

Network security - Assignment 4

Nisha M
CS19BTECH11012

Question 1

The browser used was google chrome and the version 98.0.4758.102 (Official Build) (64-bit).

Question 2

The various protocols noticed under “Protocol” include :

1. DNS protocol - The IP address of the hostname is queried (hostname - www.icicibank.com)

Time	Source	Destination	Protocol	Length	Info
15 1.704538976	192.168.3.14.104	192.168.36.53	DNS	84	Standard query 0x4607 A icicibank.com OPT
15 1.704538984	192.168.3.14.104	192.168.36.53	DNS	86	Standard query response 0x809 A icicibank.com A 203.171.210...
32 1.795331884	192.168.36.53	192.168.36.53	DNS	88	Standard query 0x933b A www.icicibank.com OPT
34 1.841265094	192.168.36.53	192.168.114.104	DNS	186	Standard query response 0x933b A www.icicibank.com CNAME www...
324 2.641310164	192.168.36.53	192.168.36.53	DNS	106	Standard query 0x78af A icicibanksmartsearch.senseforth.com O...
325 2.641594996	192.168.36.53	192.168.36.53	DNS	104	Standard query 0xc35c A www-google-analytics.l.google.com OPT
327 2.645537369	192.168.36.53	192.168.114.104	DNS	120	Standard query response 0xc35c A www-google-analytics.l.google...
328 2.645537376	192.168.36.53	192.168.114.104	DNS	98	Standard query 0xc35c A www-googleapis.com OPT
334 2.669668206	192.168.36.53	192.168.114.104	DNS	114	Standard query response 0xdce8 A safestring.googleapis.com ...
352 2.686926014	192.168.36.53	192.168.114.104	DNS	138	Standard query response 0x78af A icicibanksmartsearch.sensefor...
522 2.856454253	192.168.114.104	192.168.36.53	DNS	90	Standard query 0xct1d A clients4.google.com OPT
523 2.859549956	192.168.36.53	192.168.114.104	DNS	130	Standard query response 0xct1d A clients4.google.com CNAME cl...
533 2.992234886	192.168.114.104	192.168.36.53	DNS	87	Standard query 0xd9f1 A icici.nanorep.co OPT
592 3.098476365	192.168.36.53	192.168.114.104	DNS	90	Standard query 0xd9f1 A icici.nanorep.co OPT
593 3.098517482	192.168.36.53	192.168.114.104	DNS	104	Standard query 0x648c A www-googletagmanager.l.google.com OPT
600 3.098517482	192.168.36.53	192.168.114.104	DNS	120	Standard query response 0x648c A www-googletagmanager.l.google...
619 3.120860310	192.168.36.53	192.168.114.104	DNS	106	Standard query response 0x7bbc A leads.icicibank.com A 103.87...
626 3.128113489	192.168.36.53	192.168.114.104	DNS	138	Standard query response 0xd9f1 A icici.nanorep.co CNAME int-...

2. TCP protocol - This is the TCP handshake that includes the SYN, ACK and integrity check as well (by checking for the checksum)
3. TLSv1.2/TLSv1.3 - This is the TLS handshake that includes the client hello , server hello messages etc.
4. HTTP - Get requests with the url : <https://www.icicibank.com>

Question 3

```

> Frame 2099: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface wlo1, id 0
> Ethernet II, Src: 68:3e:26:71:ac:23 (68:3e:26:71:ac:23), Dst: HewlettP_a9:8b:f7 (5c:8a:38:a9:8b:f7)
> Internet Protocol Version 4, Src: 192.168.114.14, Dst: 104.65.72.32
> Transmission Control Protocol, Src Port: 36036, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  > Handshake Protocol: Client Hello

```

```

  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 78
  ▾ Handshake Protocol: Server Hello

