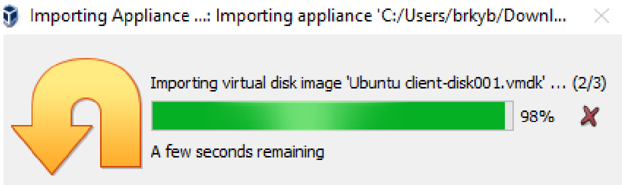
Environment configuration.

import virtual machine images.

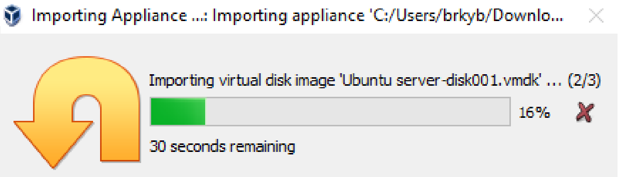


Importing Appliance ...: Importing appliance 'C:/Users/brkyb/Downl...

Importing virtual disk image 'Ubuntu client-disk001.vmdk' ... (2/3)

98%

A few seconds remaining



Importing Appliance ...: Importing appliance 'C:/Users/brkyb/Downlo...

Importing virtual disk image 'Ubuntu server-disk001.vmdk' ... (2/3)

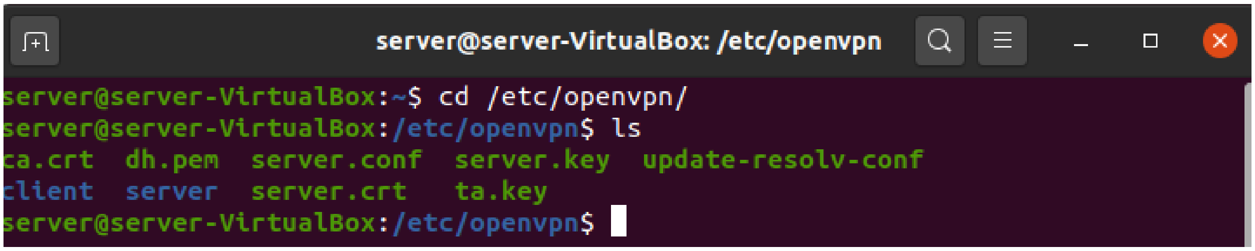
16%

30 seconds remaining

Server configuration:

1. Check if the configuration file exist in /etc/openvpn and see the content of server.conf.

2. There should be the following files in /etc/openvpn/:

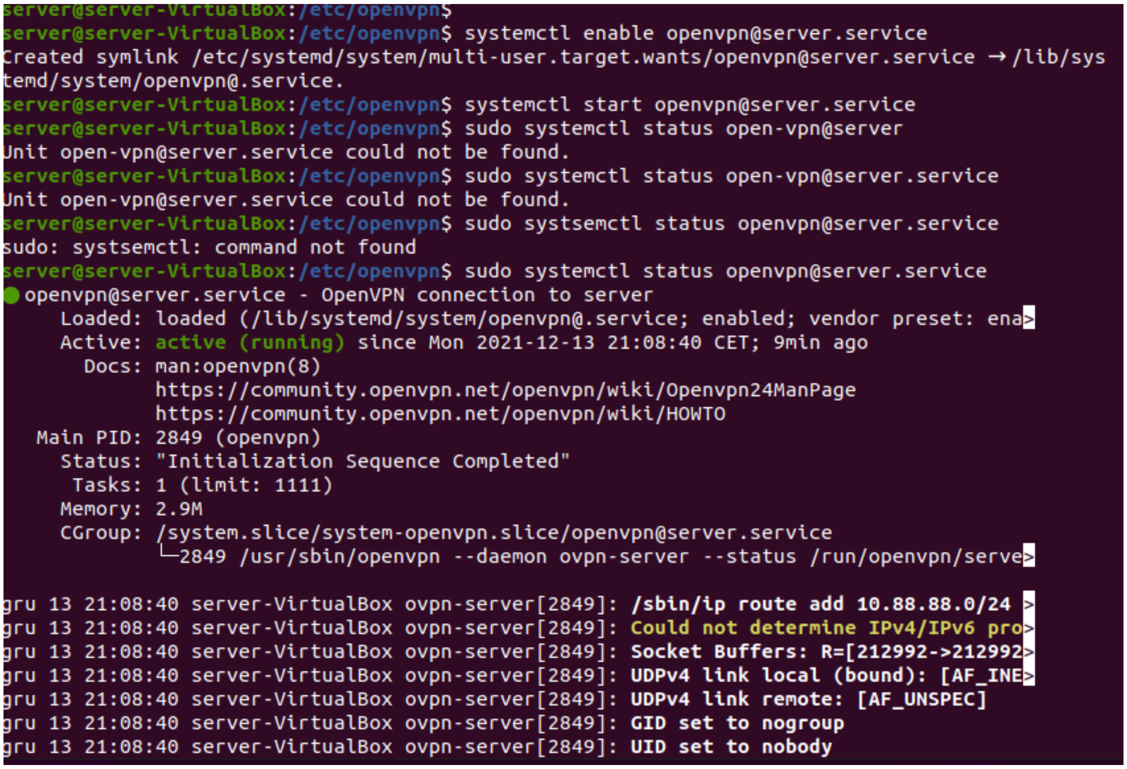


server@server-VirtualBox: /etc/openvpn

```
server@server-VirtualBox:~$ cd /etc/openvpn/
server@server-VirtualBox:/etc/openvpn$ ls
ca.crt  dh.pem  server.conf  server.key  update-resolv-conf
client  server  server.crt   ta.key
server@server-VirtualBox:/etc/openvpn$
```

In order to see the content of the file; used ls command.

3. To start the VPN server, run sudo systemctl start openvpn@server.service To check the status of the VPN service, type: sudo systemctl status openvpn@server



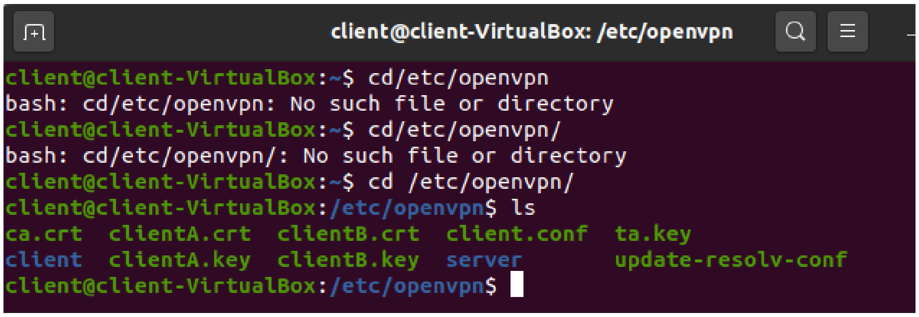
```
server@server-VirtualBox:/etc/openvpn$
server@server-VirtualBox:/etc/openvpn$ systemctl enable openvpn@server.service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn@server.service → /lib/sys
temd/system/openvpn@.service.
server@server-VirtualBox:/etc/openvpn$ systemctl start openvpn@server.service
server@server-VirtualBox:/etc/openvpn$ sudo systemctl status open-vpn@server
Unit open-vpn@server.service could not be found.
server@server-VirtualBox:/etc/openvpn$ sudo systemctl status open-vpn@server.service
Unit open-vpn@server.service could not be found.
server@server-VirtualBox:/etc/openvpn$ sudo systsemctl status openvpn@server.service
sudo: systsemctl: command not found
server@server-VirtualBox:/etc/openvpn$ sudo systemctl status openvpn@server.service
● openvpn@server.service - OpenVPN connection to server
     Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled; vendor preset: ena>
     Active: active (running) since Mon 2021-12-13 21:08:40 CET; 9min ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 2849 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 1111)
     Memory: 2.9M
     CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
             └─2849 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/serve>

gru 13 21:08:40 server-VirtualBox ovpn-server[2849]: /sbin/ip route add 10.88.88.0/24 >
gru 13 21:08:40 server-VirtualBox ovpn-server[2849]: Could not determine IPv4/IPv6 pro>
gru 13 21:08:40 server-VirtualBox ovpn-server[2849]: Socket Buffers: R=[212992->212992>
gru 13 21:08:40 server-VirtualBox ovpn-server[2849]: UDPv4 link local (bound): [AF_INE>
gru 13 21:08:40 server-VirtualBox ovpn-server[2849]: UDPv4 link remote: [AF_UNSPEC]
gru 13 21:08:40 server-VirtualBox ovpn-server[2849]: GID set to nogroup
gru 13 21:08:40 server-VirtualBox ovpn-server[2849]: UID set to nobody
```

