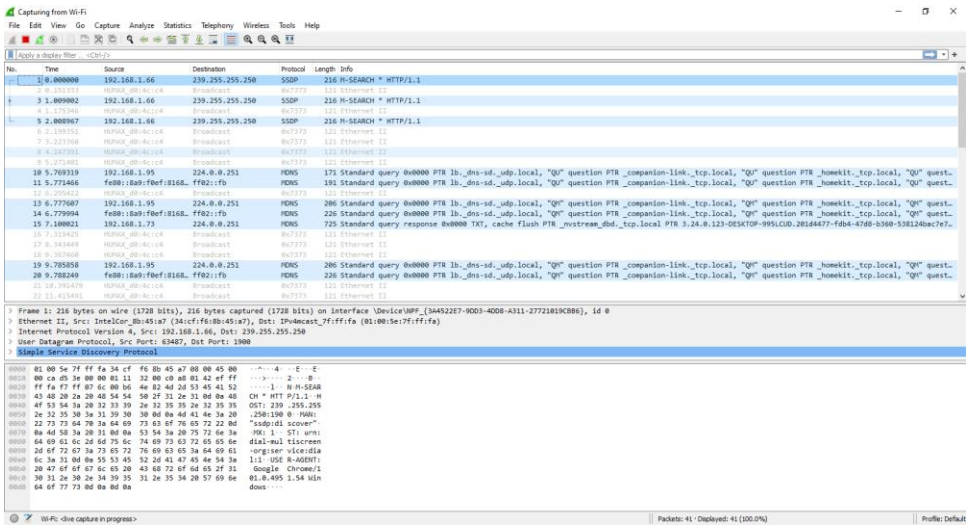
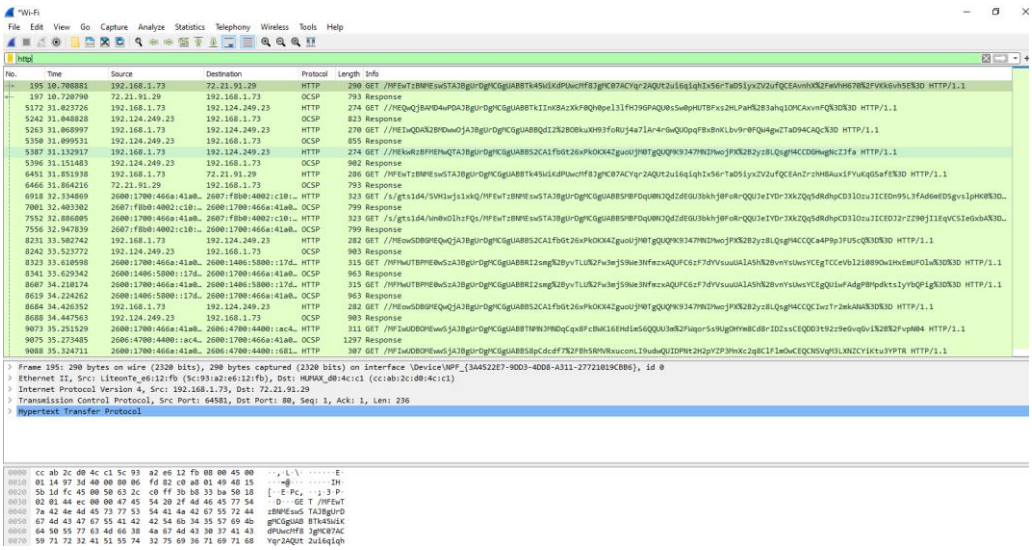
Farzad Kheirabadi
CYB 555
Final

555 - Final

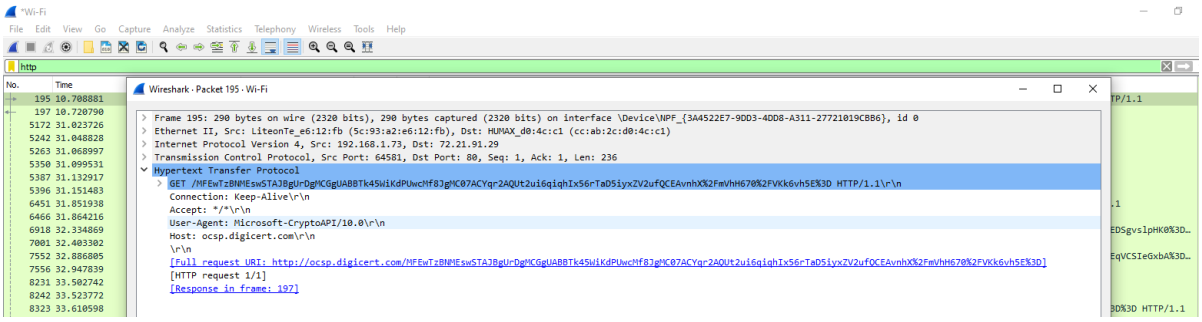
1-



2-



Farzad Kheirabadi
CYB 555
Final

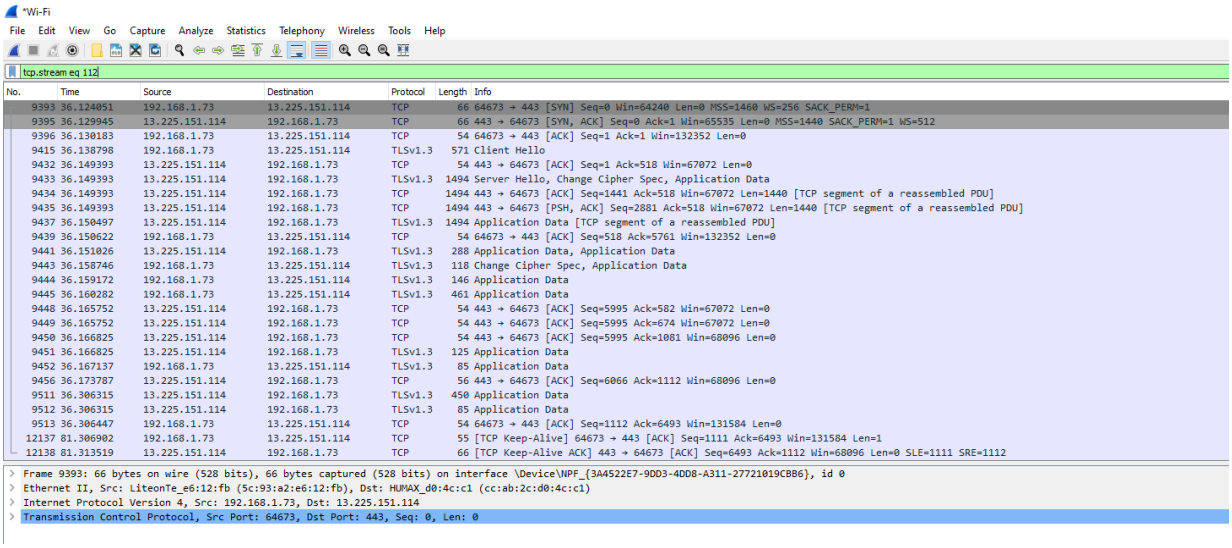


Passive attack

Can monitor, view the system data. It is difficult for the victim to pay attention to passive attacks because this type of attack is carried out covertly. The purpose of the passive attack is to access or scan open data and network vulnerabilities.

Active attack

It can be network abuse in which attackers alter or modify the content and affect the source of the system. Victims can be notified of an active attack. This type of attack can threaten their integrity and accessibility.



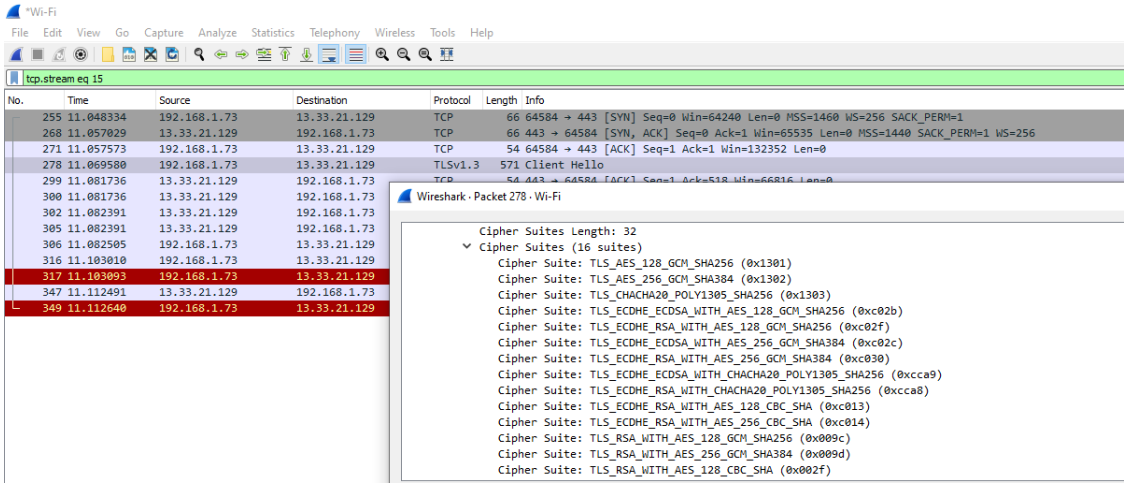
An attack occurs when similar packets are sent from a different IP address to the service provider.

