

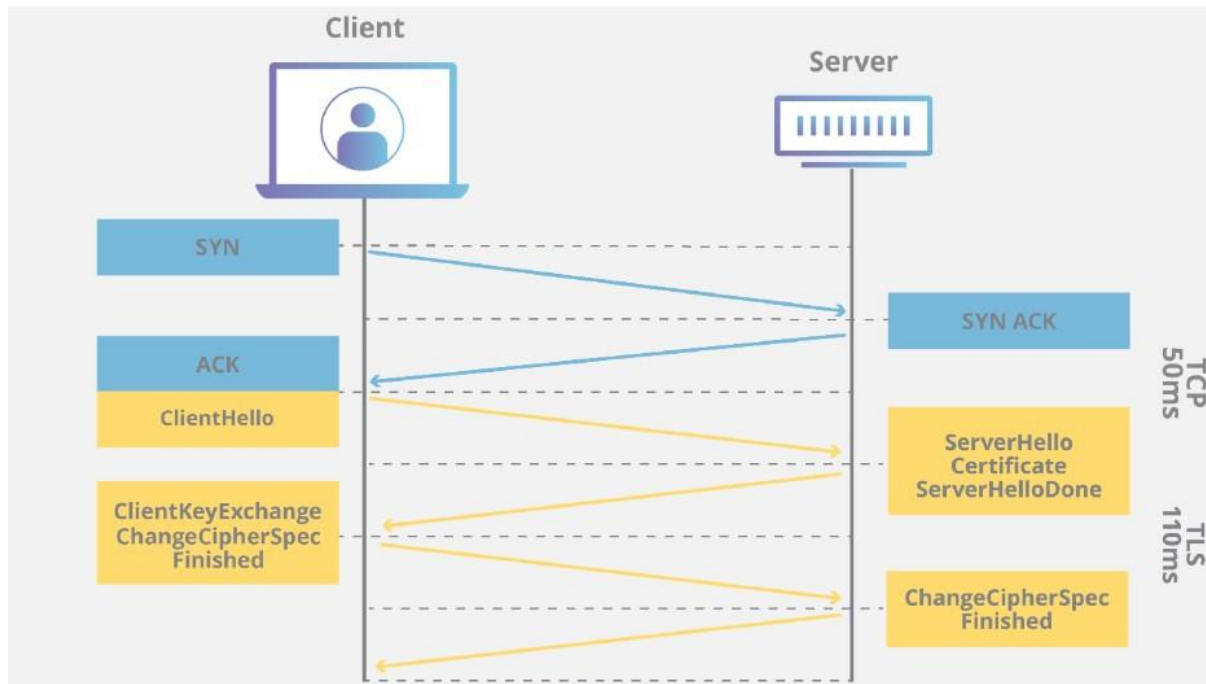
Name: Rithik Sarvesh Bharathiraja

UID: 120395246

Course: ENPM693

Task: Homework 6

## Part – 1



This is a packet capture of the conversation between the client and badssl.com

Client hello

Following important parameters are sent to the server in the client\_hello message

Version – TLS version

Timestamp – to prevent replay attack

random bytes - generated by the client

Session ID – To check whether the connection was established already.

Cipher suites – The types of cipher suites supported by the client

No.	Time	Source	Destination	Protocol	Length	Info
260	7.338818	172.16.125.223	52.143.87.28	TLSv1.2	276	Client Hello
264	7.407814	52.143.87.28	172.16.125.223	TLSv1.2	1025	Server Hello, Certificate, Serve
266	7.410330	172.16.125.223	52.143.87.28	TLSv1.2	212	Client Key Exchange, Change Ciph

<ul style="list-style-type: none"> <li>Transport Layer Security           <ul style="list-style-type: none"> <li>TLSv1.2 Record Layer: Handshake Protocol: Client Hello               <ul style="list-style-type: none"> <li>Content Type: Handshake (22)</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Length: 217</li> <li>Handshake Protocol: Client Hello                   <ul style="list-style-type: none"> <li>Handshake Type: Client Hello (1)</li> <li>Length: 213</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Random: 6636abf5af8fcbcd5db4e10b6fef11d4df83ed36c2819a473d95139fd85c168a                       <ul style="list-style-type: none"> <li>GMT Unix Time: May 4, 2024 17:43:17.000000000 Eastern Daylight Time</li> <li>Random Bytes: af8fcbcd5db4e10b6fef11d4df83ed36c2819a473d95139fd85c168a</li> </ul> </li> <li>Session ID Length: 0</li> <li>Cipher Suites Length: 38</li> <li>Cipher Suites (19 suites)                           <ul style="list-style-type: none"> <li>Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	<pre> 0000 00 01 21 06 b 0010 01 06 50 42 4 0020 57 1c 15 5a 0 0030 02 05 b4 95 0 0040 03 66 36 ab f 0050 d4 df 83 ed 3 0060 8a 00 00 26 c 0070 c0 28 c0 27 c 0080 00 3d 00 3c 0 0090 00 2a 00 28 0 00a0 70 72 6f 64 2 00b0 69 63 72 6f 7 00c0 01 00 00 00 0 00d0 18 00 0b 00 0 00e0 05 08 06 04 0 00f0 02 06 01 06 0 0100 68 32 08 68 7 0110 01 00 01 00 </pre>
--	--

## Server hello

In response to client hello, server sends the server\_hello message. In this, server chooses the cipher suite and sends that to the client. Along with that, session is established and unique session ID is generated and sent to the client.