Client’s configuration:

1. Check if the configuration file exist in /etc/openvpn and see the content of client.conf.

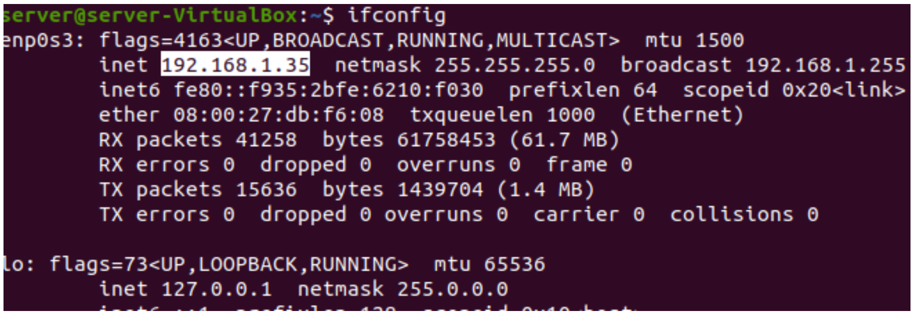
2. There should be the following files in /etc/openvpn/:   clientA.key and clientB.key – client key, • clientA.crt and clientB.crt – client certificate, • ta.key - HMAC signature – TLS authentication • client.conf – configuration file, • ca.crt – CA certificate,s



```
client@client-VirtualBox:~$ cd/etc/openvpn
bash: cd/etc/openvpn: No such file or directory
client@client-VirtualBox:~$ cd/etc/openvpn/
bash: cd/etc/openvpn/: No such file or directory
client@client-VirtualBox:~$ cd /etc/openvpn/
client@client-VirtualBox:/etc/openvpn$ ls
ca.crt  clientA.crt  clientB.crt  client.conf  ta.key
client  clientA.key  clientB.key  server       update-resolv-conf
client@client-VirtualBox:/etc/openvpn$ 
```

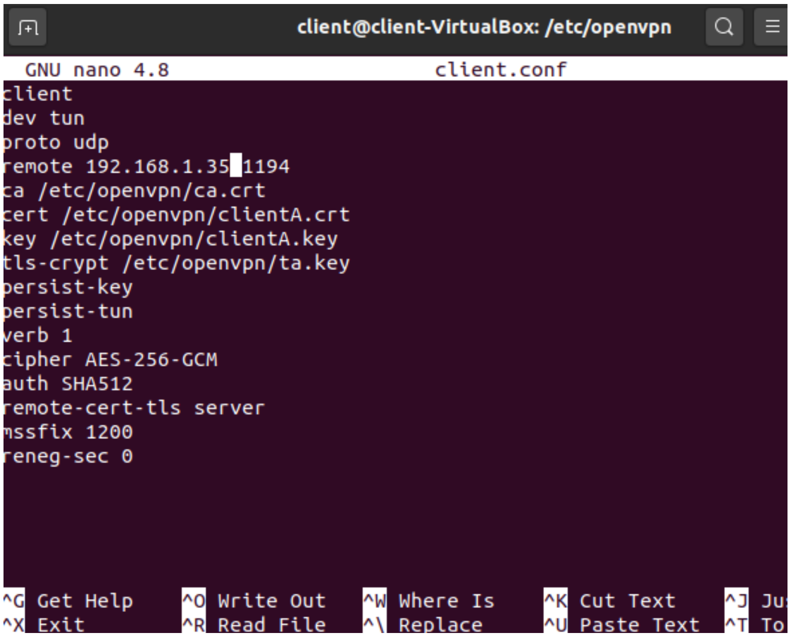
3. Adjust client.conf file.

