

Computer Networks Lab

ASSIGNMENT – 13

Rahul Cheryala, 210010012

PART – 2: A first look at the captured trace

2368	21.149406608	10.250.61.113	128.119.240.84	TCP	74	48956 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
2369	21.149523592	10.250.61.113	128.119.240.84	TCP	74	48968 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
2375	21.395652593	128.119.240.84	10.250.61.113	TCP	66	443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2376	21.395734732	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
2377	21.397788484	10.250.61.113	128.119.240.84	TLSv1.2	720	Client Hello (SNI=www.cics.umass.edu)
2381	21.403870057	128.119.240.84	10.250.61.113	TCP	66	443 → 48968 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2382	21.403883911	10.250.61.113	128.119.240.84	TCP	54	48968 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
2383	21.404308156	10.250.61.113	128.119.240.84	TLSv1.2	720	Client Hello (SNI=www.cics.umass.edu)
2387	21.644744382	128.119.240.84	10.250.61.113	TCP	60	443 → 48956 [ACK] Seq=1 Ack=667 Win=30592 Len=0
2389	21.648945323	128.119.240.84	10.250.61.113	TLSv1.2	1514	Server Hello
2390	21.648975388	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
2391	21.649580224	128.119.240.84	10.250.61.113	TCP	2690	443 → 48956 [PSH, ACK] Seq=1461 Ack=667 Win=30592 Len=2636 [TCP segment of a reassembled PDU]

1. Packet Number 2368 contains the initial TCP SYN message
2. TCP connection is set before the first TLS message is sent from the client to server

PART – 3: The TLS Handshake: Client Hello message

2368	21.149406608	10.250.61.113	128.119.240.84	TCP	74	48956 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
2369	21.149523592	10.250.61.113	128.119.240.84	TCP	74	48968 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
2375	21.395652593	128.119.240.84	10.250.61.113	TCP	66	443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2376	21.395734732	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
2377	21.397788484	10.250.61.113	128.119.240.84	TLSv1.2	720	Client Hello (SNI=www.cics.umass.edu)
2381	21.403870057	128.119.240.84	10.250.61.113	TCP	66	443 → 48968 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2382	21.403883911	10.250.61.113	128.119.240.84	TCP	54	48968 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
2383	21.404308156	10.250.61.113	128.119.240.84	TLSv1.2	720	Client Hello (SNI=www.cics.umass.edu)
2387	21.644744382	128.119.240.84	10.250.61.113	TCP	60	443 → 48956 [ACK] Seq=1 Ack=667 Win=30592 Len=0
2389	21.648945323	128.119.240.84	10.250.61.113	TLSv1.2	1514	Server Hello
2390	21.648975388	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
2391	21.649580224	128.119.240.84	10.250.61.113	TCP	2690	443 → 48956 [PSH, ACK] Seq=1461 Ack=667 Win=30592 Len=2636 [TCP segment of a reassembled PDU]
2392	21.649580224	128.119.240.84	10.250.61.113	TCP	54	48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0

1. The packet number of the TLS client's Hello message is 2377.

2. My client is running TLS version 1.2

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 661
  > Handshake Protocol: Client Hello
```

3. 17 Cipher Suites are supported by the client

```
Cipher Suites Length: 17
  Cipher Suites (17 suites)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    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_CHACHA20_POLY1305_SHA256 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    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_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    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
```

4. The first two hexadecimal digits in the random bytes field of the Client Hello message are ed.