3-

Farzad Kheirabadi
CYB 555
Final

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Using the Diffie Hellmann key exchange algorithm, an elliptical curve is created and in such cases the key is not generated on the client side, instead the secure key uses a special algorithm that includes encryption using the public server key as in the password you see shows the hash algorithm used. We see that it uses SHA256.



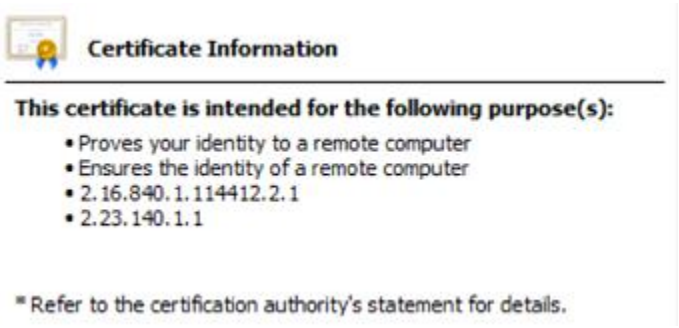
So, the cipher set is basically a set of encryption rules for TLS loss. This creates a secure key for encryption in the TLS protocol. In this password set, the key is generated in the web browser site and then this key is sent to the encrypted web server which is the public key.

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc09d)

```
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
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_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
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 (0x0035)
Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
```

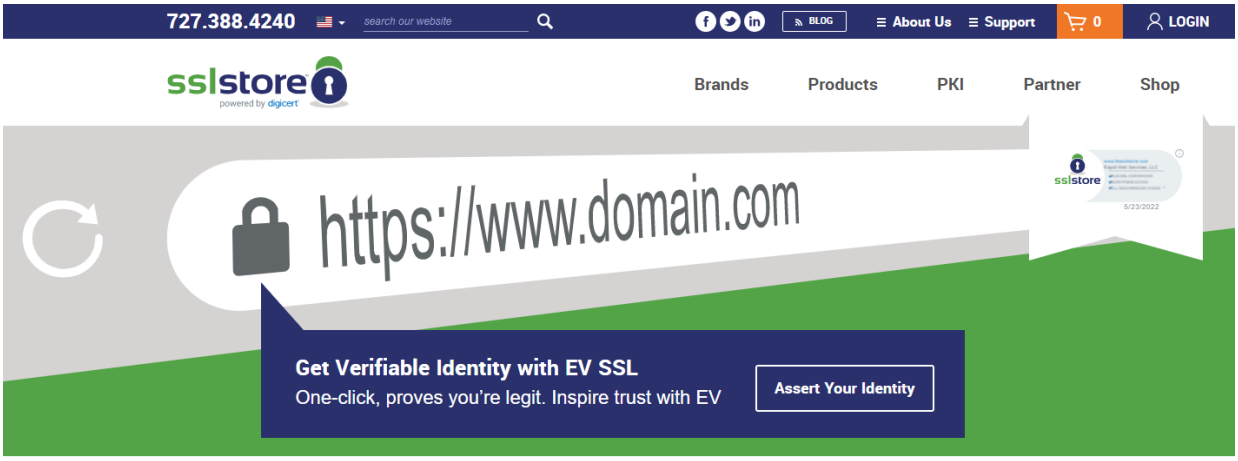
Farzad Kheirabadi
CYB 555
Final

4-



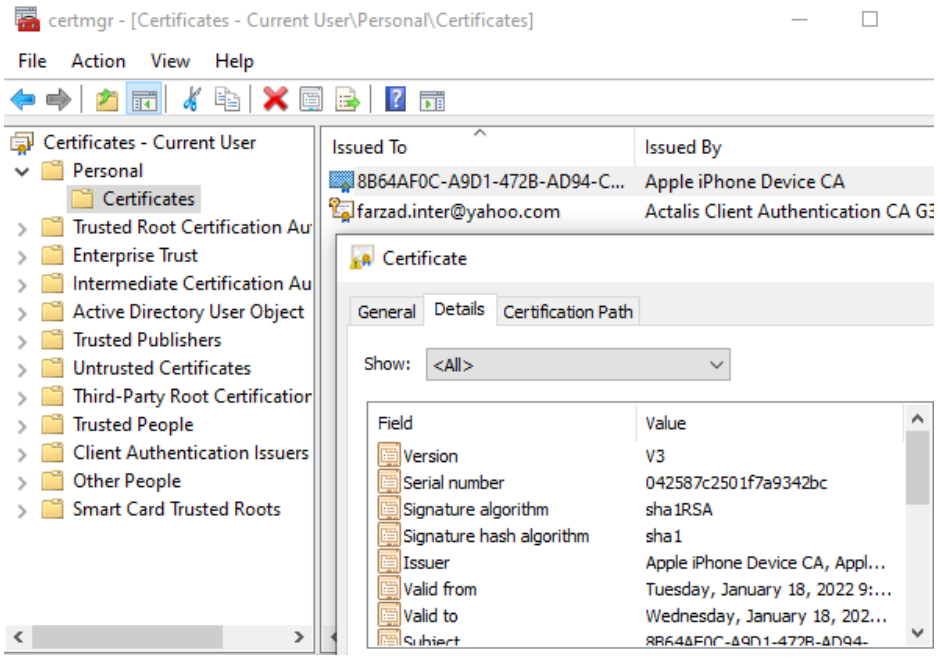
Public Key

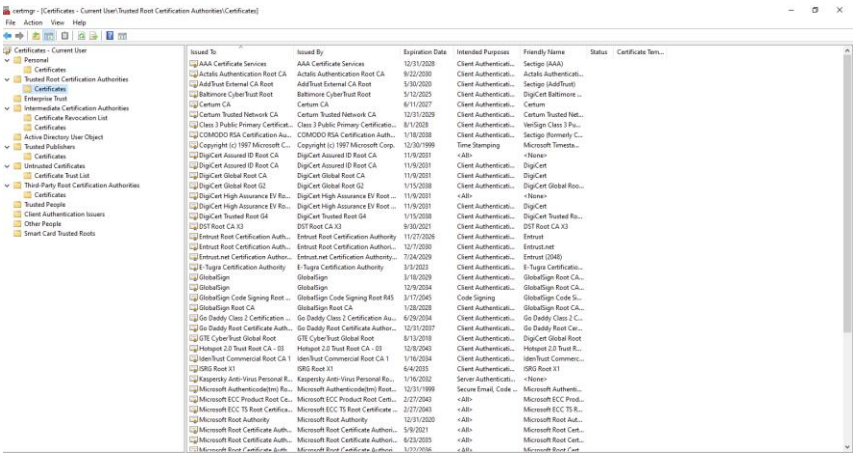
30 82 01 0a 02 82 01 01 00 db 60 75 e0 ac a2 79 65 83 ee b0 8c 5e a8 bc c2 dc 1b f6 eb 51 df 76 4c 4f 8d 78 e3 fb be ed a0 61 ea cb 5b df 27 fa ea c7 35 18 6b 96 c7 ff ad 57 0b ca 98 7e 34 7b c9 da fc f9 a1 b8 fe b1 c0 48 88 6d 0d 82 fa e3 b3 c2 d4 2c aa 28 33 c2 1a 62 e8 91 f7 cc e7 9d ea 49 a2 a8 bc 8f aa 9b 11 28 6c 40 9f 5d 80 e6 e7 e6 b0 ac e6 ab d4 e8 73 6b a8 6e 7d d4 1a aa 41 db 80 80 2e b7 7c 81 f9 32 de 19 09 a5 68 9c 5e f3 c9 1a 7b a2 d1 07 86 fc 41 2d 11 e1 6c 85 41 68 bf 58 67 cb 15 7c 49 cb ef 42 b2 09 e2 71 be a9 1e 8a 40 c9 06 21 94 ac 49 58 63 92 34 d8 bb 0d 4a d2 d4 95 70 13 9f 10 49 9b 38 66 07 bc e5 a6 3b 7e be dc e4 ba 01 6a 54 0b bc 03 1e 91 5a 6e ad e3 1a e9 26 bd 05 8f 92 90 9f c9 a2 46 6d 09 e8 ea e3 9d dd fd c5 7b 66 63 5e b4 b0 f4 c3 10 90 bf 96 d9 14 31 d9 02 03 01 00 01