Server inet;



```
server@server-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.35  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f935:2bfe:6210:f030  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:f6:08  txqueuelen 1000  (Ethernet)
        RX packets 41258  bytes 61758453 (61.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15636  bytes 1439704 (1.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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>
```

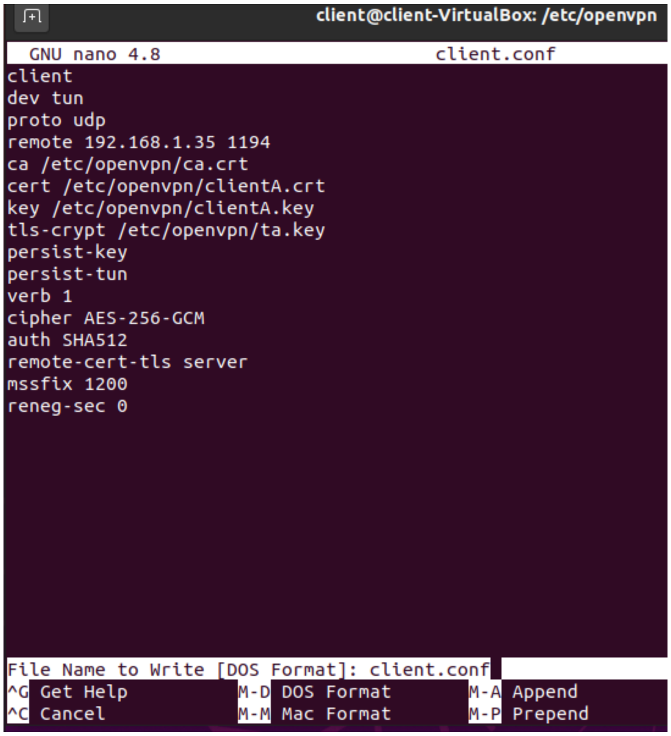


```
  GNU nano 4.8                         client.conf
client
dev tun
proto udp
remote 192.168.1.35 1194
ca /etc/openvpn/ca.crt
cert /etc/openvpn/clientA.crt
key /etc/openvpn/clientA.key
tls-crypt /etc/openvpn/ta.key
persist-key
persist-tun
verb 1
cipher AES-256-GCM
auth SHA512
remote-cert-tls server
mssfix 1200
reneg-sec 0




^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Ju
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To
```

