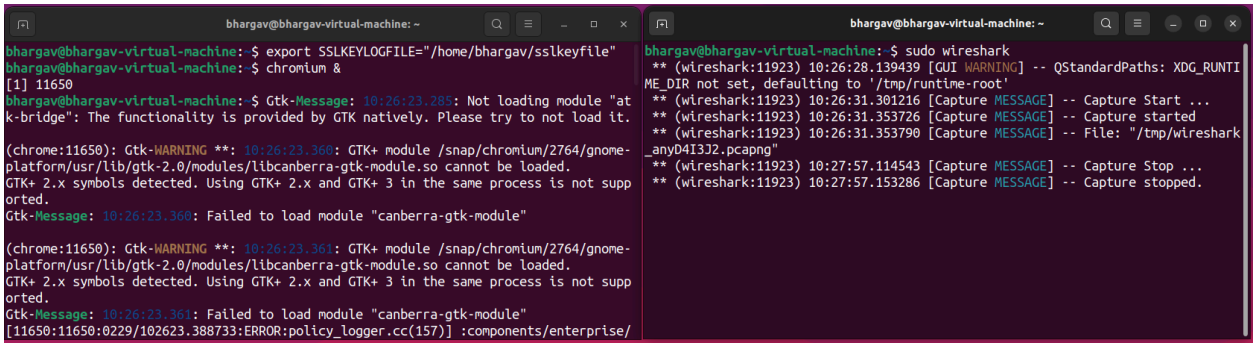
Assignment 6: Decrypting TLS and HTTP(S) using Wireshark++
Report - CS23MTECH11026 - Bhargav Patel

PART-A: Decrypt TLS handshake and HTTPS messages between your browser and the web server of Bank X

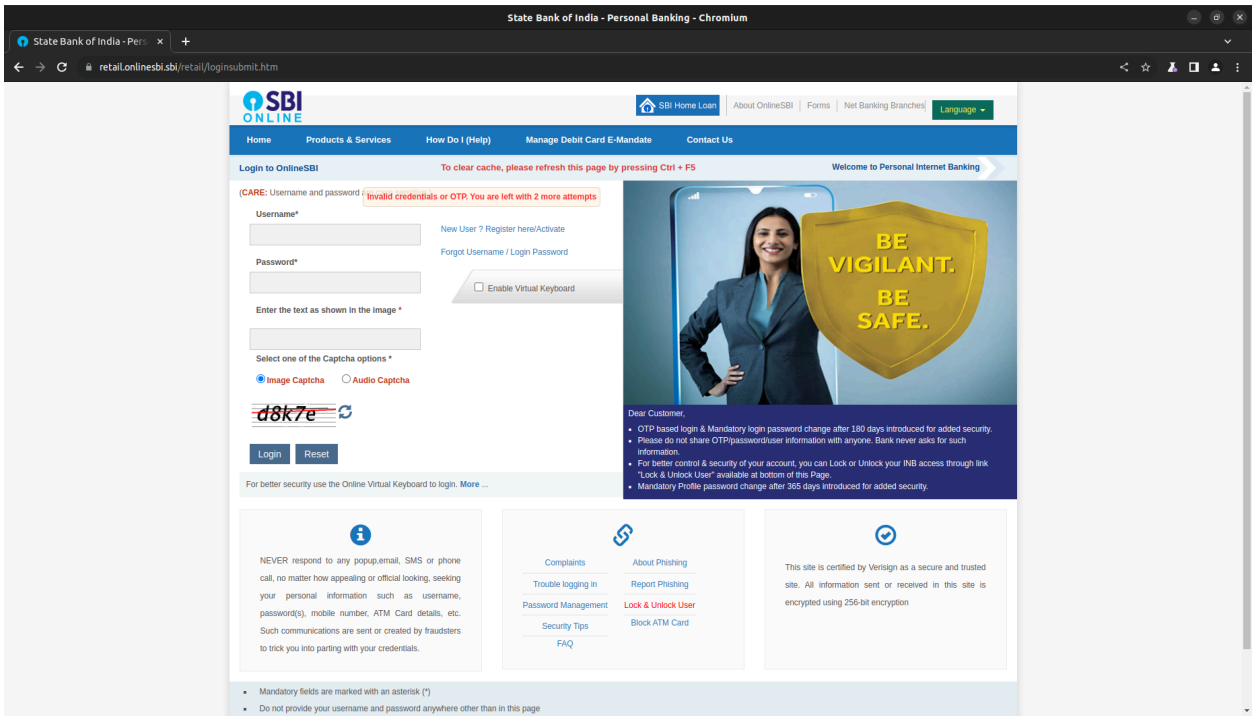
N = 26 % 4 + 1 = 3 (SBI)



1. Set - SSLKEYLOGFILE

2. Start wireshark

3. Start browser (chromium &)

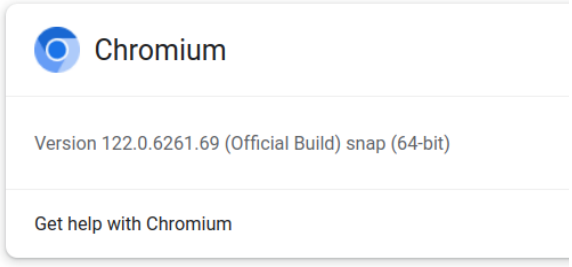


4. Navigate to netbanking login page of SBI, then enter username and pass which fails

5. Stopped the wireshark capture and stored as CS23MTECH11026-SBI.pcapng (attached in tar file.) (before SSLKEYLOGFILE took the SS and saved as encrypted.pcapng and after SSLKEYLOGFILE gave the name CS23MTECH11026-SBI.pcapng). Both **Deliverable-1 & 2** are in tarball file.

PART - B

1. **What browser did you use, what's the version number?**
   Browser: Chromium
   Version: 122.0.6261.69



2. **List out various protocols that you noticed in the column named "Protocol" in the wireshark GUI from the time you keyed in the hostname of the bank in the browser till you start viewing application data. For each such protocol, mention its purpose in brief.**
   TLS: Provides secure communication over the internet.
   TCP: Ensures reliable, ordered, and error-checked delivery of a stream of packets on the internet.
   HTTP: Used for transmitting data between a web server and a web browser.
   DNS: Resolves domain names to IP addresses
   UDP: Connectionless protocol which offers faster, but less reliable method of communication
   QUIC: Provides faster and secure connection on the internet. Use HTTP3.

3. **Each of the TLS records begins with the same three fields (with possibly different values). One of these fields is "content type" and has a length of one byte. List all three fields and their lengths for the first 10 records in the trace.**

   1st TLS Record : Client hello (Similarly checked for the other TLS records

```
Frame 2414: 573 bytes on wire (4584 bits), 573 bytes captured
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.49.128, Dst: 103.68.
Transmission Control Protocol, Src Port: 37952, Dst Port: 443,
Transport Layer Security
▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  ▸ Handshake Protocol: Client Hello
```

TLS Record	Content Type	Version	Length
1	Handshake (22)	TLS 1.0 (0x0301)	512
2	Handshake (22)	TLS 1.2 (0x0303)	122
3	Handshake (22)	TLS 1.2 (0x0303)	4097
4	Change Cipher Spec (20)	TLS 1.2 (0x0303)	1
5	Handshake (22)	TLS 1.0 (0x0301)	512
6	Handshake (22)	TLS 1.2 (0x0303)	282
7	Handshake (22)	TLS 1.2 (0x0303)	122
8	Change Cipher Spec (20)	TLS 1.2 (0x0303)	1
9	Handshake (22)	TLS 1.2 (0x0303)	282
10	Application data (23)	TLS 1.2 (0x0303)	1389

I also observed that some TLS records contains multiple TLS records in like Server Hello there was TLS records for Handshake, Change Cipher Spec, Encrypted Extension, Certificate. For simplicity I have considered the 1st one of particular TLS record.

4. **What are the key extensions that you noticed in the Client Hello message? By observing the Server Hello message, explain what extensions really used by the server for establishing TLS pipe?**

   Extensions they agreed upon:

   - Supported Version: TLS 1.3 (0x0304)
   - Key Share Entry: Group: x25519, Key Exchange length: 32
   - ALPN protocol: application_layer_protocol_negotiation (len=11)
   - Cipher Suite negotiated : TLS_AES_256_GCM_SHA384 (0x130)

Client Hello extensions:

```
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.49.128, Dst: 103.68.221.191
Transmission Control Protocol, Src Port: 37952, Dst Port: 443, Seq: 1, Ack: 1, Len
Transport Layer Security
▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 508
      Version: TLS 1.2 (0x0303)
      Random: 0318e620e2caa99db76bdf5e74618907948f59748fcecba8c5d77ade5202905b
      Session ID Length: 32
      Session ID: b54bcbf2e623d85ab1f120070a5635f69cfab6fc28c1f24316bcb1111f93c7d0
      Cipher Suites Length: 32
    ▸ Cipher Suites (16 suites)
      Compression Methods Length: 1
    ▸ Compression Methods (1 method)
      Extensions Length: 403
    ▸ Extension: Reserved (GREASE) (len=0)
    ▸ Extension: compress_certificate (len=3)
    ▸ Extension: key_share (len=43)
    ▸ Extension: supported_versions (len=7)
    ▸ Extension: signed_certificate_timestamp (len=0)
    ▸ Extension: session_ticket (len=0)
    ▸ Extension: ec_point_formats (len=2)
    ▸ Extension: server_name (len=25)
    ▸ Extension: psk_key_exchange_modes (len=2)
    ▸ Extension: application_settings (len=5)
    ▸ Extension: renegotiation_info (len=1)
    ▸ Extension: application_layer_protocol_negotiation (len=14)
    ▸ Extension: status_request (len=5)
    ▸ Extension: extended_master_secret (len=0)
    ▸ Extension: Unknown type 65037 (len=186)
    ▸ Extension: signature_algorithms (len=18)
    ▸ Extension: supported_groups (len=10)
    ▸ Extension: Reserved (GREASE) (len=1)
    ▸ Extension: padding (len=5)
      [JA3 Fullstring: 771,2570-4865-4866-4867-49195-49199-49196-49200-52393-52392-
      [JA3: 5b39a709699f8fbc7122df54ea019423]
```

