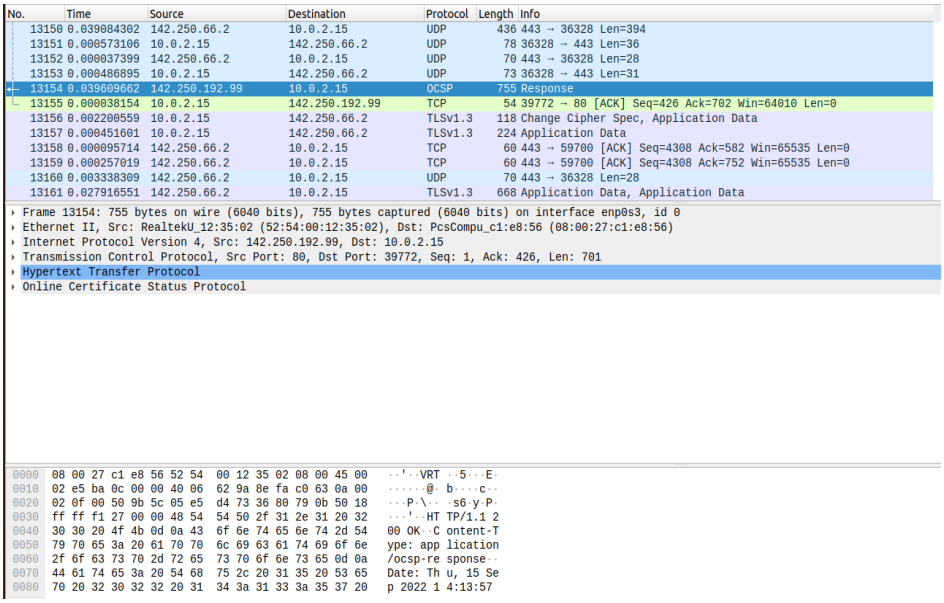
Joy Makwana (20110086)

PART-3

A)

OCSP:

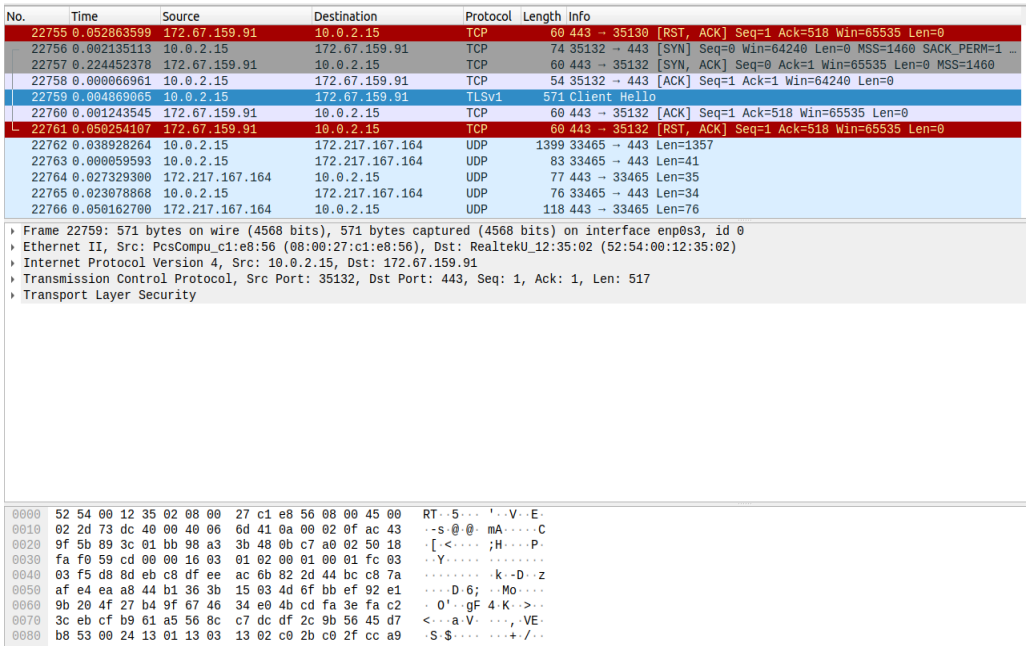
The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. Messages transferred via OCSP are generally encoded with ASN.1 and are transmitted over HTTP. Some of the web browsers like Mozilla use OCSP to validate HTTP certificates.
RFC is 6960



TLSv1:

Transport layer service protocol guarantees communications security over a computer network. Although the protocol is widely used in voice-over IP, instant messaging, and email.Its use in HTTP is still the most commonly known.