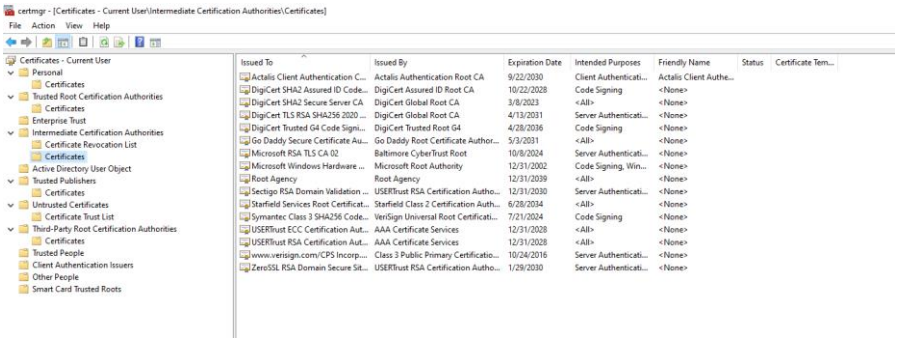
Farzad Kheirabadi
CYB 555
Final

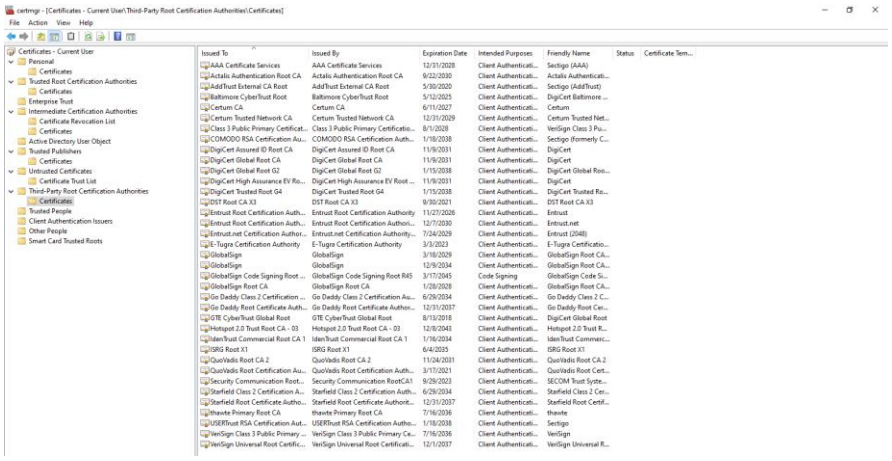
5-

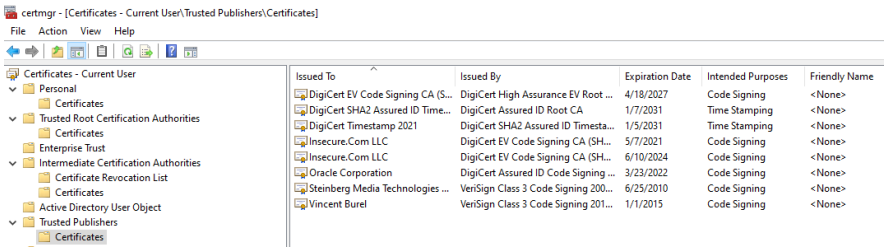




Farzad Kheirabadi
CYB 555
Final







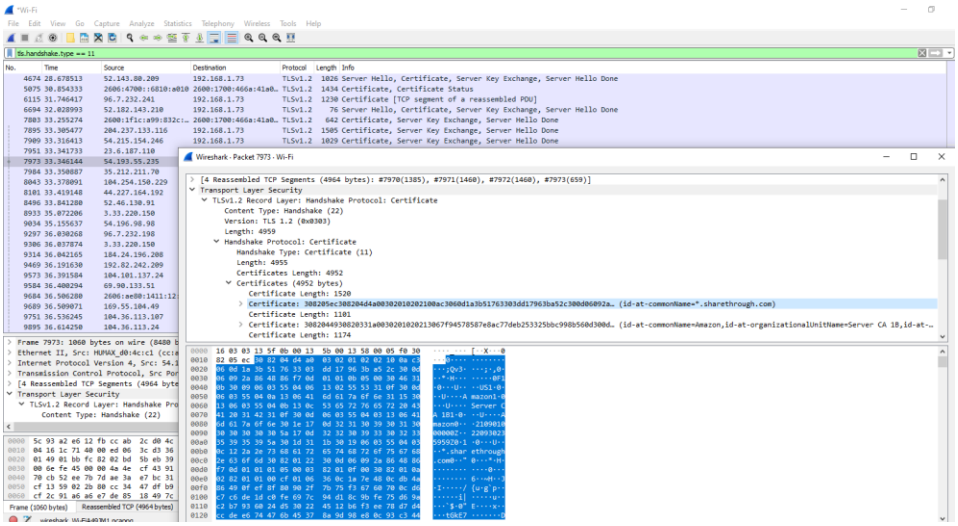
Digital certificates make it possible for digital signatures to be used to authenticate digital information. To digitally sign an office document, you must have a current, expired digital certificate. Digital certificates are usually issued by a Certificate Authority (CA), which is a trusted third-party entity that issues digital certificates for use by others.

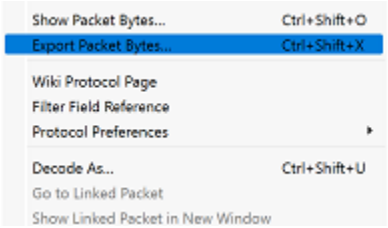
A digital certificate is essential for a digital signature because it provides a public key that can be used to authenticate a private key associated with a digital signature. Digital certificates make it possible for digital signatures to be used to authenticate digital information.

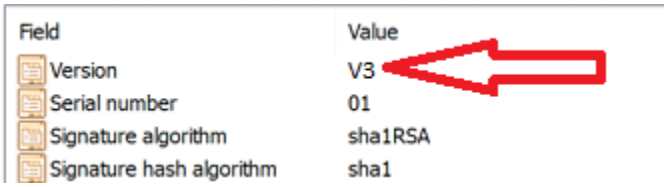
- First by checking the domain information in the ICANN search
- Create a certificate signing request

Farzad Kheirabadi
CYB 555
Final

- Domain validation is done by sending a certificate signing request to the certification authority.
- Install the certificate

