bfbe119235b97f91ee36bc28c...

Session ID Length: 32

Session ID: 82bf4cc1b5105376d469ea8984fa40775c15f886cddfc2fa...

Cipher Suites Length: 42

Cipher Suites (21 suites)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009f)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009e)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)

0030 02 00 f5 31 00 00 10 03 03 01 38 01 00 01 34 03 ...1...8...4...

0040 03 05 a0 09 32 d9 d8 00 dc 0f bb f8 f1 52 12 e4 ...e...2...R...

0050 bf be 11 92 35 b9 7f 91 ee e3 6b c2 8c e4 36 bd ...5...k...6...

Content Type (tls.record.content\_type), 1 byte

Packets: 444 - Di

The content type is 22, for Handshake Message, with a handshake type: Client Hello

4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

5. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

- Public key algorithm: RSA
- Symmetric-key algorithm: RC4
- Hash algorithm: MD5

ServerHello Record:



**6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?**

- The cipher suite utilizes RSA for public key cryptography.
- RC4 is employed as the symmetric-key cipher in the suite.
- The MD5 hash algorithm is used within the cipher suite.

The image shows a Wireshark capture of an SSL/TLS handshake. The top pane displays a list of packets, with packet 9 (Server Hello) selected. The middle pane shows the details of the TLSv1.2 Record Layer, Handshake Protocol: Server Hello. The bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet 9: TLSv1.2 Record Layer: Handshake Protocol: Server Hello**

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 99
- Handshake Protocol: Server Hello
  - Handshake Type: Server Hello (2)
  - Length: 95
  - Version: TLS 1.2 (0x0303)
  - Random: ba8cfe50d0d5ff1cc9123fad798d5a7074fe3d328b685709...
  - Session ID Length: 32
  - Session ID: 5b5cba18b9ac5fc6e1ad55378db66d5b4ae6dbbcb107c999...
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
  - Compression Method: null (0)
  - Extensions Length: 23
    - Extension: server\_name (len=0)
    - Extension: ec\_point\_formats (len=2)
    - Extension: renegotiation\_info (len=1)
    - Extension: session\_ticket (len=0)
    - Extension: extended\_master\_secret (len=0)

**7. Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?**

- The record includes a nonce listed under "Random."
- The nonce is 32 bits long, with 28 bits for data and 4 bits for the time.
- The primary purpose of the nonce is to prevent a replay attack.

**8. Does this record include a session ID? What is the purpose of the session ID?**

It does offer a distinct and enduring identifier for the SSL session, which is transmitted without encryption.

**9. Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?**

There isn't a certificate; it's stored in a different record. It does fit within a sole Ethernet frame.