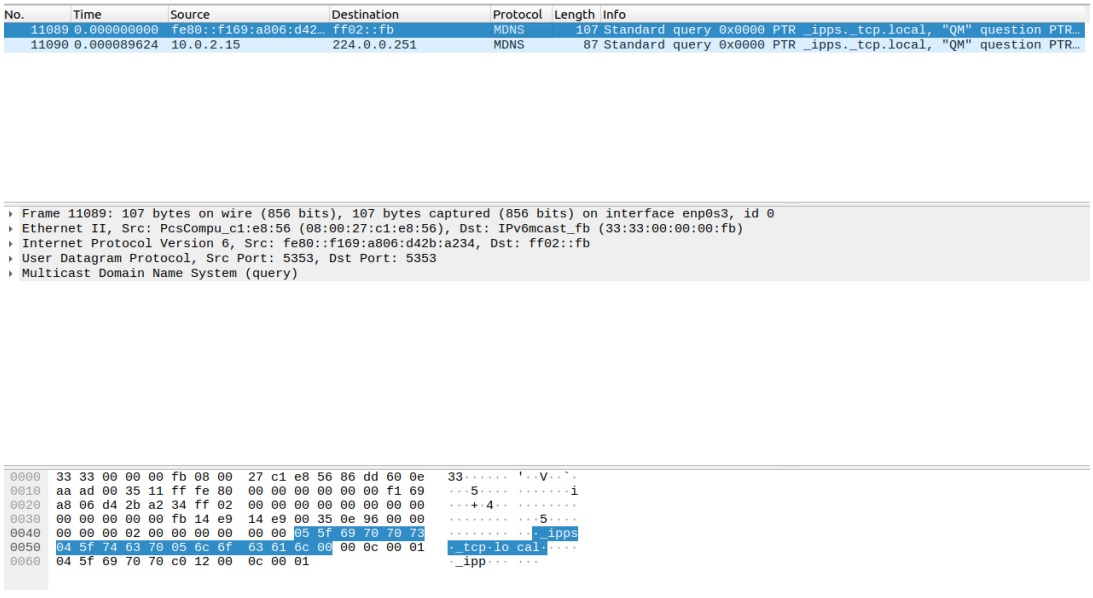
RFC is 2246



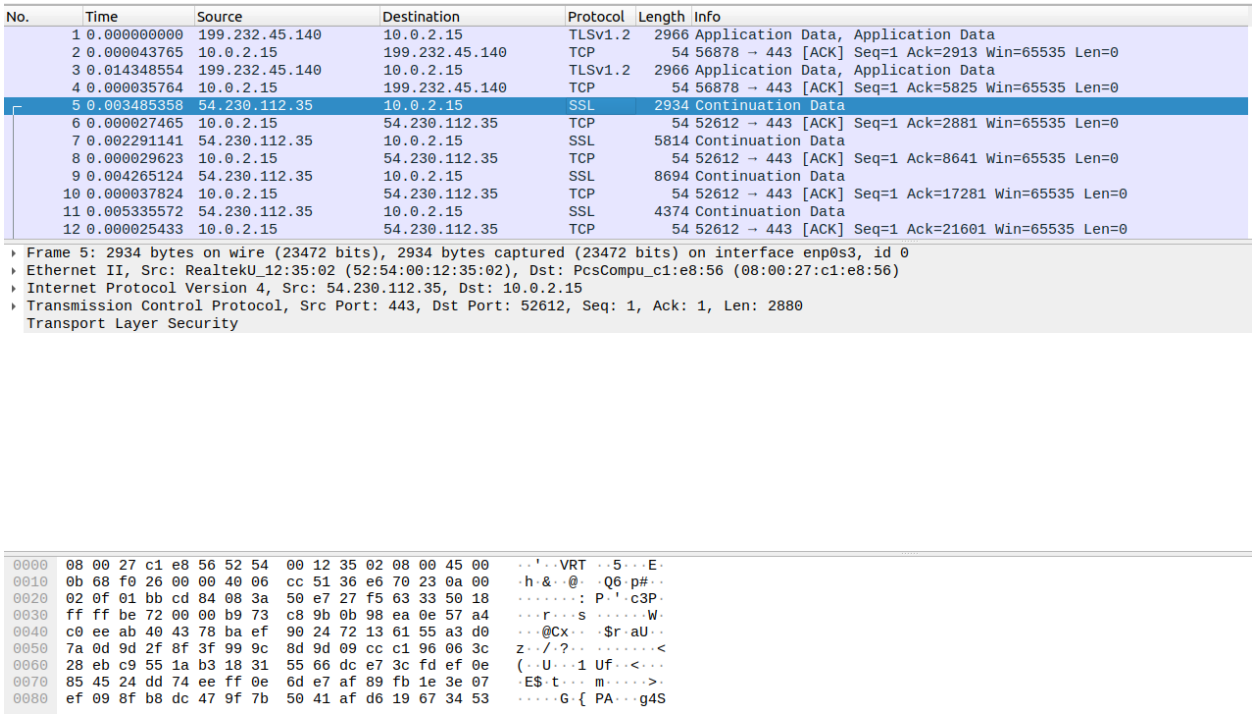
Multicast DNS:

mDNS message is a UDP packet transmitted using IPv4, IPv6, and UDP ports.mDNS also helps to resolve hostnames to IP addresses within small networks that do not include a local name server. It uses operating semantics as unicast DNS.

RFC is 6762



SSL: secure socket layer provides security to the data that is transferred between the server and the client. SSL encrypts the link between server and client due to which security gets enhanced. RFC is 6101



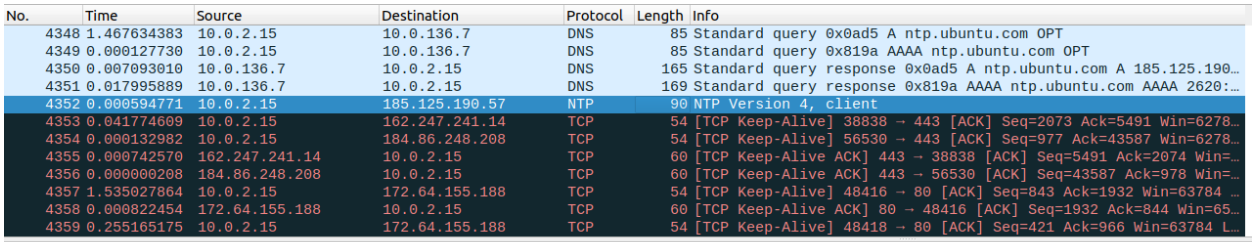
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	199.232.45.140	10.0.2.15	TLSv1.2	2966	Application Data, Application Data
2	0.000043765	10.0.2.15	199.232.45.140	TCP	54	56878 → 443 [ACK] Seq=1 Ack=2913 Win=65535 Len=0
3	0.014348554	199.232.45.140	10.0.2.15	TLSv1.2	2966	Application Data, Application Data
4	0.000035764	10.0.2.15	199.232.45.140	TCP	54	56878 → 443 [ACK] Seq=1 Ack=5825 Win=65535 Len=0
5	0.003485358	54.230.112.35	10.0.2.15	SSL	2934	Continuation Data
6	0.000027465	10.0.2.15	54.230.112.35	TCP	54	52612 → 443 [ACK] Seq=1 Ack=2881 Win=65535 Len=0
7	0.002291141	54.230.112.35	10.0.2.15	SSL	5814	Continuation Data
8	0.000029623	10.0.2.15	54.230.112.35	TCP	54	52612 → 443 [ACK] Seq=1 Ack=8641 Win=65535 Len=0
9	0.004265124	54.230.112.35	10.0.2.15	SSL	8694	Continuation Data
10	0.000037824	10.0.2.15	54.230.112.35	TCP	54	52612 → 443 [ACK] Seq=1 Ack=17281 Win=65535 Len=0
11	0.005335572	54.230.112.35	10.0.2.15	SSL	4374	Continuation Data
12	0.000025433	10.0.2.15	54.230.112.35	TCP	54	52612 → 443 [ACK] Seq=1 Ack=21601 Win=65535 Len=0

```
▸ Frame 5: 2934 bytes on wire (23472 bits), 2934 bytes captured (23472 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_c1:e8:56 (08:00:27:c1:e8:56)
▸ Internet Protocol Version 4, Src: 54.230.112.35, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 52612, Seq: 1, Ack: 1, Len: 2880
  Transport Layer Security
```

```
0000  08 00 27 c1 e8 56 52 54  00 12 35 02 08 00 45 00   ··'··VRT ··5···E·
0010  0b 68 f0 26 00 00 40 06  cc 51 36 e6 70 23 0a 00   ·h·&··@· ·Q6·p#··
0020  02 0f 01 bb cd 84 08 3a  50 e7 27 f5 63 33 50 18   ·······: P·'·c3P·
0030  ff ff be 72 00 00 b9 73  c8 9b 0b 98 ea 0e 57 a4   ···r···s ······W·
0040  c0 ee ab 40 43 78 ba ef  90 24 72 13 61 55 a3 d0   ···@Cx·· ·$r·aU··
0050  7a 0d 9d 2f 8f 3f 99 9c  8d 9d 09 cc c1 96 06 3c   z··/·?·· ·······<
0060  28 eb c9 55 1a b3 18 31  55 66 dc e7 3c fd ef 0e   (··U···1 Uf··<···
0070  85 45 24 dd 74 ee ff 0e  6d e7 af 89 fb 1e 3e 07   ·E$·t··· m·····>·
0080  ef 09 8f b8 dc 47 9f 7b  50 41 af d6 19 67 34 53   ·····G·{ PA···g4S
```

