

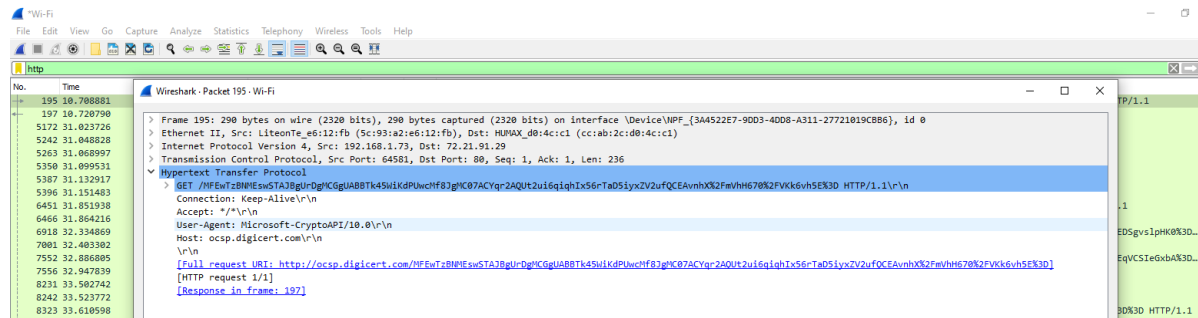
**2-**

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Icons]
Time Source Destination Protocol Length Info
195 108-7088881 192.168.1.73 192.72.91.29 HTTP 200 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
196 192.72.91.29 192.168.1.73 HTTP 793 Response
51572 31.827276 192.168.1.73 192.124.249.23 HTTP 274 GET /?HQcQJ3B4WdPQ4JgBgDgCgUABRT1nE8X2K6FqWqEj1fH3GQWQ45uWqHtP8x5PaR26B3aHj01C4CwvEQU30D HTTP/1.1
5242 31.848820 192.124.249.23 192.168.1.73 OCSP 823 Response
5300 31.860997 192.168.1.73 192.124.249.23 HTTP 270 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
5359 31.899531 192.124.249.23 192.168.1.73 OCSP 793 Response
5387 31.132971 192.168.1.73 192.124.249.23 HTTP 274 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
5396 31.154403 192.124.249.23 192.168.1.73 OCSP 962 Response
5440 31.855139 192.168.1.73 192.72.91.29 HTTP 270 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
5446 31.864616 72.21.91.29 192.168.1.73 OCSP 793 Response
5932 32.334680 2000:1700:4604::1a4b::2000:1700:4602::1c10:: HTTP 323 GET /?1g1t1A/VH3x1x1qQ/?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
7800 32.401392 2000:1700:4602::1c10::2000:1700:4604::1a4b:: HTTP 323 GET /?1g1t1A/hn0h01z1fQ/?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
7850 32.408608 2000:1700:4602::1c10::2000:1700:4604::1a4b:: HTTP 793 Response
7550 32.394739 2000:1700:4602::1c10::2000:1700:4604::1a4b:: HTTP 793 Response
8235 32.150274 192.168.1.73 192.124.249.23 HTTP 270 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
8424 32.523772 192.124.249.23 192.168.1.73 OCSP 963 Response
8321 33.619594 2000:1700:4604::1a4b::2000:1400:5000:1774:: HTTP 315 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
8341 33.619701 2000:1700:4604::1a4b::2000:1400:5000:1774:: HTTP 315 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
8407 33.21074 2000:1700:4604::1a4b::2000:1400:5000:1774:: HTTP 315 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
8639 34.224262 2000:1400:5000:1774::2000:1700:4604::1a4b:: OCSP 963 Response
8688 34.224262 2000:1700:4604::1a4b::2000:1400:5000:1774:: HTTP 315 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
8694 34.447563 192.124.249.23 192.168.1.73 OCSP 963 Response
9075 35.251529 2000:1700:4604::1a4b::2000:4700:4400::1a4b:: HTTP 311 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1
9075 35.274485 2000:4700:4400::1a4b::2000:1700:4604::1a4b:: OCSP 1297 Response
9075 35.324711 2000:1700:4604::1a4b::2000:4700:4400::1a4b:: HTTP 367 GET /?PwUwZBMEw5a7A9gDgCgAB8B52CA1f6t26vPKXK4Zgu0y?PqGQW3x147W9IjPKX2y2z8LgQCACQc4A4PpJfU5cX0R30D HTTP/1.1

=====
Time Info: 190 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface \Device\NPF_{3A4522E7-900D-4008-4311-2772163C0B65}, id 0
Frame 195: 190 bytes captured on interface \Device\NPF_{3A4522E7-900D-4008-4311-2772163C0B65}, id 0
Ethernet II, Src: Liteonite_80:12:1f:5c (9c:83:92:a6:12:f1), Dst: MAXIM_00:4c:1c (cc:bb:12:c1:00:4c:1c)
Transmission Protocol Version 4, Src: 192.168.1.73, Dst: 72.21.91.29
Hypertext Transfer Protocol
cc ab 97 34 5d 00 80 36 f6 82 c0 01 49 45 15 ..g.....ZH
80 14 c5 40 50 63 2c c0 3f 30 b8 35 b0 18 .....D E C ; 3 P
01 08 4e 40 07 45 54 20 47 40 46 57 75 d ..-G/?PwUw
42 4d 4d 77 53 54 41 42 67 55 72 44 2bREwZBMEw5a7A9gDgCg
67 4d 43 67 55 41 42 62 54 35 67 69 40 ..G?PwUwZBMEw5a7A9gDgCg
69 57 77 63 46 66 38 67 43 38 37 43 3f ..@PwUwZBMEw5a7A9gDgCg
57 72 32 41 55 74 32 75 69 38 67 69 71 ..G?PwUwZBMEw5a7A9gDgCg

```

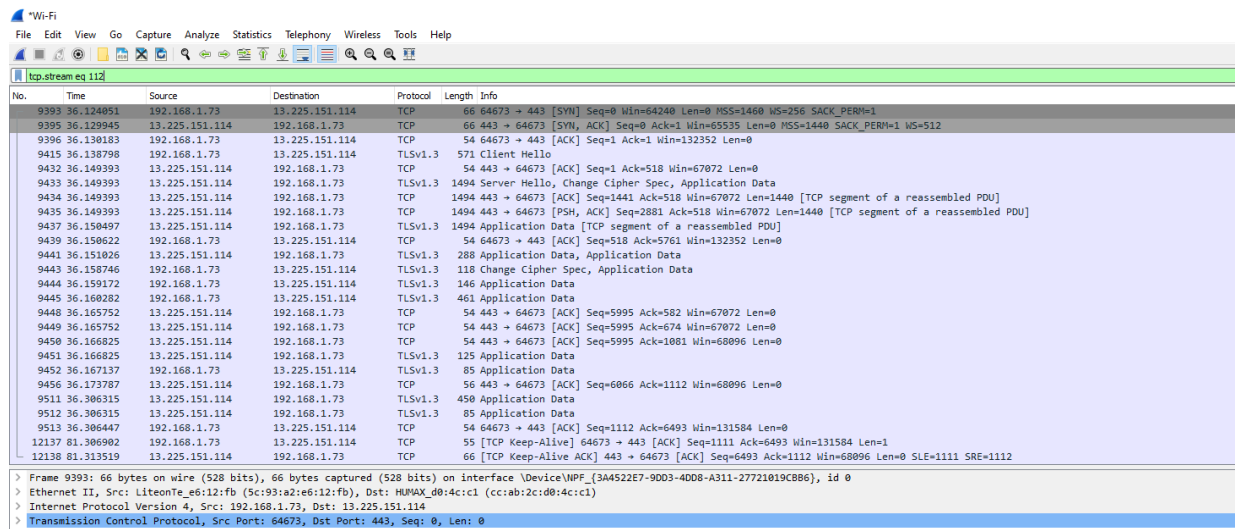


## Passive attack

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

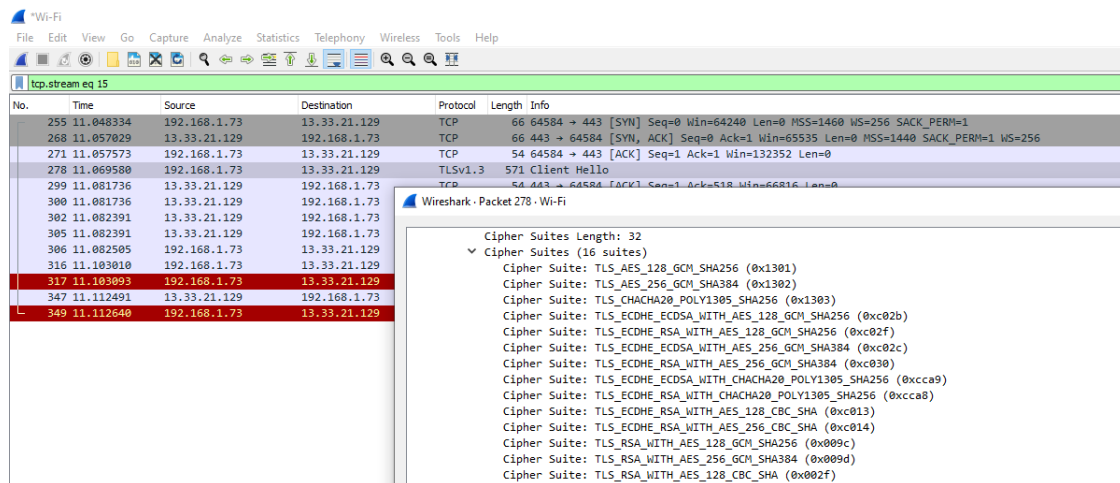
It can be network abuse in which attackers alter or modify the content and affect the source of the system. Victims can be notified of an active attack. This type of attack can threaten their integrity and accessibility.