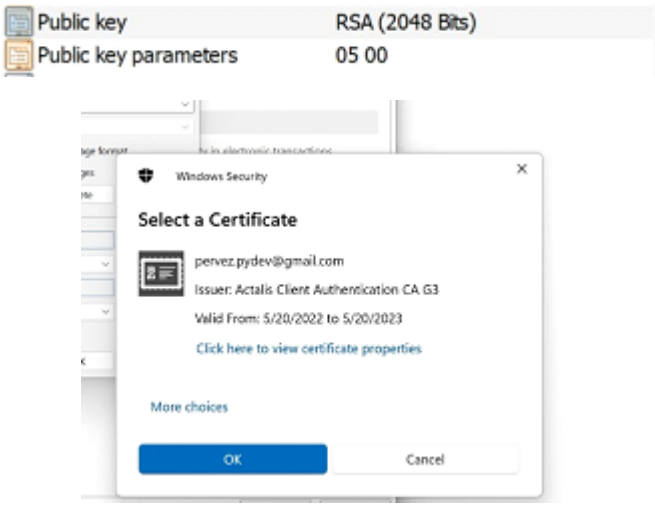


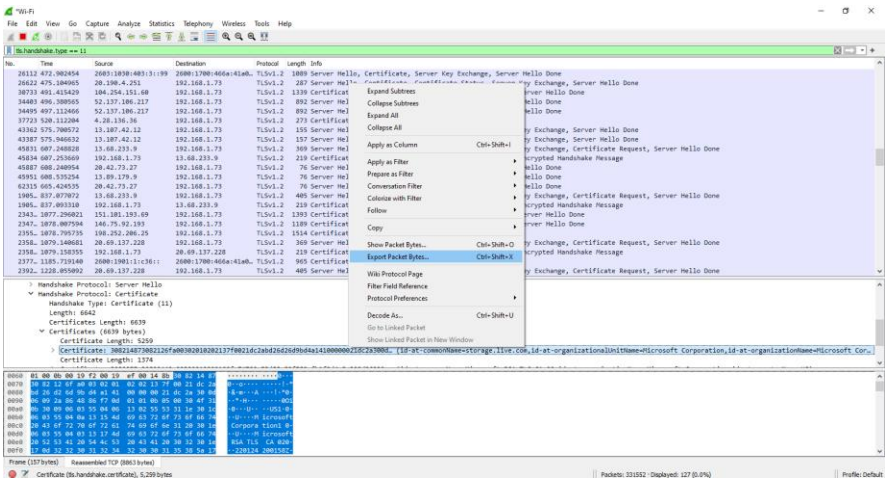




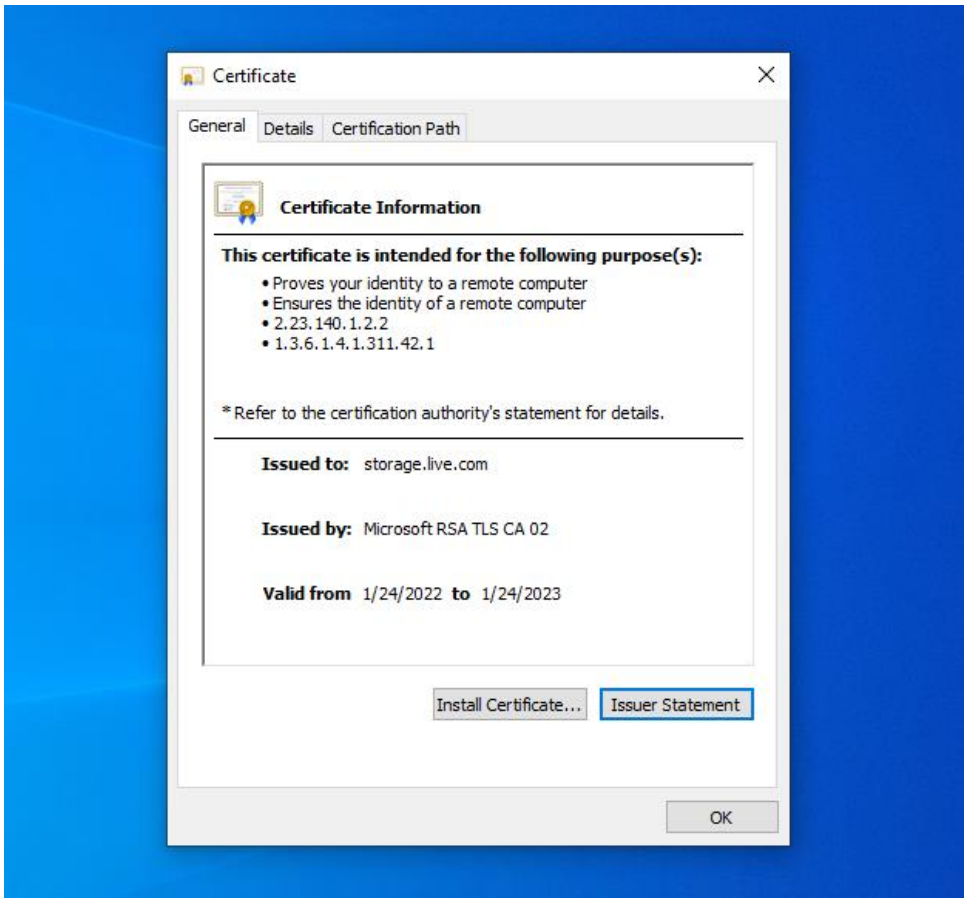
Farzad Kheirabadi
CYB 555
Final

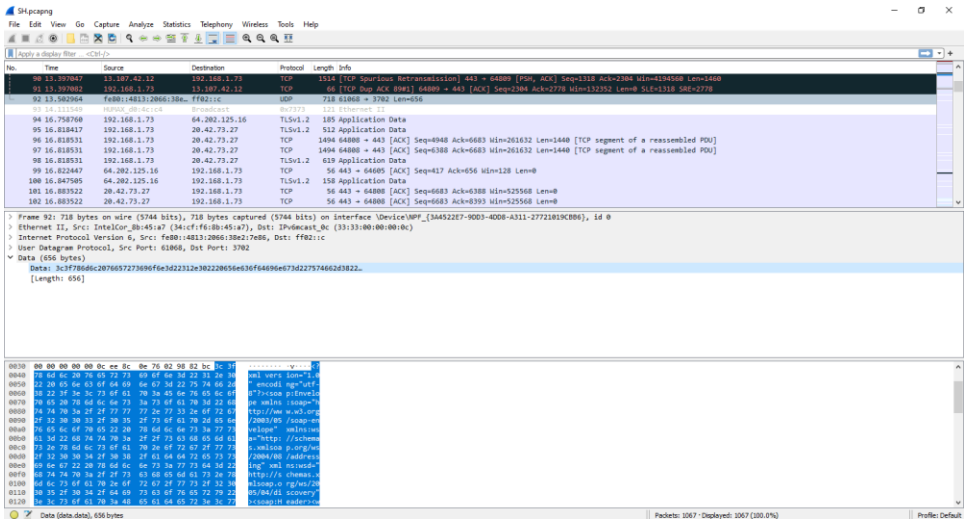
6-



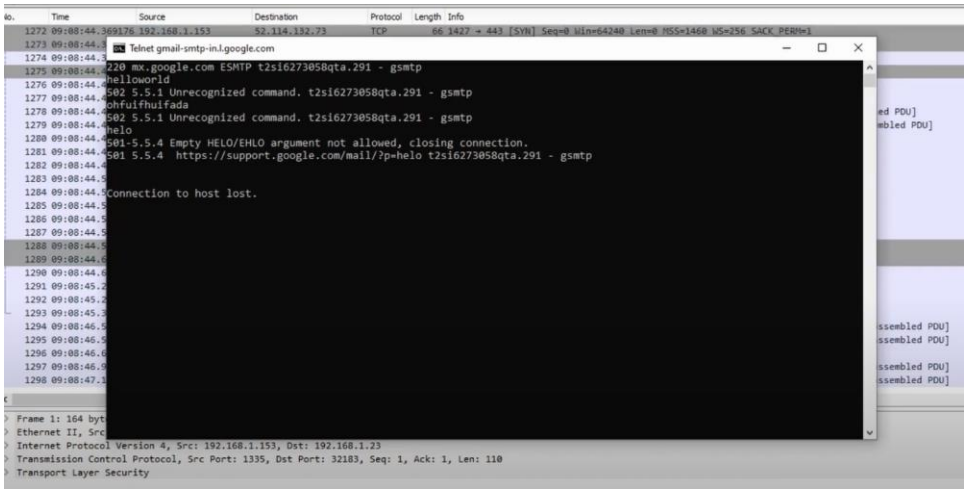


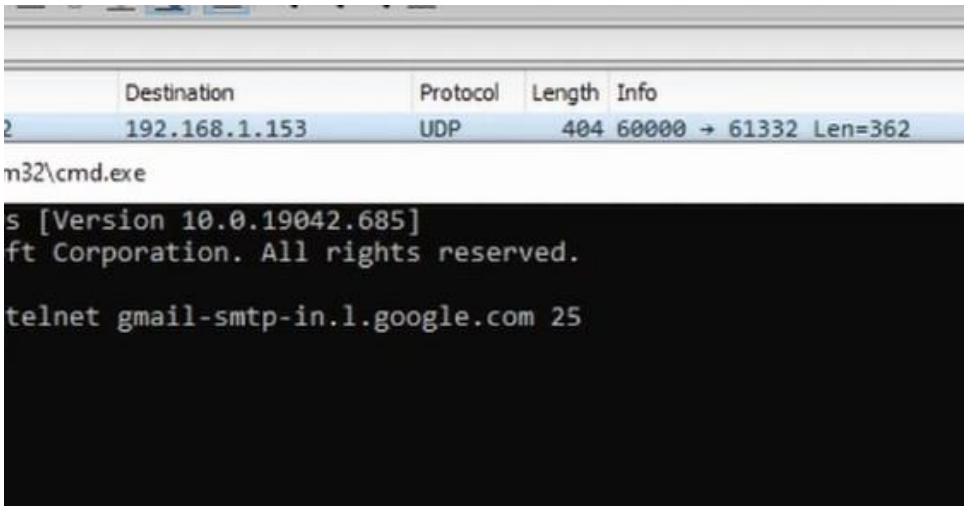
Farzad Kheirabadi
CYB 555
Final

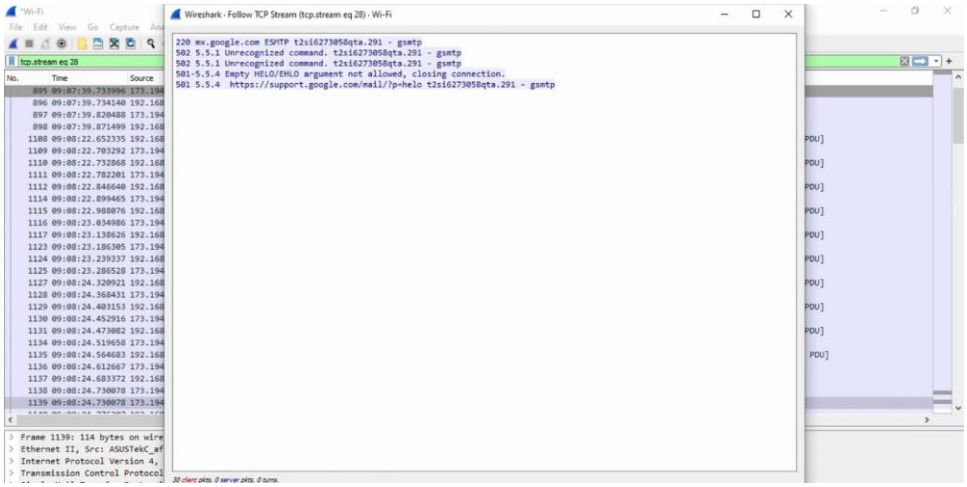




Farzad Kheirabadi
CYB 555
Final

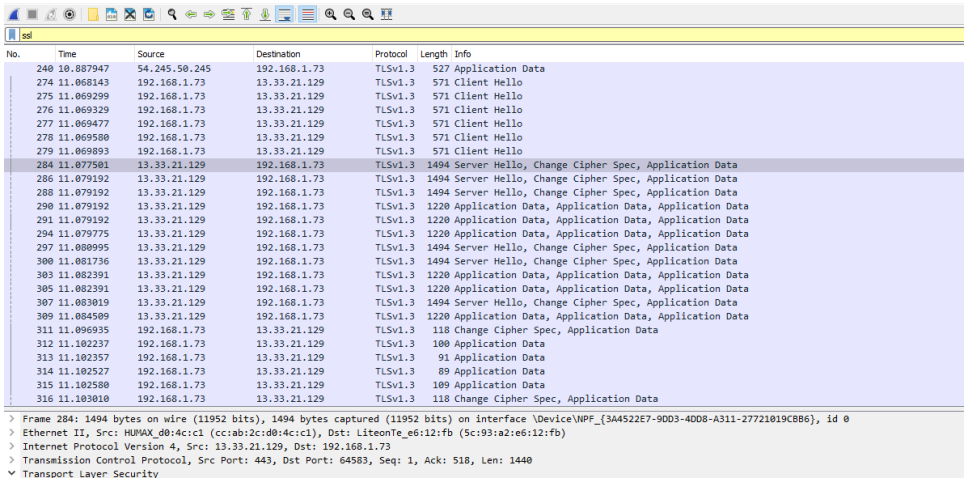






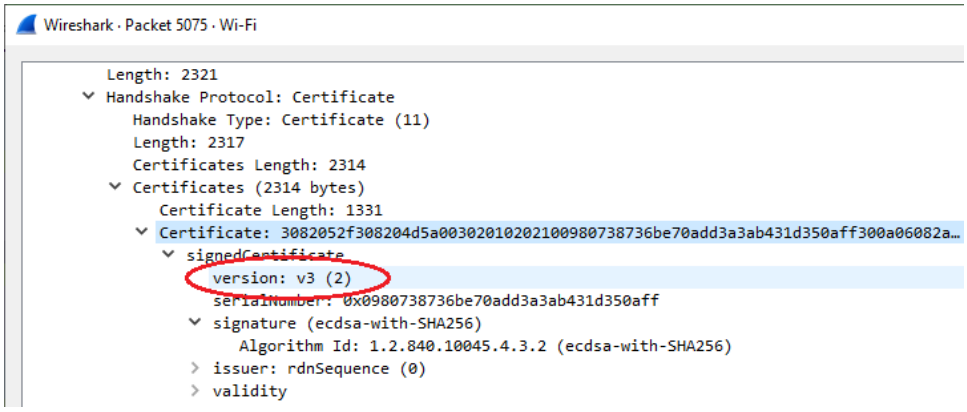
Farzad Kheirabadi
CYB 555
Final

7-

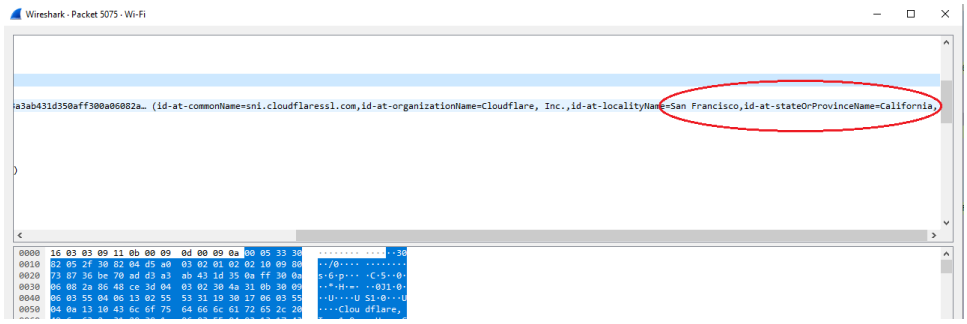


No.	Time	Source	Destination	Protocol	Length	Info
240	10.887947	54.245.50.245	192.168.1.73	TLSv1.3	527	Application Data
274	11.068143	192.168.1.73	13.33.21.129	TLSv1.3	571	Client Hello
275	11.069299	192.168.1.73	13.33.21.129	TLSv1.3	571	Client Hello
276	11.069329	192.168.1.73	13.33.21.129	TLSv1.3	571	Client Hello
277	11.069477	192.168.1.73	13.33.21.129	TLSv1.3	571	Client Hello
278	11.069580	192.168.1.73	13.33.21.129	TLSv1.3	571	Client Hello
279	11.069893	192.168.1.73	13.33.21.129	TLSv1.3	571	Client Hello
284	11.077501	13.33.21.129	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
286	11.079192	13.33.21.129	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
288	11.079192	13.33.21.129	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
290	11.079192	13.33.21.129	192.168.1.73	TLSv1.3	1220	Application Data, Application Data, Application Data
291	11.079192	13.33.21.129	192.168.1.73	TLSv1.3	1220	Application Data, Application Data, Application Data
294	11.079775	13.33.21.129	192.168.1.73	TLSv1.3	1220	Application Data, Application Data, Application Data
297	11.080995	13.33.21.129	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
300	11.081736	13.33.21.129	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
303	11.082391	13.33.21.129	192.168.1.73	TLSv1.3	1220	Application Data, Application Data, Application Data
305	11.082391	13.33.21.129	192.168.1.73	TLSv1.3	1220	Application Data, Application Data, Application Data
307	11.083019	13.33.21.129	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
309	11.084509	13.33.21.129	192.168.1.73	TLSv1.3	1220	Application Data, Application Data, Application Data
311	11.096935	192.168.1.73	13.33.21.129	TLSv1.3	118	Change Cipher Spec, Application Data
312	11.102237	192.168.1.73	13.33.21.129	TLSv1.3	100	Application Data
313	11.102357	192.168.1.73	13.33.21.129	TLSv1.3	91	Application Data
314	11.102527	192.168.1.73	13.33.21.129	TLSv1.3	89	Application Data
315	11.102580	192.168.1.73	13.33.21.129	TLSv1.3	109	Application Data