NTP (version 4):

The network time protocol is a networking protocol for clock synchronization between computer systems for clock synchronization, variable-latency data networks. The current protocol version is 4 whose RFC is 1305



No.	Time	Source	Destination	Protocol	Length	Info
4348	1.467634383	10.0.2.15	10.0.136.7	DNS	85	Standard query 0x0ad5 A ntp.ubuntu.com OPT
4349	0.000127730	10.0.2.15	10.0.136.7	DNS	85	Standard query 0x819a AAAA ntp.ubuntu.com OPT
4350	0.007093010	10.0.136.7	10.0.2.15	DNS	165	Standard query response 0x0ad5 A ntp.ubuntu.com A 185.125.190…
4351	0.017995889	10.0.136.7	10.0.2.15	DNS	169	Standard query response 0x819a AAAA ntp.ubuntu.com AAAA 2620:…
4352	0.000594771	10.0.2.15	185.125.190.57	NTP	90	NTP Version 4, client
4353	0.041774609	10.0.2.15	162.247.241.14	TCP	54	[TCP Keep-Alive] 38838 → 443 [ACK] Seq=2073 Ack=5491 Win=6278…
4354	0.000132982	10.0.2.15	184.86.248.208	TCP	54	[TCP Keep-Alive] 56530 → 443 [ACK] Seq=977 Ack=43587 Win=6278…
4355	0.000742570	162.247.241.14	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 443 → 38838 [ACK] Seq=5491 Ack=2074 Win=…
4356	0.000000208	184.86.248.208	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 443 → 56530 [ACK] Seq=43587 Ack=978 Win=…
4357	1.535027864	10.0.2.15	172.64.155.188	TCP	54	[TCP Keep-Alive] 48416 → 80 [ACK] Seq=843 Ack=1932 Win=63784 …
4358	0.000822454	172.64.155.188	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 48416 [ACK] Seq=1932 Ack=844 Win=65…
4359	0.255165175	10.0.2.15	172.64.155.188	TCP	54	[TCP Keep-Alive] 48418 → 80 [ACK] Seq=421 Ack=966 Win=63784 L…

```
▸ Frame 4352: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_c1:e8:56 (08:00:27:c1:e8:56), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 185.125.190.57
▸ User Datagram Protocol, Src Port: 49615, Dst Port: 123
▸ Network Time Protocol (NTP Version 4, client)
```