```

```
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 2884
    ▶ Handshake Protocol: Certificate
  ▼ Transport Layer Security
    ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate Status
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 479
      ▶ Handshake Protocol: Certificate Status
    ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
      ▶ Handshake Protocol: Server Key Exchange
    ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
      ▶ Handshake Protocol: Server Hello Done
```

```
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 70
  ▶ Handshake Protocol: Client Key Exchange
▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  Content Type: Change Cipher Spec (20)
  Version: TLS 1.2 (0x0303)
  Length: 1
  Change Cipher Spec Message
▼ TLSv1.2 Record Layer: Handshake Protocol: Finished
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 40
  ▶ Handshake Protocol: Finished
```

```
Transport Layer Security
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 100
    Encrypted Application Data: 00000000000000001493850bcdfccd3ee6a33f054d541a56e...
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 1041
    Encrypted Application Data: 00000000000000002de6d15785f561fd263d4ddac823bdf82...
  ▶ HyperText Transfer Protocol 2
  ▶ HyperText Transfer Protocol 2
```

```
Transport Layer Security
  - TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 202
  - Handshake Protocol: New Session Ticket
  - TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
  - TLSv1.2 Record Layer: Handshake Protocol: Finished
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
  - Handshake Protocol: Finished
```

```
Transport Layer Security
  - TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 1243
    Encrypted Application Data: 65975fd3a767929d3ef2dc...b74430298a148...
  - HyperText Transfer Protocol 2
```

```
Transport Layer Security
  - TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 38
    Encrypted Application Data: 0000000000000045b3f5cf299d27fb82533c1887143eddf...
  - HyperText Transfer Protocol 2
```

```
Transport Layer Security
  - TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 2883
    Encrypted Application Data: 65975fd3a767929e644d044c26d5596755b4c8aab54d36ad...
    TLS segment data (1822 bytes)
  - HyperText Transfer Protocol 2
    - Stream: HEADERS, Stream ID: 18, Length 626, 200 OK
    - Stream: DATA, Stream ID: 18, Length 393 (partial entity body)
```

```

- Transport Layer Security
  - TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 2883
    Encrypted Application Data: 65975fd3a767929f6d7579a4e2312f6af5bc9ec8f98bd882...
    TLS segment data (2859 bytes)
    TLS segment data (600 bytes)
  > [2 Reassembled TLS segments (4081 bytes): #58(1822), #60(2259)]
- HyperText Transfer Protocol 2
  - Stream: DATA, Stream ID: 18, Length 4072 (partial entity body)
    Length: 4072
    Type: DATA (0)
  - Flags: 0x00
    .... .0 = End Stream: False
    .... 0... = Padded: False
    0000 .00. = Unused: 0x00
    0.... .... .... .... .... .... = Reserved: 0x0
    .000 0000 0000 0000 0000 0000 0001 0010 = Stream Identifier: 18
    [Pad Length: 0]
    Reassembled body in frame: 221
  Data: 679974de0a28953e06921399e9afa6aa5555471d079e277a...

```

Question 4

Cipher suites offered by the client are :

```

Cipher Suites Length: 32
- Cipher Suites (16 suites)
  Cipher Suite: Reserved (GREASE) (0x7a7a)
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
  Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  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 (0xccaa9)
  Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa8)
  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)

```

The first two cipher suites offered by client are :

1. Reserved (GREASE) (0x7a7a)
2. TLS_AES_128_GCM_SHA256 (0x1301)

The last one is TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

The cipher suite selected by the server is :

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

```

- Transport Layer Security
  - TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 78
  - Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 74
    Version: TLS 1.2 (0x0303)
  > Random: 7f411d48a15aa4eb3a291a008e1e9d0604a073b526c6890d...
    Session ID Length: 0
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    ...

```

Question5

```
  ▾ Server Name Indication extension
    Server Name list length: 20
    Server Name Type: host_name (0)
    Server Name length: 17
    Server Name: www.icicibank.com
```

Server name identification is used to host several TLS certificates from different sites on a single IP address.

Question 6

Client Hello

```
  ▾ Extension: application_layer_protocol_negotiation (len=14)
    Type: application_layer_protocol_negotiation (16)
    Length: 14
    ALPN Extension Length: 12
  ▾ ALPN Protocol
    ALPN string length: 2
    ALPN Next Protocol: h2
    ALPN string length: 8
    ALPN Next Protocol: http/1.1
```

Server Hello

```
  ▾ Extension: application_layer_protocol_negotiation (len=5)
    Type: application_layer_protocol_negotiation (16)
    Length: 5
    ALPN Extension Length: 3
  ▾ ALPN Protocol
    ALPN string length: 2
    ALPN Next Protocol: h2
```

ALPN, which is independent of application-layer protocols, allows the application layer to negotiate which protocol should be implemented through a secure connection while eliminating needless round trips.

The server has selected h2 as shown in the above image .

Question 7

status_request- This actually means the certificate status request which the client asks for the server, so that when the server responds back it will send the desired certificate status

```
Extension: status_request (len=5)
Type: status_request (5)
Length: 5
Certificate Status Type: OCSP (1)
Responder ID list Length: 0
Request Extensions Length: 0
```

supported_versions- The "supported versions" extension is used by the client to specify which TLS versions it supports. Servers MUST NOT utilize the ClientHello.legacy version value for version negotiation and MUST ONLY use the "supported versions" extension to determine client preferences if this extension is present in the ClientHello. Servers MUST ONLY USE the version of TLS that is available in that extension and MUST DISREGARD any unknown versions that are present in that extension.

```
Extension: supported_versions (len=7)
Type: supported_versions (43)
Length: 7
Supported Versions length: 6
Supported Version: Unknown (0xdada)
Supported Version: TLS 1.3 (0x0304)
Supported Version: TLS 1.2 (0x0303)
```