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

## 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.

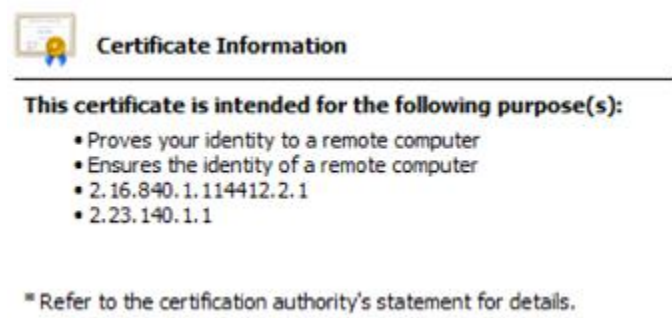


So, the cipher set is basically a set of encryption rules for TLS loss. This creates a secure key for encryption in the TLS protocol. In this password set, the key is generated in the web browser site and then this key is sent to the encrypted web server which is the public key.

## TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc09d)

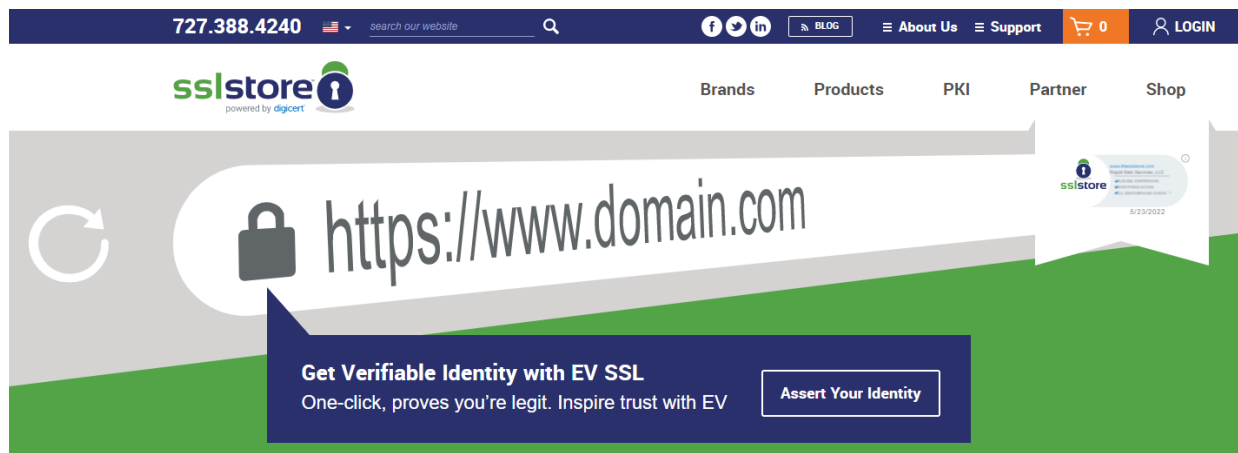
```
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)
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)
```

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-

certmgr - [Certificates - Current User\Personal\Certificates]

File Action View Help

Certificates - Current User

- Personal
  - Certificates
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Objects
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Client Authentication Issuers
  - Other People
  - Smart Card Trusted Roots

Issued To: 8B64AF0C-A9D1-472B-AD94-C...  
farzad.inter@yahoo.com

Issued By: Apple iPhone Device CA  
Actalis Client Authentication CA G3

Certificate

General Details Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	042587c2501f7a9342bc
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Apple iPhone Device CA, Appl...
Valid from	Tuesday, January 18, 2022 9:...
Valid to	Wednesday, January 18, 202...
Subject	8B64AF0C-A9D1-472B-AD94-

certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Help

Issued To	Issued By	Expiration Date	Intended Purpose	Friendly Name	Status	Certificate Tem...
Actalis Authentication Root CA	Actalis Authentication Root CA	12/31/2020	Client Authentication...	Actalis (Actalis)		
Actalis External CA Root	Actalis External CA Root	9/22/2020	Client Authentication...	Actalis Authentication...		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/10/2025	Client Authentication...	Design (AddTrust)		
Centum CA	Centum CA	6/11/2027	Client Authentication...	Centum		
Centum Trusted Network CA	Centum Trusted Network CA	12/31/2029	Client Authentication...	Centum Trusted Net...		
Class 3 Public Primary Certification...	Class 3 Public Primary Certification...	8/1/2028	Client Authentication...	Issuing Class 3 Pri...		
COMODO RSA Certification Auth...	COMODO RSA Certification Auth...	1/18/2028	Client Authentication...	Design (Formerly C...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp...	12/30/1999	Time Stamping	Microsoft Time...		
Digicert Assured ID Root CA	Digicert Assured ID Root CA	11/9/2021	Client Authentication...	<None>		
Digicert Assured ID Root CA	Digicert Assured ID Root CA	11/9/2021	Client Authentication...	Digicert		
Digicert Global Root CA	Digicert Global Root CA	11/9/2021	Client Authentication...	Digicert		
Digicert Global Root G2	Digicert Global Root G2	1/15/2028	Client Authentication...	Digicert Global Root...		
Digicert High Assurance EV Root...	Digicert High Assurance EV Root...	11/9/2021	<None>	<None>		
Digicert High Assurance EV Root...	Digicert High Assurance EV Root...	11/9/2021	Client Authentication...	Digicert		
Digicert Trusted Root G4	Digicert Trusted Root G4	1/15/2028	Client Authentication...	Digicert Trusted Ro...		
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authentication...	DST Root CA X3		
Entrust Root Certification Auth...	Entrust Root Certification Auth...	11/27/2026	Client Authentication...	Entrust		
Entrust Root Certification Auth...	Entrust Root Certification Auth...	12/7/2020	Client Authentication...	Entrust.net		
Entrust.net Certification Auth...	Entrust.net Certification Auth...	7/24/2029	Client Authentication...	Entrust (DAD)		
E-Traffic Certification Authority	E-Traffic Certification Authority	3/5/2021	Client Authentication...	E-Traffic Certificati...		
GlobalSign	GlobalSign	3/10/2029	Client Authentication...	GlobalSign Root CA...		
GlobalSign	GlobalSign	12/9/2024	Client Authentication...	GlobalSign Root CA...		
GlobalSign Code Signing Root R5	GlobalSign Code Signing Root R5	3/17/2045	Code Signing	GlobalSign Code Si...		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authentication...	GlobalSign Root CA...		
Go Daddy Class 2 Certification...	Go Daddy Class 2 Certification...	6/29/2024	Client Authentication...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Auth...	12/31/2027	Client Authentication...	Go Daddy Root Cer...		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2016	Client Authentication...	Digicert Global Root		
HiTrust 2.0 Trust Root CA - (S)	HiTrust 2.0 Trust Root CA - (S)	12/8/2040	Client Authentication...	HiTrust 2.0 Trust R...		
