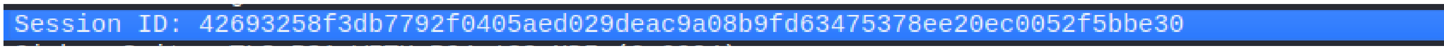
SSL/TLS Assignment (Ryan Foster – 1473396)

- This is an individual lab assignment.
- The due date is Tonight.
- For this assignment, you will need to use Wireshark and the attached “**https-justlaunchpage**”.
- Please make the solutions readable and highlight the answers.
- Follow the usual naming convention.

Note: Provide screenshots for each answer.

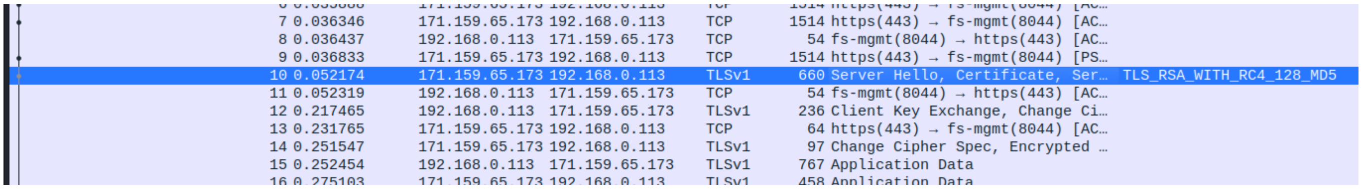
1. What is the session ID of the SSL/TLS handshaking?



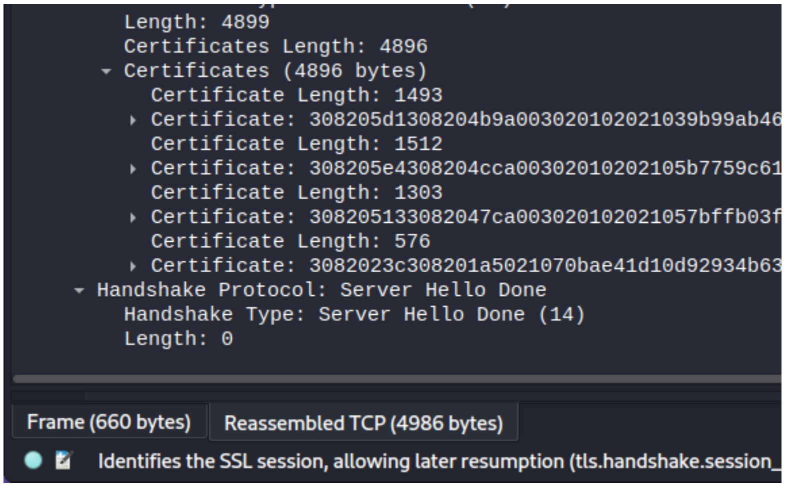
```
Session ID: 42693258f3db7792f0405aed029deac9a08b9fd63475378ee20ec0052f5bbe30
```

2. What is the length (bytes) of the certificate that the server shared with the client?

Total of 4896. There were several certificates though (1493, 1512, 1303, 576)



```
 7 0.036346   171.159.65.173 192.168.0.113   TCP    1514 https(443) → fs-mgmt(8044) [AC…
 8 0.036437   192.168.0.113  171.159.65.173  TCP      54 fs-mgmt(8044) → https(443) [AC…
 9 0.036833   171.159.65.173 192.168.0.113   TCP    1514 https(443) → fs-mgmt(8044) [PS…
10 0.052174   171.159.65.173 192.168.0.113   TLSv1   660 Server Hello, Certificate, Ser…  TLS_RSA_WITH_RC4_128_MD5
11 0.052319   192.168.0.113  171.159.65.173  TCP      54 fs-mgmt(8044) → https(443) [AC…
12 0.217465   192.168.0.113  171.159.65.173  TLSv1   236 Client Key Exchange, Change Ci…
13 0.231765   171.159.65.173 192.168.0.113   TCP      64 https(443) → fs-mgmt(8044) [AC…
14 0.251547   171.159.65.173 192.168.0.113   TLSv1    97 Change Cipher Spec, Encrypted …
15 0.252454   192.168.0.113  171.159.65.173  TLSv1   767 Application Data
16 0.275103   171.159.65.173 192.168.0.113   TLSv1   458 Application Data
```