Server Hello extensions:

```
Frame 2429: 4152 bytes on wire (33216 bits), 4152 bytes captured (33216 bits) on i
Linux cooked capture v1
Internet Protocol Version 4, Src: 103.68.221.191, Dst: 192.168.49.128
Transmission Control Protocol, Src Port: 443, Dst Port: 37952, Seq: 1, Ack: 518, L
Transport Layer Security
▾ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
  ▾ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 118
      Version: TLS 1.2 (0x0303)
      Random: 3b75cfd122a5c424c91e09e8d2b47308c74e1a01ae9224bf92fdf24394fd49df
      Session ID Length: 32
      Session ID: b54bcbf2e623d85ab1f120070a5635f69cfab6fc28c1f24316bcb1111f93c7d0
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Compression Method: null (0)
      Extensions Length: 46
    ▸ Extension: supported_versions (len=2)
    ▸ Extension: key_share (len=36)
      [JA3S Fullstring: 771,4866,43-51]
      [JA3S: 15af977ce25de452b96affa2addb1036]
▾ TLSv1.3 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
▾ TLSv1.3 Record Layer: Handshake Protocol: Encrypted Extensions
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 58
    [Content Type: Handshake (22)]
  ▾ Handshake Protocol: Encrypted Extensions
      Handshake Type: Encrypted Extensions (8)
      Length: 37
      Extensions Length: 35
    ▸ Extension: server_name (len=0)
    ▸ Extension: supported_groups (len=12)
    ▸ Extension: application_layer_protocol_negotiation (len=11)
```

5. **Cipher Suites in ClientHello Record: Look at the first two and the last cipher suites offered by the client and compare them. What cipher suite the server selected?**

```
Frame 2414: 573 bytes on wire (4584 bits), 573 bytes captured (4584 bits) on
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.49.128, Dst: 103.68.221.191
Transmission Control Protocol, Src Port: 37952, Dst Port: 443, Seq: 1, Ack:
Transport Layer Security
▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 508
      Version: TLS 1.2 (0x0303)
      Random: 0318e620e2caa99db76bdf5e74618907948f59748fcecba8c5d77ade520290
      Session ID Length: 32
      Session ID: b54bcbf2e623d85ab1f120070a5635f69cfab6fc28c1f24316bcb1111f
      Cipher Suites Length: 32
    ▾ Cipher Suites (16 suites)
        Cipher Suite: Reserved (GREASE) (0x0a0a)
        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 (0xcca9)
        Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Compression Methods Length: 1
```

1: TLS_AES_128_GCM_SHA256 (0x1301)
2: TLS_AES_256_GCM_SHA384 (0x1302)
Last: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

2nd Cipher Suite Selected by Server

```
▾ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
  ▾ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 118
      Version: TLS 1.2 (0x0303)
      Random: 3b75cfd122a5c424c91e09e8d2b47308c74e1a01ae9224
      Session ID Length: 32
      Session ID: b54bcbf2e623d85ab1f120070a5635f69cfab6fc28
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Compression Method: null (0)
```

Comparing all the 3 cipher suites (1st, 2nd, last) offered by the client to the server. The second one is the most secure because it uses a longer key length (AES_256), SHA_384 more stronger than SHA_256 and GCM is more secure than CBC (using CBC poodle attack may happen.)

6. **What is the SNI value in ClientHello Record? What's its purpose? In other words, why is the client advertising it to the server?**

   SNI: Server Name Indication. Basically it indicates which hostname of a server the client is attempting to connect to. So that at the server end no confusion is there for the connection establishment, because the server may host multiple hostname with same IP address.

```
▾ Extension: server_name (len=25)
    Type: server_name (0)
    Length: 25
  ▾ Server Name Indication extension
      Server Name list length: 23
      Server Name Type: host_name (0)
      Server Name length: 20
      Server Name: retail.onlinesbi.sbi
▸ Extension: psk_key_exchange_modes (len=2)
▸ Extension: application_settings (len=5)
```

7. **What is the ALPN value(s) in ClientHello Record? What's its purpose? Which one the server selected?**

   ALPN: Using application layer protocol negotiation the client indicated that this protocols are supported at my end (application layer protocol) then the server selects among one of them and sends it in Server_Hello record.

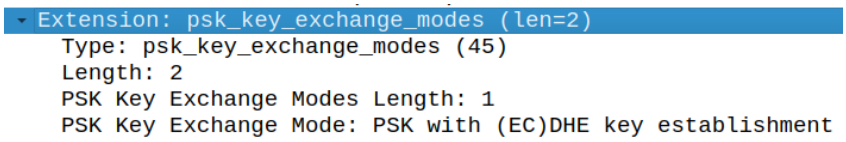
```
▸ Extension: renegotiation_info (len=1)
▾ Extension: application_layer_protocol_negotiation (len=14)
    Type: application_layer_protocol_negotiation (16)
    Length: 14
    ALPN Extension Length: 12
  ▾ ALPN Protocol
      ALPN string length: 2
      ALPN Next Protocol: h2
      ALPN string length: 8
      ALPN Next Protocol: http/1.1
▸ Extension: status_request (len=5)
```

8. **Does the ClientHello contain status_request, supported_versions, psk_key_exchange_modes extensions? If so, what do they convey to the server?**

   Yes, the ClientHello contains those extensions mentioned in the question.

```
▸ Extension: key_share (len=43)
▾ Extension: supported_versions (len=7)
    Type: supported_versions (43)
    Length: 7
    Supported Versions length: 6
    Supported Version: Reserved (GREASE) (0x3a3a)
    Supported Version: TLS 1.3 (0x0304)
    Supported Version: TLS 1.2 (0x0303)
▾ Extension: signed_certificate_timestamp (len=0)
```

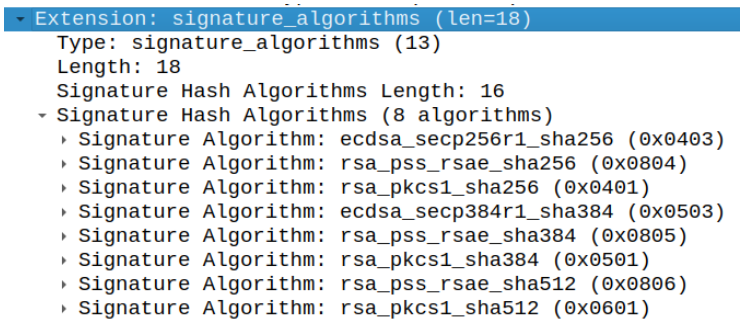
```
    ALPN Next Protocol: http/1.1
Extension: status_request (len=5)
  Type: status_request (5)
  Length: 5
  Certificate Status Type: OCSP (1)
  Responder ID list Length: 0
  Request Extensions Length: 0
```



status_request: it says that client support for certificate status request extension means to get a certificate from the server in the TLS handshake itself.
supported_verisons: it conveys which TLS versions are supported by the client
psk_key_exchange_modes: it conveys pre_share_key exchange modes supported by the client.
All the above things supported at client end are given and allows the server to select from them and send it back in ServerHello.

9. **Does ClientHello Record contain the Signature_algorithms extension? What's its purpose?**

   Yes, Using signature_algorithms extension it conveys which algorithms are supported for digital signature in TLS handshake. Further server selects the most compatible one and sends it back to the client in ServerHello record.



10. **Does the client offer any Random number, key share, Supported Groups and PSK in ClientHello Record? How will be these used by the Server?**

    Yes, except PSK the client contains all the other mentioned extensions. The server uses the client's random number and server's random number to generate other required keys. Using one of the supported groups from the client the key exchange methods are selected by the server. Using key share (shared secret) to generate the PMS (pre master secret). As PSK is not in the client hello the server can't resume the older session.