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	1/16/2024	Client Authentication...	IdenTrust Commenc...		
OID Root X1	OID Root X1	6/4/2021	Client Authentication...	OID Root X1		
Responsible Adult Visual Personal R...	Responsible Adult Visual Personal R...	1/16/2022	Secure Authentication...	<None>		
Microsoft Authentication Root...	Microsoft Authentication Root...	12/31/1999	Secure Email, Code...	Microsoft Authenti...		
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Cert...	2/27/2040	<None>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate...	2/27/2040	<None>	Microsoft ECC TS R...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<None>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Auth...	5/9/2021	<None>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Auth...	6/23/2025	<None>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Auth...	1/22/2026	<None>	Microsoft Root Cert...		

Farzad Kheirabadi  
CYB 555  
Final

The first screenshot shows the 'Intermediate Certification Authorities' view. The second screenshot shows the 'Third-Party Root Certification Authorities' view. The third screenshot shows the 'Trusted Publishers' view. Each view displays a list of certificates with columns for Issued To, Issued By, Expiration Date, Intended Purposes, Friendly Name, Status, and Certificate Template.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
Actalis Client Authentication C...	Actalis Authentication Root CA	9/22/2030	Client Authentication...	Actalis Client Auth...		
DigiCert SHA2 Assured ID Code...	DigiCert Assured ID Root CA	10/22/2028	Code Signing	<None>		
DigiCert SHA2 Secure Server CA	DigiCert Global Root CA	3/8/2023	<All>	<None>		
DigiCert TLS RSA SHA256 2020...	DigiCert Global Root CA	4/13/2031	Server Authentication...	<None>		
DigiCert Trusted G4 Code Signi...	DigiCert Trusted Root G4	4/28/2036	Code Signing	<None>		
Go Daddy Secure Certificate Au...	Go Daddy Root Certificate Autho...	5/3/2031	<All>	<None>		
Microsoft TLS CA 02	Baltimore CyberTrust Root	10/9/2024	Server Authentication...	<None>		
Microsoft Windows Hardware ...	Microsoft Root Authority	12/31/2002	Code Signing, Win...	<None>		
Root Agency	Root Agency	12/31/2030	<All>	<None>		
Sectigo RSA Domain Validation ...	USERTrust RSA Certification Autho...	12/31/2030	Server Authentication...	<None>		
Starfield Services Root Certific...	Starfield Class 2 Certification Auth...	6/28/2034	<All>	<None>		
Symantec Class 3 SHA256 Code...	VeriSign Universal Root Certificat...	7/21/2024	Code Signing	<None>		
USERTrust ECC Certification Aut...	AAA Certificate Services	12/31/2030	<All>	<None>		
USERTrust RSA Certification Aut...	AAA Certificate Services	12/31/2030	<All>	<None>		
www.verisign.com/CP5 Incomp...	Class 3 Public Primary Certificatio...	10/24/2016	Server Authentication...	<None>		
ZeroSSL RSA Domain Secure S...	USERTrust RSA Certification Autho...	1/29/2030	Server Authentication...	<None>		

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authentication...	Sectigo (AAA)		
Actalis Authentication Root CA	Actalis Authentication Root CA	9/22/2030	Client Authentication...	Actalis Authentica...		
AddTrust External CA Root	AddTrust External CA Root	5/8/2020	Client Authentication...	Sectigo (AddTrust)		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authentication...	DigiCert Baltimore ...		
Certum CA	Certum CA	6/11/2027	Client Authentication...	Certum		
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authentication...	Certum Trusted Net...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2023	Client Authentication...	VeriSign Class 3 Pu...		
COMODO RSA Certification Aut...	COMODO RSA Certification Auth...	1/18/2030	Client Authentication...	Sectigo (Comodo)		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication...	DigiCert Global Ro...		
DigiCert High Assurance EV Root...	DigiCert High Assurance EV Root...	11/9/2031	Client Authentication...	DigiCert		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authentication...	DigiCert Trusted Ro...		
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authentication...	DST Root CA X3		
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/27/2026	Client Authentication...	Entrust		
Entrust Root Certification Auth...	Entrust Root Certification Authority...	12/1/2030	Client Authentication...	Entrust.net		
Entrust.net Certification Auth...	Entrust.net Certification Authority...	7/24/2029	Client Authentication...	Entrust (DSS)		
E-Tugra Certification Authority	E-Tugra Certification Authority	3/4/2023	Client Authentication...	E-Tugra Certificat...		
GlobalSign	GlobalSign	3/18/2028	Client Authentication...	GlobalSign Root CA...		
GlobalSign Code Signing Root...	GlobalSign Code Signing Root R15	3/17/2045	Code Signing	GlobalSign Code Si...		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authentication...	GlobalSign Root CA...		
Go Daddy Class 2 Certification...	Go Daddy Class 2 Certification Au...	6/28/2034	Client Authentication...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Autho...	12/31/2037	Client Authentication...	Go Daddy Root Ce...		
OTR CyberTrust Global Root	OTR CyberTrust Global Root	6/15/2016	Client Authentication...	DigiCert Global Root		
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Client Authentication...	Hotspot 2.0 Trust R...		
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	1/16/2034	Client Authentication...	IdenTrust Commer...		
GBS Root X1	GBS Root X1	6/4/2033	Client Authentication...	GBS Root X1		
Quintado Root CA 2	Quintado Root CA 2	11/24/2031	Client Authentication...	Quintado Root CA 2		
Quintado Root Certification Aut...	Quintado Root Certification Auth...	3/17/2021	Client Authentication...	Quintado Root Cert...		
Security Communication RootCA1	Security Communication RootCA1	6/28/2023	Client Authentication...	SECUM Trust Syst...		
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	6/28/2034	Client Authentication...	Starfield Class 2 Ce...		
Starfield Root Certificate Auth...	Starfield Root Certificate Autho...	12/31/2037	Client Authentication...	Starfield Root Cert...		
Thawte Primary Root CA	Thawte Primary Root CA	7/16/2036	Client Authentication...	Thawte		
USERTrust RSA Certification Aut...	USERTrust RSA Certification Autho...	1/18/2038	Client Authentication...	Sectigo		
VeriSign Class 3 Public Primary...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Client Authentication...	VeriSign		
VeriSign Universal Root Certific...	VeriSign Universal Root Certificat...	12/1/2037	Client Authentication...	VeriSign Universal R...		