psk_key_exchange_modes - Servers MUST terminate the handshake if clients supply "pre shared key" without a "psk key exchange modes" extension. Servers must not use a key exchange mechanism not supported by the client. This modification also limits the modes that may be used with PSK resumption. Servers should not send new session tickets with tickets that are incompatible with the advertised modes

```
Extension: psk_key_exchange_modes (len=2)
Type: psk_key_exchange_modes (45)
Length: 2
PSK Key Exchange Modes Length: 1
PSK Key Exchange Mode: PSK with (EC)DHE key establishment (psk_dhe_ke) (1)
```

Question8

The client hello does contain “signature_algorithms” in its record. The purpose of it is to tell the server which sighash algorithm pairs may be utilized in the SSL handshake messages.

```
  ▾ Extension: signature_algorithms (len=18)
    Type: signature_algorithms (13)
    Length: 18
    Signature Hash Algorithms Length: 16
    ▾ Signature Hash Algorithms (8 algorithms)
      ▶ Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403)
      ▶ Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
      ▶ Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
      ▶ Signature Algorithm: ecdsa_secp384r1_sha384 (0x0503)
      ▶ Signature Algorithm: rsa_pss_rsae_sha384 (0x0805)
      ▶ Signature Algorithm: rsa_pkcs1_sha384 (0x0501)
      ▶ Signature Algorithm: rsa_pss_rsae_sha512 (0x0806)
      ▶ Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
```

Question 9

Random - 32 bytes generated by a secure random number generator. TLS uses random values:

1. in public protocol fields such as the public Random values in the ClientHello and ServerHello.
2. To generate keying material

```
  ▾ Random: f95a1e8a8713f29d5e6a5b003628f8c7b8ce6eb9193fc574...
    GMT Unix Time: Jul 27, 2102 14:10:42.000000000 IST
    Random Bytes: 8713f29d5e6a5b003628f8c7b8ce6eb9193fc57498c60b33...
    Session ID Length: 22
```

Key share - The cryptographic parameters of the endpoint are stored in the "key share" extension. Clients MAY send an empty client shares vector to the server in order to request group selection, at the penalty of an extra round trip.

```
  ▾ Extension: key_share (len=43)
    Type: key_share (51)
    Length: 43
    ▾ Key Share extension
      Client Key Share Length: 41
      ▾ Key Share Entry: Group: Reserved (GREASE), Key Exchange length: 1
        Group: Reserved (GREASE) (56026)
        Key Exchange Length: 1
        Key Exchange: 00
      ▾ Key Share Entry: Group: x25519, Key Exchange length: 32
        Group: x25519 (29)
        Key Exchange Length: 32
        Key Exchange: d5bc2e82c123984de80f96d028922c4c97cd1136169146cf...
```

Supported groups - When sent by the client, the "supported_groups" extension indicates

the named groups which the client supports for key exchange. If the server prefers a different group than those in the "key share" extension but is still ready to accept the ClientHello, it SHOULD send "supported groups" to update the client's view of its preferences.

```
  ▾ Extension: supported_groups (len=10)
    Type: supported_groups (10)
    Length: 10
    Supported Groups List Length: 8
    ▾ Supported Groups (4 groups)
      Supported Group: Reserved (GREASE) (0xdada)
      Supported Group: x25519 (0x001d)
      Supported Group: secp256r1 (0x0017)
      Supported Group: secp384r1 (0x0018)
```

PSK - The semantics of this addition are that the client only permits the usage of PSKs with certain modes, which limits the use of both the PSKs presented in this ClientHello and those supplied by the server via NewSessionTicket.

```
  ▾ Extension: psk_key_exchange_modes (len=2)
    Type: psk_key_exchange_modes (45)
    Length: 2
    PSK Key Exchange Modes Length: 1
    PSK Key Exchange Mode: PSK with (EC)DHE key establishment (psk_dhe_ke) (1)
```

Question 10

The browser/TLS versions supported by the client are shown in the below snapshot

```
  ▾ Extension: supported_versions (len=7)
    Type: supported_versions (43)
    Length: 7
    Supported Versions length: 6
    Supported Version: Unknown (0xdada)
    Supported Version: TLS 1.3 (0x0304)
    Supported Version: TLS 1.2 (0x0303)
```

The version selected by the server is shown in the below snapshot

```
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 78
```