No.	Time	Source	Destination	Protocol	Length	Info
260	7.338818	172.16.125.223	52.143.87.28	TLSv1.2	276	Client Hello
264	7.407814	52.143.87.28	172.16.125.223	TLSv1.2	1025	Server Hello, Certificate, Serve
266	7.410330	172.16.125.223	52.143.87.28	TLSv1.2	212	Client Key Exchange, Change Ciph

<ul style="list-style-type: none"> <li>Handshake Type: Server Hello (2)</li> <li>Length: 90</li> <li>Version: TLS 1.2 (0x0303)</li> <li>Random: 6636abf5ea5911508f51f76fc4ac75339564f1b09f1b2319ba52b375f70f468a           <ul style="list-style-type: none"> <li>GMT Unix Time: May 4, 2024 17:43:17.000000000 Eastern Daylight Time</li> <li>Random Bytes: ea5911508f51f76fc4ac75339564f1b09f1b2319ba52b375f70f468a</li> </ul> </li> <li>Session ID Length: 32</li> <li>Session ID: 823f0000a88787a1fcd55535dc12c278ed4d16c3c1ec628d91c20dd86f780b15</li> <li>Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>Compression Method: null (0)</li> <li>Extensions Length: 18           <ul style="list-style-type: none"> <li>Extension: application_layer_protocol_negotiation (len=5)</li> <li>Extension: extended_master_secret (len=0)</li> <li>Extension: renegotiation_info (len=1)               <ul style="list-style-type: none"> <li>[JA3S Fullstring: 771,49196,16-23-65281]</li> <li>[JA3S: a02d7ceb8c8cbb4da2e6007f5a1c91e4]</li> </ul> </li> </ul> </li> </ul>	<pre> 0000 16 03 03 09 0010 59 11 50 8f 0020 1b 23 19 ba 0030 a8 87 87 a1 0040 c1 ec 62 8d 0050 12 00 10 00 0060 00 01 00 0b 0070 e1 30 82 03 0080 42 11 91 04 0090 0a 06 08 2a 00a0 30 09 06 03 00b0 03 55 04 08 00c0 31 10 30 0e 00d0 6e 64 31 1e 00e0 72 6f 73 6f 00f0 6f 6e 31 40 0100 72 6f 73 6f 0110 6e 74 20 44 0120 53 65 63 75 </pre>
---	---

After server\_hello, the server sends its certificate to the client.

No.	Time	Source	Destination	Protocol	Length	Info
260	7.338818	172.16.125.223	52.143.87.28	TLsv1.2	276	Client Hello
264	7.407814	52.143.87.28	172.16.125.223	TLsv1.2	1025	Server Hello, Certificate, Serve
266	7.410330	172.16.125.223	52.143.87.28	TLsv1.2	212	Client Key Exchange, Change Ciph

Handshake Protocol: Certificate	0000	1^
Handshake Type: Certificate (11)	0010	5^
Length: 2145	0020	1^
Certificates Length: 2142	0030	a:
▼ Certificates (2142 bytes)	0040	c:
Certificate Length: 997	0050	1:
> Certificate: 308203e130820367a00302010202133300000042119104585ab451bc00000000042300a... (id-at-commonName=*.prod.do	0060	0:
Certificate Length: 1139	0070	e:
> Certificate: 3082046f308203f6a0030201020213330000009066cb601e4418e730000000009300a... (id-at-commonName=Microsoft	0080	4:
	0090	0:
	00a0	3:

In certificate, it comes up with various important parameters like

- Signature
- Issuer
- Validity
- Subject

▼ Certificate: 308203e130820367a00302010202133300000042119104585ab451bc00000000042300a... (id-at-commonName=*.prod.do
▼ signedCertificate
version: v3 (2)
serialNumber: 0x3300000042119104585ab451bc000000000042
▼ signature (ecdsa-with-SHA384)
Algorithm Id: 1.2.840.10045.4.3.3 (ecdsa-with-SHA384)
▼ issuer: rdnSequence (0)
> rdnSequence: 5 items (id-at-commonName=Microsoft ECC Content Distribution Secure Server CA 2.1,id-at-organ
▼ validity
> notBefore: utcTime (0)
> notAfter: utcTime (0)
▼ subject: rdnSequence (0)
> rdnSequence: 6 items (id-at-commonName=*.prod.do.dsp.mp.microsoft.com,id-at-organizationalUnitName=DSP,id-
> subjectPublicKeyInfo
> extensions: 8 items
> algorithmIdentifier (ecdsa-with-SHA384)
Padding: 0
encrvoted: 3065023018ec359f4f22826b3d97701e8d03c18f1d69343df74e694f585a8c94ea84316a...