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
DigiCert EV Code Signing CA (S...	DigiCert High Assurance EV Root ...	4/18/2027	Code Signing	<None>
DigiCert SHA2 Assured ID Time...	DigiCert Assured ID Root CA	1/7/2031	Time Stamping	<None>
DigiCert Timestamp 2021	DigiCert SHA2 Assured ID Timesta...	1/5/2031	Time Stamping	<None>
Insecure.Com LLC	DigiCert EV Code Signing CA (SH...	5/7/2021	Code Signing	<None>
Insecure.Com LLC	DigiCert EV Code Signing CA (SH...	6/10/2024	Code Signing	<None>
Oracle Corporation	DigiCert Assured ID Code Signing ...	3/23/2022	Code Signing	<None>
Steinberg Media Technologies ...	VeriSign Class 3 Code Signing 200...	6/25/2010	Code Signing	<None>
Vincent Burel	VeriSign Class 3 Code Signing 201...	1/1/2015	Code Signing	<None>

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

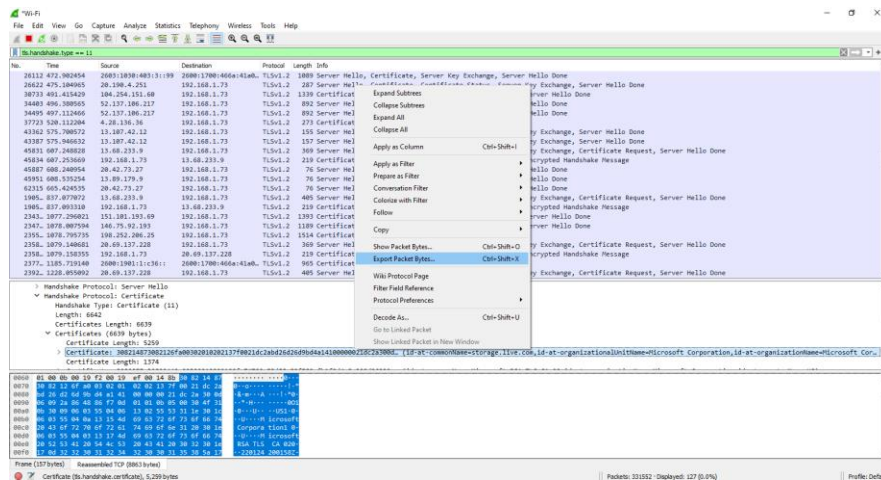
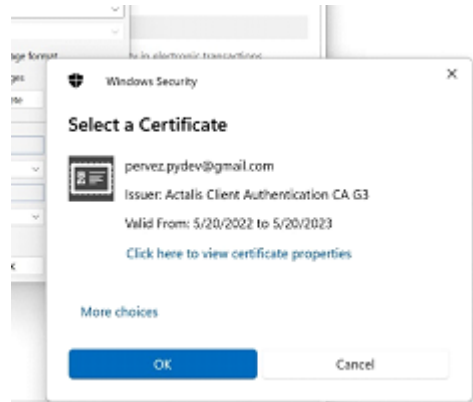


- [illegible]

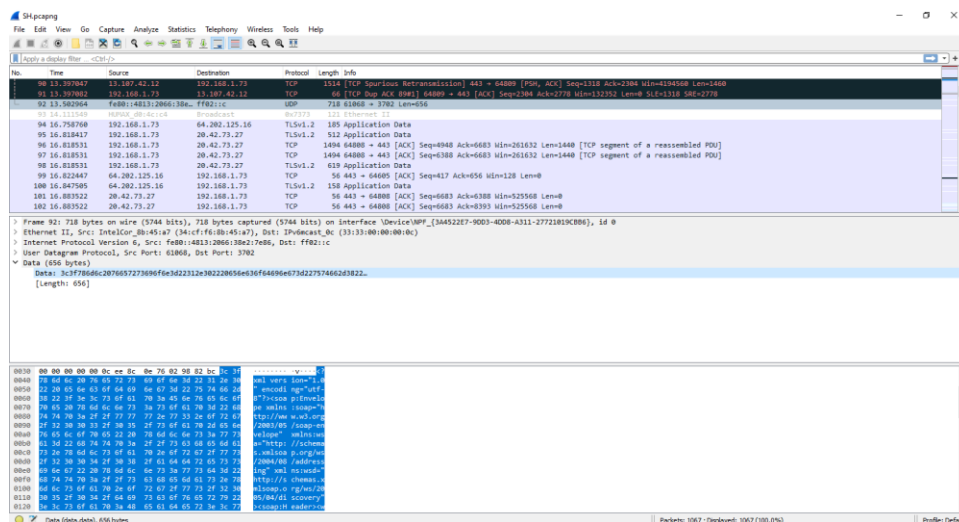
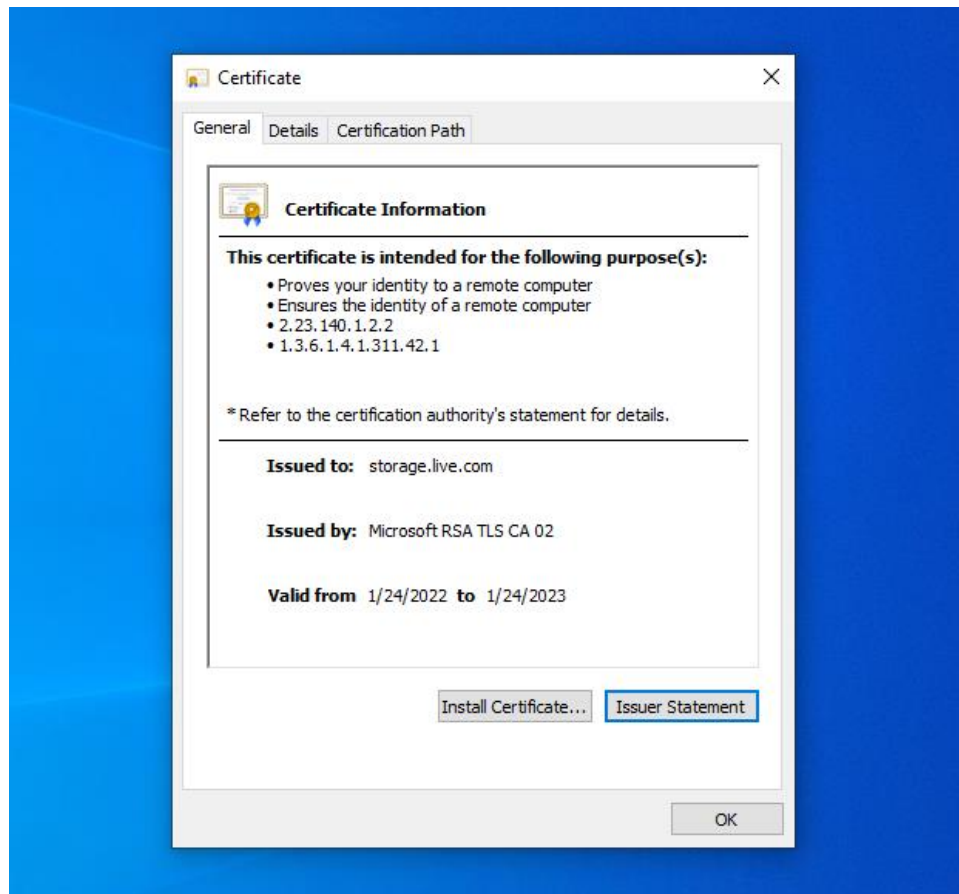
[illegible]

Field	Value
Version	V3
Serial number	01
Signature algorithm	sha1RSA
Signature hash algorithm	sha1

6-



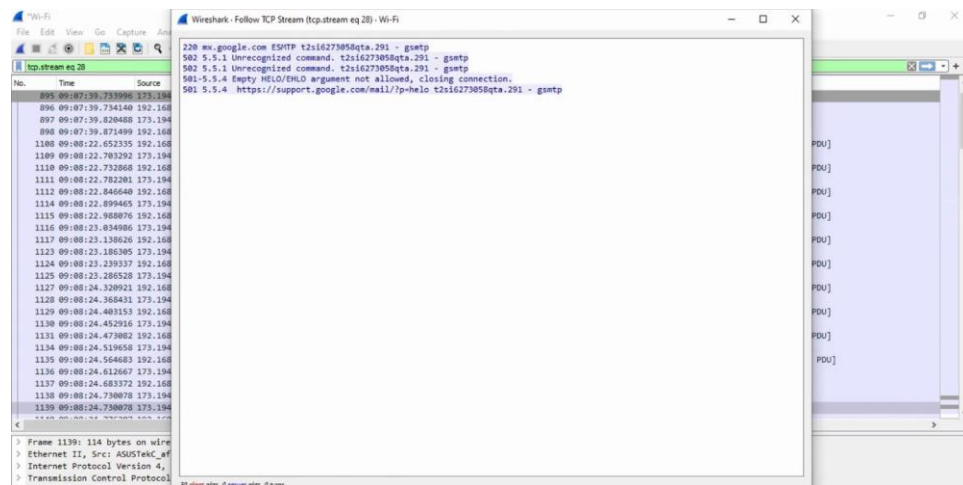
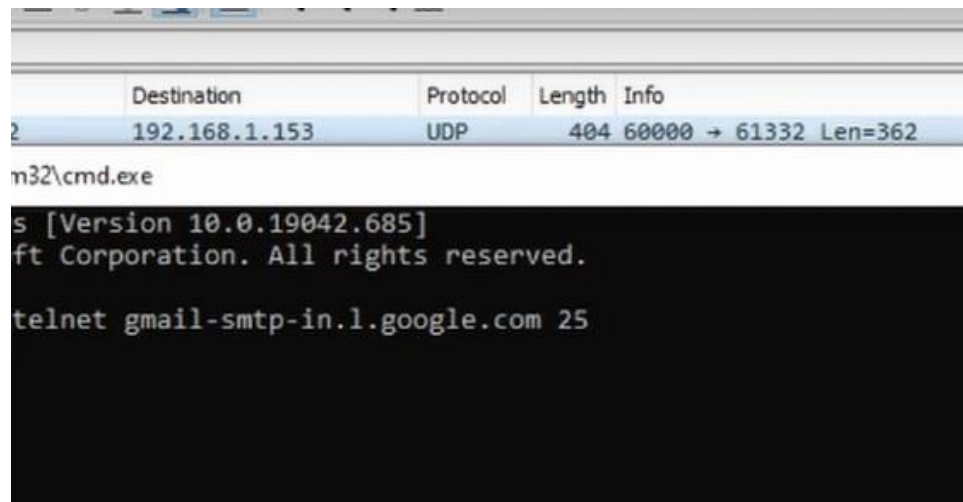
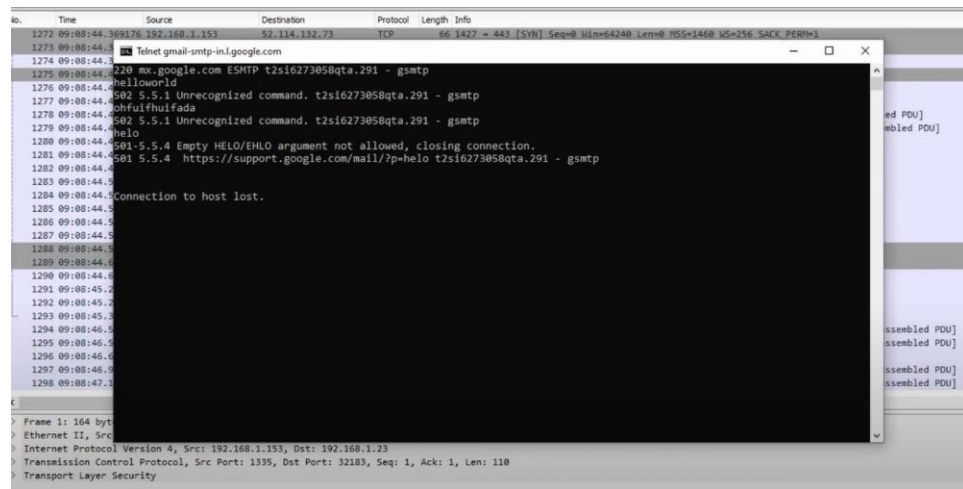




Farzad Kheirabadi

CYB 555

Final



7-

No.	Time	Source	Destination	Protocol	Length	Info
248	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	11.086935	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\_{3A4522E7-9003-4008-A311-27721019C886}, id 0  
> Ethernet II, Src: HPVAX\_00:4e:c1 (cc:ab:2c:d0:4e: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  
▼ Transport Layer Security

Wireshark · Packet 5075 · Wi-Fi

Length: 2321

- Handshake Protocol: Certificate
  - Handshake Type: Certificate (11)