Question 11

```
- TLSv1.2 Record Layer: Handshake Protocol: Certificate
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 2884
  - Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 2880
    Certificates Length: 2877
    - Certificates (2877 bytes)
      Certificate Length: 1695
      > Certificate: 3082069b30820583a0030201020210016cba7af77ac3d7ae... (id-at-commonName=*.icicibank.com, id-at-organizationName=ICIC
      Certificate Length: 1176
      > Certificate: 308204943082037ca003020102021001fda3eb6eca75c888... (id-at-commonName=DigiCert SHA2 Secure Server CA, id-at-organiz
```

As we can infer from the above snapshot, the server has returned two certificates to the client :

1. The server certificate (*.icicibank.com)
2. The intermediate CA certificate(DigiCert SHA2 Secure Server CA)

Server certificates are used to authenticate the identity of a server whereas the intermediate CA certificates are used to authenticate end user certificates. The relation is that the intermediate certificate connects the server certificate to the root certificate of the CA. They constitute the SSL chain of trust, which is an ordered list of certificates that allows the receiver (a web browser) to verify the sender (your secure server) and the CA are trustworthy.

Question 12

The key exchange algorithm that the client and server agreed upon is “Elliptic Curve Diffie–Hellman Key Exchange”. It is proven to provide perfect forward secrecy. The parameters that got exchanged are shown in the below snapshot:

```
- TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 333
  - Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 329
    - EC Diffie-Hellman Server Params
      Curve Type: named_curve (0x03)
      Named Curve: secp256r1 (0x0017)
      Pubkey Length: 65
      Pubkey: 0496b4b24ade8271877e0dcba7d8e390f82883d70808301...
      - Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
        Signature Length: 256
        Signature: 888cccd1760a29ca771ae2a7612d3ee5ace69edc6313790b8...
```

Question 13

```
Certificate: 3082069b30820583a0030201020210016cba7af77ac3d7ae...
(id-at-commonName=*.icicibank.com,id-at-organizationName=ICICI
Bank
Limited,id-at-localityName=Mumbai,id-at-stateOrProvinceName=Maha
rashtra,id-at-countryName=IN)
```

From the above information we can conclude that the certificate is of the type **OV** since it is providing detailed information .

Question 14

`id-at-commonName=*.icicibank.com` Indicates that the bank is using a wild-card type certificate.

Question 15

```
- Transport Layer Security
  - TLSv1.2 Record Layer: Handshake Protocol: Certificate Status
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 479
  - Handshake Protocol: Certificate Status
    Handshake Type: Certificate Status (22)
    Length: 475
    Certificate Status Type: OCSP (1)
    OCSP Response Length: 471
  - OCSP Response
    responseStatus: successful (0)
    > responseBytes
```

Using the OCSP response status, the client may determine whether or not the certificate has been revoked. From the above snapshot, we can see that the OCSP response status is successful indicating the certificate has been revoked.

The server supports the OCSP stapling.

Question 16

```
▼ Extension (SignedCertificateTimestampList)
  Extension Id: 1.3.6.1.4.1.11129.2.4.2 (SignedCertificateTimestampList)
  Serialized SCT List Length: 358
  ▶ Signed Certificate Timestamp (Google 'Argon2022' log)
  ▶ Signed Certificate Timestamp (DigiCert Nessie2022 Log)
  ▶ Signed Certificate Timestamp (Cloudflare 'Nimbus2022' Log)
```

As we can see from the above snapshot, in the extension SCT three servers have logged the certificate of the bank. With the help of these log servers, it gives the freedom to query the servers about the certificates and also the timestamp they were included at.

Question 17

```
▼ Transport Layer Security
  ▷ TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 2883
    Encrypted Application Data: 65975fd3a767929f6d7579a4e2312f6af5bc9ec8f98bd882...
    ▶ TLS segment data (2859 bytes)
    ▶ TLS segment data (600 bytes)
  ▷ [2 Reassembled TLS segments (4081 bytes): #58(1822), #60(2259)]
  ▷ HyperText Transfer Protocol 2
```

The application data is encrypted using symmetric key encryption, with the encryption key being the master key that can only be retrieved once.

Yes, the records containing application data include a separate MAC.

Wireshark doesn't distinguish between the encrypted application data and the MAC.

Question 18

1. CLIENT_HANDSHAKE_TRAFFIC_SECRET - The hex-encoded handshake traffic secret for the client side. HANDSHAKE SECRET and ECDH parameters were used to create this value.
2. CLIENT_RANDOM - 48 bytes for the master secret, encoded as 96 hexadecimal characters. A random function was used to choose.
3. CLIENT_TRAFFIC_SECRET_0 - The first hex-encoded application traffic secret for the client side. This is derived from MASTER_SECRET.
4. SERVER_TRAFFIC_SECRET_0 - The first hex-encoded application traffic secret for the server side. This is derived from MASTER_SECRET.