▼ Certificate: 3082046f308203f6a0030201020213330000009066cb601e4418e730000000009300a... (id-at-commonName=Microsoft
▼ signedCertificate
version: v3 (2)
serialNumber: 0x330000009066cb601e4418e7300000000009
▼ signature (ecdsa-with-SHA384)
Algorithm Id: 1.2.840.10045.4.3.3 (ecdsa-with-SHA384)
▼ issuer: rdnSequence (0)
> rdnSequence: 5 items (id-at-commonName=Microsoft ECC Product Root Certificate Authority 2018,id-at-organiz
▼ validity
> notBefore: utcTime (0)
> notAfter: utcTime (0)
▼ subject: rdnSequence (0)
> rdnSequence: 5 items (id-at-commonName=Microsoft ECC Content Distribution Secure Server CA 2.1,id-at-orgar
▼ subjectPublicKeyInfo
> algorithm (id-ecPublicKey)
Padding: 0
subjectPublicKey: 049645c315953e93915f1744c6633086145660c5a6bd5f1d03681028939aebe305952abb...
> extensions: 10 items

To exchange keys, server sends the key exchange algorithm and its parameter.

- ▼ Handshake Protocol: Server Key Exchange
  - Handshake Type: Server Key Exchange (12)
  - Length: 175
- ▼ EC Diffie-Hellman Server Params
  - Curve Type: named\_curve (0x03)
  - Named Curve: secp384r1 (0x0018)
  - Pubkey Length: 97
  - Pubkey: 040e6f2d9416ff684086e1e3a9f0e011208c3cc8ab20c7affd9608ebb4696c0521f9313e...
- ▼ Signature Algorithm: ecdsa\_secp256r1\_sha256 (0x0403)
  - Signature Hash Algorithm Hash: SHA256 (4)
  - Signature Hash Algorithm Signature: ECDSA (3)
  - Signature Length: 70
  - Signature: 30440220cfc9478f7ed24a7f7171f3d6d241311d9d0422faa6d1930fda18e96419304c6...

At last, the server sends the server\_hello\_done message to mark the end of server hello

No.	Time	Source	Destination	Protocol	Length	Info
260	7.338818	172.16.125.223	52.143.87.28	TLSv1.2	276	Client Hello
264	7.407814	52.143.87.28	172.16.125.223	TLSv1.2	1025	Server Hello, Certificate, ...
266	7.410330	172.16.125.223	52.143.87.28	TLSv1.2	212	Client Key Exchange, Change...

> Frame 264: 1025 bytes on wire (8200 bits), 1025 bytes captured (8200 bits) on interface \Device\NPF_{32F17190-CA93-45DD-...}
> Ethernet II, Src: RuckusWi_10:2d:5c (1c:b9:c4:10:2d:5c), Dst: Chongqin_be:48:bd (ac:d5:64:be:48:bd)
> Internet Protocol Version 4, Src: 52.143.87.28, Dst: 172.16.125.223
> Transmission Control Protocol, Src Port: 443, Dst Port: 5466, Seq: 1461, Ack: 223, Len: 971
> [2 Reassembled TCP Segments (2431 bytes): #263(1460), #264(971)]
▼ Transport Layer Security
▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 2426
> Handshake Protocol: Server Hello
> Handshake Protocol: Certificate
> Handshake Protocol: Server Key Exchange
▼ Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)
Length: 0

Client key exchange and cipher change spec

In response, the client sends its parameter for key exchange and it acknowledges that the server has chosen a cipher suite.



No.	Time	Source	Destination	Protocol	Length	Info
260	7.338818	172.16.125.223	52.143.87.28	TLSv1.2	276	Client Hello
264	7.407814	52.143.87.28	172.16.125.223	TLSv1.2	1025	Server Hello, Certificate, Serve
266	7.410330	172.16.125.223	52.143.87.28	TLSv1.2	212	Client Key Exchange, Change Ciph

Transport Layer Security
 

- TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 102
- Handshake Protocol: Client Key Exchange
  - Handshake Type: Client Key Exchange (16)
  - Length: 98
  - EC Diffie-Hellman Client Params
    - Pubkey Length: 97
    - Pubkey: 046e91650f001115de87b4bd066c8724408f13529d6fa746cb14db8fb57b549163b8f183...
- 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

0000  
0010  
0020  
0030  
0040  
0050  
0060  
0070  
0080  
0090  
00a0  
00b0  
00c0  
00d0

## Server reply

Server acknowledges the client's acknowledgement and starts sending in the data after that.