<table>
<tr>
<td>

```
▾ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
    Random: 0318e620e2caa99db76bdf5e74618907948
    Session ID Length: 32
    Session ID: b54bcbf2e623d85ab1f120070a5635f
```

</td>
<td>

```
▾ Extension: key_share (len=43)
      Type: key_share (51)
      Length: 43
    ▸ Key Share extension
  ▸ Extension: supported_versions (len=7)
  ▸ Extension: signed_certificate_timestamp
  ▸ Extension: session_ticket (len=0)
```

</td>
</tr>
<tr>
<td>

```
▾ Extension: supported_groups (len=10)
    Type: supported_groups (10)
    Length: 10
    Supported Groups List Length: 8
  ▾ Supported Groups (4 groups)
      Supported Group: Reserved (GREASE) (0x1a1a)
      Supported Group: x25519 (0x001d)
      Supported Group: secp256r1 (0x0017)
      Supported Group: secp384r1 (0x0018)
```

</td>
<td>ClientHello don’t have PSK</td>
</tr>
</table>

11. **What TLS versions your browser/client is supporting? Which one the server selected? Is it the same value as that used in the Record layer header and the Handshake header? Explain.**

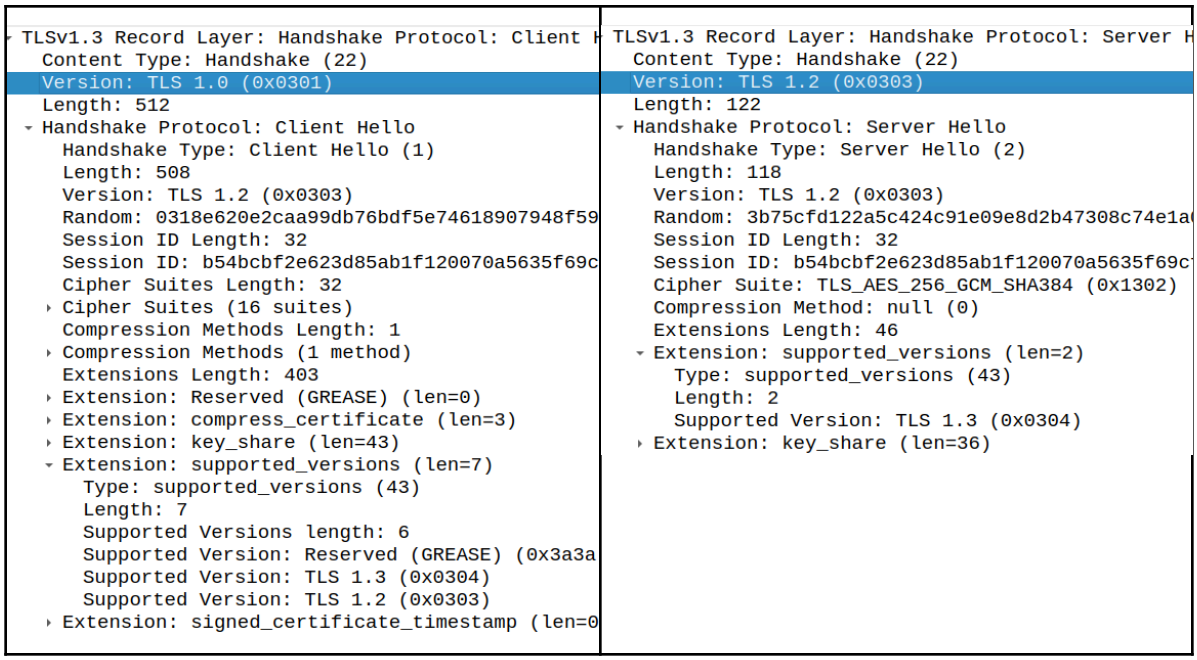
TLS versions supported by Client

```
▾ Extension: supported_versions (len=7)
    Type: supported_versions (43)
    Length: 7
    Supported Versions length: 6
    Supported Version: Reserved (GREASE) (0x3a3a)
    Supported Version: TLS 1.3 (0x0304)
    Supported Version: TLS 1.2 (0x0303)
```

TLS versions supported by Server

```
▾ Extension: supported_versions (len=2)
    Type: supported_versions (43)
    Length: 2
    Supported Version: TLS 1.3 (0x0304)
▾ Extension: key_share (len=36)
```

Looking at ClientHello and ServerHello in my case both have the different TLS version in the Record layer and Handshake protocol. This could be the reason to have compatibility with the legacy devices (middle boxes) which do not support higher versions of TLS (1.3). Using this kind of implementation maintains the compatibility with legacy devices as well as maintaining security by having higher versions in handshake protocol. Below are the images for the same.

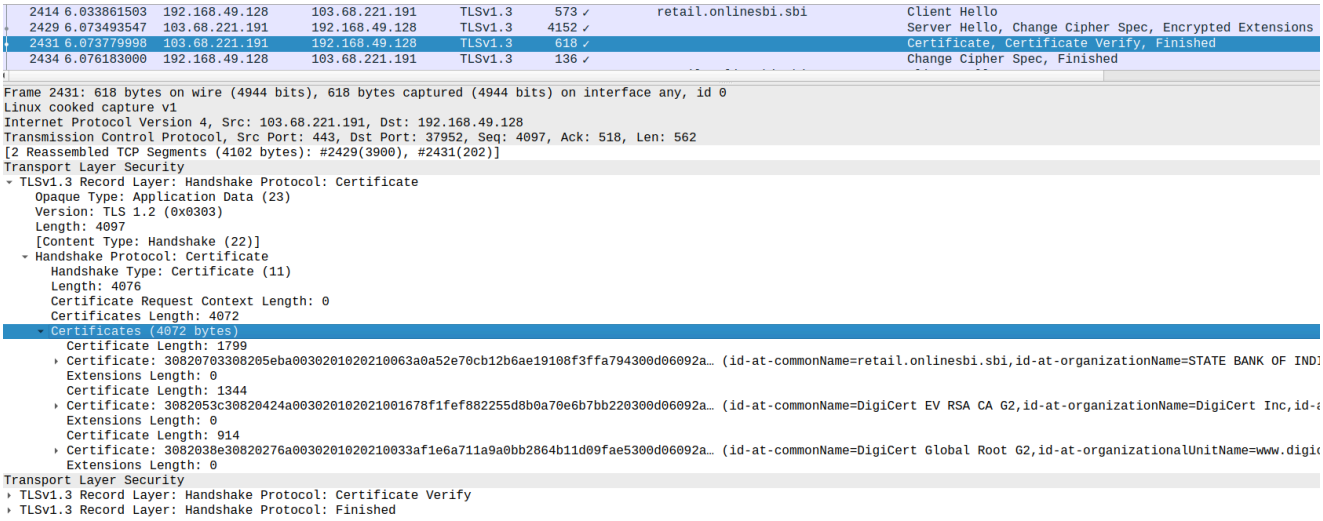


12. Look at Certificate Record from the server to the client: How many certificates did the server return and how are they related? Who is the issuer of the Bank's certificate? What type of public key the bank is using?

The server returns a total of 3 certificates. The relation between them is as follows:
1. End entity certificate (onlinesbi.sbi)
2. Intermediate certificate (DigiCert EV RSA CA G2)
3. Root certificate (DigiCert Global Root G2)

Bank's certificate issuer: (image from wireshark and website attached in next page)
Issuer Name
Country Name: US
Organization: DigiCert Inc
Common Name: DigiCert EV RSA CA G2

Public key used by Bank:
3082010a0282010100a6557fb29c23fc79f89d90f6754ece3a2690b837ea8e6ed6188afcf6ca
7c6f4b454d98de4f3da3785e0c4a1a818d6fc3bb4c386e040b1fbbcb508b42e9e21765e2c0d
0caf4e5c60ac94753321569f6c4ecb0e0b0fccbbadedfbeed2b443df62bb30acab8fcd15f842c
341e1552764e90fa8570bb05c302031774b380a1591f197b3a2bc3d559cfba5dbedf3b3a8e5
2c1d3a38c06d22a982f4d827f28f1b1d3717ecf4cb126f46fea09f97f5ad615465c9250d4f4f3c
a60254d9a66911dea74d4b171d930154cbbb6cdc61882f8b74897af2f221594feebe7deefcaa
36ecc2669d5925b6889562bb3726062498bc5594543c1f47e8f2bc4ddc1bb39d4bc5c515302
03010001



```
  2414 6.033861503  192.168.49.128  103.68.221.191  TLSv1.3   573 ✓  retail.onlinesbi.sbi  Client Hello
  2429 6.073493547  103.68.221.191  192.168.49.128  TLSv1.3  4152 ✓                         Server Hello, Change Cipher Spec, Encrypted Extensions
  2431 6.073779998  103.68.221.191  192.168.49.128  TLSv1.3   618 ✓                         Certificate, Certificate Verify, Finished
  2434 6.076183000  192.168.49.128  103.68.221.191  TLSv1.3   136 ✓                         Change Cipher Spec, Finished

Frame 2431: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 103.68.221.191, Dst: 192.168.49.128
Transmission Control Protocol, Src Port: 443, Dst Port: 37952, Seq: 4097, Ack: 518, Len: 562
[2 Reassembled TCP Segments (4102 bytes): #2429(3900), #2431(202)]
Transport Layer Security
▾ TLSv1.3 Record Layer: Handshake Protocol: Certificate
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 4097
    [Content Type: Handshake (22)]
  ▾ Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 4076
      Certificate Request Context Length: 0
      Certificates Length: 4072
    ▾ Certificates (4072 bytes)
        Certificate Length: 1799
      ▸ Certificate: 30820703308205eba0030201020210063a0a52e70cb12b6ae19108f3ffa794300d06092a… (id-at-commonName=retail.onlinesbi.sbi,id-at-organizationName=STATE BANK OF INDI
        Extensions Length: 0
        Certificate Length: 1344
      ▸ Certificate: 3082053c30820424a00302010202100167 8f1fef882255d8b0a70e6b7bb220300d06092a… (id-at-commonName=DigiCert EV RSA CA G2,id-at-organizationName=DigiCert Inc,id-a
        Extensions Length: 0
        Certificate Length: 914
      ▸ Certificate: 3082038e30820276a0030201020210033af1e6a711a9a0bb2864b11d09fae5300d06092a… (id-at-commonName=DigiCert Global Root G2,id-at-organizationalUnitName=www.digi
        Extensions Length: 0
Transport Layer Security
▸ TLSv1.3 Record Layer: Handshake Protocol: Certificate Verify
▸ TLSv1.3 Record Layer: Handshake Protocol: Finished
```

