Task 3: TLS Communication Inspection & Analysis (8 pts)

Objective: Analyze HTTPS using tools learned in Week 4

Instructions:

1. Connect to any HTTPS website using openssl s_client

2. Extract and document:

○ Certificate chain (Root → Intermediate → Leaf)

○ Cipher suite used

○ TLS version

3. Capture a TLS handshake using Wireshark and highlight:

○ Client Hello

○ Server Certificate

○ Key Exchange

4. Briefly describe how TLS provides confidentiality and integrity

Deliverables:

● Screenshots of openssl output and Wireshark capture

● Summary document: tls_summary.txt

1 Connect to any HTTPS website using openssl s_client

```
C:\Users\Lenovo>cd desktop/SANGU_TEST/module_1

C:\Users\Lenovo\Desktop\SANGU_TEST\module_1>

C:\Users\Lenovo\Desktop\SANGU_TEST\module_1>openssl s_client -connect www.pinterest.com:443

CONNECTED(000001C8)

depth=1 C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
```

```
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = US, ST = California, L = San Francisco, O = "Pinterest, Inc.", CN = *.pinterest.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = San Francisco, O = "Pinterest, Inc.", CN = *.pinterest.com
   i:C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Aug  5 00:00:00 2024 GMT; NotAfter: Aug  7 23:59:59 2025 GMT
 1 s:C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 30 00:00:00 2021 GMT; NotAfter: Mar 29 23:59:59 2031 GMT
---
Server certificate
```

```
-----BEGIN CERTIFICATE-----
MIIM8TCCC9mgAwIBAgIQDgXiP/rK22IMXIn4pzVE2DANBgkqhkiG9w0BAQsFADBZ
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTMwMQYDVQQDEypE
aWdpQ2VydCBHbG9iYWwgRzIgVExTIFJTQSBTSEEyNTYgMjAyMCBDQTEwHhcNMjQw
ODA1MDAwMDAwWhcNMjUwODA3MjM1OTU5WjBuMQswCQYDVQQGEwJVUzETMBEGA1UE
CBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEYMBYGA1UEChMP
UGludGVyZXN0LCBJbmMuMRgwFgYDVQQDDA8qLnBpbnRlcmVzdC5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+/5gtjDGh+2t1QTvaBkSa6DszE+on
HpumTBKM+dfRpl6VxwQPsr1JDhFgEEC04iNiioMYRv/jzPUx+7EPMkvcJwT4Bpve
OIv8qMDvypV1xZyw3aQp6N824p+G+t/f4haqoFDbIbYF5ONpsXg2aWdJPOP+ZCeP
UA3QR+EvuEIEybPNu91FXzSgFfiOWL+hsMmhPnQnWH4c1JfzGXGbE73XPBMzSCpb
SErO2vIAnClqfmxB+rp31wBNrFW6dUToEXpVsU4/e2ccZg6QkTFXy5iWQOzM5O0H
b7toWb8PFG8ZMn6Qi5y91je6PjrmvllWNZyCzeemw7ZXfh8H3aasVVkZAgMBAAGj
```