316	11.103010	192.168.1.73	13.33.21.129	TLSv1.3	118	Change Cipher Spec, Application Data

```
> Frame 284: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{3A4522E7-9DD3-4DD8-A311-27721019CBB6}, id 0
> Ethernet II, Src: HUMAX_d0:4c:c1 (cc:ab:2c:d0:4c:c1), Dst: LiteonTe_e6:12:fb (5c:93:a2:e6:12:fb)
> Internet Protocol Version 4, Src: 13.33.21.129, Dst: 192.168.1.73
> Transmission Control Protocol, Src Port: 443, Dst Port: 64583, Seq: 1, Ack: 518, Len: 1440
v Transport Layer Security
```



```
Wireshark · Packet 5075 · Wi-Fi
    Length: 2321
  v Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 2317
      Certificates Length: 2314
    v Certificates (2314 bytes)
        Certificate Length: 1331
      v Certificate: 3082052f308204d5a003020102021009807387 36be70add3a3ab431d350aff300a06082a…
        v signedCertificate
            version: v3 (2)
            serialNumber: 0x0980738736be70add3a3ab431d350aff
          v signature (ecdsa-with-SHA256)
              Algorithm Id: 1.2.840.10045.4.3.2 (ecdsa-with-SHA256)
          > issuer: rdnSequence (0)
          > validity
```



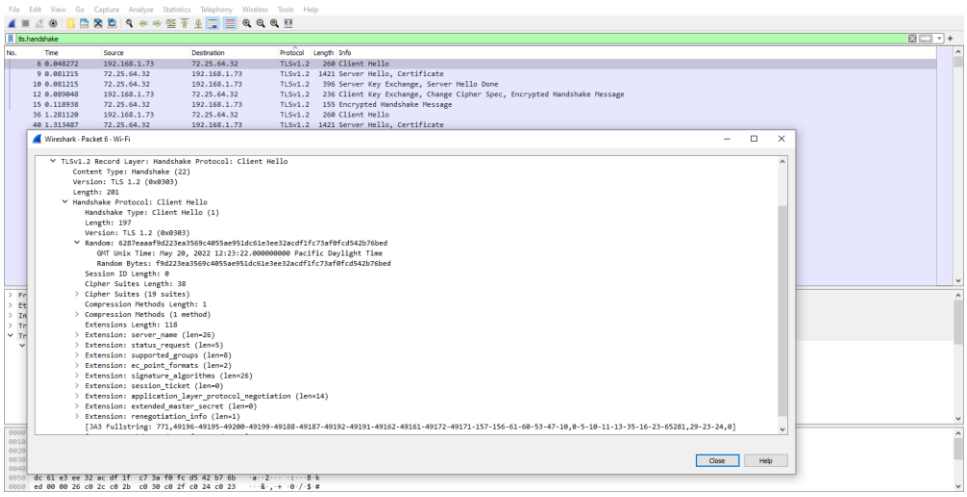
```
Wireshark · Packet 5075 · Wi-Fi
a3ab431d350aff300a06082a… (id-at-commonName=sni.cloudflaressl.com,id-at-organizationName=Cloudflare, Inc.,id-at-localityName=San Francisco,id-at-stateOrProvinceName=California,
)

0000  16 03 03 09 11 0b 00 09  0d 00 09 0a 00 05 33 30   ··· ··· ··· ··· ··30
0010  82 05 2f 30 82 04 d5 a0  03 02 01 02 02 10 09 80   ··/0··· ··· ··· ···
0020  73 87 36 be 70 ad d3 a3  ab 43 1d 35 0a ff 30 0a   s·6·p··· ·C·5··0·
0030  06 08 2a 86 48 ce 3d 04  03 02 30 4a 31 0b 30 09   ··*·H·=· ··0J1·0·
0040  06 03 55 04 06 13 02 55  53 31 19 30 17 06 03 55   ··U····U S1·0···U
0050  04 0a 13 10 43 6c 6f 75  64 66 6c 61 72 65 2c 20   ····Clou dflare, 
```

Farzad Kheirabadi
CYB 555
Final

- Observe the traffic captured in the top Wireshark packet list pane.
- Select the second TLS packet, labeled Server Hello.
- Observe the packet details in the middle Wireshark packet details pane.
- Expand Secure Sockets Layer, TLS, and Handshake Protocol to view SSL/TLS details.

Authenticate the identity of the server via the server's public key and the SSL certificate authority's digital signature. Transport Layer Security (TLS) provides security in communication between two hosts. It provides integrity, authentication and confidentiality. It is used mostly in web browsers but can be used with any protocol that uses TCP as the transport layer.



A TLS/SSL handshake is the process that starts this secure communication session that uses the TLS/SSL encryption technique.