4. Remember to change the name of the client certificate and key in client.conf for client A and B



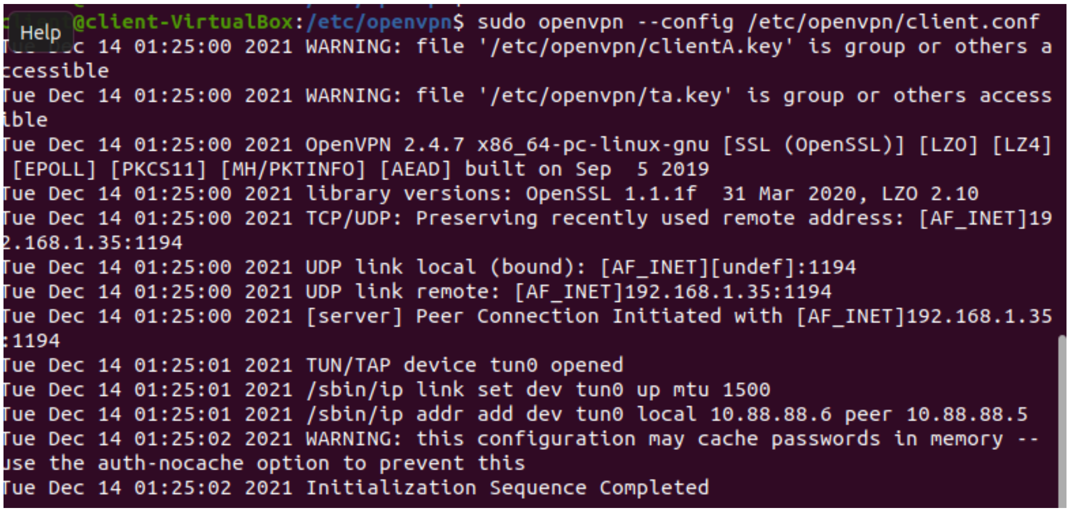
```
  GNU nano 4.8                                client.conf
client
dev tun
proto udp
remote 192.168.1.35 1194
ca /etc/openvpn/ca.crt
cert /etc/openvpn/clientA.crt
key /etc/openvpn/clientA.key
tls-crypt /etc/openvpn/ta.key
persist-key
persist-tun
verb 1
cipher AES-256-GCM
auth SHA512
remote-cert-tls server
mssfix 1200
reneg-sec 0







File Name to Write [DOS Format]: client.conf
^G Get Help           M-D DOS Format          M-A Append
^C Cancel             M-M Mac Format          M-P Prepend
```



```
@client-VirtualBox:/etc/openvpn$ sudo openvpn --config /etc/openvpn/client.conf
Tue Dec 14 01:25:00 2021 WARNING: file '/etc/openvpn/clientA.key' is group or others a
ccessible
Tue Dec 14 01:25:00 2021 WARNING: file '/etc/openvpn/ta.key' is group or others access
ible
Tue Dec 14 01:25:00 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
 [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2019
Tue Dec 14 01:25:00 2021 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Tue Dec 14 01:25:00 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]19
2.168.1.35:1194
Tue Dec 14 01:25:00 2021 UDP link local (bound): [AF_INET][undef]:1194
Tue Dec 14 01:25:00 2021 UDP link remote: [AF_INET]192.168.1.35:1194
Tue Dec 14 01:25:00 2021 [server] Peer Connection Initiated with [AF_INET]192.168.1.35
:1194
Tue Dec 14 01:25:01 2021 TUN/TAP device tun0 opened
Tue Dec 14 01:25:01 2021 /sbin/ip link set dev tun0 up mtu 1500
Tue Dec 14 01:25:01 2021 /sbin/ip addr add dev tun0 local 10.88.88.6 peer 10.88.88.5
Tue Dec 14 01:25:02 2021 WARNING: this configuration may cache passwords in memory --
use the auth-nocache option to prevent this
Tue Dec 14 01:25:02 2021 Initialization Sequence Completed
```