ggmeMIIJmjAfBgNVHSMEGDAWgBR0hYDAZsffN97PvSk3qgMdvu3NFzAdBgNVHQ4E

FgQU8IS8L7vxVAZ4hLUvLlSAi0tAUlwwggYsBgNVHREEggYjMIIGH4IPKi5waW50

ZXJlc3QuY29tggwqLnBpbmltZy5jb22CEoucGludGVyZXN0LmluZm+CFyoucGlu

dGVyZXN0LmVuZ2luZWVyaW5nghMqLnBpbnRlcmVzdG1haWwuY29tgg4qLnBpbnRl

cmVzdC5hdIIOKi5waW50ZXJlc3QuY2iCDioucGludGVyZXN0LmRlgg4qLnBpbnRl

cmVzdC5ka4IOKi5waW50ZXJlc3QuaWWCDioucGludGVyZXN0Lmpwgg4qLnBpbnRl

cmVzdC5rcoIOKi5waW50ZXJlc3QubXiCDioucGludGVyZXN0LnB0gg4qLnBpbnRl

cmVzdC5zZYIRKi5waW50ZXJlc3QuY28uYXSCESoucGludGVyZXN0LmNvLmtyghEq

LnBpbnRlcmVzdC5jby51a4ISKi5waW50ZXJlc3QuY29tLm14ggZwaW4uaXSCDXBp

bnRlcmVzdC5jb22CCnBpbmltZy5jb22CDnBpbnRlcmVzdC5pbmZvghVwaW50ZXJl

c3QuZW5naW5lZXJpbmeCEXBpbnRlcmVzdG1haWwuY29tggxwaW50ZXJlc3QuYXSC

DHBpbnRlcmVzdC5jaIIMcGludGVyZXN0LmRlggxwaW50ZXJlc3QuZGuCDHBpbnRl

cmVzdC5pZYIMcGludGVyZXN0LmpwggxwaW50ZXJlc3Qua3KCDHBpbnRlcmVzdC5t

eIIMcGludGVyZXN0LnB0ggxwaW50ZXJlc3Quc2WCD3BpbnRlcmVzdC5jby5hdIIP

cGludGVyZXN0LmNvLmtygg9waW50ZXJlc3QuY28udWuCEHBpbnRlcmVzdC5jb20u

bXiCDioucGludGVyZXN0LmNhgg4qLnBpbnRlcmVzdC5mcoIMcGludGVyZXN0LmNh

ggxwaW50ZXJlc3QuZnKCEHBpbnRlcmVzdC5jb20uYXWCEioucGludGVyZXN0LmNv

bS5hdYIMcGludGVyZXN0Lm56gg4qLnBpbnRlcmVzdC5ueoIMcGludGVyZXN0LmVz

gg4qLnBpbnRlcmVzdC5lc4IMcGludGVyZXN0LmNsgg4qLnBpbnRlcmVzdC5jbIIM

cGludGVyZXN0LnBogg4qLnBpbnRlcmVzdC5waIIMcGludGVyZXN0Lmlugg4qLnBp

bnRlcmVzdC5pboIPcGludGVyZXN0LmNvLmlughEqLnBpbnRlcmVzdC5jby5pboIM

cGludGVyZXN0LmJlgg4qLnBpbnRlcmVzdC5iZYIMcGludGVyZXN0LnBlgg4qLnBp

bnRlcmVzdC5wZYIMcGludGVyZXN0LmNvgg4qLnBpbnRlcmVzdC5jb4IQcGludGVy

ZXN0LmNvbS5weYISKi5waW50ZXJlc3QuY29tLnB5ghBwaW50ZXJlc3QuY29tLmJv

ghIqLnBpbnRlcmVzdC5jb20uYm+CEHBpbnRlcmVzdC5jb20uZWOCEioucGludGVy

ZXN0LmNvbS5lY4IMcGludGVyZXN0LmVjgg4qLnBpbnRlcmVzdC5lY4IMcGludGVy

ZXN0Lmh1gg4qLnBpbnRlcmVzdC5odYIQcGludGVyZXN0LmNvbS52boISKi5waW50

ZXJlc3QuY29tLnZuggxwaW50ZXJlc3QuaXSCDioucGludGVyZXN0Lml0ghBwaW50

ZXJlc3QuY29tLnBlghIqLnBpbnRlcmVzdC5jb20ucGWCEHBpbnRlcmVzdC5jb20u dXmCEioucGludGVyZXN0LmNvbS51eYIPcGludGVyZXN0LmNvLm56ghEqLnBpbnRl

cmVzdC5jby5ueoIMcGludGVyZXN0LnVrgg4qLnBpbnRlcmVzdC51a4IMcGludGVy

ZXN0LnZugg4qLnBpbnRlcmVzdC52boIMcGludGVyZXN0Lmlkgg4qLnBpbnRlcmVz

dC5pZIIMcGludGVyZXN0LnRogg4qLnBpbnRlcmVzdC50aIIMcGludGVyZXN0LnR3

gg4qLnBpbnRlcmVzdC50d4IMcGludGVyZXN0Lm5sgg4qLnBpbnRlcmVzdC5ubIIX

Ki50ZXN0aW5nLnBpbnRlcmVzdC5jb20wPgYDVR0gBDcwNTAzBgZngQwBAgIwKTAn

BggrBgEFBQcCARYbaHR0cDovL3d3dy5kaWdpY2VydC5jb20vQ1BTMA4GA1UdDwEB

/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwgZ8GA1UdHwSB

lzCBlDBIoEagRIZCaHR0cDovL2NybDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv

YmFsRzJUTFNSU0FTSEEyNTYyMDIwQ0ExLTEuY3JsMEigRqBEhkJodHRwOi8vY3Js

NC5kaWdpY2VydC5jb20vRGlnaUNlcnRHbG9iYWxHMlRMU1JTQVNIQTI1NjIwMjBD

QTEtMS5jcmwwgYcGCCsGAQUFBwEBBHsweTAkBggrBgEFBQcwAYYYaHR0cDovL29j

c3AuZGlnaWNlcnQuY29tMFEGCCsGAQUFBzAChkVodHRwOi8vY2FjZXJ0cy5kaWdp

Y2VydC5jb20vRGlnaUNlcnRHbG9iYWxHMlRMU1JTQVNIQTI1NjIwMjBDQTEtMS5j

cnQwDAYDVR0TAQH/BAIwADCCAX0GCisGAQQB1nkCBAIEggFtBIIBaQFnAHUA3dzK

NJXX4RYF55Uy+sef+D0cUN/bADoUEnYKLKy7yCoAAAGRI3jtgAAABAMARjBEAiBX

gktrjyWu9jrOy+0fDj6uiMrgSuTnR8g+zM54XwJpBgIgJFEbT5IpClQKboZzcWtS

3qxFFq7BEvxtbRkYt7e9Ti8AdwDm0jFjQHeMwRBBBtdxuc7B0kD2loSG+7qHMh39

HjeOUAAAAZEjeO2UAAAEAwBIMEYCIQCTKQUvkaYKpsmvRXIKyUkSET5MUN74vAbp

B3FGGiarzwIhAPrcJ6tjaGaxBJxewo2+7ZGCeIg9isKtG+/InkXGhcVRAHUAzPsP

aoVxCWX+lZtTzumyfCLphVwNl422qX5UwP5MDbAAAAGRI3jtggAABAMARjBEAiA7

5VLeNx9l6iTi6Qr1S9VrtKjkv96dLaw9IztemFzVyAIgHCZ/5RE/e59BgrTQcejb

YStcoT4AtFKPovWGkVZM2gwwDQYJKoZIhvcNAQELBQADggEBADS2HhDe8ajAxcQJ

Qj324a8jIMAPdqjL7y3TrOoCKSRyVKt4Ja4wgsxt3jlXoPgzU4kSEBqscOvEQQuz

r0HPDYCe8wKEeiTyPyBBvOECmsiS1PE4jslVe8uPeyB6OwZe6iHWqevaVM0gFm2V

ivXQvRhTqK3Pn9j9ozqX+LLg+O3F87aU7+s1Vovo5hV7rsIe0tHHtuWKh194tANE

IlgXQFaeg++9JlH+GCZwpPoZPN0KE4hMInbQYVzF9Fkl1iBZ2qQksAkPJ+LSARYJ

H1j5GhAgiX+vEemLcLZVva//RsS+mmNV9ICqsQB8sZ79ta1wyu87w4xBB8Jg0ZST

Z04JR+k=

```
-----END CERTIFICATE-----
subject=C = US, ST = California, L = San Francisco, O = "Pinterest, Inc.", CN = *.pinterest.com
issuer=C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 5094 bytes and written 387 bytes
Verification error: unable to get local issuer certificate
---
New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 20 (unable to get local issuer certificate)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_128_GCM_SHA256
    Session-ID: C225B4FA0DF9AC82DEC3D21B90F981A342B3C8C0B5EC3EAC7F2EBC0A3CF3D87B
    Session-ID-ctx:
```

```
    Resumption PSK:
6EDB9A0FBBA305502F38669C1A9D4BE54F2B145EDBAD6ECC2F381B93DF43C1C0

    PSK identity: None

    PSK identity hint: None

    SRP username: None

    TLS session ticket lifetime hint: 86400 (seconds)

    TLS session ticket:

    0000 - cb 13 ae f2 9f e8 63 8b-25 f8 77 95 19 89 f1 c5   ......c.%.w.....

    0010 - c8 b8 61 3e 74 6c c5 ca-2c 9c 43 86 f4 fd 2a c0   ..a>tl..,.C...*.

    0020 - c2 1d bd 52 91 6f ff 1b-1c fa b1 ba c7 d7 9d b5   ...R.o..........

    0030 - c8 37 ff 80 4d 2f 57 86-b3 cc 22 27 59 6f 6b 65   .7..M/W..."'Yoke

    0040 - e1 0a 16 b7 05 2c 6e 73-1c fd 93 aa e1 44 a3 b3   .....,ns.....D..

    0050 - 22 7c 87 0c 07 7c 03 99-d1 e7 85 9e 18 32 55 75   "|...|.......2Uu

    0060 - e9 7a 6a cd bb 48 58 e5-27 bf 9f c6 80 2a 9d 70   .zj..HX.'....*.p

    0070 - bb f6 dc f2 f8 00 c9 75-b8 60 44 44 77 4e f4 3b   .......u.`DDwN.;

    0080 - e8 f6 0e d4 95 1d 83 c4-9d 85 6a 89 e7 e2 53 ec   ..........j...S.

    0090 - 18 0b b9 e0 30 76 cc e3-55 89 25 fa 67 90 cb b4   ....0v..U.%.g...


    Start Time: 1745593553

    Timeout   : 7200 (sec)

    Verify return code: 20 (unable to get local issuer certificate)

    Extended master secret: no

    Max Early Data: 0

---

read R BLOCK
```

2. Extract and document:

A. Certificate Chain

Root → Intermediate → Leaf

Root Certificate (not directly shown in output but referenced):

- C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2

The root certificate (DigiCert Global Root G2) is not included in the handshake, because error appears:

verify error:num=20:unable to get local issuer certificate

Intermediate Certificate:

- C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
- C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
- Valid: Mar 30 00:00:00 2021 GMT to Mar 29 23:59:59 2031 GMT
- Key: RSA 2048-bit

Leaf Certificate:

- C = US, ST = California, L = San Francisco, O = "Pinterest, Inc.", CN = *.pinterest.com
- Issuer: C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
- Valid: Aug 5 00:00:00 2024 GMT to Aug 7 23:59:59 2025 GMT
- Key: RSA 2048-bit

B. Cipher suite used

Cipher: TLS_AES_128_GCM_SHA256

- AES 128-bit key in Galois/Counter Mode (GCM)
- SHA-256 is used to authenticate message

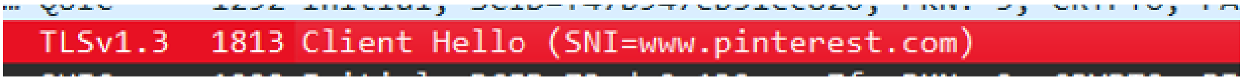
C. TLS version

Connection is using **TLSv1.3**, as indicated in output:

New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256

3. Capture a TLS handshake using Wireshark and highlight:

○ Client Hello



```
TLSv1.3   1813 Client Hello (SNI=www.pinterest.com)
```

○ Server Certificate

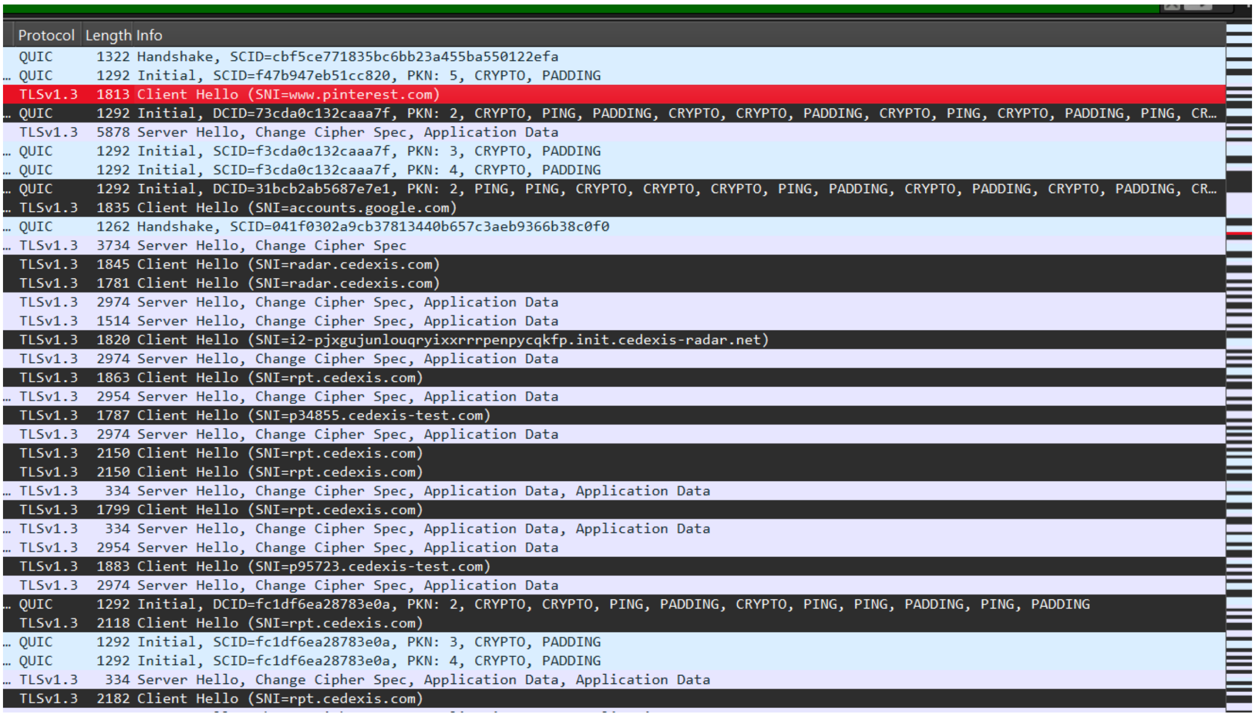
In TLS 1.3 handshake messages are more compressed and encrypted compared to TLS 1.2, so server certificate message is typically included within Server Hello and encrypted handshake messages. In my screenshot, packets like “**TLSv1.3 Server Hello, Change Cipher Spec, Application Data**” are doing multiple things:

- **Server Hello** – completes key exchange.
- **Change Cipher Spec** – signal that encrypted communication will follow.
- **Application Data** – includes encrypted handshake messages and Certificate.