```
Random: d714ec03ed1741521f42ca4af95aaafea4bf5d577fd764630f5b392a2a3ee15d
  GMT Unix Time: May 6, 2084 22:59:39.000000000 India Standard Time
  Random Bytes: ed1741521f42ca4af95aaafea4bf5d577fd764630f5b392a2a3ee15d
  Session ID Length: 32
  Session ID: 31453134213879cbea2cf64039933d3bdf9efb52d1a80c6f7ed9123c66a485e2
```

5. The random bytes field in the TLS Client Hello message allows the client and server to calculate the secret key to encrypt message data. The random byte string is encrypted with the server's public key.

PART-4: The TLS Handshake: Server Hello message

1. Packet number 2389 in my trace that contains the TLS Sever Hello message
2. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) has been chosen by the server among those offered in the earlier Client Hello message

```
-
  Version: TLS 1.2 (0x0303)
  Random: 26cf633c3db7687e89c2ee4ec08221ed4c6acee93e4ea6995d275e4aa4ae60c1
    GMT Unix Time: Aug 20, 1990 09:42:44.000000000 India Standard Time
    Random Bytes: 3db7687e89c2ee4ec08221ed4c6acee93e4ea6995d275e4aa4ae60c1
  Session ID Length: 0
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Compression Method: null (0)
  Extensions Length: 21
  > Extension: server_name (len=0)
  > Extension: renegotiation_info (len=1)
```

3. Yes, the packet contains random bytes.
4. Packet number 2393 in our trace corresponds to the TLS message containing the public key certificate for the www.cics.umass.edu server.
5. The trace reveals three certificates with common names: www.cs.umass.edu, InCommon RSA Server CA, and USERTrust RSA Certification Authority. These certificates are associated with the University of Massachusetts Amherst, InCommon/Internet2, and the USERTRUST network, respectively.
6. The certificate issued for id-at-commonName=www.cs.umass.edu is signed by the InCommon RSA Server CA.

```

    > validity
  > subject: rdnsSequence (0)
    > rdnsSequence: 4 items (id-at-commonName=www.cs.umass.edu,id-at-organizationName=University...
      > RDnsSequence item: 1 item (id-at-countryName=US)
      > RDnsSequence item: 1 item (id-at-stateOrProvinceName=Massachusetts)
      > RDnsSequence item: 1 item (id-at-organizationName=University of Massachusetts Amherst)
      > RDnsSequence item: 1 item (id-at-commonName=www.cs.umass.edu)
    > subjectPublicKeyInfo

```

7. The digital signature algorithm used by the CA to sign this certificate is sha256WithRSAEncryption. The Algorithm Id is 1.2.840.113549.1.1.11

```

  > Certificates (4890 bytes)
    Certificate Length: 1842
  > Certificate [truncated]: 3082072e30820616a00302010202103090854915311cde05eb63eb08
    > signedCertificate
      version: v3 (2)
      serialNumber: 0x3090854915311cde05eb63eb08727271
      > signature (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
      > issuer: rdnsSequence (0)
        > rdnsSequence: 6 items (id-at-commonName=InCommon RSA Server CA,id-at-orgar

```

8. The first four hexadecimal digits are 00b3

