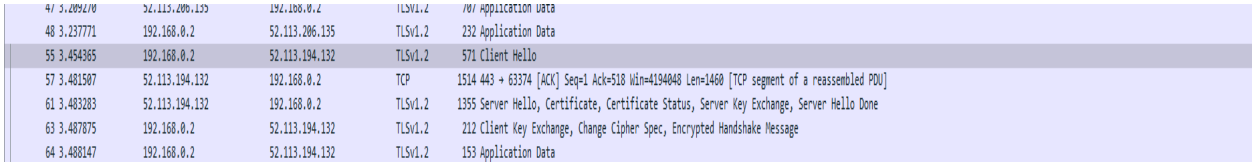
Silas Davis
3/27/2022
423 HW3/Lab 3

I Silas Davis declare that I have completed this assignment in accordance with the UAB Academic Integrity Code and the UAB CS Honor Code. I have read the UAB Academic Integrity Code and understand that any breach of the Code may result in severe penalties.

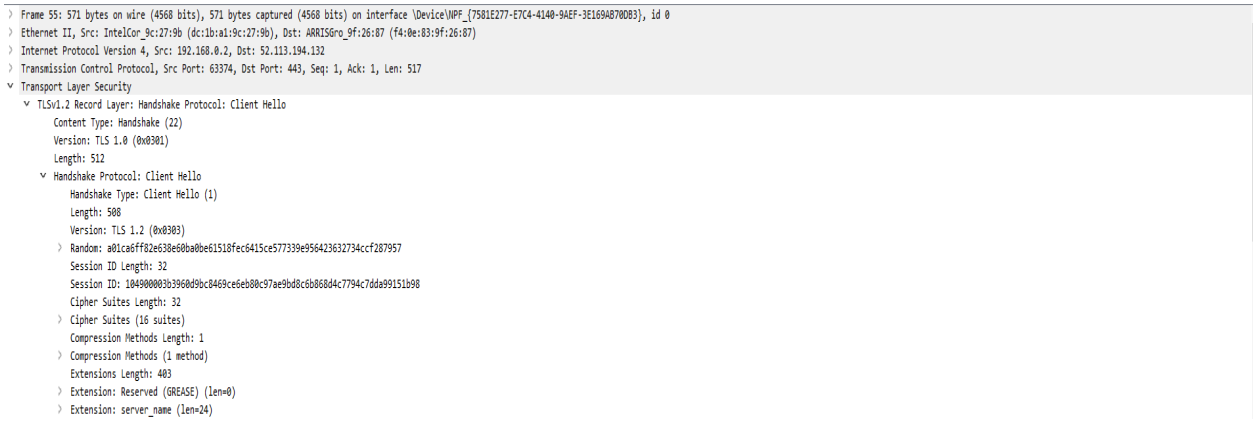
Student signature/initials: SD

Date: 3/27/2022

1.
    a. The CA is the Sectigo RSA Extended Validation Secure Server which was issued by USERTrust RSA Certification Authority. This CA is trusted by the browser.
    b. .
    c. No, this certificate has not expired.
    d. http://crl.sectigo.com/SectigoRSAExtendedValidationSecureServerCA.crl
    e. RSA
    f. RSA (2048 Bits)
    g. 30 82 01 0a 02 82 01 01 00 e7 78 67 a7 3d 8e 3a 19 3f f6 08 e4 f0 97 f9 d7 f0 b3 3b 73 c6 4f 44 91 dd 51 76 3c b5 0a 10 a6 2b 05 2f 7c 95 a1 2f bd 15 c6 fe e6 f5 ea 85 8d ee 46 32 e2 7b 2a 36 c0 95 88 ad c4 be 5d 57 09 62 ee f3 d4 43 31 48 44 0f 48 6b 14 e4 90 de 8f 41 e1 0d f9 c7 a9 b8 0e 33 fc 3b 40 87 4d da dc 8e 8a b6 95 e9 2b 5f 7e db 58 95 88 06 9e 75 54 21 bc 4f 1d ae 8f ba 0e 07 a8 0d b7 ae 34 6e 39 fc 52 e0 e3 10 71 62 91 55 f6 b6 48 8c 2a 8c 83 63 9d 25 3d b7 f6 b1 47 33 dc 57 38 01 ad 29 10 c6 8d 08 4e 84 e4 3e d5 8f ca 65 25 ba 88 c8 40 0f 5f a2 fc 3f 10 bc 97 08 b5 46 88 e7 a5 22 8e 96 ae 7a bc 87 36 71 43 9e fd 38 b0 54 68 b7 ab ac 40 16 8b d3 24 5f 54 55 a9 b7 b7 a2 b6 32 5b 51 cf 3e c7 ae 3a 13 8d e1 27 ff 77 6e fa 42 be 05 00 20 7b 4a 10 81 eb 35 b7 6e 21 37 9d 93 41 02 03 01 00 01



47	3.209270	52.113.206.135	192.168.0.2	TLSv1.2	787 Application Data
48	3.237771	192.168.0.2	52.113.206.135	TLSv1.2	232 Application Data
55	3.454365	192.168.0.2	52.113.194.132	TLSv1.2	571 Client Hello
57	3.481507	52.113.194.132	192.168.0.2	TCP	1514 443 → 63374 [ACK] Seq=1 Ack=518 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
61	3.483283	52.113.194.132	192.168.0.2	TLSv1.2	1355 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
63	3.487875	192.168.0.2	52.113.194.132	TLSv1.2	212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
64	3.488147	192.168.0.2	52.113.194.132	TLSv1.2	153 Application Data



```
> Frame 55: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{75B1E277-E7C4-4140-9AEF-3E169AB70DB3}, id 0
> Ethernet II, Src: IntelCor_9c:27:9b (dc:1b:a1:9c:27:9b), Dst: ARRISGro_9f:26:87 (f4:0e:83:9f:26:87)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 52.113.194.132
> Transmission Control Protocol, Src Port: 63374, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
      > Random: a01ca6ff82e638e60ba0be61518fec6415ce577339e956423632734ccf287957
        Session ID Length: 32
        Session ID: 104900003b3960d9bc8469ce6eb80c97ae9bd8c6b868d4c7794c7dda99151b98
        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: server_name (len=24)
```

2.

A. `Handshake (22)` The number in parenthesis next to Handshake under “Content Type” is the number identifying the SSL Handshake type. (22)

B. `Application Data (23)` The number in parenthesis. (23)

C. `Change Cipher Spec (20)` The number in parenthesis. (20)

D.

E. `Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)` Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

```
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)
```

F. `Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)`

- 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)

G.

```
Random: a01ca6ff82e638e60ba0be61518fec6415ce577339e956423632734ccf287957
```

Random:
A01ca6ff82e638e60ba0be61518fec6415ce577339e956423632734ccf2
87957

H. The only question that has a different response is Gm pertaining to the Random Value.

Random:
c04edd5d4e911c1d4f4d167e884d4e86f20729c00756d18dfef952abffd1
1f7b

```
Random: c04edd5d4e911c1d4f4d167e884d4e86f20729c00756d18dfef952abffd11f7b
```