5. EXPORTER_SECRET - The hex-encoded exporter secret. This is derived from MASTER_SECRET.
6. SERVER_HANDSHAKE_TRAFFIC_SECRET - The hex-encoded handshake traffic secret for the server side. HANDSHAKE SECRET and ECDH parameters were used to create this value.

Question 19

There is a scope for session resumption since the server is keeping track of the recently used session ID's

```

▼ TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 202
  ▼ Handshake Protocol: New Session Ticket
    Handshake Type: New Session Ticket (4)
    Length: 198
    ▼ TLS Session Ticket
      Session Ticket Lifetime Hint: 83100 seconds (23 hours, 5 minutes)
      Session Ticket Length: 192
      Session Ticket: 000022a6ac77ea95900d73fdeb4e4094a217614373643bd6...
  
```

From the above snapshot we can see that it is based on session ID/session tickets and not on psk.

The role of session tickets in TLS 1.3 is that ,when a client reconnects to server with a session ID, the server can quickly look up the session keys and resume the encrypted communication.

Question 20

To establish a secure connection, a full TLS handshake needs two round trips.

We can achieve it with just one round trip with the help of TLS session resumption i.e half of the number of round trips can be reduced.

Question 21

Wireshark - All Addresses · CS19BTECH11012.pcapng								
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
All Addresses	3189				0.1380	100%	2.8300	3.262
74.125.68.154	47				0.0020	1.47%	0.2300	4.643
65.2.91.176	210				0.0091	6.59%	1.5800	3.271
52.172.161.242	21				0.0009	0.66%	0.1900	4.192
49.44.178.83	14				0.0006	0.44%	0.1000	5.779
49.44.178.66	14				0.0006	0.44%	0.1000	6.139
49.44.119.163	29				0.0013	0.91%	0.1300	6.018
40.69.200.41	39				0.0017	1.22%	0.1000	7.671
34.96.102.137	165				0.0071	5.17%	0.4500	2.691
255.255.255.255	4				0.0002	0.13%	0.0300	8.667
239.255.255.250	43				0.0019	1.35%	0.0200	1.001
224.0.0.251	24				0.0010	0.75%	0.0400	0.371
224.0.0.22	2				0.0001	0.06%	0.0100	2.419
224.0.0.2	12				0.0005	0.38%	0.0400	4.160
216.58.200.141	6				0.0003	0.19%	0.0600	16.631
216.58.200.132	63				0.0027	1.98%	0.1900	7.825
216.239.36.54	54				0.0023	1.69%	0.2300	4.053
203.189.92.162	134				0.0058	4.20%	0.4000	15.398
203.171.210.25	16				0.0007	0.50%	0.1500	1.705
192.168.36.53	56				0.0024	1.76%	0.0600	2.641
192.168.115.48	9				0.0004	0.28%	0.0200	12.254
192.168.115.255	2				0.0001	0.06%	0.0100	2.830
192.168.115.157	3				0.0001	0.09%	0.0100	7.967
192.168.114.91	2				0.0001	0.06%	0.0100	22.899
192.168.114.86	4				0.0002	0.13%	0.0100	7.438
192.168.114.84	3				0.0001	0.09%	0.0100	7.335
192.168.114.83	3				0.0001	0.09%	0.0100	17.373
192.168.114.75	1				0.0000	0.03%	0.0100	22.185
192.168.114.72	4				0.0002	0.13%	0.0100	0.270
192.168.114.49	4				0.0002	0.13%	0.0400	8.667
192.168.114.44	2				0.0001	0.06%	0.0100	7.232
192.168.114.43	10				0.0004	0.31%	0.0200	0.576
192.168.114.41	2				0.0001	0.06%	0.0100	2.419
192.168.114.23	2				0.0001	0.06%	0.0100	4.161
192.168.114.150	11				0.0005	0.34%	0.0200	3.342
192.168.114.15	2				0.0001	0.06%	0.0100	4.162
192.168.114.146	3				0.0001	0.09%	0.0100	15.938
192.168.114.13	2				0.0001	0.06%	0.0100	7.233

Display filter:

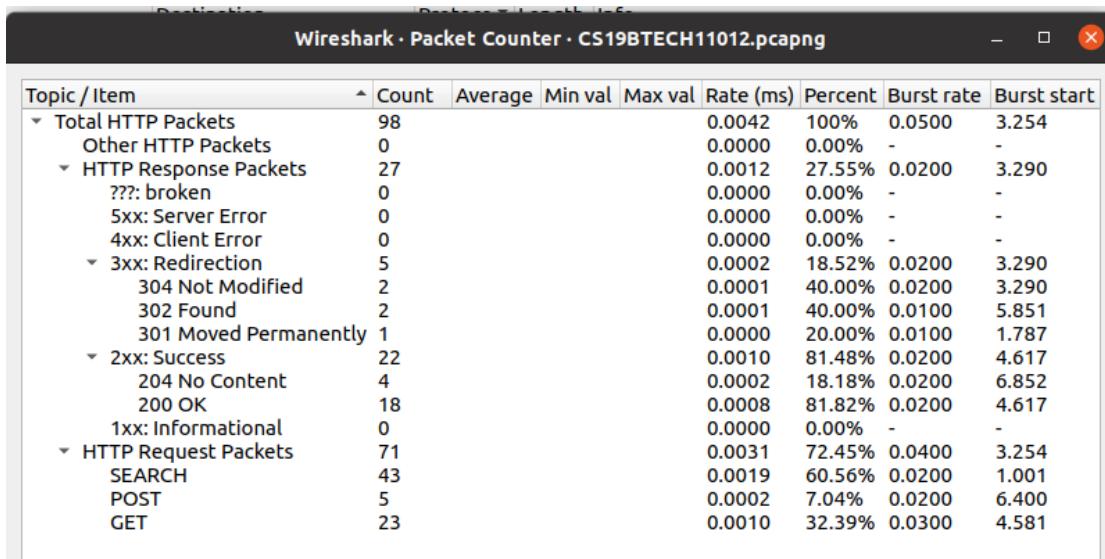
Duration of the HTTPS session is 20 secs and the total number of packets exchanged is 3189 packets.

Question 22

The number of packets exchanged over the TLS pipeline is 1240 .

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	1184	100.0	2613699	1,257 k	0	0
Ethernet	100.0	1184	0.6	16576	7,976	0	0
Internet Protocol Version 4	100.0	1184	0.9	23680	11 k	0	0
Transmission Control Protocol	100.0	1184	98.5	2573443	1,238 k	0	0
Transport Layer Security	104.7	1240	161.7	4225442	2,033 k	360	61584

Question 23



From the above snapshot, we can observe that the total number of HTTP packets is 98 out of which :

1. HTTP Request - 23 packets
2. HTTP response - 5 packets

The packet that carried the response that included the Net Banking LOG-IN page of ICICI bank is shown below:

```
1 HTTP/1.1 200 OK
1 Date: Sun, 27 Feb 2022 15:39:15 GMT
1 Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
1 X-Powered-By:
2 VIEW_ID: AuthenticationScreen
2 Cache-Control: no-store
3 Pragma: no-cache
4 Expires: 0
5 Title: Log in to Internet Banking
6 X-XSS-Protection: 1; mode=block
7 X-Frame-Options: SAMEORIGIN
8 Vary: Accept-Encoding
9 Content-Encoding: gzip
10 Keep-Alive: timeout=10, max=98
11 Connection: Keep-Alive
12 Transfer-Encoding: chunked
13 Content-Type: text/html;charset=UTF-8
14 Content-Language: en-US
15 Set-Cookie: NSC_jogjojuz.jdjdjcbo1.dpn_64.224=fffffffffaf181aa745525d5f4f58
16 GMT;path=/;secure;httponly
17
```

- Hypertext Transfer Protocol

- [truncated]GET /corp/AuthenticationController?FORMSGROUP_ID_=AuthenticationFG&_STARTTI
- [truncated]Expert Info (Chat/Sequence): GET /corp/AuthenticationController
- Request Method: GET
- Request URI [truncated]: /corp/AuthenticationController?FORMSGROUP_ID_=Authenti
- Request URI Path: /corp/AuthenticationController
- Request URI Query [truncated]: FORMSGROUP_ID_=AuthenticationFG&_STARTTI