```

  > signedCertificate
    version: v3 (2)
    serialNumber: 0x3090854915311cde05eb63eb08727271
    > signature (sha256WithRSAEncryption)
    > issuer: rdnsSequence (0)
    > validity
    > subject: rdnsSequence (0)
    > subjectPublicKeyInfo
      > algorithm (rsaEncryption)
      > subjectPublicKey [truncated]: 3082010a0282010100b39e7296158da80176a2f1035c7c61f06120f9852...
        modulus: 0x00b39e7296158da80176a2f1035c7c61f06120f9852aad0d20d4931a30842fec1b8724...
        publicExponent: 65537
    > extensions: 10 items

```

9. 2393 is the packet number in our trace for the TLS message part that contains the Server Hello Done TLS record.

2393	21.656660051	128.119.240.84	10.250.61.113	TLSv1.2	1277 Certificate, Server Key Exchange, Server Hello Done
2394	21.656674341	10.250.61.113	128.119.240.84	TCP	54 48956 → 443 [ACK] Seq=667 Ack=5320 Win=64128 Len=0
2395	21.657927688	10.250.61.113	128.119.240.84	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2396	21.660972956	128.119.240.84	10.250.61.113	TCP	60 443 → 48968 [ACK] Seq=1 Ack=667 Win=30592 Len=0
2397	21.666003008	128.119.240.84	10.250.61.113	TLSv1.2	1514 Server Hello
2398	21.666011245	10.250.61.113	128.119.240.84	TCP	54 48968 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
2399	21.666641392	128.119.240.84	10.250.61.113	TCP	1514 443 → 48968 [ACK] Seq=1461 Ack=667 Win=30592 Len=1460 [TCP segment of a reasse
2400	21.666643092	10.250.61.113	128.119.240.84	TCP	54 48968 → 443 [ACK] Seq=667 Ack=2921 Win=64128 Len=0
2401	21.667104357	128.119.240.84	10.250.61.113	TCP	1230 443 → 48968 [PSH, ACK] Seq=2921 Ack=667 Win=30592 Len=1176 [TCP segment of a r
2402	21.667113152	10.250.61.113	128.119.240.84	TCP	54 48968 → 443 [ACK] Seq=667 Ack=4097 Win=64128 Len=0
2403	21.667120487	128.119.240.84	10.250.61.113	TLSv1.2	1277 Certificate, Server Key Exchange, Server Hello Done

PART-5: The TLS Handshake: wrapping up the handshake

1. Packet number 2395 in the trace corresponds to the TLS message containing the public key information, Change Cipher Spec, and Encrypted Handshake message sent from the client to the server.
2. The client does not send its own CA-signed public key certificate back to the server.

PART-6: Application data

1) The client and server utilize the Advanced Encryption Standard (AES) as the symmetric key cryptography algorithm to encrypt application data.

2) The determination and declaration of the symmetric key cryptography algorithm used for securing communication occur during the "Cipher Suite Negotiation" step within the "ClientHello" and "ServerHello" messages of the TLS handshake protocol.

```
Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 657
  Version: TLS 1.2 (0x0303)
  Random: f5d32f06f03a18c7c0dd0ff405568113ad740a9e27992db3fc2d6da3f621ed0c
  Session ID Length: 32
  Session ID: 4f2251574781996020fd0c00055bdcef9c101ab8df78a5585481ee9187a895a1
  Cipher Suites Length: 34
  Cipher Suites (17 suites)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    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_CHACHA20_POLY1305_SHA256 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)
    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_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
```

3. Packet no 2449 is the packet carrying first encrypted message (encrypted application data) from client to server

No.	Time	Source	Destination	Protocol	Length	Info
2404	21.684597088	10.250.61.113	128.119.240.84	TCP	54	48968 → 443 [ACK] Seq=667 Ack=5320 Win=64128 Len=0
2405	21.687425657	10.250.61.113	128.119.240.84	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2448	21.912016005	128.119.240.84	10.250.61.113	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2449	21.912791761	10.250.61.113	128.119.240.84	TLSv1.2	539	Application Data
2451	21.946948756	128.119.240.84	10.250.61.113	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2452	21.989370282	10.250.61.113	128.119.240.84	TCP	54	48968 → 443 [ACK] Seq=793 Ack=5594 Win=64128 Len=0
2472	22.197915811	128.119.240.84	10.250.61.113	TCP	60	443 → 48956 [ACK] Seq=5594 Ack=1278 Win=31872 Len=0

```
> Frame 2449: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface enp2s0, id 0
> Ethernet II, Src: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.250.61.113, Dst: 128.119.240.84
> Transmission Control Protocol, Src Port: 48956, Dst Port: 443, Seq: 793, Ack: 5594, Len: 485
> Transport Layer Security
  > TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 480
    Encrypted Application Data [truncated]: 00000000000001143dc0decfd145c2d7ebf56483c7ade5fa683426e8c5681f2790a19a3c8db82b97d4752b9b4eba6508b49640d0c281d3de19c464ecf457d326c2697a28026d3
    [Application Data Protocol: Hypertext Transfer Protocol]
```

4. Given that this trace was generated by fetching the homepage of www.cics.umass.edu, the encrypted application data likely contains content corresponding to the homepage of the website.
5. Packet 6545 contains the client to server TLS message to shutdown the TLS connection