  - Length: 2317
  - Certificates Length: 2314
  - Certificates (2314 bytes)
    - Certificate Length: 1331
    - Certificate: 3082052f308204d5a00302010202100980738736be70add3a3ab431d350aff300a06082a...
    - signedCertificate
      - version: v3 (2)
      - serialNumber: 0x0980738736be70add3a3ab431d350aff
      - signature (ecdsa-with-SHA256)
        - Algorithm Id: 1.2.840.10045.4.3.2 (ecdsa-with-SHA256)
      - issuer: rdnSequence (0)
      - validity

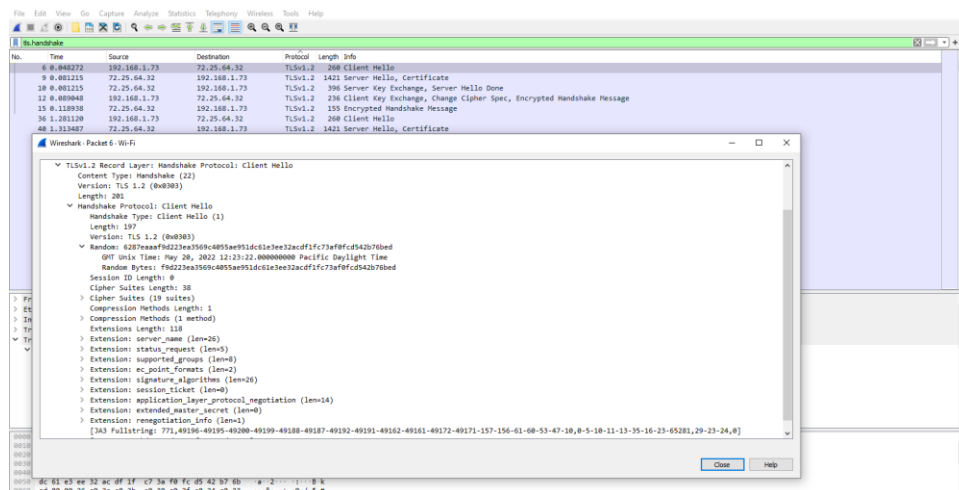
Wireshark · Packet 5075 · Wi-Fi

a3ab431d350aff300a06082a... (id-at-commonName=sn1.cloudflaressl.com,id-at-organizationName=Cloudflare, Inc.,id-at-localityName=San Francisco,id-at-stateOrProvinceName=California)

0000 16 03 03 09 11 0b 00 00 0d 00 00 0a 00 05 33 3a .....-30-  
0010 82 05 2f 30 82 04 45 a0 03 02 01 02 02 10 09 08 .../0.....  
0020 73 87 36 be 70 ad d3 a3 ab 43 1d 35 0a ff 30 0a ...s6p...C.S-0-  
0030 06 08 2a 06 40 ce 50 04 03 02 30 43 51 00 20 06 ...s6p...031-0-  
0040 06 03 55 04 06 13 00 55 53 31 19 30 17 06 03 55 ...U...U S:0-0-  
0050 04 0a 13 10 43 6c 6f 75 64 66 6c 61 72 65 2c 20 ...Cloudflare,  
.....

- 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.

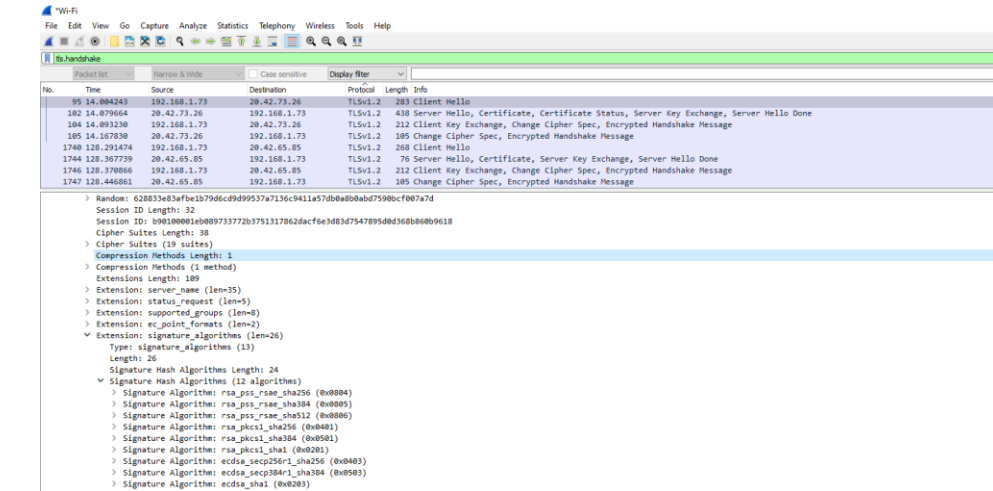
Authenticate the identity of the server via the server's public key and the SSL certificate authority's digital signature. Transport Layer Security (TLS) provides security in communication between two hosts. It provides integrity, authentication and confidentiality. It is used mostly in web browsers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



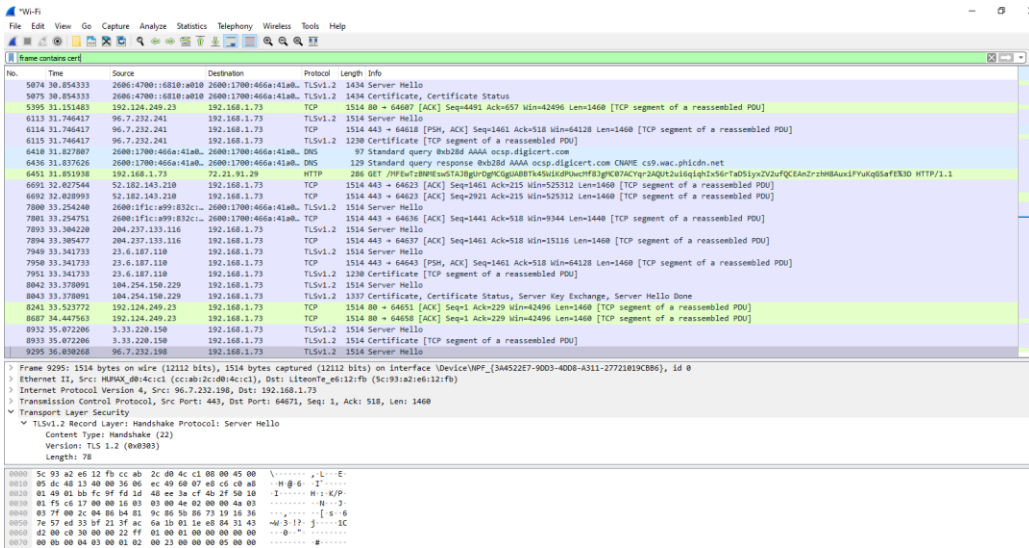
A TLS/SSL handshake is the process that starts this secure communication session that uses the TLS/SSL encryption technique.