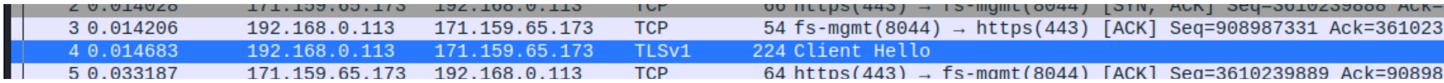


```
        Length: 4899
        Certificates Length: 4896
      ▾ Certificates (4896 bytes)
          Certificate Length: 1493
        ▸ Certificate: 308205d1308204b9a003020102021039b99ab46
          Certificate Length: 1512
        ▸ Certificate: 308205e4308204cca00302010202105b7759c61
          Certificate Length: 1303
        ▸ Certificate: 308205133082047ca003020102021057bffb03f
          Certificate Length: 576
        ▸ Certificate: 3082023c308201a5021070bae41d10d92934b63
    ▾ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

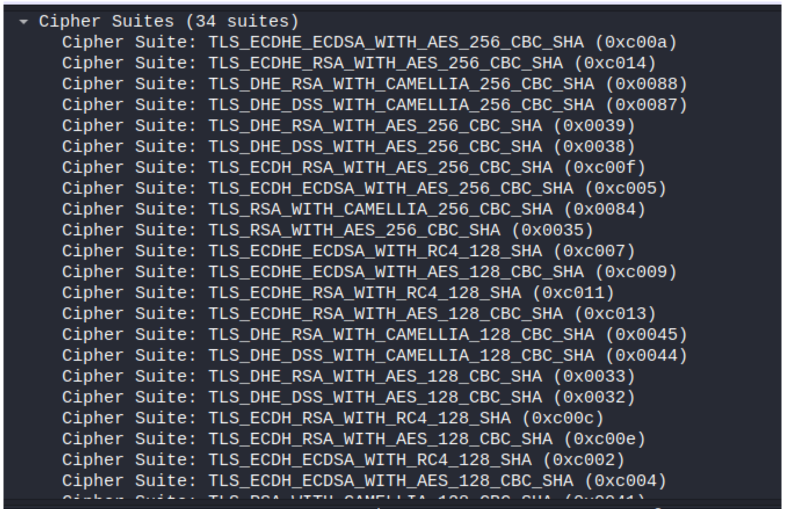
Frame (660 bytes)
Reassembled TCP (4986 bytes)
Identifies the SSL session, allowing later resumption (tls.handshake.session_

3A. How many cipher suites are supported by the client’s browser?

34



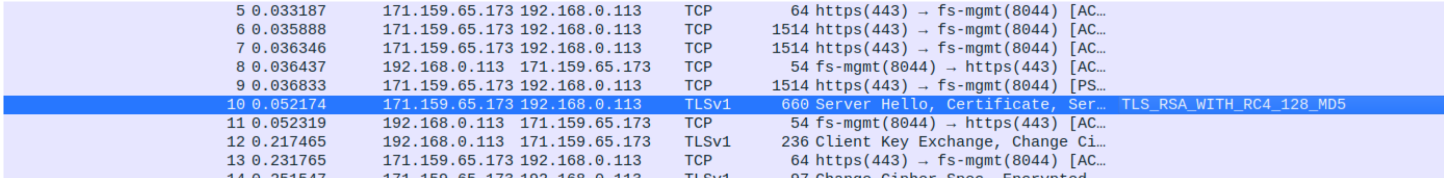
```
2 0.014028   171.159.65.173   192.168.0.113    TCP      66 https(443) → fs-mgmt(8044) [SYN, ACK] Seq=3610239888 Ack=
3 0.014206   192.168.0.113    171.159.65.173   TCP      54 fs-mgmt(8044) → https(443) [ACK] Seq=908987331 Ack=361023
4 0.014683   192.168.0.113    171.159.65.173   TLSv1   224 Client Hello
5 0.033187   171.159.65.173   192.168.0.113    TCP      64 https(443) → fs-mgmt(8044) [ACK] Seq=3610239889 Ack=90898
```