Chain of trust

```
▾ Certificates (4072 bytes)
    Certificate Length: 1799
  ▾ Certificate: 30820703308205eba0030201020210063a0a52e70cb12b6ae19108f3ffa794300d06092a… (id-at-commonName=retail.onlinesbi.sbi,id-at-orga
    ▾ signedCertificate
        version: v3 (2)
        serialNumber: 0x063a0a52e70cb12b6ae19108f3ffa794
      ▸ signature (sha256WithRSAEncryption)
      ▾ issuer: rdnSequence (0)
        ▾ rdnSequence: 3 items (id-at-commonName=DigiCert EV RSA CA G2,id-at-organizationName=DigiCert Inc,id-at-countryName=US)
          ▸ RDNSequence item: 1 item (id-at-countryName=US)
          ▸ RDNSequence item: 1 item (id-at-organizationName=DigiCert Inc)
          ▸ RDNSequence item: 1 item (id-at-commonName=DigiCert EV RSA CA G2)
      ▸ validity
      ▸ subject: rdnSequence (0)
      ▸ subjectPublicKeyInfo
      ▸ extensions: 10 items
    ▸ algorithmIdentifier (sha256WithRSAEncryption)
      Padding: 0
      encrypted: 8ab3139ce32cb0cfb12732bff14cb9b92bd643929abbb7d41191c24b777aea38d144589e…
    Extensions Length: 0
    Certificate Length: 1344
  ▸ Certificate: 3082053c30820424a00302010202100167 8f1fef882255d8b0a70e6b7bb220300d06092a… (id-at-commonName=DigiCert EV RSA CA G2,id-at-org
    Extensions Length: 0
    Certificate Length: 914
  ▸ Certificate: 3082038e30820276a0030201020210033af1e6a711a9a0bb2864b11d09fae5300d06092a… (id-at-commonName=DigiCert Global Root G2,id-at-
    Extensions Length: 0
```

Issuer of Bank's certificate

```
▾ Certificate: 30820703308205eba0030201020210063a0a52e70cb12b6ae19108f3ffa794300d06092a… (id-at-commonName=retail.onlinesbi.sbi,
  ▾ signedCertificate
      version: v3 (2)
      serialNumber: 0x063a0a52e70cb12b6ae19108f3ffa794
    ▸ signature (sha256WithRSAEncryption)
    ▾ issuer: rdnSequence (0)
      ▾ rdnSequence: 3 items (id-at-commonName=DigiCert EV RSA CA G2,id-at-organizationName=DigiCert Inc,id-at-countryName=US)
        ▸ RDNSequence item: 1 item (id-at-countryName=US)
        ▸ RDNSequence item: 1 item (id-at-organizationName=DigiCert Inc)
        ▸ RDNSequence item: 1 item (id-at-commonName=DigiCert EV RSA CA G2)
    ▸ validity
    ▸ subject: rdnSequence (0)
    ▾ subjectPublicKeyInfo
      ▸ algorithm (rsaEncryption)
      ▸ subjectPublicKey: 3082010a0282010100a6557fb29c23fc79f89d90f6754ece3a2690b837ea8e6ed6188afc…
    ▸ extensions: 10 items
  ▸ algorithmIdentifier (sha256WithRSAEncryption)
    Padding: 0
    encrypted: 8ab3139ce32cb0cfb12732bff14cb9b92bd643929abbb7d41191c24b777aea38d144589e…
  Extensions Length: 0
  Certificate Length: 1344
▸ Certificate: 3082053c30820424a00302010202100167 8f1fef882255d8b0a70e6b7bb220300d06092a… (id-at-commonName=DigiCert EV RSA CA G2
  Extensions Length: 0
  Certificate Length: 914
▸ Certificate: 3082038e30820276a0030201020210033af1e6a711a9a0bb2864b11d09fae5300d06092a… (id-at-commonName=DigiCert Global Root
  Extensions Length: 0
```

Public key used by Bank

13. **Comment on the key exchange algorithm agreed upon, what are the parameters that got exchanged between client and server to derive the session keys.**

    In my trace file there is no trace of Server Key exchange which carries the information which I have asked in the question. But the classmate has the same Bank so I asked him if he got any trace of the server key exchange. So, fortunately he got one and the same I have answered over here.
    A variant of Diffie Hellman is used for elliptic curve cryptography for key exchange.

14. **Which certificate type (DV/OV/EV) the bank is using?**

    There is no direct way to check what is the type of certificate, but the below given extended information about end entity (subject field, certificate policy extension and organization details) ensures that the certificate type is EV (Extended validation)

```
▾ subject: rdnSequence (0)
  ▾ rdnSequence: 8 items (id-at-commonName=retail.onlinesbi.sbi,id-at-organizationName=STATE BANK OF INDIA,
    ▸ RDNSequence item: 1 item (jurisdictionOfIncorporationCountryName=IN)
    ▸ RDNSequence item: 1 item (id-at-businessCategory=Government Entity)
    ▸ RDNSequence item: 1 item (id-at-serialNumber=Government Entity)
    ▸ RDNSequence item: 1 item (id-at-countryName=IN)
    ▸ RDNSequence item: 1 item (id-at-stateOrProvinceName=Maharashtra)
    ▸ RDNSequence item: 1 item (id-at-localityName=Mumbai)
    ▸ RDNSequence item: 1 item (id-at-organizationName=STATE BANK OF INDIA)
    ▸ RDNSequence item: 1 item (id-at-commonName=retail.onlinesbi.sbi)
▸ subjectPublicKeyInfo
▾ extensions: 10 items
  ▸ Extension (id-ce-authorityKeyIdentifier)
  ▸ Extension (id-ce-subjectKeyIdentifier)
  ▾ Extension (id-ce-subjectAltName)
      Extension Id: 2.5.29.17 (id-ce-subjectAltName)
    ▾ GeneralNames: 2 items
      ▸ GeneralName: dNSName (2)
      ▸ GeneralName: dNSName (2)
  ▸ Extension (id-ce-keyUsage)
  ▸ Extension (id-ce-extKeyUsage)
  ▸ Extension (id-ce-cRLDistributionPoints)
  ▾ Extension (id-ce-certificatePolicies)
      Extension Id: 2.5.29.32 (id-ce-certificatePolicies)
    ▾ CertificatePoliciesSyntax: 2 items
      ▾ PolicyInformation
          policyIdentifier: 2.16.840.1.114412.2.1 (US company arc.114412.2.1)
      ▾ PolicyInformation
          policyIdentifier: 2.23.140.1.1 (joint-iso-itu-t.23.140.1.1)
        ▸ policyQualifiers: 1 item
  ▸ Extension (id-pe-authorityInfoAccess)
```

Info. about extended certificate policy extension

15. Which certificate type (single or multi-domain or wild-card) the bank is using?

SBI bank uses multi-domain certificate type. It can be known in the Subject Alternative Name field of the certificate.

2 Domain names: retail.onlinesbi.sbi, www.retail.onlinesbi.sbi

```
2414 6.0338615… 192.168.49.128  103.68.221.191  TLSv1.3   573 ✓       retail.onlinesbi.sbi        Client Hello
2429 6.0734935… 103.68.221.191  192.168.49.128  TLSv1.3  4152 ✓                                   Server Hello, Change Cipher Spec, Encry
2431 6.0737799… 103.68.221.191  192.168.49.128  TLSv1.3   618 ✓                                   Certificate, Certificate Verify, Finish
2434 6.0761830… 192.168.49.128  103.68.221.191  TLSv1.3   136 ✓                                   Change Cipher Spec, Finished
2443 6.0771167… 192.168.49.128  103.68.221.191  TLSv1.3   573 ✓       retail.onlinesbi.sbi        Client Hello
2452 6.1150040… 103.68.221.191  192.168.49.128  TLSv1.3   630 ✓                                   New Session Ticket, New Session Ticket
2453 6.1327533… 103.68.221.191  192.168.49.128  TLSv1.3  4714 ✓                                   Server Hello, Change Cipher Spec, Encry
2455 6.1331926… 192.168.49.128  103.68.221.191  TLSv1.3   136 ✓                                   Change Cipher Spec, Finished
```

```
  ▾ Certificate: 30820703308205eba003020102021006 3a0a52e70cb12b6ae19108f3ffa794300d06092a… (id-at-commonName=retail.onlinesbi.sbi,id-at
    ▾ signedCertificate
        version: v3 (2)
        serialNumber: 0x063a0a52e70cb12b6ae19108f3ffa794
      ▸ signature (sha256WithRSAEncryption)
      ▸ issuer: rdnSequence (0)
      ▸ validity
      ▸ subject: rdnSequence (0)
      ▸ subjectPublicKeyInfo
      ▾ extensions: 10 items
        ▸ Extension (id-ce-authorityKeyIdentifier)
        ▸ Extension (id-ce-subjectKeyIdentifier)
        ▾ Extension (id-ce-subjectAltName)
            Extension Id: 2.5.29.17 (id-ce-subjectAltName)
          ▾ GeneralNames: 2 items
            ▾ GeneralName: dNSName (2)
                dNSName: retail.onlinesbi.sbi
            ▾ GeneralName: dNSName (2)
                dNSName: www.retail.onlinesbi.sbi
        ▸ Extension (id-ce-keyUsage)
        ▸ Extension (id-ce-extKeyUsage)
```

SAN field

16. How can the client check whether the certificate is revoked or not: OCSP/CRL? Do the client and server support OCSP stapling?