○ Key Exchange

key exchange is provided during this process of TLS 1.3 handshake but it's not exactly shown as separate "Key Exchange" packet like in TLS 1.2. In TLS 1.3, key exchange happens during the Client Hello and Server Hello.

- **“TLSv1.3 Client Hello (SNI=www.pinterest.com)”** Includes the Client's Key Share (e.g., using X25519 or P-256 curve) which is client's contribution to the Elliptic Curve Diffie-Hellman (ECDHE) key exchange.
- **“TLSv1.3 Server Hello, Change Cipher Spec, Application Data”** Includes the Server's Key Share (e.g., X25519), which Finalizes shared secret generation for symmetric encryption.



```
  Protocol Length Info
  QUIC      1322 Handshake, SCID=cbf5ce771835bc6bb23a455ba550122efa
… QUIC      1292 Initial, SCID=f47b947eb51cc820, PKN: 5, CRYPTO, PADDING
  TLSv1.3   1813 Client Hello (SNI=www.pinterest.com)
… QUIC      1292 Initial, DCID=73cda0c132caaa7f, PKN: 2, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING, PING, CR…
  TLSv1.3   5878 Server Hello, Change Cipher Spec, Application Data
… QUIC      1292 Initial, SCID=f3cda0c132caaa7f, PKN: 3, CRYPTO, PADDING
… QUIC      1292 Initial, SCID=f3cda0c132caaa7f, PKN: 4, CRYPTO, PADDING
… QUIC      1292 Initial, DCID=31bcb2ab5687e7e1, PKN: 2, PING, PING, CRYPTO, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, CR…
… TLSv1.3   1835 Client Hello (SNI=accounts.google.com)
… QUIC      1262 Handshake, SCID=041f0302a9cb37813440b657c3aeb9366b38c0f0
… TLSv1.3   3734 Server Hello, Change Cipher Spec
  TLSv1.3   1845 Client Hello (SNI=radar.cedexis.com)
  TLSv1.3   1781 Client Hello (SNI=radar.cedexis.com)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1514 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1820 Client Hello (SNI=i2-pjxgujunlouqryixxrrrpenpycqkfp.init.cedexis-radar.net)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1863 Client Hello (SNI=rpt.cedexis.com)
… TLSv1.3   2954 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1787 Client Hello (SNI=p34855.cedexis-test.com)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   2150 Client Hello (SNI=rpt.cedexis.com)
  TLSv1.3   2150 Client Hello (SNI=rpt.cedexis.com)
… TLSv1.3    334 Server Hello, Change Cipher Spec, Application Data, Application Data
  TLSv1.3   1799 Client Hello (SNI=rpt.cedexis.com)
… TLSv1.3    334 Server Hello, Change Cipher Spec, Application Data, Application Data
… TLSv1.3   2954 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1883 Client Hello (SNI=p95723.cedexis-test.com)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
… QUIC      1292 Initial, DCID=fc1df6ea28783e0a, PKN: 2, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, PING, PING, PADDING, PING, PADDING
  TLSv1.3   2118 Client Hello (SNI=rpt.cedexis.com)
… QUIC      1292 Initial, SCID=fc1df6ea28783e0a, PKN: 3, CRYPTO, PADDING
… QUIC      1292 Initial, SCID=fc1df6ea28783e0a, PKN: 4, CRYPTO, PADDING
… TLSv1.3    334 Server Hello, Change Cipher Spec, Application Data, Application Data
  TLSv1.3   2182 Client Hello (SNI=rpt.cedexis.com)
```

4. Briefly describe how TLS provides confidentiality and integrity

Wireshark capture shows TLS handshake stages:

Client Hello. On this stage browser initiates handshake, sends supported TLS versions, cipher suites and SNI to www.pinterest.com. We can see in capture “Client Hello (SNI= www.pinterest.com)”

Server Hello. Server selects cipher suite and replies with server certificate, change cipher spec, Encrypted Handshake Message.

Key Exchange and Cipher Agreement. server and client securely exchange key.

Change Cipher Spec. browser and Server switch to encrypted communication using shared symmetric key.