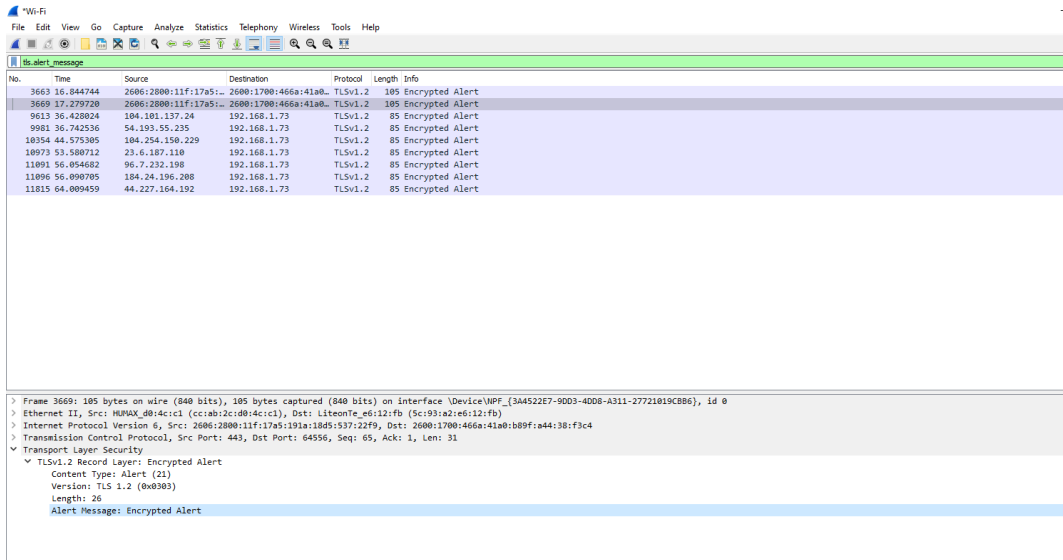
During a TLS handshake the following processes will occur in the order below:

- 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.



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".





The image shows a Wireshark packet capture of a TLS connection. The packet list pane displays several packets, with packet 3669 selected. The packet details pane shows the structure of the selected packet, which is a TLS alert message.

No.	Time	Source	Destination	Protocol	Length	Info
3663	16.844744	2606:2800:11f:17a5::	2600:1700:466a:41a0::	TLSv1.2	105	Encrypted Alert
3669	17.279720	2606:2800:11f:17a5::	2600:1700:466a:41a0::	TLSv1.2	105	Encrypted Alert
9613	26.428024	104.101.137.24	192.168.1.73	TLSv1.2	85	Encrypted Alert
9981	36.742536	54.193.55.235	192.168.1.73	TLSv1.2	85	Encrypted Alert
10354	44.575305	104.254.150.229	192.168.1.73	TLSv1.2	85	Encrypted Alert
10973	53.580712	23.6.187.110	192.168.1.73	TLSv1.2	85	Encrypted Alert
11091	56.054682	96.7.232.198	192.168.1.73	TLSv1.2	85	Encrypted Alert
11096	56.090705	184.24.196.208	192.168.1.73	TLSv1.2	85	Encrypted Alert
11815	64.009459	44.227.164.192	192.168.1.73	TLSv1.2	85	Encrypted Alert

Frame 3669: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF\_{3A4522E7-90D3-40D8-A311-27721019CB86}, id 0

Ethernet II, Src: HUPAX\_d0:4c:c1 (cc:ab:2c:d0:4c:c1), Dst: LiteonTe\_e6:12:fb (5c:93:a2:e6:12:fb)

Internet Protocol Version 6, Src: 2606:2800:11f:17a5:191a:18d5:537:22f9, Dst: 2600:1700:466a:41a0:b89f:a44:38:f3c4

Transmission Control Protocol, Src Port: 443, Dst Port: 64556, Seq: 65, Ack: 1, Len: 31

Transport Layer Security

▼ TLSv1.2 Record Layer: Encrypted Alert

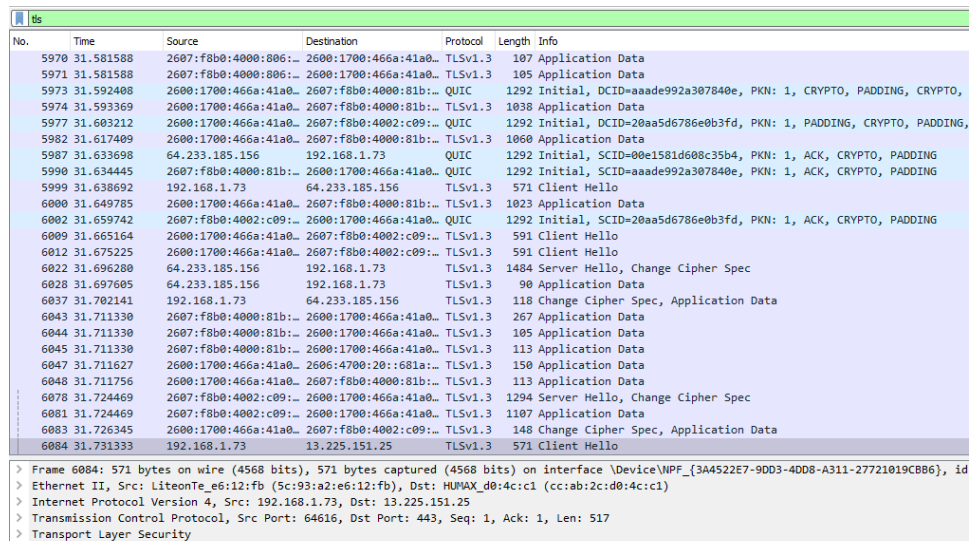
Content Type: Alert (21)

Version: TLS 1.2 (0x0303)

Length: 26

Alert Message: Encrypted Alert

8-



The image shows a Wireshark packet capture of a TLS connection. The packet list pane displays several packets, with packet 6084 selected. The packet details pane shows the structure of the selected packet, which is a TLS handshake message.