The Client is allowing for the OCSP stapling of the certificate provided by the server. But at the server end there is nothing related to the OCSP stapling. But in the server's response certificate there are the links for the OCSP and CRL list.

```
… 5.569373… 142.250.193.99 192.168.49.128 QUIC     1294 ✓                              Initial, SCID
… 6.033861… 192.168.49.128 103.68.221.191 TLSv1.3  573 ✓       retail.onlinesbi.sbi      Client Hello
… 6.073493… 103.68.221.191 192.168.49.128 TLSv1.3 4152 ✓                              Server Hello,
… 6.073779… 103.68.221.191 192.168.49.128 TLSv1.3  618 ✓                              Certificate,
… 6.076183… 192.168.49.128 103.68.221.191 TLSv1.3  136 ✓                              Change Cipher
… 6.077116… 192.168.49.128 103.68.221.191 TLSv1.3  573 ✓       retail.onlinesbi.sbi      Client Hello
… 6.115004… 103.68.221.191 192.168.49.128 TLSv1.3  630 ✓                              New Session T
… 6.132753… 103.68.221.191 192.168.49.128 TLSv1.3 4714 ✓                              Server Hello,
… 6.133192… 192.168.49.128 103.68.221.191 TLSv1.3  136 ✓                              Change Cipher
```

```
▸ Extension: compress_certificate (len=3)
▸ Extension: key_share (len=43)
▸ Extension: supported_versions (len=7)
▸ Extension: signed_certificate_timestamp (len=0)
▸ Extension: session_ticket (len=0)
▸ Extension: ec_point_formats (len=2)
▸ Extension: server_name (len=25)
▸ Extension: psk_key_exchange_modes (len=2)
▸ Extension: application_settings (len=5)
▸ Extension: renegotiation_info (len=1)
▸ Extension: application_layer_protocol_negotiation (len=14)
▾ 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
▸ Extension: extended_master_secret (len=0)
```

Client allows for OCSP stapling

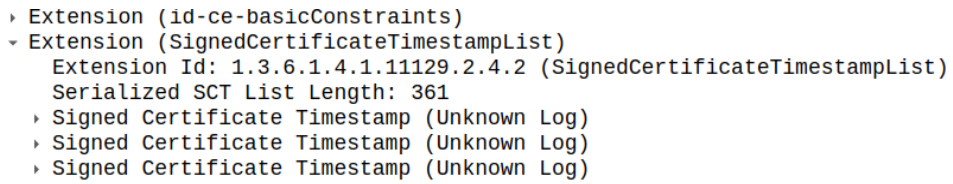
```
… 6.033861… 192.168.49.128 103.68.221.191 TLSv1.3  573 ✓       retail.onlinesbi.sbi      Client Hello
… 6.073493… 103.68.221.191 192.168.49.128 TLSv1.3 4152 ✓                              Server Hello, Change Cipher
… 6.073779… 103.68.221.191 192.168.49.128 TLSv1.3  618 ✓                              Certificate, Certificate Ve
… 6.076183… 192.168.49.128 103.68.221.191 TLSv1.3  136 ✓                              Change Cipher Spec, Finishe
… 6.077116… 192.168.49.128 103.68.221.191 TLSv1.3  573 ✓       retail.onlinesbi.sbi      Client Hello
```

```
    ▸ signature (sha256WithRSAEncryption)
    ▸ issuer: rdnSequence (0)
    ▸ validity
    ▸ subject: rdnSequence (0)
    ▸ subjectPublicKeyInfo
    ▾ extensions: 10 items
      ▸ Extension (id-ce-authorityKeyIdentifier)
      ▸ Extension (id-ce-subjectKeyIdentifier)
      ▸ Extension (id-ce-subjectAltName)
      ▸ Extension (id-ce-keyUsage)
      ▸ Extension (id-ce-extKeyUsage)
      ▸ Extension (id-ce-cRLDistributionPoints)
      ▸ Extension (id-ce-certificatePolicies)
      ▾ Extension (id-pe-authorityInfoAccess)
          Extension Id: 1.3.6.1.5.5.7.1.1 (id-pe-authorityInfoAccess)
        ▾ AuthorityInfoAccessSyntax: 2 items
          ▾ AccessDescription
              accessMethod: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
            ▾ accessLocation: 6
                uniformResourceIdentifier: http://ocsp.digicert.com
          ▾ AccessDescription
              accessMethod: 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers)
            ▾ accessLocation: 6
                uniformResourceIdentifier: http://cacerts.digicert.com/DigiCertEVRSACAG2.crt
```

Can't find track for the OCSP stapling but have links for OCSP and CRL list in server certificate response

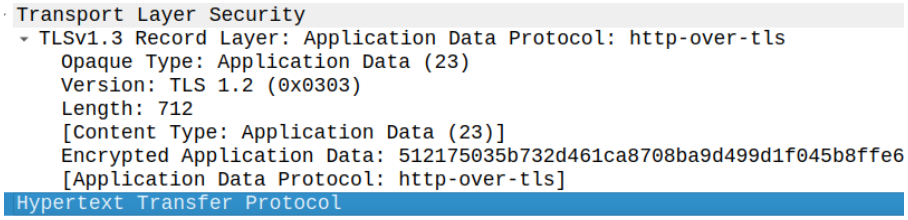
17. **How many log servers logged the certificate of the bank? What role does the log server play in the Web PKI ecosystem? Refer: SCT extension.**

    By checking the SCT extension in the certificate response of the server. We can check the Signed certificate Timestamp list which will show how many servers the band website is logged in. The certificate timestamp logs allows the security experts to monitor and analyze the certificates. Also, It contributes to transparency by making certificate issuance publicly accessible and recorded.



18. **How is the application data being encrypted? Do the records containing application data include a separate MAC? Does Wireshark distinguish between the encrypted application data and the MAC?**

    The application data is being encrypted using the negotiated cipher suite between client and server during handshake (ClientHello & ServerHello). As we know, that server has selected the cipher suite TLS_AES_256_GCM_SHA384 (0x1302). Yes (if SSLKEYLOGFILE is provided), wireshark distinguishes between encrypted application data and MAC. MAC is generated separately for each TLS record containing the application data and derived key (Process done in the record layer, then passed on to the Transport layer).



19. **Look at various keys logged in the file pointed to by the SSLKEYLOGFILE environment variable in your host OS and describe their usage. Also comment on how they are derived from nonces and other parameters using HKDF. Which entity in your system does this job on-the-fly?**

CLIENT_HANDSHAKE_TRAFFIC_SECRET, SERVER_HANDSHAKE_TRAFFIC_SECRET
Used to secure the client / server handshake traffic.
Derived using handshake secret

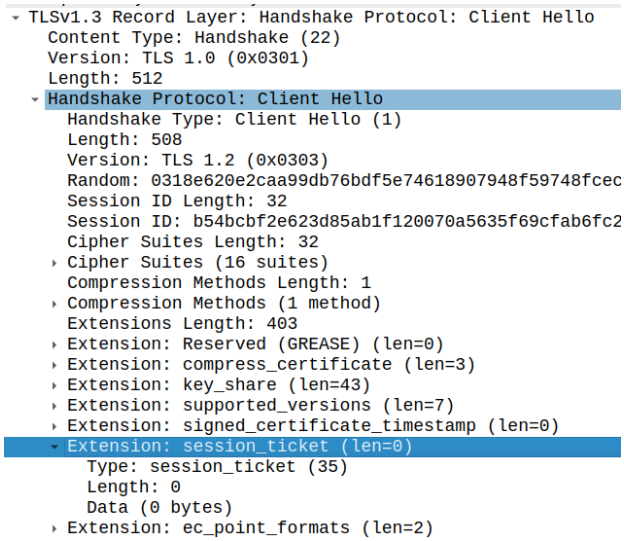
CLIENT_TRAFFIC_SECRET_0, SERVER_TRAFFIC_SECRET_0
Used to secure the client / server application data traffic.
Derived using Master Secret

EXPORTER_SECRET
Used for generating key material
Derived using Master Secret

The above keys are derived on-the-fly by client and server in the part of the handshake **key generation schedule** using HKDF-expand function (which takes input as nonces like derived early secret, 00000…., (EC)DHE, derived handshake secret, etc)

20. **Do you see any support for session resumption in the trace? What do you find inside the session ticket, if it is used? Is it based on Session ID/Session ticket or PSK based Session ticket? Do the session IDs play any role in TLS 1.3?**

Yes, there is support for session resumption which can be seen in the session_ticket extension of ClientHello. The session resumption is based on session ID / session ticket.
ClientHello session_ticket extension:

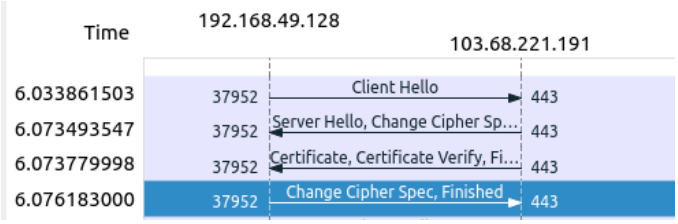


After some time the server has sent the New_session ticket record which is shown below. It contains session ticket lifetime, age and nonce length. The role of session ticket TLS1.3 is for the resumption purpose which increases the performance of secure connection establishment because it reduces 1 RTT time from the handshake.