0000	47 45 54 20 2f 63 6f 72 70 2f 41 75 74 68 65 6e	GET /cor p/Authen
0010	74 69 63 61 74 69 6f 6e 43 6f 6e 74 72 6f 6c 6c	tication Controll
0020	65 72 3f 46 4f 52 4d 53 47 52 4f 55 50 5f 49 44	er?FORMS GROUP_ID
0030	5f 5f 3d 41 75 74 68 65 6e 74 69 63 61 74 69 6f	=Authenticatio
0040	6e 46 47 26 5f 5f 53 54 41 52 54 5f 54 52 41 4e	nFG&_ST ART_TRAN
0050	5f 46 4c 41 47 5f 5f 3d 59 26 46 47 5f 42 55 54	_FLAG=_Y&FG_BUT
0060	54 4f 4e 53 5f 5f 3d 4c 4f 41 44 26 41 43 54 49	TONS=_L OAD&ACTI
0070	4f 4e 2e 4c 4f 41 44 3d 59 26 41 75 74 68 65 6e	ON.LOAD=_Y&Authen
0080	74 69 63 61 74 69 6f 6e 46 47 2e 4c 4f 47 49 4e	tication FG.LOGIN
0090	5f 46 4c 41 47 3d 31 26 42 41 4e 4b 5f 49 44 3d	_FLAG=1& BANK_ID=
00a0	49 43 49 26 49 54 4d 3d 6e 6c 69 5f 70 65 72 73	ICI&ITM=_nli_pers
00b0	6f 6e 61 6c 62 5f 70 65 72 73 6f 6e 61 6c 5f 6c	onalb_pe rsonal_1
00c0	6f 67 69 6e 5f 62 74 6e 26 5f 67 61 3d 32 2e 32	ogin_btn &_ga=2.2
00d0	31 33 37 38 38 33 30 38 2e 31 32 38 30 39 37 39	13788308 .1280979
00e0	30 32 2e 31 36 34 35 39 36 38 34 35 39 2d 31 31	02.16459 68459-11
00f0	33 34 36 36 31 31 35 33 2e 31 36 34 35 39 36 38	34661153 .1645968
0100	34 35 39 26 5f 67 6c 3d 31 2a 32 36 31 33 67 77	459&_gl= 1*2613gw
0110	2a 5f 67 61 2a 4d 54 45 7a 4e 44 59 32 4d 54 45	*_ga*MTE zNDY2MTE
0120	31 4d 79 34 78 4e 6a 51 31 4f 54 59 34 4e 44 55	1My4xNjQ 10TY4NDU
0130	35 2a 5f 67 61 5f 53 4b 42 37 38 47 48 54 46 56	5*_ga_SK B78GHTFV
0140	2a 4d 54 59 30 4e 54 6b 33 4e 6a 4d 31 4d 79 34	*MTY0NTk 3NjM1My4

Frame (416 bytes) Reassembled TCP (1798 bytes) Decrypted TLS (1769 bytes)

The response messages do carry security related directives like XSS, sameorigin, HSTS.

Question 24

- Hypertext Transfer Protocol

- POST /corp/AuthenticationController;jsessionid=0000T8D8KRDiABkgXpoZG0wI207:R05p6kjhr?bw&
- [Expert Info (Chat/Sequence): POST /corp/AuthenticationController;jsessionid=0000T8D8KRDiABkgXpoZG0wI207:R05p6kjhr?bw&]
- Request Method: POST
- Request URI: /corp/AuthenticationController;jsessionid=0000T8D8KRDiABkgXpoZG0wI207:R05p6kjhr?bw&

0000	44 55 4d 4d 59 31 3d 26 44 55 4d 4d 59 32 3d 26	DUMMY1=& DUMMY2=&
0010	41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 46 47	Authenti cationFG
0020	2e 55 53 45 52 5f 50 52 49 4e 43 49 50 41 4c 3d	.USER_PR INCIPAL=
0030	6e 69 73 68 61 26 64 75 6d 6d 79 70 77 64 31 3d	nisha&du mmypwd1=
0040	26 64 75 6d 6d 79 70 77 64 32 3d 26 41 75 74 68	&dummypw d2=&Auth
0050	65 6e 74 69 63 61 74 69 6f 6e 46 47 2e 41 43 43	enticati onFG.ACC
0060	45 53 53 5f 43 4f 44 45 3d 36 38 64 61 64 38 39	ESS_CODE =68dad89
0070	63 35 30 31 35 38 30 61 64 62 63 33 66 32 39 34	c501580a dbc3f294
0080	62 39 36 38 66 31 62 38 34 33 63 64 30 33 34 62	b968f1b8 43cd034b
0090	64 61 35 62 65 38 33 61 39 30 66 38 64 37 31 65	da5be83a 90f8d71e
00a0	39 36 32 61 32 37 32 36 61 61 65 30 66 36 64 39	962a2726 aae0f6d9
00b0	32 36 36 35 38 31 61 61 31 39 32 65 35 32 64 64	266581aa 192e52dd
00c0	30 61 36 65 64 33 32 65 31 34 37 62 38 62 37 30	0a6ed32e 147b8b70
00d0	36 30 32 66 39 39 34 33 36 34 32 65 64 34 35 36	602f9943 642ed456
00e0	63 32 32 34 66 37 30 39 37 64 33 66 65 34 61 32	c224f709 7d3fe4a2
00f0	35 66 61 66 39 34 62 65 38 37 39 30 63 34 61 37	5faf94be 8790c4a7
0100	36 33 32 33 66 64 65 32 65 33 34 65 30 61 36 34	6323fde2 e34e0a64
0110	30 32 31 31 61 36 62 32 36 33 31 30 65 66 34 33	0211a6b2 6310ef43
0120	39 62 33 31 64 39 64 64 66 30 30 64 62 30 64 35	9b31d9dd f00db0d5
0130	33 62 61 38 62 62 34 37 35 34 62 61 35 34 34 34	3ba8bb47 54ba5444
0140	35 38 39 38 66 32 39 63 37 63 31 36 30 31 61 39	5898f29c 7c1601a9