3. TLS communications

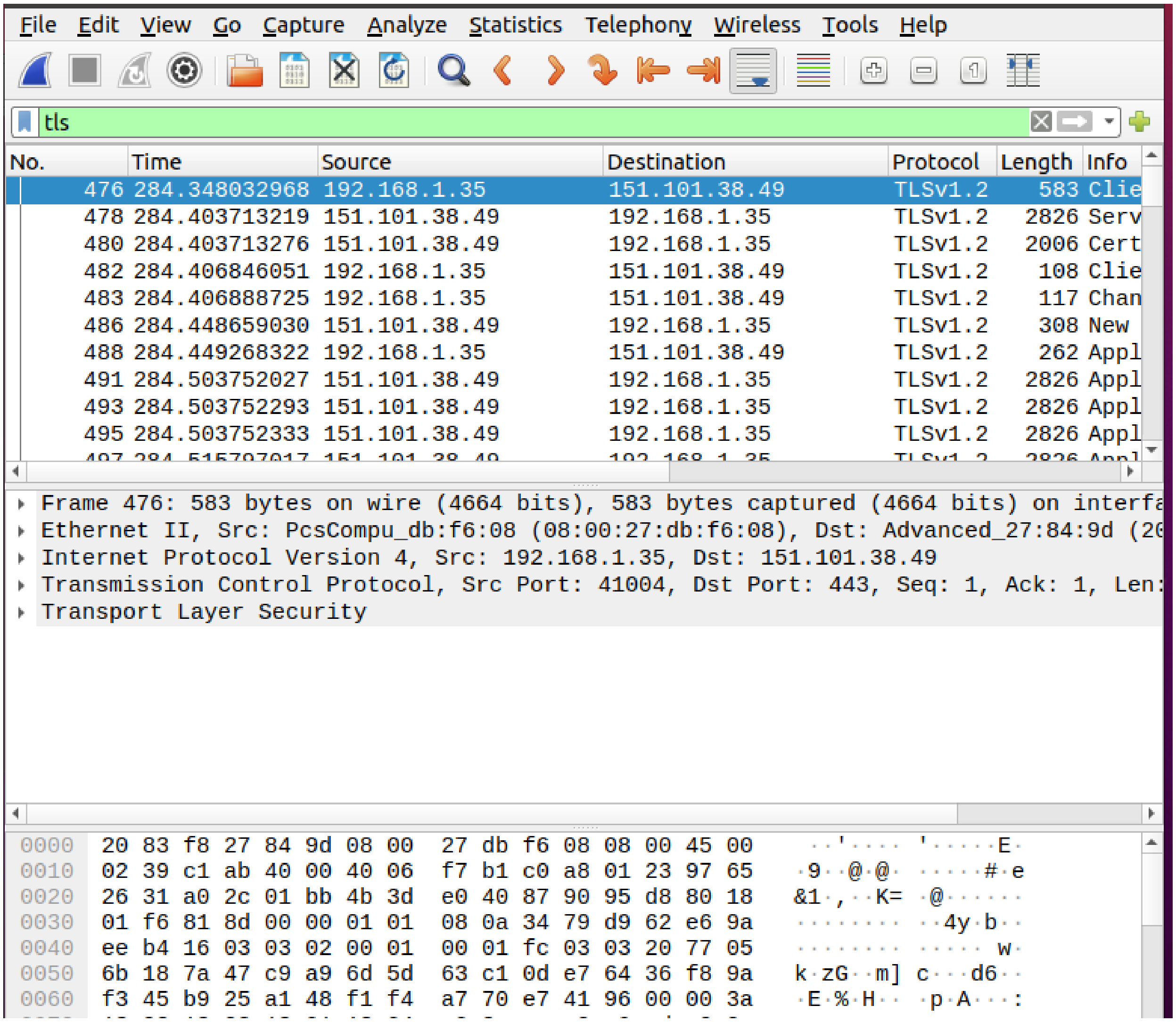
The point aims to analyze the TLS 1.2/TLS 1.3 communications. Get acquainted with TLS/SSL versions 1.2 and 1.3, find the advantages and disadvantages of each version.

I. Task 1:

- **Capture the network traffic on the physical network interface (usually, the name starts with en…),**

- **Filter only the records for TLS/SSL communication. Filter expression for TLS/SSL in Wireshark: ssl.record.version == 0x0303,**

- **Study the TLS/SSL records in detail.**



No.	Time	Source	Destination	Protocol	Length	Info
476	284.348032968	192.168.1.35	151.101.38.49	TLSv1.2	583	Clie
478	284.403713219	151.101.38.49	192.168.1.35	TLSv1.2	2826	Serv
480	284.403713276	151.101.38.49	192.168.1.35	TLSv1.2	2006	Cert
482	284.406846051	192.168.1.35	151.101.38.49	TLSv1.2	108	Clie
483	284.406888725	192.168.1.35	151.101.38.49	TLSv1.2	117	Chan
486	284.448659030	151.101.38.49	192.168.1.35	TLSv1.2	308	New
488	284.449268322	192.168.1.35	151.101.38.49	TLSv1.2	262	Appl
491	284.503752027	151.101.38.49	192.168.1.35	TLSv1.2	2826	Appl
493	284.503752293	151.101.38.49	192.168.1.35	TLSv1.2	2826	Appl
495	284.503752333	151.101.38.49	192.168.1.35	TLSv1.2	2826	Appl
497	284.515797017	151.101.38.49	192.168.1.35	TLSv1.2	2826	Appl

```
▸ Frame 476: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interfa
▸ Ethernet II, Src: PcsCompu_db:f6:08 (08:00:27:db:f6:08), Dst: Advanced_27:84:9d (20
▸ Internet Protocol Version 4, Src: 192.168.1.35, Dst: 151.101.38.49
▸ Transmission Control Protocol, Src Port: 41004, Dst Port: 443, Seq: 1, Ack: 1, Len:
▸ Transport Layer Security
```

```
0000  20 83 f8 27 84 9d 08 00  27 db f6 08 08 00 45 00   ··'····· '·····E·
0010  02 39 c1 ab 40 00 40 06  f7 b1 c0 a8 01 23 97 65   ·9··@·@· ·····#·e
0020  26 31 a0 2c 01 bb 4b 3d  e0 40 87 90 95 d8 80 18   &1·,··K= ·@······
0030  01 f6 81 8d 00 00 01 01  08 0a 34 79 d9 62 e6 9a   ········ ··4y·b··
0040  ee b4 16 03 03 02 00 01  00 01 fc 03 03 20 77 05   ········ ····· w·
0050  6b 18 7a 47 c9 a9 6d 5d  63 c1 0d e7 64 36 f8 9a   k·zG··m] c···d6··
0060  f3 45 b9 25 a1 48 f1 f4  a7 70 e7 41 96 00 00 3a   ·E·%·H·· ·p·A···:
```