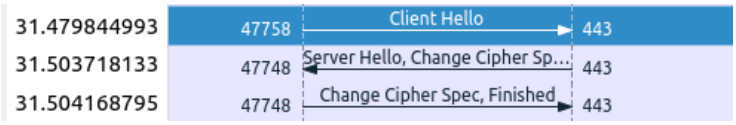
```
 2452 6.115004050 103.68.221.191   192.168.49.128    TLSv1.3    630 ✓
 2453 6.132753361 103.68.221.191   192.168.49.128    TLSv1.3    4714 ✓

Frame 2452: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 103.68.221.191, Dst: 192.168.49.128
Transmission Control Protocol, Src Port: 443, Dst Port: 37952, Seq: 4659,
Transport Layer Security
▾ TLSv1.3 Record Layer: Handshake Protocol: New Session Ticket
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 282
    [Content Type: Handshake (22)]
  ▾ Handshake Protocol: New Session Ticket
      Handshake Type: New Session Ticket (4)
      Length: 261
    ▾ TLS Session Ticket
        Session Ticket Lifetime Hint: 300 seconds (5 minutes)
        Session Ticket Age Add: 1438400864
        Session Ticket Nonce Length: 8
        Session Ticket Nonce: 0000000000000000
        Session Ticket Length: 240
        Session Ticket: 00f8fff82c01000066fedf65000000006091c6edf1366789cd
        Extensions Length: 0
▾ TLSv1.3 Record Layer: Handshake Protocol: New Session Ticket
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 282
    [Content Type: Handshake (22)]
  ▾ Handshake Protocol: New Session Ticket
      Handshake Type: New Session Ticket (4)
      Length: 261
    ▾ TLS Session Ticket
        Session Ticket Lifetime Hint: 300 seconds (5 minutes)
        Session Ticket Age Add: 2238964854
        Session Ticket Nonce Length: 8
        Session Ticket Nonce: 0000000000000001
        Session Ticket Length: 240
        Session Ticket: 00f8fff82c01000066fedf650000000027c5752b04e52b2482
        Extensions Length: 0
```

21. **How long does it take for TLS to establish a secure (TLS) pipe? How much of it could be reduced when session resumption is used? You may have to revisit the bank site after a while to force session resumption. Answer this question by looking at the flow graph feature in wireshark.**

Taking the time difference of the ClientHello record and Finished record
= 6.076183000 − 6.033861503 = 0.042321497 ms



For the case of session resumption the below are the details for the time taken to establish the TLS pipe = 31.504168795 - 31.479844993 = 0.024323802 ms
Therefore implementing session resumption the time for establishing TLS pipe approximately reduces by 0.020 ms.



22. What is the duration of the HTTPS session, how many IP packets are exchanged in the browsing session (starting from the first TCP SYN packet till TCP FIN packet)?

Duration of HTTPS session = last Server FIN TLS record - first ClientHello TLS record
= 31.534 - 0.026
= 31.508 ms

IP packets exchanged = last TCP FIN packet - first TCP SYN packet
= 3399 - 9
= 3390 IP packets got exchanged

23. How many TLS connections are established with the bank server and its affiliated servers?

The below given server name can be found in the trace with which the client or the server is establishing the TLS connection. Then by calculating the no. of ClientHello we can get the no. of TLS connections, there are 26 of them in my trace for SBI bank website.

1. optimizationguide-pa.googleapis.com
2. encrypted-tbn0.gstatic.com
3. fonts.gstatic.com
4. www.gstatic.com
5. content-autofill.googleapis.com
6. apis.google.com
7. retail.onlinesbi.sbi
8. cdn.page-source.com
9. update.googleapis.com
10. safebrowsing.googleapis.com

Source	Destination	Protocol	Length	Text iter	Server Name
192.168.49.128	142.250.196.10	TLSv1.3	579	✓	optimizationguide-pa.googleapis.com
142.250.196.10	192.168.49.128	TLSv1.3	1468	✓	
142.250.196.10	192.168.49.128	TLSv1.3	3508	✓	
192.168.49.128	142.250.196.10	TLSv1.3	130	✓	
142.250.196.10	192.168.49.128	HTTP2	1054	✓	
192.168.49.128	142.250.196.14	TLSv1.3	666	✓	encrypted-tbn0.gstatic.com
192.168.49.128	142.250.196.14	TLSv1.3	602	✓	encrypted-tbn0.gstatic.com
142.250.196.14	192.168.49.128	TLSv1.3	1468	✓	
142.250.196.14	192.168.49.128	TLSv1.3	3140	✓	
192.168.49.128	142.250.196.14	TLSv1.3	130	✓	
142.250.196.14	192.168.49.128	TLSv1.3	1468	✓	
142.250.196.14	192.168.49.128	HTTP2	1036	✓	
192.168.49.128	142.250.196.14	QUIC	1294	✓	encrypted-tbn0.gstatic.com
142.250.196.14	192.168.49.128	QUIC	1294	✓	
142.250.196.14	192.168.49.128	QUIC	1294	✓	

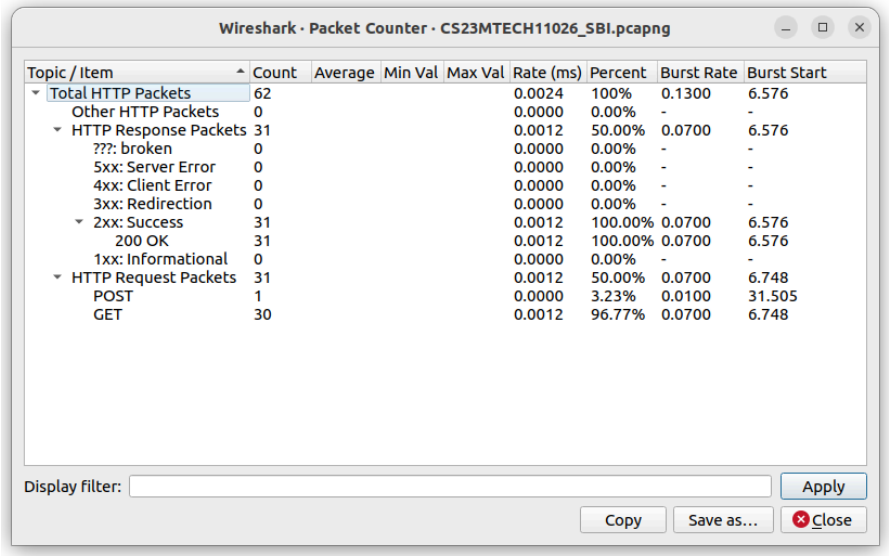
Source	Destination	Protocol	Length	Text iter	Server Name
142.250.196.14	192.168.49.128	QUIC	1008	✓	
192.168.49.128	142.250.196.35	TLSv1.3	657	✓	fonts.gstatic.com
142.250.196.35	192.168.49.128	TLSv1.3	1468	✓	
142.250.196.35	192.168.49.128	TLSv1.3	3132	✓	
192.168.49.128	142.250.196.35	TLSv1.3	130	✓	
142.250.196.35	192.168.49.128	HTTP2	1018	✓	
192.168.49.128	142.250.196.35	QUIC	1294	✓	
192.168.49.128	142.250.193.99	TLSv1.3	623	✓	www.gstatic.com
192.168.49.128	142.250.193.99	TLSv1.3	573	✓	www.gstatic.com
142.250.196.35	192.168.49.128	QUIC	1294	✓	
192.168.49.128	142.250.193.99	TLSv1.3	655	✓	www.gstatic.com
192.168.49.128	142.250.193.99	TLSv1.3	655	✓	www.gstatic.com
192.168.49.128	142.250.193.99	TLSv1.3	623	✓	www.gstatic.com
192.168.49.128	142.250.193.99	TLSv1.3	573	✓	www.gstatic.com
142.250.193.99	192.168.49.128	TLSv1.3	4541	✓	

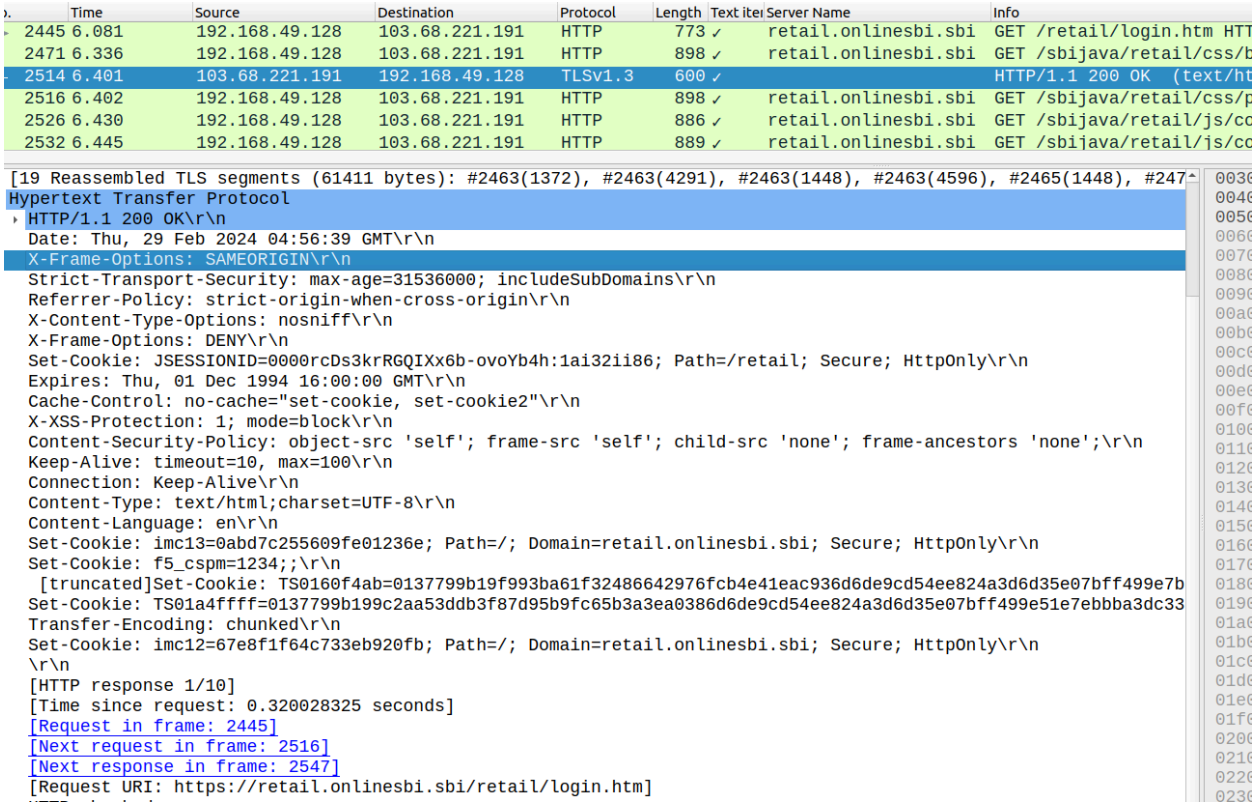
Source	Destination	Protocol	Length	Text iter	Server Name
142.250.193.99	192.168.49.128	HTTP2	1014	✓	
192.168.49.128	142.250.196.74	TLSv1.3	671	✓	content-autofill.googleapis.com
142.250.196.74	192.168.49.128	TLSv1.3	1468	✓	
142.250.196.74	192.168.49.128	TLSv1.3	3506	✓	
192.168.49.128	142.250.196.74	TLSv1.3	130	✓	
142.250.196.74	192.168.49.128	HTTP2	1046	✓	
192.168.49.128	142.250.182.142	TLSv1.3	591	✓	apis.google.com
142.250.182.142	192.168.49.128	TLSv1.3	1468	✓	
142.250.182.142	192.168.49.128	TLSv1.3	3119	✓	
192.168.49.128	142.250.182.142	TLSv1.3	130	✓	
142.250.182.142	192.168.49.128	HTTP2	1014	✓	
192.168.49.128	142.250.193.99	QUIC	1294	✓	
142.250.193.99	192.168.49.128	QUIC	1294	✓	
192.168.49.128	103.68.221.191	TLSv1.3	573	✓	retail.onlinesbi.sbi
103.68.221.191	192.168.49.128	TLSv1.3	4152	✓	