During a TLS handshake the following processes will occur in the order below:

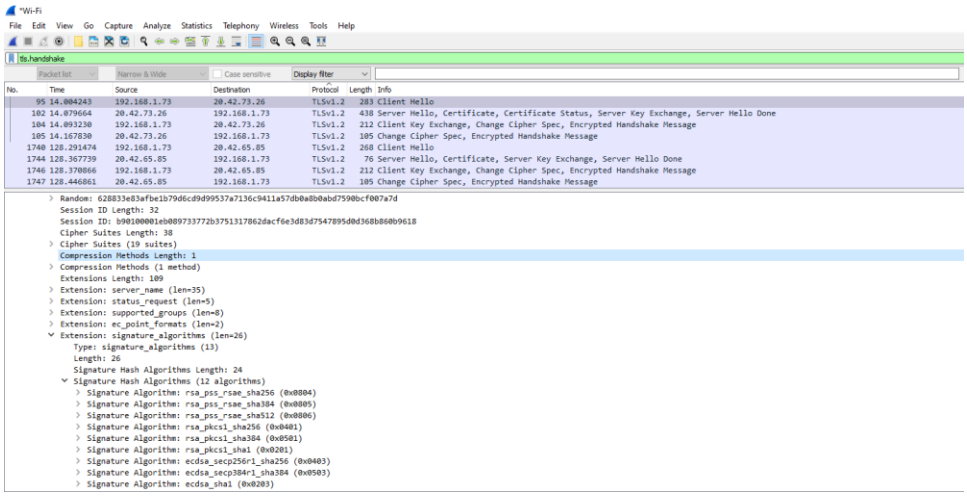
- The client and server exchange messages to acknowledge each other.

- Then they verify each other's identity.

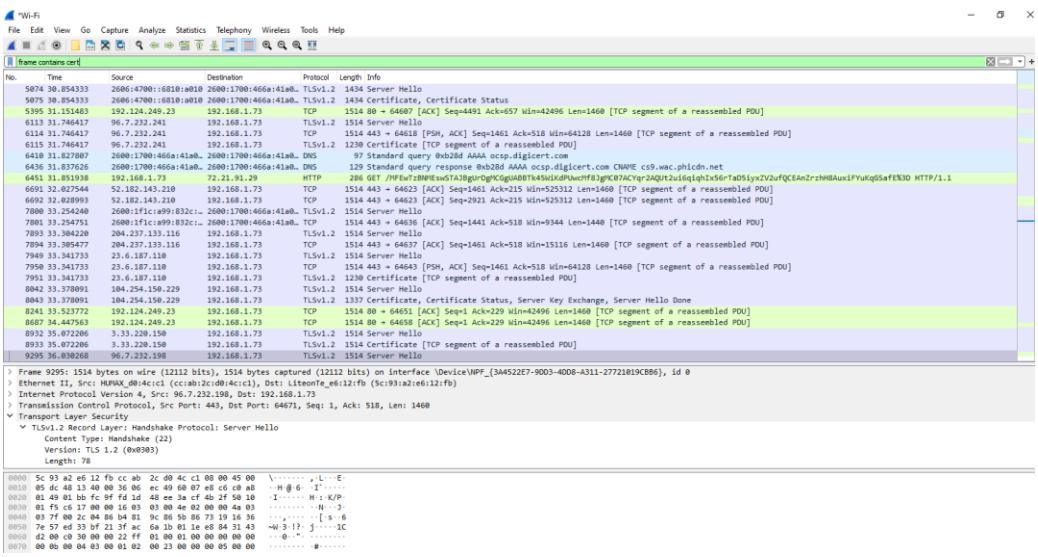
- Establish the encryption algorithms they will use for securing communicated messages.

- And agree on session keys.

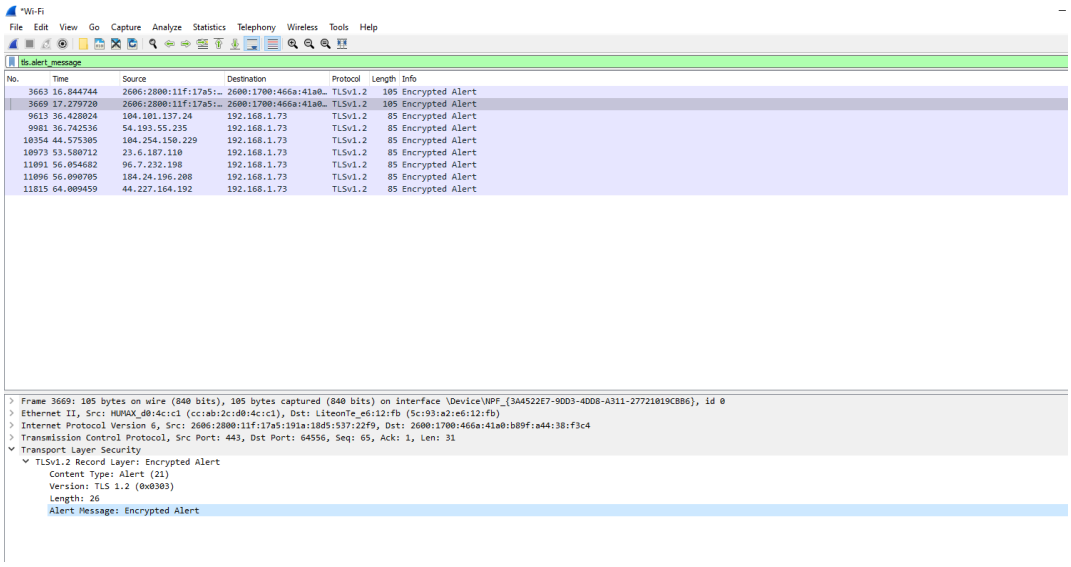
Farzad Kheirabadi
CYB 555
Final



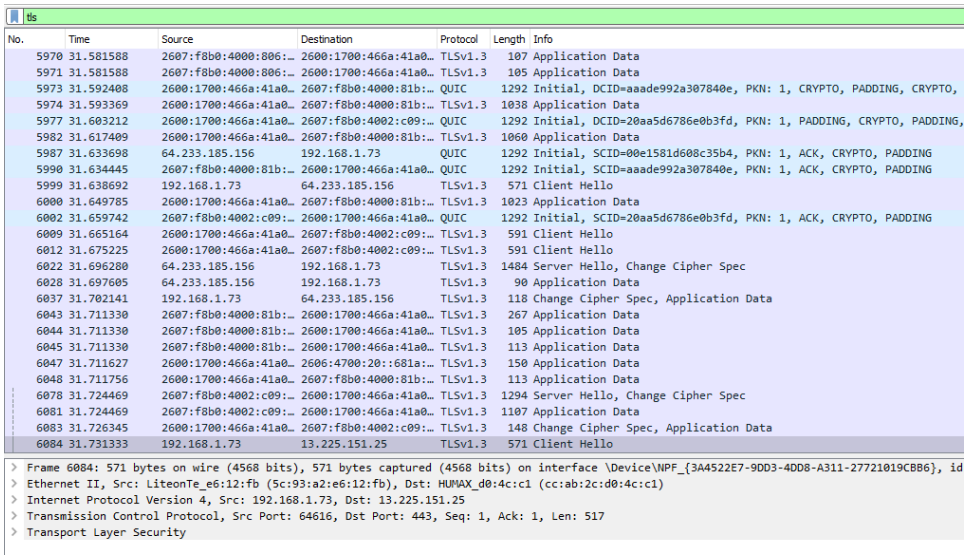
They all refer to the same algorithm. The SHA-1 hash function has only one output size while SHA-2 has several (256, 384, 512). Whenever you see "SHA256", "SHA384" or "SHA512", it refers to "SHA-2".



Farzad Kheirabadi
CYB 555
Final



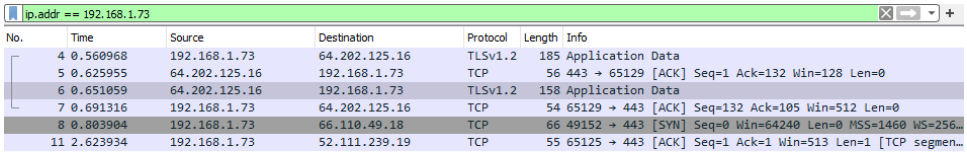
8-



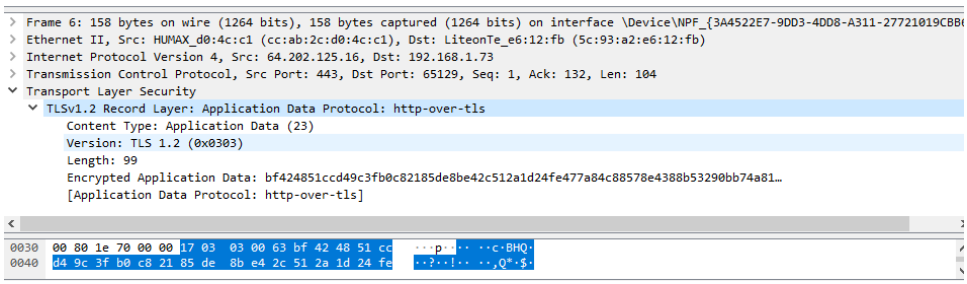
TLS is an accepted security protocol designed to facilitate the privacy and security of data for Internet communications. One of the key uses of TLS is to encrypt the connection between web applications and servers, such as web browsers that load a website.

Farzad Kheirabadi
CYB 555
Final

This protocol allows both peers to verify their identities. When used in a browser, this authentication mechanism allows the client to verify that the server is what it claims and not someone who simply pretends to be the destination by forging a name or IP address. This verification is based on the trust chain. Refer to the trust chain. And certification authorities at the end, the server can also optionally authenticate the client.