II. Questions:

• Is TLS and SSL the same protocol?

TLS: TRANSPORT LAYER SECURİTY, SSL: SECURE SOCKET LAYER

TLS is an successor protocol to SSL. TLS is an improved version of the SSL. İt works in much the same way as the SSL. Using thr encryption to project the transfer of data and information. The two terms are often used interchangeably in the industry although SSL is still widely used.

Thus, TLS is an updated version of the SSL, its more secure version of the SSL. So basically they kind of similar but not the as same as each other.

• What is a TLS/SSL handshake?

The SSL or TLS handshake enables the SSL or TLS client and server to establish the secret keys with which they communicate . ... SSL or TLS then uses the shared key for the symmetric encryption of messages, which is faster than asymmetric encryption.

Steps of TLS;exchanging encryption capabilities, authenticating the SSL certificate, and exchanging/generating a session key.

Both parties agree on a single cipher suite and generate the session keys (symmetric keys) to encrypt and decrypt the information during an SSL session

• What does the TLS/SSL protocol provide, give examples of its applications (at least 2)?

SSL(Secure Socket Layer) and TLS(Transport Layer Security) are popular cryptographic protocols that are used to imbue web communications with integrity, security, and resilience against unauthorized tampering.

TLDR: SSL/TLS encrypts communications between a client and server, primarily web browsers and web sites/app. SSL encryptioni and its more modern and secure replacement, TLS encryption, protect data sent over the internet or a computer network.

• Which versions of the protocol are currently the most popular?

As we mentioned above about the explanation of the TLS and SSL protocol. While TLS 1.2 is currently the most widely-used version of the SSL/TLS protocol, TLS 1.3 (the latest version) is already supported in the current versions of most major web browsers.

• Which version offers higher security and why?

To sum everything up, TLS and SSL are both protocols to authenticate and encrypt the transfer of data on the Internet. The two are tightly linked and TLS is really just the more modern, secure version of SSL.

• Which version offers higher performance?

Recently TLS has more higher performance than SSL protocol. Even most modern web browsers not longer support SSL2.0 AND 3.0. For example chrome stopped supporting SSL 3.0 all the way back in 2014.andmost major browsers are planning to stop supporting TLS 1.0 and TLS1.1 İN 2020. Since new versions of the TLS protocol are released than the olders are losts interest. Last version for now which is most secure is TLS1.3 version.

Based on the traffic captured, analyze the recorded TLS/SSL traffic.

• Which version of the protocol has been captured?

İn the wireshark when capturing the network traffic TLS protocol has been captured.

• What kind of messages does a handshake consist of (connection establishment)?

In place of the term "handshake", FTP RFC 3659 substitutes the term "conversation" for the passing of commands. A simple handshaking protocol might only involve the receiver sending a message meaning "I received your last message and I am ready for you to send me another one."

• What does the version of the protocol use depend on?

n the TLS handshake the client announces the best version it can do to the server . If the server supports protocol versions which are equal or less to the clients version it will reply with the best of these