```
▾ Cipher Suites (34 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
    Cipher Suite: TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
    Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
    Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
    Cipher Suite: TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
    Cipher Suite: TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
    Cipher Suite: TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
    Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
    Cipher Suite: TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
    Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
    Cipher Suite: TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
```

3B. What is the cipher suite that the server selected?

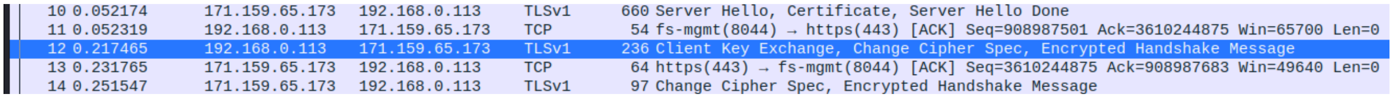
TLS_RSA_WITH_RC4_128_MD5



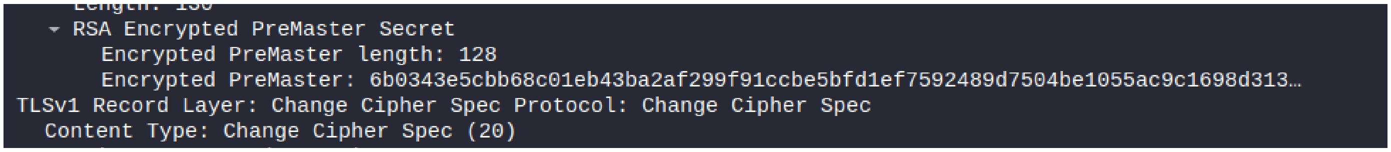
```
 5 0.033187   171.159.65.173 192.168.0.113   TCP      64 https(443) → fs-mgmt(8044) [AC…
 6 0.035888   171.159.65.173 192.168.0.113   TCP    1514 https(443) → fs-mgmt(8044) [AC…
 7 0.036346   171.159.65.173 192.168.0.113   TCP    1514 https(443) → fs-mgmt(8044) [AC…
 8 0.036437   192.168.0.113  171.159.65.173  TCP      54 fs-mgmt(8044) → https(443) [AC…
 9 0.036833   171.159.65.173 192.168.0.113   TCP    1514 https(443) → fs-mgmt(8044) [PS…
10 0.052174   171.159.65.173 192.168.0.113   TLSv1   660 Server Hello, Certificate, Ser…  TLS_RSA_WITH_RC4_128_MD5
11 0.052319   192.168.0.113  171.159.65.173  TCP      54 fs-mgmt(8044) → https(443) [AC…
12 0.217465   192.168.0.113  171.159.65.173  TLSv1   236 Client Key Exchange, Change Ci…
13 0.231765   171.159.65.173 192.168.0.113   TCP      64 https(443) → fs-mgmt(8044) [AC…
14 0.251547   171.159.65.173 192.168.0.113   TLSv1    97 Change Cipher Spec, Encrypted
```

4. What is the length of the RSA Encrypted PreMaster Secret that is used to generate the Master Secret and session keys by the server and client?

128



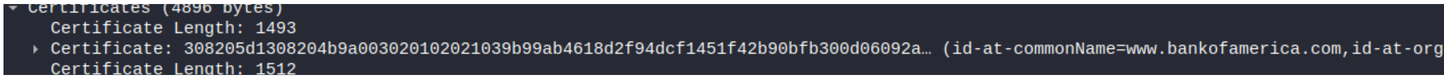
```
10 0.052174   171.159.65.173  192.168.0.113   TLSv1   660 Server Hello, Certificate, Server Hello Done
11 0.052319   192.168.0.113   171.159.65.173  TCP      54 fs-mgmt(8044) → https(443) [ACK] Seq=908987501 Ack=3610244875 Win=65700 Len=0
12 0.217465   192.168.0.113   171.159.65.173  TLSv1   236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
13 0.231765   171.159.65.173  192.168.0.113   TCP      64 https(443) → fs-mgmt(8044) [ACK] Seq=3610244875 Ack=908987683 Win=49640 Len=0
14 0.251547   171.159.65.173  192.168.0.113   TLSv1    97 Change Cipher Spec, Encrypted Handshake Message
```



```
      Length: 130
    ▾ RSA Encrypted PreMaster Secret
        Encrypted PreMaster length: 128
        Encrypted PreMaster: 6b0343e5cbb68c01eb43ba2af299f91ccbe5bfd1ef7592489d7504be1055ac9c1698d313…
TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  Content Type: Change Cipher Spec (20)
```

5. What is the name of the company that the client is talking with?

Bank of America



```
▾ Certificates (4896 bytes)
    Certificate Length: 1493
  ▸ Certificate: 308205d1308204b9a003020102021039b99ab4618d2f94dcf1451f42b90bfb300d06092a… (id-at-commonName=www.bankofamerica.com,id-at-org
    Certificate Length: 1512
```