No.	Time	Source	Destination	Protocol	Length	Info
5970	31.581588	2607:f8b0:4000:806::	2600:1700:466a:41a0::	TLSv1.3	107	Application Data
5971	31.581588	2607:f8b0:4000:806::	2600:1700:466a:41a0::	TLSv1.3	105	Application Data
5973	31.592408	2600:1700:466a:41a0::	2607:f8b0:4000:81b::	QUIC	1292	Initial, DCID=aaade992a307840e, PKN: 1, CRYPTO, PADDING, CRYPTO,
5974	31.593369	2600:1700:466a:41a0::	2607:f8b0:4000:81b::	TLSv1.3	1038	Application Data
5977	31.603212	2600:1700:466a:41a0::	2607:f8b0:4000:81b::	QUIC	1292	Initial, DCID=20aa5d6786e0b3fd, PKN: 1, PADDING, CRYPTO, PADDING,
5982	31.617409	2600:1700:466a:41a0::	2607:f8b0:4000:81b::	TLSv1.3	1060	Application Data
5987	31.633698	64.233.185.156	192.168.1.73	QUIC	1292	Initial, SCID=00e1581d608c35b4, PKN: 1, ACK, CRYPTO, PADDING
5990	31.634445	2607:f8b0:4000:81b::	2600:1700:466a:41a0::	QUIC	1292	Initial, SCID=aaade992a307840e, PKN: 1, ACK, CRYPTO, PADDING
5999	31.638692	192.168.1.73	64.233.185.156	TLSv1.3	571	Client Hello
6000	31.649785	2600:1700:466a:41a0::	2607:f8b0:4000:81b::	TLSv1.3	1023	Application Data
6002	31.659742	2607:f8b0:4002:c09::	2600:1700:466a:41a0::	QUIC	1292	Initial, SCID=20aa5d6786e0b3fd, PKN: 1, ACK, CRYPTO, PADDING
6009	31.665164	2600:1700:466a:41a0::	2607:f8b0:4002:c09::	TLSv1.3	591	Client Hello
6012	31.675225	2600:1700:466a:41a0::	2607:f8b0:4002:c09::	TLSv1.3	591	Client Hello
6022	31.696280	64.233.185.156	192.168.1.73	TLSv1.3	1484	Server Hello, Change Cipher Spec
6028	31.697605	64.233.185.156	192.168.1.73	TLSv1.3	90	Application Data
6037	31.702141	192.168.1.73	64.233.185.156	TLSv1.3	118	Change Cipher Spec, Application Data
6043	31.711330	2607:f8b0:4000:81b::	2600:1700:466a:41a0::	TLSv1.3	267	Application Data
6044	31.711330	2607:f8b0:4000:81b::	2600:1700:466a:41a0::	TLSv1.3	105	Application Data
6045	31.711330	2607:f8b0:4000:81b::	2600:1700:466a:41a0::	TLSv1.3	113	Application Data
6047	31.711627	2600:1700:466a:41a0::	2606:4700:20:681a::	TLSv1.3	150	Application Data
6048	31.711756	2600:1700:466a:41a0::	2607:f8b0:4000:81b::	TLSv1.3	113	Application Data
6078	31.724469	2607:f8b0:4002:c09::	2600:1700:466a:41a0::	TLSv1.3	1294	Server Hello, Change Cipher Spec
6081	31.724469	2607:f8b0:4002:c09::	2600:1700:466a:41a0::	TLSv1.3	1107	Application Data
6083	31.726345	2600:1700:466a:41a0::	2607:f8b0:4002:c09::	TLSv1.3	148	Change Cipher Spec, Application Data
6084	31.731333	192.168.1.73	13.225.151.25	TLSv1.3	571	Client Hello

Frame 6084: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF\_{3A4522E7-90D3-40D8-A311-27721019CB86}, id 0

Ethernet II, Src: LiteonTe\_e6:12:fb (5c:93:a2:e6:12:fb), Dst: HUPAX\_d0:4c:c1 (cc:ab:2c:d0:4c:c1)

Internet Protocol Version 4, Src: 192.168.1.73, Dst: 13.225.151.25

Transmission Control Protocol, Src Port: 64616, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

Transport Layer Security

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.



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.

ip.addr == 192.168.1.73					
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	
▼ Transport Layer Security	
▼ 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
▼ Certificates (4067 bytes)
    Certificate Length: 1800
    ▼ Certificate: 308207043088205eca003020102021002acff05c
        ▼ 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.

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.

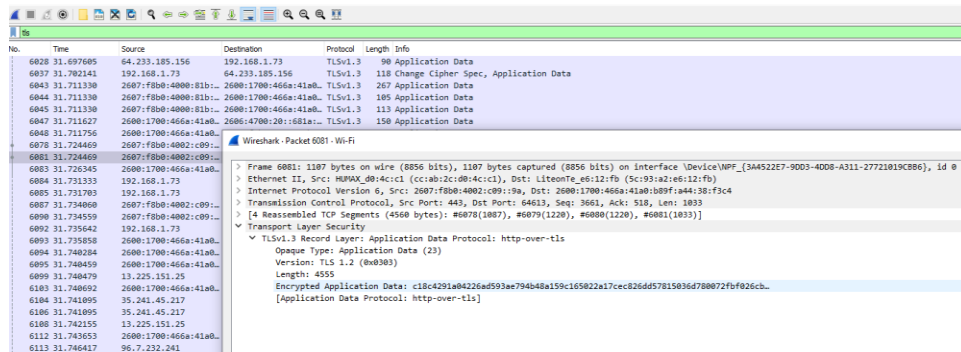
325	15.719219	192.168.1.73	54.204.196.80	TLSv1.2	180	Client Key Exchange, Change Cipher Spec,
328	15.739851	2607:f8b0:4002:c09:...	2600:1700:466a:41a0...	TLSv1.3	1294	Server Hello, Change Cipher Spec
331	15.739851	2607:f8b0:4002:c09:...	2600:1700:466a:41a0...	TLSv1.3	1055	Application Data
333	15.743632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

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.

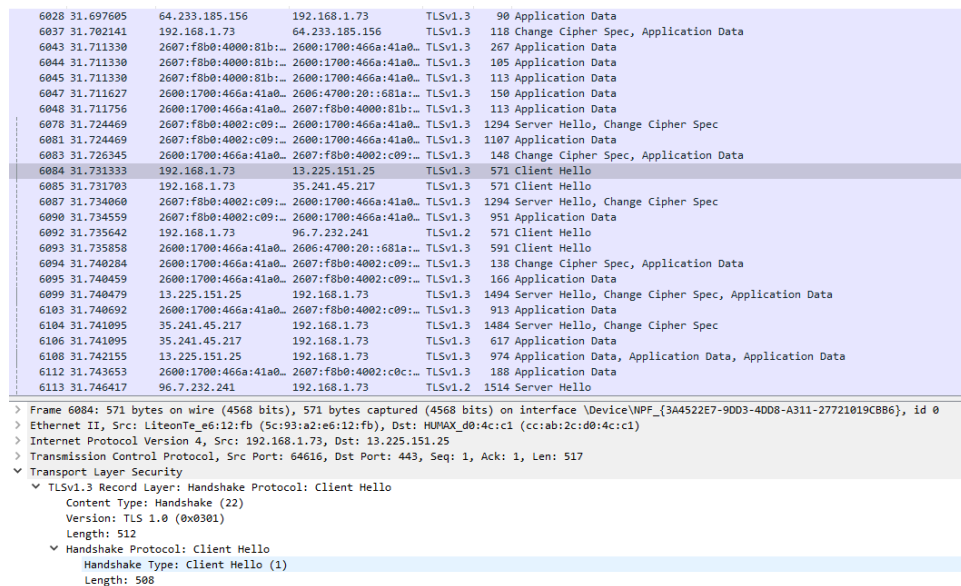


The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows packets 6028 through 6113. Packet 6081 is selected, showing details for the TLSv1.3 Record Layer, Application Data Protocol, and the application data itself. The application data is encrypted and contains the text: [Application Data Protocol: http-over-tls].