Source	Destination	Protocol	Length	Text iter	Server Name
192.168.49.128	216.58.196.170	TLSv1.3	671	✓	content-autofill.googleapis.com
216.58.196.170	192.168.49.128	TLSv1.3	1468	✓	
216.58.196.170	192.168.49.128	TLSv1.3	3505	✓	
192.168.49.128	216.58.196.170	TLSv1.3	130	✓	
216.58.196.170	192.168.49.128	HTTP2	1046	✓	
192.168.49.128	54.38.211.230	TLSv1.2	659	✓	cdn.page-source.com
54.38.211.230	192.168.49.128	TLSv1.2	1220	✓	
192.168.49.128	54.38.211.230	TLSv1.2	214	✓	
54.38.211.230	192.168.49.128	HTTP2	176	✓	
192.168.49.128	54.38.211.230	TLSv1.2	595	✓	cdn.page-source.com
54.38.211.230	192.168.49.128	TLSv1.2	210	✓	
192.168.49.128	54.38.211.230	TLSv1.2	107	✓	
192.168.49.128	103.68.221.191	TLSv1.3	931	✓	retail.onlinesbi.sbi
192.168.49.128	103.68.221.191	TLSv1.3	899	✓	retail.onlinesbi.sbi
103.68.221.191	192.168.49.128	TLSv1.3	332	✓	

24. How many HTTP request/response packets are exchanged in the browsing session? Identify the packet(s) that carried the response that included the Netbanking LOG-IN page of the bank. Do these response messages carry any security related directives like XSS, sameorigin, HSTS?

HTTP Response packets - 31
HTTP Request packets - 31
Total 62 packets were exchanged in this browsing session. I identified the login html page (get request from client) which is responded back by HTTP 200 OK from the server. But rather than just a login html page many more requests are there for loading images, other required requests for the net banking page of SBI. Also the SS for the same (Net banking login page, security related directives) is attached at the end of this question.





	Time	Source	Destination	Protocol	Length	Text itei	Server Name	Info
2445	6.081	192.168.49.128	103.68.221.191	HTTP	773	✓	retail.onlinesbi.sbi	GET /retail/login.htm HTT
2471	6.336	192.168.49.128	103.68.221.191	HTTP	898	✓	retail.onlinesbi.sbi	GET /sbijava/retail/css/b
2514	6.401	103.68.221.191	192.168.49.128	TLSv1.3	600	✓		HTTP/1.1 200 OK (text/ht
2516	6.402	192.168.49.128	103.68.221.191	HTTP	898	✓	retail.onlinesbi.sbi	GET /sbijava/retail/css/p
2526	6.430	192.168.49.128	103.68.221.191	HTTP	886	✓	retail.onlinesbi.sbi	GET /sbijava/retail/js/co
2532	6.445	192.168.49.128	103.68.221.191	HTTP	889	✓	retail.onlinesbi.sbi	GET /sbijava/retail/js/co

```
[19 Reassembled TLS segments (61411 bytes): #2463(1372), #2463(4291), #2463(1448), #2463(4596), #2465(1448), #247
Hypertext Transfer Protocol
▸ HTTP/1.1 200 OK\r\n
  Date: Thu, 29 Feb 2024 04:56:39 GMT\r\n
  X-Frame-Options: SAMEORIGIN\r\n
  Strict-Transport-Security: max-age=31536000; includeSubDomains\r\n
  Referrer-Policy: strict-origin-when-cross-origin\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Frame-Options: DENY\r\n
  Set-Cookie: JSESSIONID=0000rcDs3krRGQIXx6b-ovoYb4h:1ai32ii86; Path=/retail; Secure; HttpOnly\r\n
  Expires: Thu, 01 Dec 1994 16:00:00 GMT\r\n
  Cache-Control: no-cache="set-cookie, set-cookie2"\r\n
  X-XSS-Protection: 1; mode=block\r\n
  Content-Security-Policy: object-src 'self'; frame-src 'self'; child-src 'none'; frame-ancestors 'none';\r\n
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html;charset=UTF-8\r\n
  Content-Language: en\r\n
  Set-Cookie: imc13=0abd7c255609fe01236e; Path=/; Domain=retail.onlinesbi.sbi; Secure; HttpOnly\r\n
  Set-Cookie: f5_cspm=1234;;\r\n
   [truncated]Set-Cookie: TS0160f4ab=0137799b19f993ba61f32486642976fcb4e41eac936d6de9cd54ee824a3d6d35e07bff499e7b
  Set-Cookie: TS01a4ffff=0137799b199c2aa53ddb3f87d95b9fc65b3a3ea0386d6de9cd54ee824a3d6d35e07bff499e51e7ebbba3dc33
  Transfer-Encoding: chunked\r\n
  Set-Cookie: imc12=67e8f1f64c733eb920fb; Path=/; Domain=retail.onlinesbi.sbi; Secure; HttpOnly\r\n
  \r\n
  [HTTP response 1/10]
  [Time since request: 0.320028325 seconds]
  [Request in frame: 2445]
  [Next request in frame: 2516]
  [Next response in frame: 2547]
  [Request URI: https://retail.onlinesbi.sbi/retail/login.htm]
```

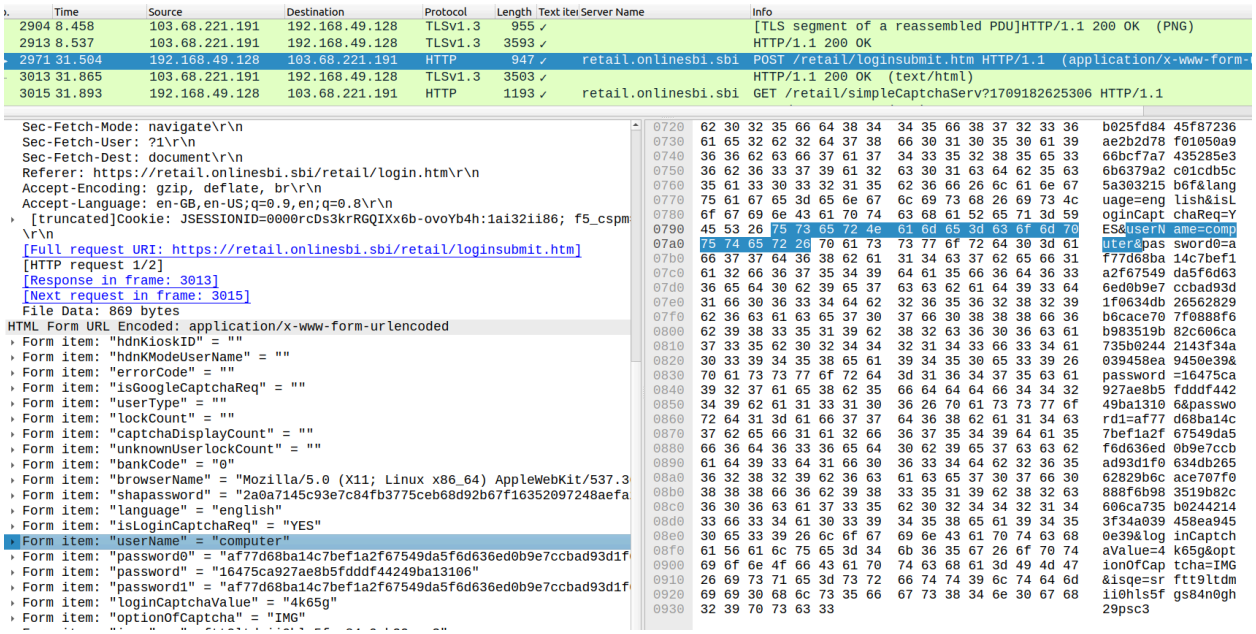
Check for the sameorigin, XSS, etc security related directives

25. Identify the HTTP packet(s) that carried LOG-IN credentials supplied by you. Look at the raw bytes displayed in the wireshark GUI and identify strings that carry your LOG-IN credentials. Are you able to find boh user id and password in the raw packet capture?

a. It's important that you only keyed in some arbitrary user id and password as part of this assignment for more safety!