No.	Time	Source	Destination	Protocol	Length	Info
260	7.338818	172.16.125.223	52.143.87.28	TLSv1.2	276	Client Hello
264	7.407814	52.143.87.28	172.16.125.223	TLSv1.2	1025	Server Hello, Certificate, Serve
266	7.410330	172.16.125.223	52.143.87.28	TLSv1.2	212	Client Key Exchange, Change Ciph
267	7.480479	52.143.87.28	172.16.125.223	TLSv1.2	105	Change Cipher Spec, Encrypted Ha

Frame 267: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF\_{32F17190-CA93-45DD-8751...}
 

- Ethernet II, Src: RuckusWi\_10:2d:5c (1c:b9:c4:10:2d:5c), Dst: Chongqin\_be:48:bd (ac:d5:64:be:48:bd)
- Internet Protocol Version 4, Src: 52.143.87.28, Dst: 172.16.125.223
- Transmission Control Protocol, Src Port: 443, Dst Port: 5466, Seq: 2432, Ack: 381, Len: 61
- Transport Layer Security
  - 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: Encrypted Handshake Message

0000  
0010  
0020  
0030  
0040  
0050  
0060  
0070  
0080  
0090  
00a0  
00b0  
00c0  
00d0

## Part 2

After following the given steps, packet capture was done after accessing <https://www.iplt20.com> website. Using the sslkeylog.txt, wireshark decrypts the data sent in the https. At the end, readable html tags were found in the below tab.

tls						
No.	Time	Source	Destination	Protocol	Length	Info
316	3.175583	142.251.16.95	172.16.125.223	TLSv1.3	343	Encrypted Extensions, Certificate
320	3.175868	152.199.6.208	172.16.125.223	HTTP2	1514	[TLS segment of a reassembled P
335	3.176401	152.199.6.208	172.16.125.223	TLSv1.3	1514	[TLS segment of a reassembled P
349	3.177185	152.199.6.208	172.16.125.223	TLSv1.3	1514	[TLS segment of a reassembled P
353	3.177514	152.199.6.208	172.16.125.223	HTTP2	718	DATA[1] (text/html)
355	3.177659	172.16.125.223	142.251.16.95	TLSv1.3	128	Change Cipher Spec, Encrypted Ex
360	3.179281	172.253.115.97	172.16.125.223	TLSv1.3	1466	Server Hello, Change Cipher Spec

> Frame 353: 718 bytes on wire	00000000	0a 3c 21 44 4f 43 54 59	50 45 20 68 74 6d 6c 3e	-<!DOCTYPE PE html>
> Ethernet II, Src: RuckusWi_1	00000010	0a 3c 68 74 6d 6c 20 6c	61 6e 67 3d 22 65 6e 22	-<html l ang="en"
> Internet Protocol Version 4,	00000020	3e 0a 3c 68 65 61 64 3e	0a 3c 73 63 72 69 70 74	>-<head> -<script
> Transmission Control Protoc	00000030	3e 0a 20 20 20 20 76 61	72 20 74 69 74 6c 65 20	>- va r title
> [4 Reassembled TCP Segments	00000040	3d 20 22 49 6e 64 69 61	6e 20 50 72 65 6d 69 65	= "India n Premie
> [2 Reassembled TLS segments	00000050	72 20 4c 65 61 67 75 65	20 4f 66 66 69 63 69 61	r League Officia
> Transport Layer Security	00000060	6c 20 57 65 62 73 69 74	65 20 2d 32 30 32 34 22	l Websit e -2024"
> [2 Reassembled TLS segments	00000070	3b 0a 20 20 20 20 77 69	6e 64 6f 77 2e 64 61 74	; wi ndow.dat
> HyperText Transfer Protocol	00000080	61 4c 61 79 65 72 20 3d	20 77 69 6e 64 6f 77 2e	aLayer = window.
> Stream: DATA, Stream ID:	00000090	64 61 74 61 4c 61 79 65	72 20 7c 7c 20 5b 5d 3b	dataLaye r [  [];
> Length: 3876	000000a0		7 2e 64 61 74 61	- win dow.data
> Type: DATA (0)	000000b0		8 7b 0a 20 20 20	Layer.pu sh({
> Flags: 0x01, End Strea	000000c0		e 74 5f 67 61 5f	'cl ient_ga_
> 0... ..	000000d0		8 39 39 38 39 27	id': '30 8089989'
	000000e0		7 63 6f 6e 74 65	, 'conte