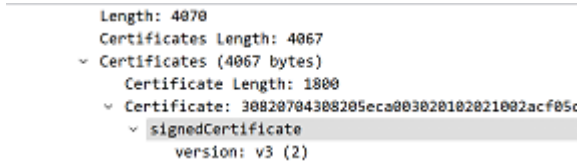


No.	Time	Source	Destination	Protocol	Length	Info
4	0.560968	192.168.1.73	64.202.125.16	TLSv1.2	185	Application Data
5	0.625955	64.202.125.16	192.168.1.73	TCP	56	443 → 65129 [ACK] Seq=1 Ack=132 Win=128 Len=0
6	0.651059	64.202.125.16	192.168.1.73	TLSv1.2	158	Application Data
7	0.691316	192.168.1.73	64.202.125.16	TCP	54	65129 → 443 [ACK] Seq=132 Ack=105 Win=512 Len=0
8	0.803904	192.168.1.73	66.110.49.18	TCP	66	49152 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256…
11	2.623934	192.168.1.73	52.111.239.19	TCP	55	65125 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segmen…



```
> Frame 6: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface \Device\NPF_{3A4522E7-9DD3-4DD8-A311-27721019CBB
> Ethernet II, Src: HUMAX_d0:4c:c1 (cc:ab:2c:d0:4c:c1), Dst: LiteonTe_e6:12:fb (5c:93:a2:e6:12:fb)
> Internet Protocol Version 4, Src: 64.202.125.16, Dst: 192.168.1.73
> Transmission Control Protocol, Src Port: 443, Dst Port: 65129, Seq: 1, Ack: 132, Len: 104
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 99
      Encrypted Application Data: bf424851ccd49c3fb0c82185de8be42c512a1d24fe477a84c88578e4388b53290bb74a81…
      [Application Data Protocol: http-over-tls]

0030  00 80 1e 70 00 00 17 03  03 00 63 bf 42 48 51 cc   ···p····  ··c·BHQ·
0040  d4 9c 3f b0 c8 21 85 de  8b e4 2c 51 2a 1d 24 fe   ··?··!·· ··,Q*·$·
```



```
    Length: 4070
    Certificates Length: 4067
  v Certificates (4067 bytes)
      Certificate Length: 1800
    v Certificate: 30820704308205eca003020102021002acf05c
      v signedCertificate
          version: v3 (2)
```

- Mine is V3

Client Hello:

The client sends a greeting message to the client with a protocol version and a list of password sets.

Farzad Kheirabadi
CYB 555
Final

No.	Time	Source	Destination	Protocol	Length	Info
308	15.645265	2620:1ec:c11::200	2600:1700:466a:41a0…	TLSv1.2	498	Application Data, Application Data
309	15.647996	192.168.1.73	54.204.196.80	TLSv1.2	571	Client Hello
311	15.659203	66.110.49.116	192.168.1.73	TLSv1.2	109	Application Data
312	15.659203	66.110.49.116	192.168.1.73	TLSv1.2	165	Application Data
316	15.683325	2600:1700:466a:41a0…	2607:f8b0:4002:c09:…	TLSv1.3	591	Client Hello
318	15.698171	66.110.49.116	192.168.1.73	TLSv1.2	201	Application Data

Server Hello:

The server with the selected password set and the server responds randomly. This message server also includes the following

318	15.698171	66.110.49.116	192.168.1.73	TLSv1.2	201	Application Data
320	15.716759	54.204.196.80	192.168.1.73	TLSv1.2	1514	Server Hello
323	15.717570	54.204.196.80	192.168.1.73	TLSv1.2	446	Certificate, Server
325	15.719219	192.168.1.73	54.204.196.80	TLSv1.2	180	Client Key Exchange,
328	15.739851	2607:f8b0:4002:c09:…	2600:1700:466a:41a0…	TLSv1.3	1294	Server Hello, Change
331	15.739851	2607:f8b0:4002:c09:…	2600:1700:466a:41a0…	TLSv1.3	1055	Application Data

Client Key Exchange:

The client then offers his help to the session key. The characteristics of this step depend on the key exchange method that is decided in the initial "Hello" messages. In this example we look at RSA, so the client wants to generate a random string of bytes called secret pre-master, then encrypt it with the server's public key and send it.

318	15.698171	66.110.49.116	192.168.1.73	TLSv1.2	201	Application Data
320	15.716759	54.204.196.80	192.168.1.73	TLSv1.2	1514	Server Hello
323	15.717570	54.204.196.80	192.168.1.73	TLSv1.2	446	Certificate, Server Key Exchange,
325	15.719219	192.168.1.73	54.204.196.80	TLSv1.2	180	Client Key Exchange, Change Cipher
328	15.739851	2607:f8b0:4002:c09:…	2600:1700:466a:41a0…	TLSv1.3	1294	Server Hello, Change Cipher Spec
331	15.739851	2607:f8b0:4002:c09:…	2600:1700:466a:41a0…	TLSv1.3	1055	Application Data

Changed Cipher Key:

The "change password" message informs the other party that it has generated the session key and is about to redirect to encrypted communications.

325	15.719219	192.168.1.73	54.204.196.80	TLSv1.2	180	Client Key Exchange, Change Cipher Spec,
328	15.739851	2607:f8b0:4002:c09:…	2600:1700:466a:41a0…	TLSv1.3	1294	Server Hello, Change Cipher Spec
331	15.739851	2607:f8b0:4002:c09:…	2600:1700:466a:41a0…	TLSv1.3	1055	Application Data
333	15.743632	2600:1700:466a:41a0…	2607:f8b0:4002:c09:…	TLSv1.3	138	Change Cipher Spec, Application Data
334	15.743747	2600:1700:466a:41a0…	2607:f8b0:4002:c09:…	TLSv1.3	166	Application Data

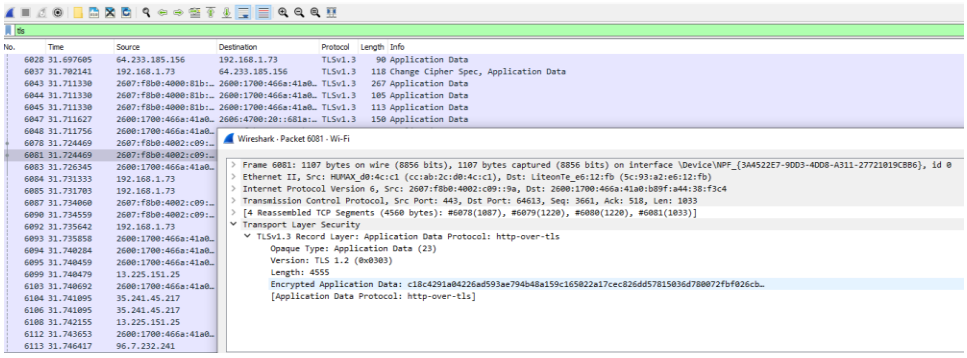
9-

A)

A WEP key allows computers on the network to exchange encrypted messages while hiding the contents of the messages from attackers. This key is what is used to connect to a

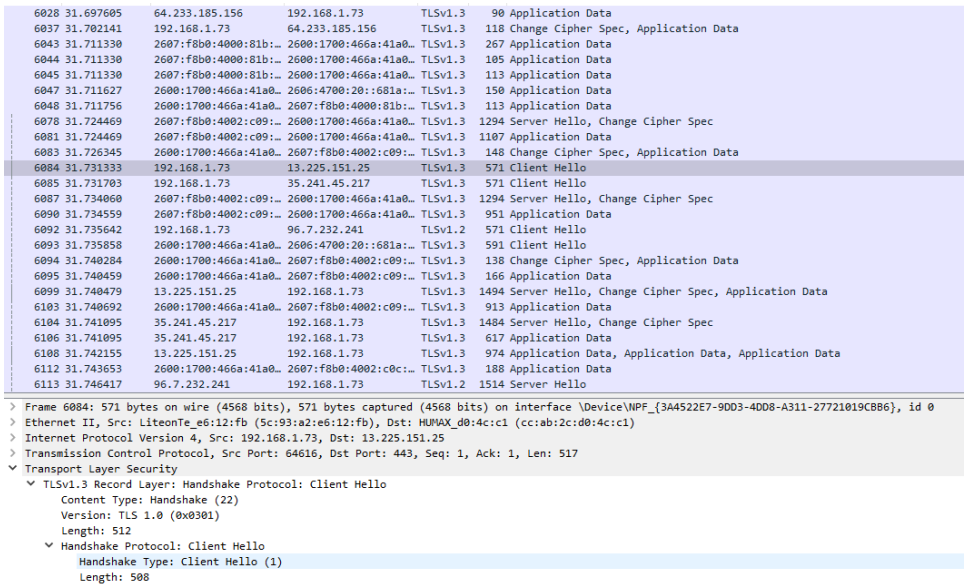
Farzad Kheirabadi
CYB 555
Final

wireless security network. WPA2 was introduced in 2004 and was an upgraded version of WPA. WPA involves checking the integrity of the message to determine if an attacker has taken or changed data packets.