How TLS Provides Confidentiality and Integrity

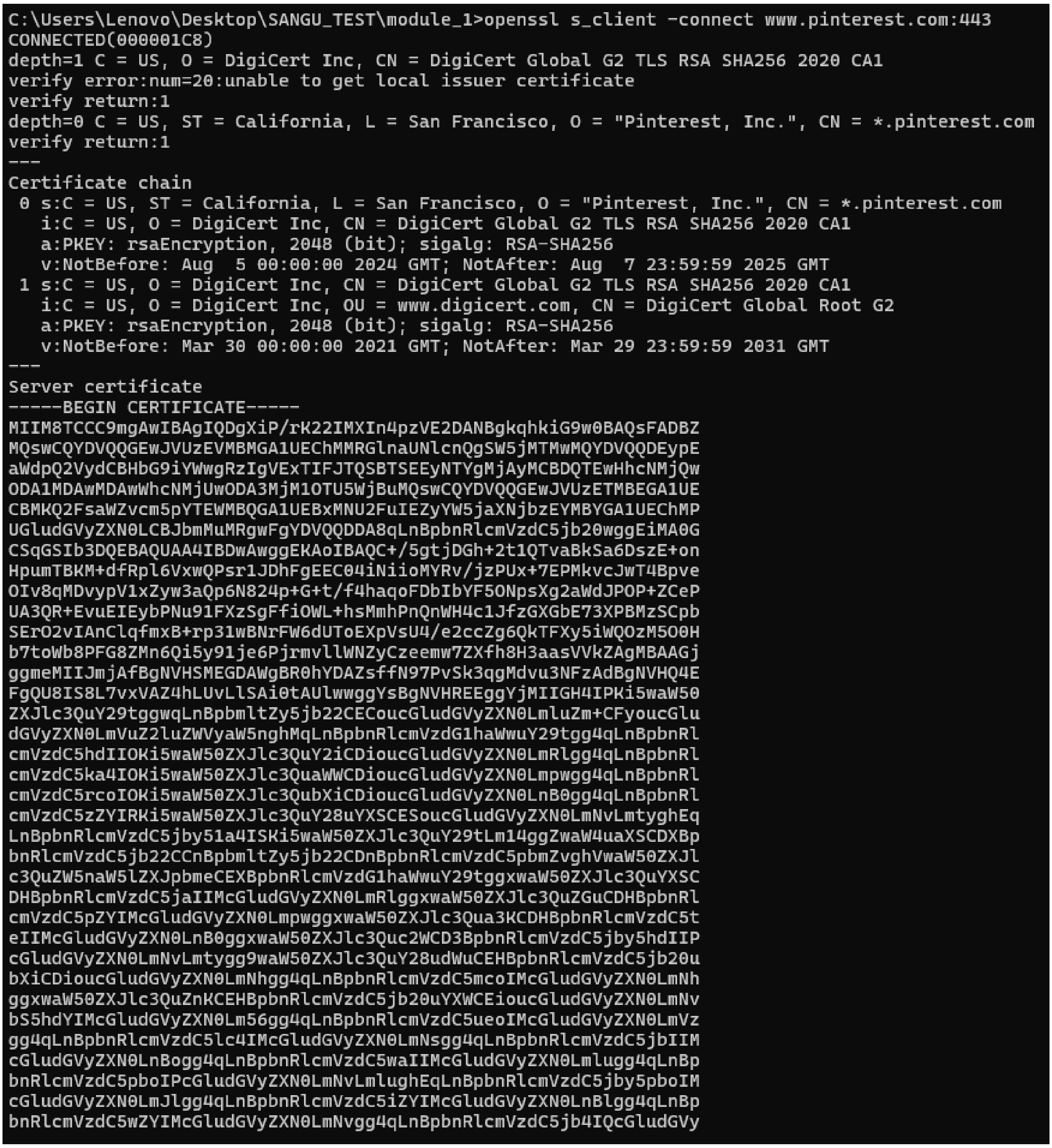
TLS is reliable security layer for HTTPS. During connection to secure website (in my case www.pinterest.com), browser and server perform TLS handshake. They establish encryption algorithms and securely exchange keys, generated using public-key cryptography. The server is authenticated using digital certificate issued by a trusted Certificate Authority (CA). After that stages exchanged data is encrypted, in my case using Ephemeral Diffie-Hellman, which supports Perfect Forward Secrecy, means the encryption keys are unique to each session and never reused. Additionally, authentication is provided by TLS using Message Authentication Codes (MACs) or AEAD ciphers to ensure data integrity.

Confidentiality is achieved using encryption, **Client Hello** and **Server Hello** messages include key shares used in an **Elliptic Curve Diffie-Hellman (ECDHE)** key exchange, this process generates **shared secret** between client and server. When key exchange is complete, both parties start using **symmetric encryption.** Cipher: TLS_AES_128_GCM_SHA256. After this point, all traffic (application data, server certificate) is encrypted, ensuring only intended recipient can read.

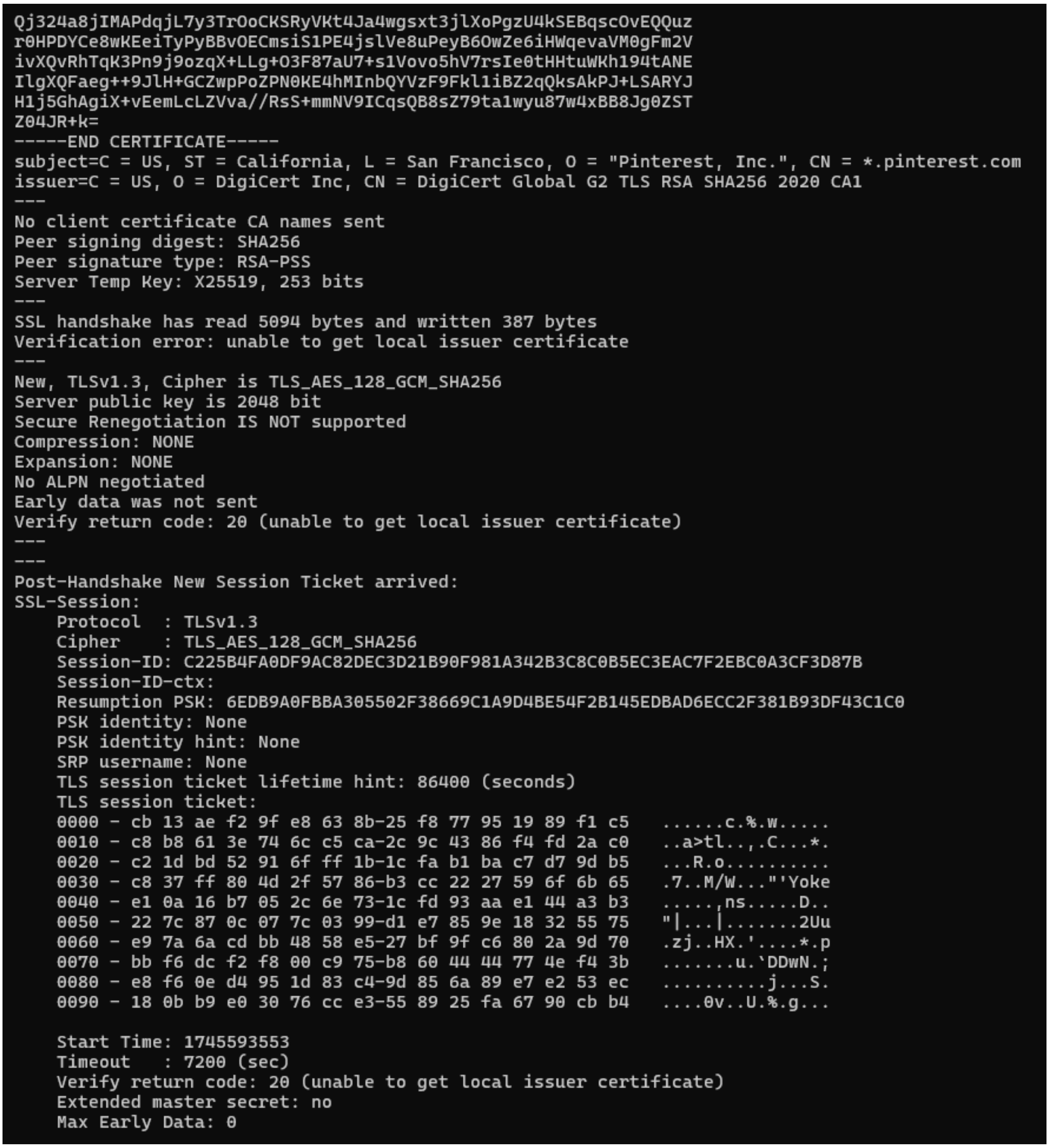
Integrity is ensured through **authenticated encryption**, TLS 1.3 is using **AEAD ciphers** (Authenticated Encryption with Associated Data), such as AES_128_GCM_SHA256, in my case. These ciphers include **built-in authentication**, which verifies that data was not altered and ensures that it came from legitimate party.