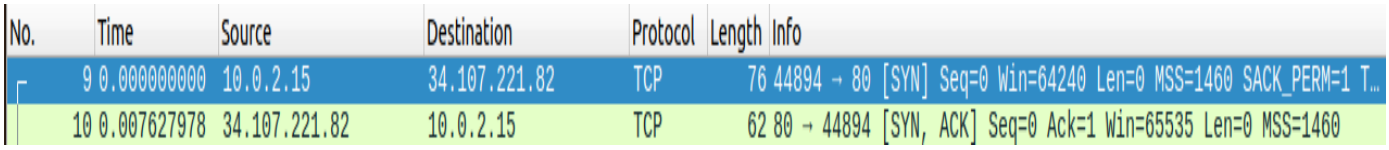
```
0000  52 54 00 12 35 02 08 00  27 c1 e8 56 08 00 45 10   RT··5··· '··V··E·
0010  00 4c 92 15 40 00 40 11  24 b6 0a 00 02 0f b9 7d   ·L··@·@· $·····}
0020  be 39 c1 cf 00 7b 00 38  84 0f 23 00 00 00 00 00   ·9···{·8 ··#·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 e6 cd f0 a1 17 06  02 c8                     ········ ··
```

B)

TCP connection: There exists a TCP connection between number 9 and number 10 as we can see from the below image.
At first, number 9 sent the data to number 10.
Source IP: 10.0.2.15, source port = 44894
Destination IP: 34.107.221.82, destination port = 80

Then, number 10 replied back to number 9 by becoming the source.
Source IP: 34.107.221.82, source port = 80
Destination IP: 10.0.2.15, destination port = 44894

- The estimated RTT for this connection is 0.007627978 s because I changed the time display format to "seconds since previous displayed packet," which can be estimated as RTT.



No.	Time	Source	Destination	Protocol	Length	Info
9	0.000000000	10.0.2.15	34.107.221.82	TCP	76	44894 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
10	0.007627978	34.107.221.82	10.0.2.15	TCP	62	80 → 44894 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

C)

Cookies in ims.iitgn.ac.in:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	Sa...	Sa...	Partition Key	Priority
_ga	GA1.1.683663692.16...	.cloudflare.com	/	2023-10-13T15:17:25.1...	29		✓	No...			Medium
cfmrk_cic	{"id":"n7KXFRP9A5SU...	.cloudflare.com	/	2022-12-07T15:17:25.0...	99						Medium
_mkto_trk	id:713-XSC-918&tok...	.cloudflare.com	/	2023-10-13T15:17:24.4...	69						Medium
_ga_PHVG60J2FD	GS1.1.1662650245.4....	.cloudflare.com	/	2023-10-13T15:17:25.1...	52		✓	No...			Medium
_fbp	fb.2.1662570352845....	.cloudflare.com	/	2023-10-12T17:05:53.5...	33						Medium
_rdt_uuid	1662650244176.aa86...	.cloudflare.com	/	2023-10-13T15:17:24.3...	59						Medium
RequestToken	5ptu1f4rkjhmeya1as...	ims.iitgn.ac.in	/	Session	36	✓		Lax			Medium
_gcl_au	1.1.1539760630.1662...	.cloudflare.com	/	2022-12-06T17:05:53.0...	32						Medium
_ga	GA1.3.746458289.16...	.iitgn.ac.in	/	2024-01-12T08:41:23.0...	29						Medium

Cookies in student portal:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	Sa...	Sa...	Partition Key	Priority
RequestToken	5ptu1f4rkjhmeya1as...	ims.iitgn.ac.in	/	Session	36	✓		Lax			Medium
_ga	GA1.3.746458289.16...	.iitgn.ac.in	/	2024-01-12T08:41:23.0...	29						Medium

Analysis:

I found two cookies with domain as iitgn.ac.in

1) Cookie name: Request token:
   Expires on: temporary cookie
   Domain: ims.iitgn.ac.in
   Size: 36
   Priority: medium
   HTTP only: true
   Cookie value: 5ptu1f4rkjhmeya1ashxedid

2) Cookie name: _ga
   Expires on: 2024-01-12T08:41:23.000Z
   Domain: .iitgn.ac.in
   Size: 29
   Priority: medium
   Cookie value: GA1.3.746458289.1617560035