B)

Yes

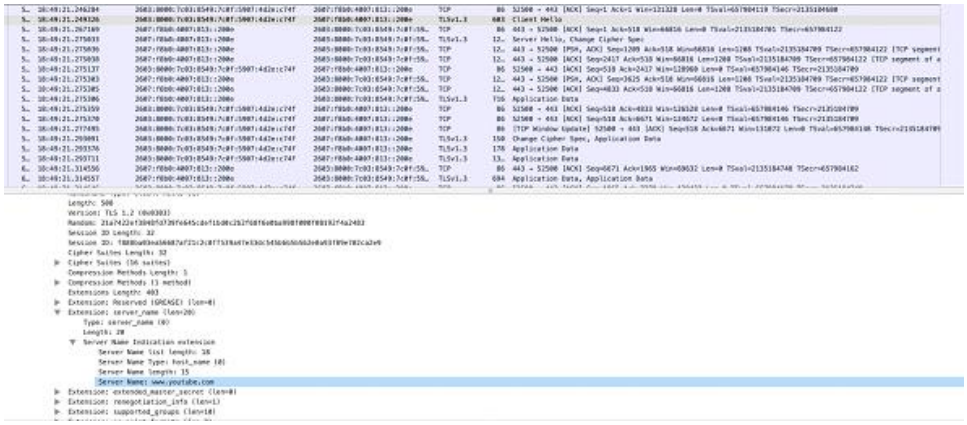


C)

It must request our local system, called the SSL key log file, to save them locally and save them to our computer. It can only decrypt certain types of programs. DTTPS and Quick are some of them. The next step is to open a browser that supports this feature, which Chrome Firefox usually does. Then we go to the site we want to test. When a client reaches a server, both the client and the server generate random keys. This is a private key that allows them to access the

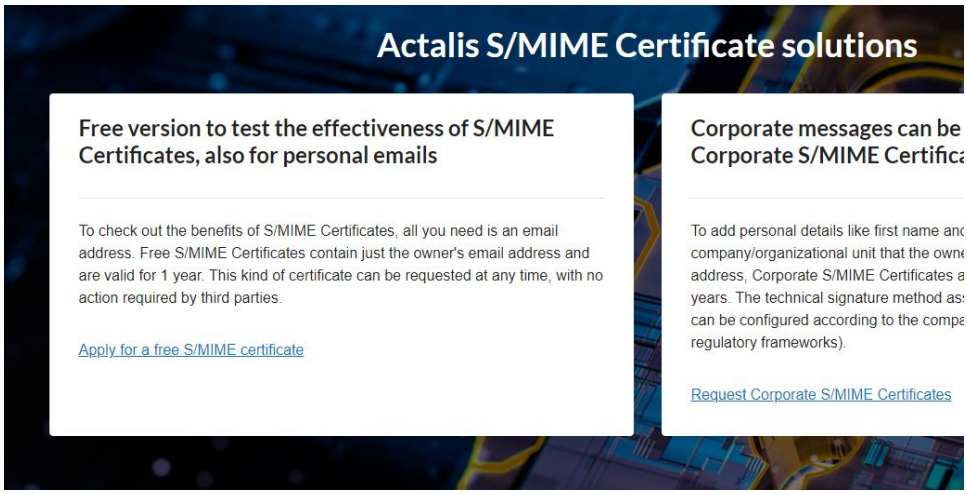
Farzad Kheirabadi
CYB 555
Final

same key on either side without sending it to the other party. Then we do our first loss from the computer to the server.



10-

Farzad Kheirabadi
CYB 555
Final



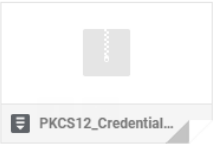
User Code: 3sood.info@gmail.com (to be included in the Tax Code field)

Private Personal Code (CRP): WM422621923582

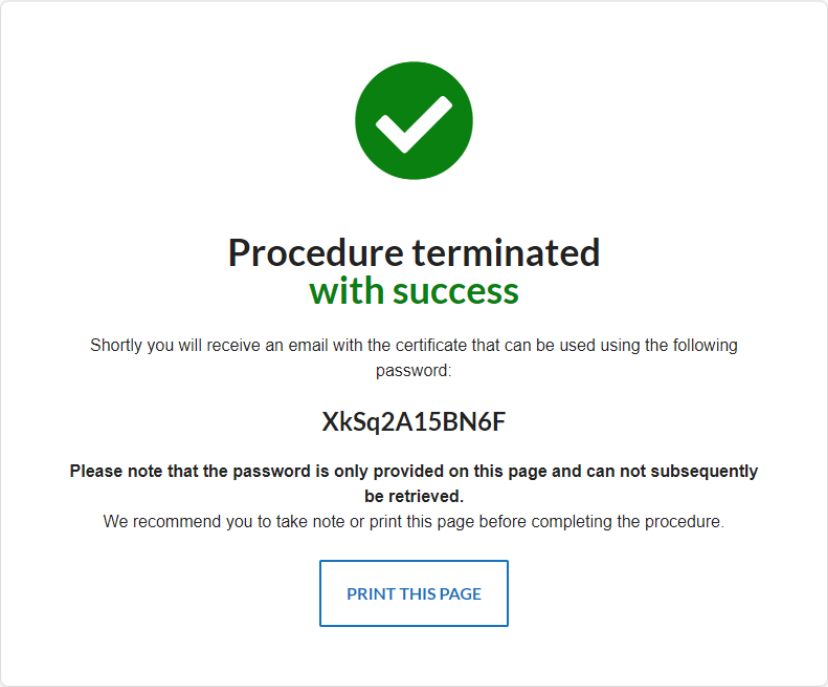
Thank you for choosing our services.

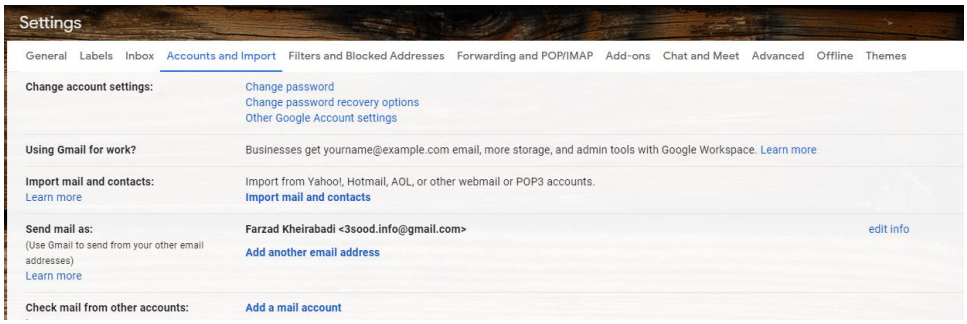
Best regards.

Actalis S.p.A.
Via S. Clemente, 53
24036 Ponte San Pietro (BG)
P.IVA 03358520867
https://www.actalis.it

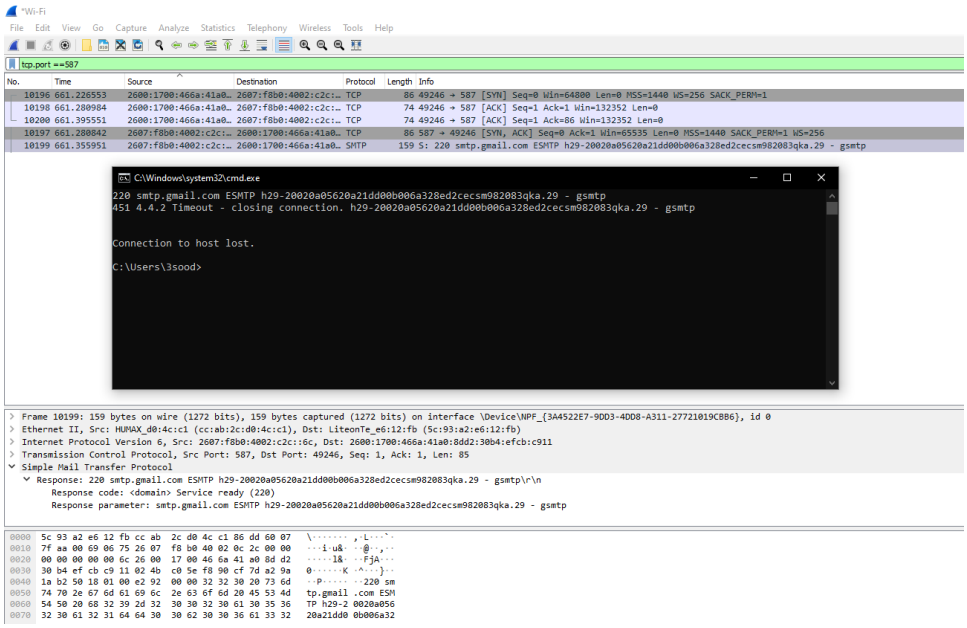


Farzad Kheirabadi
CYB 555
Final





Farzad Kheirabadi
CYB 555
Final



MIME (Secure / Multipurpose Internet Email Extensions) as the global web standard. S / MIME is used to encrypt MIME data, which is essentially email. It is based on public key infrastructure (PKI) or asymmetric encryption and improves email security by encrypting, authenticating and authenticating messages. In other words, it enables you to digitally sign your emails and make sure that only the intended recipient sees the message and is aware of it.

I. Protection against e-mail corruption during transport: Viruses, spyware, trojan horses, computer worms, rootkits, and other malicious software can not be entered by cybercriminals in the e-mail that is on the way.
II. Email forgery protection: Email recipients are protected against forgery using digital signatures. The digital signature of the official employees of the company cannot be imitated. As a result, no one can fool recipients by sending fake emails that look like corporate emails.
III. No rejection: The sender can not reject the e-mail or its contents. The digital signature confirms that the email originates from the client who signed the email.
IV. Warns recipients: Warns recipients quickly if an email or digital signature is tampered with.