TLS 1.3 begins of protection **confidentiality** and **integrity** after **Server Hello** finishes. From that point forward, all handshake messages (including the certificate) are encrypted and authenticated.

- **Screenshots of openssl output**



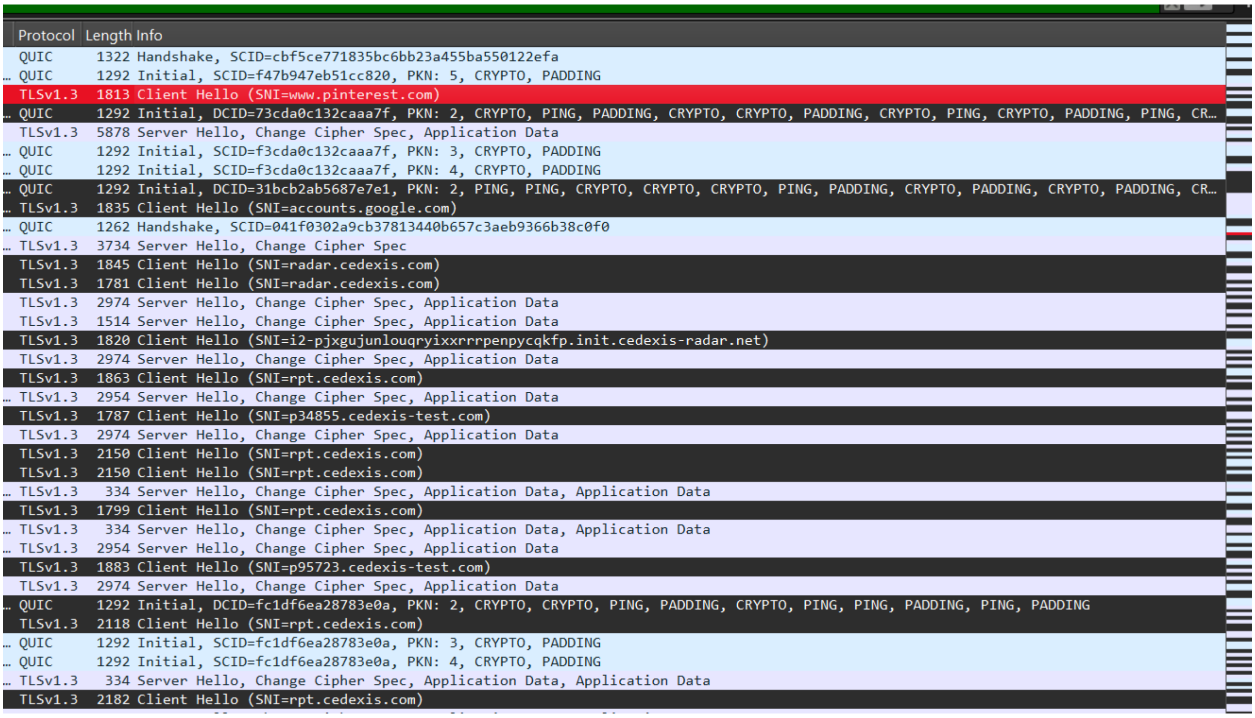
```
C:\Users\Lenovo\Desktop\SANGU_TEST\module_1>openssl s_client -connect www.pinterest.com:443
CONNECTED(000001C8)
depth=1 C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = US, ST = California, L = San Francisco, O = "Pinterest, Inc.", CN = *.pinterest.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = San Francisco, O = "Pinterest, Inc.", CN = *.pinterest.com
   i:C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Aug  5 00:00:00 2024 GMT; NotAfter: Aug  7 23:59:59 2025 GMT
 1 s:C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 30 00:00:00 2021 GMT; NotAfter: Mar 29 23:59:59 2031 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIM8TCCC9mgAwIBAgIQDgXiP/rK22IMXIn4pzVE2DANBgkqhkiG9w0BAQsFADBZ
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTMwMQYDVQQDEypE
aWdpQ2VydCBHbG9iYWwgRzIgVExTIFJTQSBTSEEyNTYgMjAyMCBDQTEwHhcNMjQw
ODA1MDAwMDAwWhcNMjUwODA3MjM1OTU5WjBuMQswCQYDVQQGEwJVUzETMBEGA1UE
CBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEYMBYGA1UEChMP
UGludGVyZXN0LCBJbmMuMRgwFgYDVQQDDA8qLnBpbnRlcmVzdC5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+/5gtjDGh+2t1QTvaBkSa6DszE+on
HpumTBKM+dfRpl6VxwQPsr1JDhFgEEC04iNiioMYRv/jzPUx+7EPMkvcJwT4Bpve
OIv8qMDvypV1xZyw3aQp6N824p+G+t/f4haqoFDbIbYF5ONpsXg2aWdJPOP+ZCeP
UA3QR+EvuEIEybPNu91FXzSgFfiOWL+hsMmhPnQnWH4c1JfzGXGbE73XPBMzSCpb
SErO2vIAnClqfmxB+rp31wBNrFW6dUToEXpVsU4/e2ccZg6QkTFXy5iWQOzM5O0H
b7toWb8PFG8ZMn6Qi5y91je6PjrmvllWNZyCzeemw7ZXfh8H3aasVVkZAgMBAAGj
ggmeMIIJmjAfBgNVHSMEGDAWgBR0hYDAZsffN97PvSk3qgMdvu3NFzAdBgNVHQ4E
FgQU8IS8L7vxVAZ4hLUvLlSAi0tAUlwwggYsBgNVHREEggYjMIIGH4IPKi5waW50
ZXJlc3QuY29tggwqLnBpbmltZy5jb22CECoucGludGVyZXN0LmluZm+CFyoucGlu
dGVyZXN0LmVuZ2luZWVyaW5nghMqLnBpbnRlcmVzdG1haWwuY29tgg4qLnBpbnRl
cmVzdC5hdIIOKi5waW50ZXJlc3QuY2iCDioucGludGVyZXN0LmRlgg4qLnBpbnRl
cmVzdC5ka4IOKi5waW50ZXJlc3QuaWWCDioucGludGVyZXN0Lmpwgg4qLnBpbnRl
cmVzdC5rcoIOKi5waW50ZXJlc3QubXiCDioucGludGVyZXN0LnB0gg4qLnBpbnRl
cmVzdC5zZYIRKi5waW50ZXJlc3QuY28uYXSCESoucGludGVyZXN0LmNvLmtyghEq
LnBpbnRlcmVzdC5jby51a4ISKi5waW50ZXJlc3QuY29tLm14ggZwaW4uaXSCDXBp
bnRlcmVzdC5jb22CCnBpbmltZy5jb22CDnBpbnRlcmVzdC5pbmZvghVwaW50ZXJl
c3QuZW5naW5lZXJpbmeCEXBpbnRlcmVzdG1haWwuY29tggxwaW50ZXJlc3QuYXSC
DHBpbnRlcmVzdC5jaIIMcGludGVyZXN0LmRlggxwaW50ZXJlc3QuZGuCDHBpbnRl
cmVzdC5pZYIMcGludGVyZXN0LmpwggxwaW50ZXJlc3Qua3KCDHBpbnRlcmVzdC5t
eIIMcGludGVyZXN0LnB0ggxwaW50ZXJlc3Quc2WCD3BpbnRlcmVzdC5jby5hdIIP