No.	Time	Source	Destination	Protocol	Length	Info
6028	31.697605	64.233.185.156	192.168.1.73	TLSv1.3	90	Application Data
6037	31.702141	192.168.1.73	64.233.185.156	TLSv1.3	118	Change Cipher Spec, Application Data
6043	31.711330	2607:f8b0:4000:81b...	2600:1700:466a:41a0...	TLSv1.3	267	Application Data
6044	31.711330	2607:f8b0:4000:81b...	2600:1700:466a:41a0...	TLSv1.3	185	Application Data
6045	31.711330	2607:f8b0:4000:81b...	2600:1700:466a:41a0...	TLSv1.3	113	Application Data
6047	31.711627	2600:1700:466a:41a0...	2606:4700:20:681a...	TLSv1.3	150	Application Data
6048	31.711756	2600:1700:466a:41a0...	2607:f8b0:4000:81b...	TLSv1.3	113	Application Data
6078	31.724469	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	1294	Server Hello, Change Cipher Spec
6081	31.724469	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	1107	Application Data
6083	31.726345	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	148	Change Cipher Spec, Application Data
6084	31.731333	192.168.1.73	13.225.151.25	TLSv1.3	571	Client Hello
6085	31.731703	192.168.1.73	35.241.45.217	TLSv1.3	571	Client Hello
6087	31.734060	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	1294	Server Hello, Change Cipher Spec
6090	31.734559	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	951	Application Data
6092	31.735642	192.168.1.73	96.7.232.241	TLSv1.2	571	Client Hello
6093	31.735858	2600:1700:466a:41a0...	2606:4700:20:681a...	TLSv1.3	591	Client Hello
6094	31.740284	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	138	Change Cipher Spec, Application Data
6095	31.740459	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	166	Application Data
6099	31.740479	13.225.151.25	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
6103	31.740692	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	913	Application Data
6104	31.741095	35.241.45.217	192.168.1.73	TLSv1.3	1484	Server Hello, Change Cipher Spec
6106	31.741095	35.241.45.217	192.168.1.73	TLSv1.3	617	Application Data
6108	31.742155	13.225.151.25	192.168.1.73	TLSv1.3	974	Application Data, Application Data
6112	31.743653	2600:1700:466a:41a0...	2607:f8b0:4002:c0c...	TLSv1.3	188	Application Data
6113	31.746417	96.7.232.241	192.168.1.73	TLSv1.2	1514	Server Hello

B)

Yes



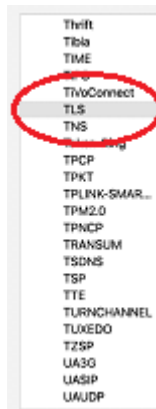
The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows packets 6028 through 6113. Packet 6084 is selected, showing details for the TLSv1.3 Record Layer, Handshake Protocol, and the client hello message. The client hello message is of type Client Hello (1) and has a length of 508 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
6028	31.697605	64.233.185.156	192.168.1.73	TLSv1.3	90	Application Data
6037	31.702141	192.168.1.73	64.233.185.156	TLSv1.3	118	Change Cipher Spec, Application Data
6043	31.711330	2607:f8b0:4000:81b...	2600:1700:466a:41a0...	TLSv1.3	267	Application Data
6044	31.711330	2607:f8b0:4000:81b...	2600:1700:466a:41a0...	TLSv1.3	185	Application Data
6045	31.711330	2607:f8b0:4000:81b...	2600:1700:466a:41a0...	TLSv1.3	113	Application Data
6047	31.711627	2600:1700:466a:41a0...	2606:4700:20:681a...	TLSv1.3	150	Application Data
6048	31.711756	2600:1700:466a:41a0...	2607:f8b0:4000:81b...	TLSv1.3	113	Application Data
6078	31.724469	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	1294	Server Hello, Change Cipher Spec
6081	31.724469	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	1107	Application Data
6083	31.726345	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	148	Change Cipher Spec, Application Data
6084	31.731333	192.168.1.73	13.225.151.25	TLSv1.3	571	Client Hello
6085	31.731703	192.168.1.73	35.241.45.217	TLSv1.3	571	Client Hello
6087	31.734060	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	1294	Server Hello, Change Cipher Spec
6090	31.734559	2607:f8b0:4002:c09...	2600:1700:466a:41a0...	TLSv1.3	951	Application Data
6092	31.735642	192.168.1.73	96.7.232.241	TLSv1.2	571	Client Hello
6093	31.735858	2600:1700:466a:41a0...	2606:4700:20:681a...	TLSv1.3	591	Client Hello
6094	31.740284	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	138	Change Cipher Spec, Application Data
6095	31.740459	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	166	Application Data
6099	31.740479	13.225.151.25	192.168.1.73	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
6103	31.740692	2600:1700:466a:41a0...	2607:f8b0:4002:c09...	TLSv1.3	913	Application Data
6104	31.741095	35.241.45.217	192.168.1.73	TLSv1.3	1484	Server Hello, Change Cipher Spec
6106	31.741095	35.241.45.217	192.168.1.73	TLSv1.3	617	Application Data
6108	31.742155	13.225.151.25	192.168.1.73	TLSv1.3	974	Application Data, Application Data
6112	31.743653	2600:1700:466a:41a0...	2607:f8b0:4002:c0c...	TLSv1.3	188	Application Data
6113	31.746417	96.7.232.241	192.168.1.73	TLSv1.2	1514	Server Hello

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

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

[illegible]

## Actalis S/MIME Certificate solutions

### Free version to test the effectiveness of S/MIME Certificates, also for personal emails

To check out the benefits of S/MIME Certificates, all you need is an email address. Free S/MIME Certificates contain just the owner's email address and are valid for 1 year. This kind of certificate can be requested at any time, with no action required by third parties.

[Apply for a free S/MIME certificate](#)

### Corporate messages can be Corporate S/MIME Certificate

To add personal details like first name and company/organizational unit that the owner address, Corporate S/MIME Certificates are valid for 10 years. The technical signature method as required by regulatory frameworks can be configured according to the company's regulatory frameworks).

[Request Corporate S/MIME Certificates](#)

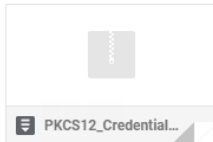
User Code: [3sood.info@gmail.com](mailto:3sood.info@gmail.com) (to be included in the Tax Code field)

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>





## Procedure terminated with success

Shortly you will receive an email with the certificate that can be used using the following password:

**XkSq2A15BN6F**

**Please note that the password is only provided on this page and can not subsequently be retrieved.**

We recommend you to take note or print this page before completing the procedure.

[PRINT THIS PAGE](#)

**Settings**

[General](#) [Labels](#) [Inbox](#) [Accounts and Import](#) [Filters and Blocked Addresses](#) [Forwarding and POP/IMAP](#) [Add-ons](#) [Chat and Meet](#) [Advanced](#) [Offline](#) [Themes](#)

**Change account settings:**

[Change password](#)  
[Change password recovery options](#)  
[Other Google Account settings](#)

**Using Gmail for work?**

Businesses get yourname@example.com email, more storage, and admin tools with Google Workspace. [Learn more](#)

**Import mail and contacts:**

[Learn more](#)  
Import from Yahoo!, Hotmail, AOL, or other webmail or POP3 accounts.  
[Import mail and contacts](#)

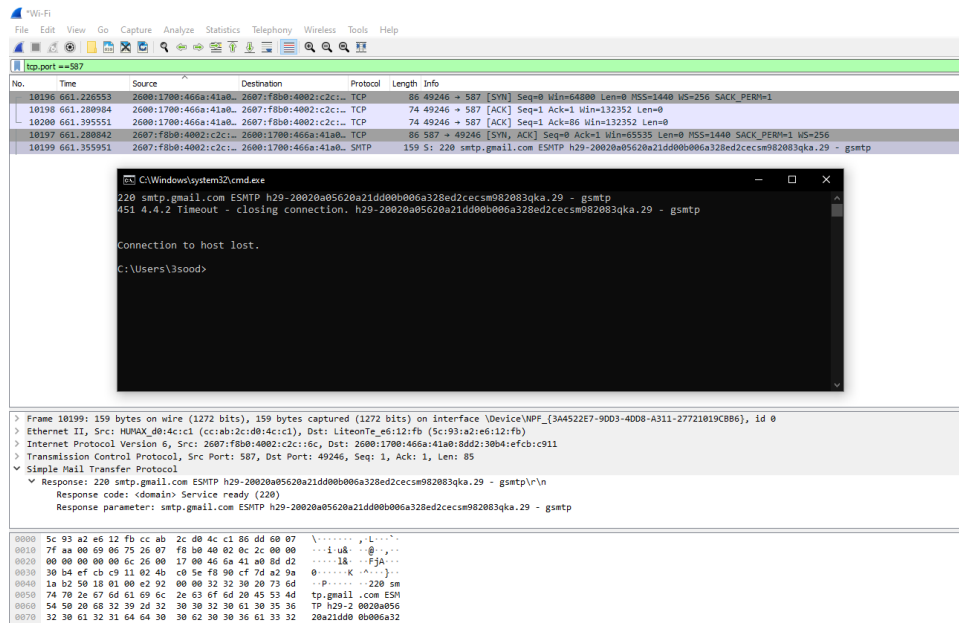
**Send mail as:**

(Use Gmail to send from your other email addresses)  
[Learn more](#)  
Farzad Kheirabadi <3sood.info@gmail.com> [edit info](#)  
[Add another email address](#)

**Check mail from other accounts:**

[Add a mail account](#)





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.