

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

No.	Time	Source	Destination	Protocol	Length	Info
13150	0.039084302	142.250.66.2	10.0.2.15	UDP	436	443 → 36328 Len=394
13151	0.000573106	10.0.2.15	142.250.66.2	UDP	78	36328 → 443 Len=36
13152	0.000037399	142.250.66.2	10.0.2.15	UDP	70	443 → 36328 Len=28
13153	0.000486895	10.0.2.15	142.250.66.2	UDP	73	36328 → 443 Len=31
13154	0.039089662	142.250.192.99	10.0.2.15	OCSP	755	Response
13155	0.000038154	10.0.2.15	142.250.192.99	TCP	54	39772 → 80 [ACK] Seq=426 Ack=702 Win=64010 Len=0
13156	0.002208559	10.0.2.15	142.250.66.2	TLSv1.3	118	Change Cipher Spec, Application Data
13157	0.000451601	10.0.2.15	142.250.66.2	TLSv1.3	224	Application Data
13158	0.000095714	142.250.66.2	10.0.2.15	TCP	60	443 → 59700 [ACK] Seq=4308 Ack=582 Win=65535 Len=0
13159	0.000257019	142.250.66.2	10.0.2.15	TCP	60	443 → 59700 [ACK] Seq=4308 Ack=752 Win=65535 Len=0
13160	0.003338309	142.250.66.2	10.0.2.15	UDP	70	443 → 36328 Len=28
13161	0.027916551	142.250.66.2	10.0.2.15	TLSv1.3	668	Application Data, Application Data
Frame 13154: 755 bytes on wire (6040 bits), 755 bytes captured (6040 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: 142.250.192.99, Dst: 10.0.2.15 Transmission Control Protocol, Src Port: 80, Dst Port: 39772, Seq: 1, Ack: 426, Len: 701 Hypertext Transfer Protocol Online Certificate Status Protocol						
0000	08 00 27 c1 e8 56 52 54	00 12 35 02 08 00 45 00	...VRT...5...E...			
0010	02 e5 ba 0c 00 00 40 06	62 9a 8e fa c0 63 0a 00@ b...c...			
0020	02 0f 09 50 9b 5c 05 e5	d4 73 36 80 79 0b 50 18	...P\...s6.y.P...			
0030	ff ff f1 27 00 00 48 54	54 50 2f 31 2e 31 20 32	...HT TP/1.1.2			
0040	30 30 20 4f 4b 0d 0a 43	6f 6e 74 65 6e 74 2d 54	00 OK Content-T			
0050	79 70 65 3a 20 61 70 70	6c 69 63 61 74 69 6f 6e	ype: application			
0060	2f 6f 63 73 70 2d 72 65	73 70 6f 6e 73 65 0d 0a	/ocsp-response...			
0070	44 61 74 65 3a 20 54 68	75 2c 20 31 35 20 53 65	Date: Thu, 15 Se			
0080	70 20 32 30 32 32 20 31	34 3a 31 33 3a 35 37 20	p 2022 1 4:13:57			

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

No.	Time	Source	Destination	Protocol	Length	Info
22755	0.052863599	172.67.159.91	10.0.2.15	TCP	60	443 → 35130 [RST, ACK] Seq=1 Ack=518 Win=65535 Len=0
22756	0.092135113	10.0.2.15	172.67.159.91	TCP	74	35132 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
22757	0.224452378	172.67.159.91	10.0.2.15	TCP	60	443 → 35132 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
22758	0.090066961	10.0.2.15	172.67.159.91	TCP	54	35132 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
22759	0.004869065	10.0.2.15	172.67.159.91	TLSv1	571	Client Hello
22760	0.091243545	172.67.159.91	10.0.2.15	TCP	60	443 → 35132 [ACK] Seq=1 Ack=518 Win=65535 Len=0
22761	0.050254107	172.67.159.91	10.0.2.15	TCP	60	443 → 35132 [RST, ACK] Seq=1 Ack=518 Win=65535 Len=0
22762	0.038928264	10.0.2.15	172.217.167.164	UDP	1399	33465 → 443 Len=1357
22763	0.090059593	10.0.2.15	172.217.167.164	UDP	83	33465 → 443 Len=41
22764	0.027329300	172.217.167.164	10.0.2.15	UDP	77	443 → 33465 Len=35
22765	0.023078868	10.0.2.15	172.217.167.164	UDP	76	33465 → 443 Len=34
22766	0.050162700	172.217.167.164	10.0.2.15	UDP	118	443 → 33465 Len=76

Frame 22759: 571 bytes on wire (4568 bits), 571 bytes captured (4568 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: 172.67.159.91
Transmission Control Protocol, Src Port: 35132, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security

0000 52 54 00 12 35 02 08 00 27 c1 e8 56 08 00 45 00 RT--5...V...E
0010 02 2d 73 dc 40 00 40 06 6d 41 0a 00 02 0f ac 43 --s_@_@:mA....C
0020 9f 5b 09 3c 01 bb 98 a3 3b 48 0b c7 a0 02 50 18 :[<....;H....P
0030 fa f0 59 c0 00 00 16 03 01 02 00 01 00 01 fc 03 --Y.....
0040 03 f5 d8 8d eb c8 df ee ac 0b 82 2d 44 bc c8 7ak-D..z
0050 af e4 ea a8 44 b1 36 3b 15 03 4d 6f bb ef 92 e1D 6;..Mo...
0060 9b 20 4f 27 b4 9f 67 46 34 e0 4b cd fa 3e fa c2 ..O'..gF 4K->..
0070 3c eb cf b9 61 a5 56 8c c7 cd df 2c 9b 56 45 d7 <...aV...VE..
0080 b8 53 00 24 13 01 13 03 13 02 c0 2b c0 2f cc a9 -S\$-...+/-..

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

No.	Time	Source	Destination	Protocol	Length	Info
11089	0.000000000	fe80::f169:a806:d42::fb	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps.tcp.local, "QM" question PTR...
11090	0.000089624	10.0.2.15	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps.tcp.local, "QM" question PTR...

Frame 11089: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_c1:e8:56 (08:00:27:c1:e8:56), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
Internet Protocol Version 6, Src: fe80::f169:a806:d42b:a234, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)

0000 33 33 00 00 00 fb 08 00 27 c1 e8 56 06 dd 60 0e 33.....V...
0010 aa ad 00 35 11 ff fe 00 00 00 00 00 00 00 f1 69 ..5.....i
0020 a8 06 d4 2b a2 34 ff 02 00 00 00 00 00 00 00 00 ..+4.....
0030 00 00 00 00 00 fb 14 e9 14 e9 00 35 0e 96 00 005....
0040 00 00 00 02 00 00 00 00 00 00 35 5f 69 70 76 7c_ipps
0050 04 5f 69 70 76 c0 12 00 0c 00 01tcp-10 cal...
0060 04 5f 69 70 76 c0 12 00 0c 00 01_1pp.....

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	..V.RT..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 a4r...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	.ES.t...m.....>..
0080	ef 09 8f b8 dc 47 9f 7b	50 41 af d6 19 67 34 53G.{ 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 0xad5 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 0xad5 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_PHV60J2FD	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