cGludGVyZXN0LmNvLmtygg9waW50ZXJlc3QuY28udWuCEHBpbnRlcmVzdC5jb20u
bXiCDioucGludGVyZXN0LmNhgg4qLnBpbnRlcmVzdC5mcoIMcGludGVyZXN0LmNh
ggxwaW50ZXJlc3QuZnKCEHBpbnRlcmVzdC5jb20uYXWCEioucGludGVyZXN0LmNv
bS5hdYIMcGludGVyZXN0Lm56gg4qLnBpbnRlcmVzdC5ueoIMcGludGVyZXN0LmVz
gg4qLnBpbnRlcmVzdC5lc4IMcGludGVyZXN0LmNsgg4qLnBpbnRlcmVzdC5jbIIM
cGludGVyZXN0LnBogg4qLnBpbnRlcmVzdC5waIIMcGludGVyZXN0Lmlugg4qLnBp
bnRlcmVzdC5pboIPcGludGVyZXN0LmNvLmlughEqLnBpbnRlcmVzdC5jby5pboIM
cGludGVyZXN0LmJlgg4qLnBpbnRlcmVzdC5iZYIMcGludGVyZXN0LnBlgg4qLnBp
bnRlcmVzdC5wZYIMcGludGVyZXN0LmNvgg4qLnBpbnRlcmVzdC5jb4IQcGludGVy
```



```
Qj324a8jIMAPdqjL7y3TrOoCKSRyVKt4Ja4wgsxt3jlXoPgzU4kSEBqscOvEQQuz
r0HPDYCe8wKEeiTyPyBBvOECmsiS1PE4jslVe8uPeyB6OwZe6iHWqevaVM0gFm2V
ivXQvRhTqK3Pn9j9ozqX+LLg+O3F87aU7+s1Vovo5hV7rsIe0tHHtuWKh194tANE
IlgXQFaeg++9JlH+GCZwpPoZPN0KE4hMInbQYVzF9Fkl1iBZ2qQksAkPJ+LSARYJ
H1j5GhAgiX+vEemLcLZVva//RsS+mmNV9ICqsQB8sZ79ta1wyu87w4xBB8Jg0ZST
Z04JR+k=
-----END CERTIFICATE-----
subject=C = US, ST = California, L = San Francisco, O = "Pinterest, Inc.", CN = *.pinterest.com
issuer=C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 5094 bytes and written 387 bytes
Verification error: unable to get local issuer certificate
---
New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 20 (unable to get local issuer certificate)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_128_GCM_SHA256
    Session-ID: C225B4FA0DF9AC82DEC3D21B90F981A342B3C8C0B5EC3EAC7F2EBC0A3CF3D87B
    Session-ID-ctx:
    Resumption PSK: 6EDB9A0FBBA305502F38669C1A9D4BE54F2B145EDBAD6ECC2F381B93DF43C1C0
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 86400 (seconds)
    TLS session ticket:
    0000 - cb 13 ae f2 9f e8 63 8b-25 f8 77 95 19 89 f1 c5   ......c.%.w.....
    0010 - c8 b8 61 3e 74 6c c5 ca-2c 9c 43 86 f4 fd 2a c0   ..a>tl..,.C...*.
    0020 - c2 1d bd 52 91 6f ff 1b-1c fa b1 ba c7 d7 9d b5   ...R.o..........
    0030 - c8 37 ff 80 4d 2f 57 86-b3 cc 22 27 59 6f 6b 65   .7..M/W..."'Yoke
    0040 - e1 0a 16 b7 05 2c 6e 73-1c fd 93 aa e1 44 a3 b3   .....,ns.....D..
    0050 - 22 7c 87 0c 07 7c 03 99-d1 e7 85 9e 18 32 55 75   "|...|.......2Uu
    0060 - e9 7a 6a cd bb 48 58 e5-27 bf 9f c6 80 2a 9d 70   .zj..HX.'....*.p
    0070 - bb f6 dc f2 f8 00 c9 75-b8 60 44 44 77 4e f4 3b   .......u.`DDwN.;
    0080 - e8 f6 0e d4 95 1d 83 c4-9d 85 6a 89 e7 e2 53 ec   ..........j...S.
    0090 - 18 0b b9 e0 30 76 cc e3-55 89 25 fa 67 90 cb b4   ....0v..U.%.g...

    Start Time: 1745593553
    Timeout   : 7200 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
    Extended master secret: no
    Max Early Data: 0
```