Frame (1301 bytes) Reassembled TCP (7027 bytes) Decrypted TLS (6998 bytes) Reassembled SSL (9136 bytes)

Both the user id and password in the raw packet capture are shown in the above and below snapshots.

```

- HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "DUMMY1" = ""
  Form item: "DUMMY2" = ""
  Form item: "AuthenticationFG.USER_PRINCIPAL" = "nisha"
  Form item: "dummypwd1" = ""
  Form item: "dummypwd2" = ""
  Form item: "AuthenticationFG.ACCESS_CODE" = "68dad89c501580adbc3f294b968f1b843cd034bda5be83a90f8d71e962a2726aae0f6d9266581aa192e52dd0a6ed3"
  Form item: "dummy1" = "4c3298a431733563b6db83f2b328a3c65ac52e0829f86c76759e7bb8d3a700430d1c7705fb6f8a482155a360aaeee81accacf1f1e0539693ad48"
  Form item: "AuthenticationFG.MENU_ID" = "RDASH"
  Form item: "Action.VALIDATE_CREDENTIALS" = "Login"
  Form item: "AuthenticationFG.RIB_COUNTRY_CODE" = "91"
  Form item: "AuthenticationFG.RIB_LOGIN_MOBILE" = ""
  Form item: "FG_BUTTONS__" = "VALIDATE_CREDENTIALS,VALIDATE_CREDENTIALS_DIG_CERT,BACK,CLEAR_VALUES"
  Form item: "AuthenticationFG.IS_FIRST_AUTHENTICATION" = "Y"
  Form item: "QS" = ""
  Form item: "MD" = ""
  Form item: "PID" = ""
  Form item: "PRN" = ""
  Form item: "ITC" = ""
  Form item: "AMT" = ""
  Form item: "CRN" = ""
  Form item: "RU" = ""
  Form item: "CG" = ""
  Form item: "ES" = ""
  Form item: "RUBACK" = "null"
  Form item: "AuthenticationFG.LOGIN_MODE_FLAG" = "U"
  Form item: "AuthenticationFG.__CALL_MODE__" = "null"
  Form item: "CATEGORY_ID" = ""
  Form item: "AuthenticationFG.PREFERRED_LANGUAGE" = "001"
  Form item: "FORMSGROUP_ID__" = "AuthenticationFG"

```

Question 25

SSL Report: [icicibank.com](https://www.ssllabs.com/ssltest/analyze.html?d=icicibank.com) (2001:df0:2fd:1:0:0:0:1)

Assessed on: Sun, 27 Feb 2022 12:29:14 UTC | [Clear cache](#)

[Scan Another »](#)



The security features implemented by the bank's web server include :

1. Providing perfect forward secrecy by using the below mention cipher suites as per TLSv1.2

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

2. OCSP stapling
3. Secure Renegotiation
4. No ECDH public server param reuse

Question 26

```
  ▾ Extension: ec_point_formats (len=2)
    Type: ec_point_formats (11)
    Length: 2
    EC point formats Length: 1
  ▾ Elliptic curves point formats (1)
    EC point format: uncompressed (0)

  ▾ Extension: compress_certificate (len=3)
    Type: compress_certificate (27)
    Length: 3
    Algorithms Length: 2
    Algorithm: brotli (2)
  ▶ Extension: Unknown type 17513 (len=5)
  ▾ Extension: Reserved (GREASE) (len=1)
    Type: Reserved (GREASE) (14906)
    Length: 1
    Data: 00
```

- The purpose of sending the extension is to notify the peer whether you support compressed points, as support for uncompressed points is required (if you support EC ciphersuites and certs at all).
If you don't support compression and don't send the extension, there's a chance the peer will send you a compressed-point cert/chain and/or ephemeral key, which you won't be able to process, and the handshake will fail, even if the peer could have used an uncompressed-point cert/chain and/or key or some other negotiable ciphersuite that would have worked.
- The sender communicates to the peer the certificate-compression techniques it is willing to apply for decompression by sending a compress certificate extension. This extension's "extension data" field MUST have the value CertificateCompressionAlgorithms.

PLAGIARISM STATEMENT

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honor violations by other students if I become aware of it.

Name: Nisha M

Date: 27/2/2022

Signature: Nisha M