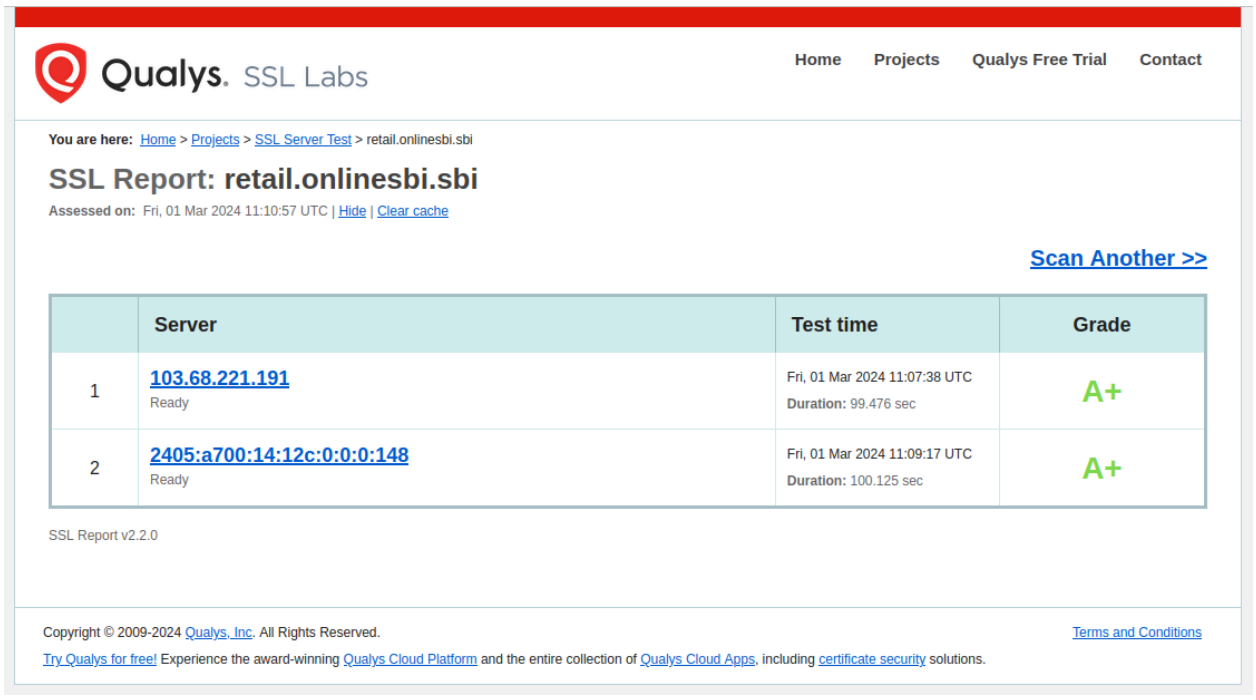
By looking at the raw bytes displayed in the wireshark GUI the username and password can be found. Here the username = computer (which i had entered) and password is encoded. But i also found there are 3 passwords mentioned in that wireshark packet (POST packet) which contains password0, password, and password1 (SS attached below)

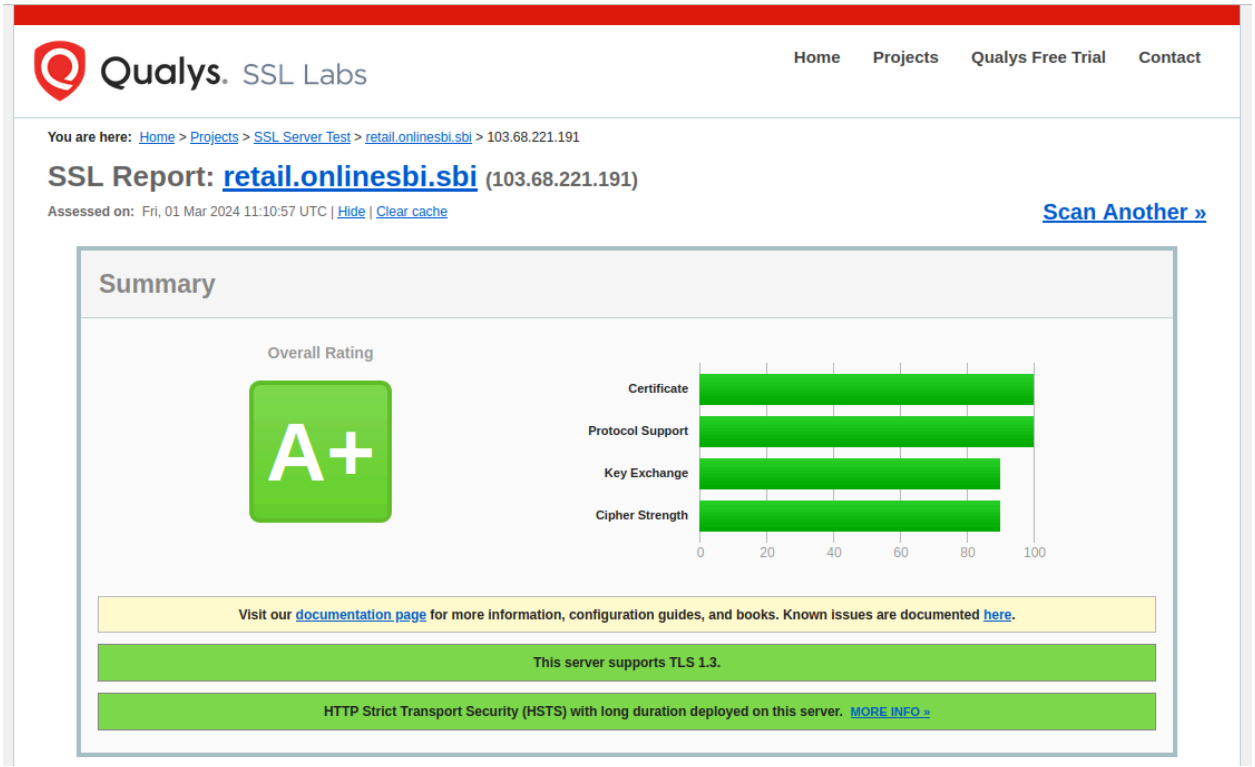
```
6f 67 69 6e 43 61 70 74  63 68 61 52 65 71 3d 59   ogĭnCapt̆ chaReq=Y
45 53 26 75 73 65 72 4e  61 6d 65 3d 63 6f 6d 70   ES&userN ame=comp
75 74 65 72 26 70 61 73  73 77 6f 72 64 30 3d 61   uter&pas sword0=a
66 37 37 64 36 38 62 61  31 34 63 37 62 65 66 31   f77d68ba 14c7bef1
61 32 66 36 37 35 34 39  64 61 35 66 36 64 36 33   a2f67549 da5f6d63
36 65 64 30 62 39 65 37  63 63 62 61 64 39 33 64   6ed0b9e7 ccbad93d
31 66 30 36 33 34 64 62  32 36 35 36 32 38 32 39   1f0634db 26562829
62 36 63 61 63 65 37 30  37 66 30 38 38 38 66 36   b6cace70 7f0888f6
62 39 38 33 35 31 39 62  38 32 63 36 30 36 63 61   b983519b 82c606ca
37 33 35 62 30 32 34 34  32 31 34 33 66 33 34 61   735b0244 2143f34a
30 33 39 34 35 38 65 61  39 34 35 30 65 33 39 26   039458ea 9450e39&
70 61 73 73 77 6f 72 64  3d 31 36 34 37 35 63 61   password =16475ca
```



Login Credentials information - username (plain text) & password (encoded)

26. Generate an SSL report of the bank using [SSL Server Test (Powered by Qualys SSL Labs)] and summarize what security features are implemented by the bank's web server for improved online banking by its customers. Does the report flag any issues with the security of the bank?





The below things were mentioned in the summary report by Qualys which lead to measures taken to improve online banking by its customers.

1. Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
2. No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

There were no red flags issues with the security of the bank.

27. Comment on and explain anything else that you found interesting in the trace!!

As of now all the major things are covered in the above question, but there is much more information that can be fetched from this TLS decryption of the bank website.

References:

1. Article: K50557518 - Decrypt SSL traffic with the SSLKEYLOGFILE environment variable on Firefox or Google Chrome using Wireshark (f5.com)
2. Wireshark Tutorial: Decrypting HTTPS Traffic (Includes SSL and TLS) (paloaltonetworks.com)
3. Decrypting TLS Streams With Wireshark: Part 1 | Didier Stevens
4. http://www.motobit.com/util/base64-decoder-encoder.asp
5. Dissecting TLS Using Wireshark (catchpoint.com)
6. https://tls13.ulfheim.net/
7. https://www.davidwong.fr/tls13/
8. SSL Server Test (Powered by Qualys SSL Labs)

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 plagiarised 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 honour violations by other students if I become aware of it.

Name: Patel Bhargav Piyushkumar
Date: 01-03-2024
Signature: PBP