Wireshark capture



```
  Protocol Length Info
  QUIC      1322 Handshake, SCID=cbf5ce771835bc6bb23a455ba550122efa
… QUIC      1292 Initial, SCID=f47b947eb51cc820, PKN: 5, CRYPTO, PADDING
  TLSv1.3   1813 Client Hello (SNI=www.pinterest.com)
… QUIC      1292 Initial, DCID=73cda0c132caaa7f, PKN: 2, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING, PING, CR…
  TLSv1.3   5878 Server Hello, Change Cipher Spec, Application Data
… QUIC      1292 Initial, SCID=f3cda0c132caaa7f, PKN: 3, CRYPTO, PADDING
… QUIC      1292 Initial, SCID=f3cda0c132caaa7f, PKN: 4, CRYPTO, PADDING
… QUIC      1292 Initial, DCID=31bcb2ab5687e7e1, PKN: 2, PING, PING, CRYPTO, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, CR…
… TLSv1.3   1835 Client Hello (SNI=accounts.google.com)
… QUIC      1262 Handshake, SCID=041f0302a9cb37813440b657c3aeb9366b38c0f0
… TLSv1.3   3734 Server Hello, Change Cipher Spec
  TLSv1.3   1845 Client Hello (SNI=radar.cedexis.com)
  TLSv1.3   1781 Client Hello (SNI=radar.cedexis.com)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1514 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1820 Client Hello (SNI=i2-pjxgujunlouqryixxrrrpenpycqkfp.init.cedexis-radar.net)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1863 Client Hello (SNI=rpt.cedexis.com)
… TLSv1.3   2954 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1787 Client Hello (SNI=p34855.cedexis-test.com)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   2150 Client Hello (SNI=rpt.cedexis.com)
  TLSv1.3   2150 Client Hello (SNI=rpt.cedexis.com)
… TLSv1.3    334 Server Hello, Change Cipher Spec, Application Data, Application Data
  TLSv1.3   1799 Client Hello (SNI=rpt.cedexis.com)
… TLSv1.3    334 Server Hello, Change Cipher Spec, Application Data, Application Data
… TLSv1.3   2954 Server Hello, Change Cipher Spec, Application Data
  TLSv1.3   1883 Client Hello (SNI=p95723.cedexis-test.com)
  TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
… QUIC      1292 Initial, DCID=fc1df6ea28783e0a, PKN: 2, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, PING, PING, PADDING, PING, PADDING
  TLSv1.3   2118 Client Hello (SNI=rpt.cedexis.com)
… QUIC      1292 Initial, SCID=fc1df6ea28783e0a, PKN: 3, CRYPTO, PADDING
… QUIC      1292 Initial, SCID=fc1df6ea28783e0a, PKN: 4, CRYPTO, PADDING
… TLSv1.3    334 Server Hello, Change Cipher Spec, Application Data, Application Data
  TLSv1.3   2182 Client Hello (SNI=rpt.cedexis.com)
```

● Summary document: tls_summary.txt

In this task, I analyzed how TLS works by connecting to an HTTPS website and capturing the handshake.

1. OpenSSL Connection to HTTPS Website

I connected to www.pinterest.com using OpenSSL.
From the output, I extracted:

- **Certificate Chain**:
  - **Root**: DigiCert Global Root G2
  - **Intermediate**: DigiCert Global G2 TLS RSA SHA256 2020 CA1
  - **Leaf**: *.pinterest.com
- **Cipher Suite Used**:
  - TLS_AES_128_GCM_SHA256
  - AES-128 in Galois/Counter Mode with SHA-256 for authentication
- **TLS Version**:
  - TLSv1.3

The server’s certificate is signed by DigiCert and uses RSA 2048-bit keys.

2. TLS Handshake Capture with Wireshark

Using Wireshark, I captured the TLS 1.3 handshake.
Important stages highlighted:

- **Client Hello**:
  - The client sends supported cipher suites and key share.
- **Server Certificate**:
  - In TLS 1.3, the server certificate is encrypted inside Application Data after Server Hello, not seen clearly in plain text.
- **Key Exchange**:
  - The key exchange happens during Client Hello and Server Hello using ECDHE (Elliptic Curve Diffie-Hellman Ephemeral).

3. How TLS Provides Confidentiality and Integrity

TLS provides **confidentiality** by encryption of all data using symmetric encryption (AES-GCM), based on shared secret generated through secure key exchange.

TLS ensures **integrity** by using AEAD ciphers (like AES-GCM) that provide both encryption and authentication.
This prevents attackers from reading or modifying data.

In TLS 1.3, confidentiality and integrity protection start after **Server Hello** is finished.