

Computer Networks

Assignment 2

2020-21

Even Semester

**Submitted By:
Abhishek Kumar
19ucs241
Lab Batch: C4**

1) What is the difference between HTTP and HTTPS?

HTTP stands for Hypertext Transfer Protocol.

HTTPS stands for Secured Hypertext Transfer Protocol.

The HTTP is transporting information over www without any security layer, and HTTPS is transporting information with the layer of security and encryption called an SSL Certificate.

In Computer Networking, HTTP works on Port 80 and HTTPS work on Port 443.

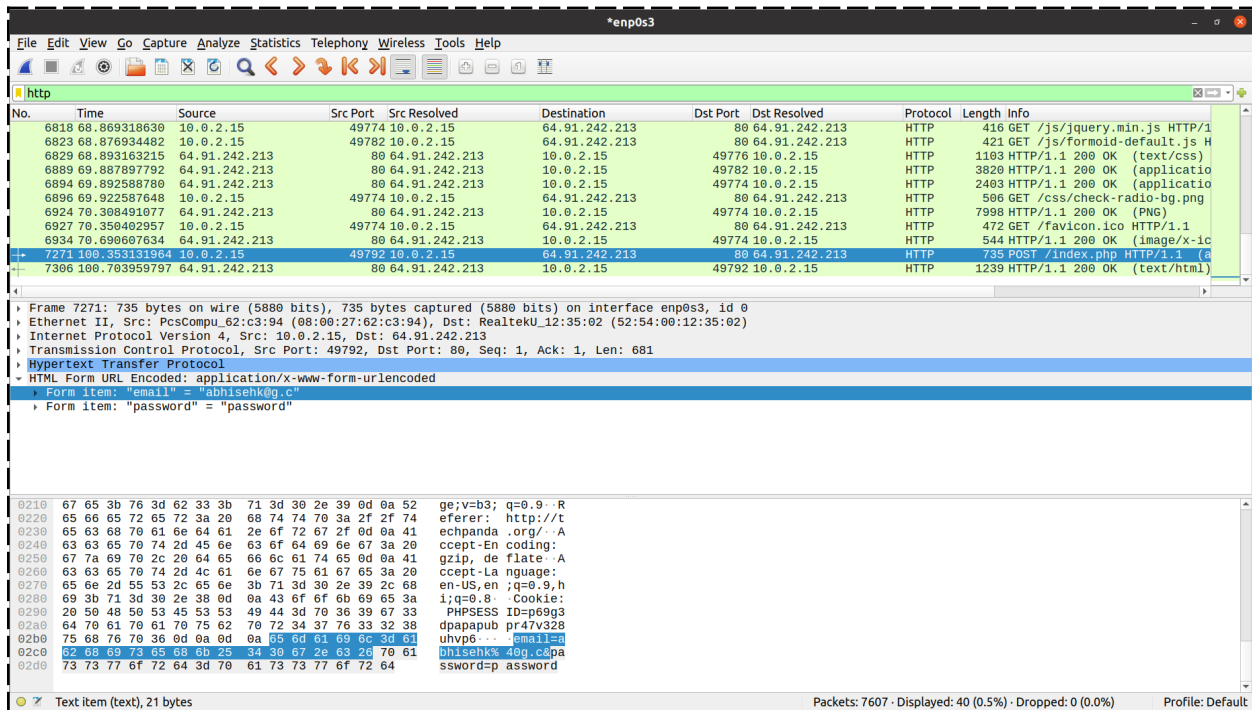
No.	Time	Src IP	Source	Src Port	Dst IP	Destination	Dst Port	Protocol	Length	Info
111	1.407280662	10.0.2.15	linux.local	37089	8.8.4.4	dns.google	53	DNS	93	Standard query 0x8e5b A stor
113	1.495050098	8.8.4.4	dns.google	53	10.0.2.15	linux.local	37089	DNS	301	Standard query response 0x8e
117	1.573198302	10.0.2.15	linux.local	52114	172.217.160.240	storage.googleapis...	80	HTTP	405	GET /update-delta/gcmjkmgdlg
143	1.852561460	10.0.2.15	linux.local	52114	172.217.160.240	storage.googleapis...	80	HTTP	397	GET /update-delta/khaoiebnk
554	15.723704917	10.0.2.15	linux.local	32984	216.58.200.165	nrt12s11-in-f165.1e...	443	TLSv1.3	571	Client Hello
589	15.873669903	10.0.2.15	linux.local	51361	8.8.4.4	dns.google	53	DNS	85	Standard query 0x1785 A ogs
597	15.935612311	8.8.4.4	dns.google	53	10.0.2.15	linux.local	60696	DNS	135	Standard query response 0x2e
602	15.961332018	8.8.4.4	dns.google	53	10.0.2.15	linux.local	51361	DNS	122	Standard query response 0x17
608	15.985345028	10.0.2.15	linux.local	54204	172.217.166.238	www3.l.google.com	443	TLSv1.3	571	Client Hello
676	16.540077894	8.8.4.4	dns.google	53	10.0.2.15	linux.local	36131	DNS	138	Standard query response 0x95
694	16.657311217	10.0.2.15	linux.local	54974	8.8.4.4	dns.google	53	DNS	96	Standard query 0x36b6 A lh6
702	16.743518454	8.8.4.4	dns.google	53	10.0.2.15	linux.local	54974	DNS	141	Standard query response 0x36

2) How is the differentiation between HTTP and HTTPS has impacted the result for the scenarios implemented?

In case of HTTP, we could easily see the email and password on POST request. While in the case of HTTPS, as data is encrypted so we can't get essential information, making it secure.

3) What is your plain text message HTTP POST message information for all the websites you have worked upon?

For <http://techpanda.org>

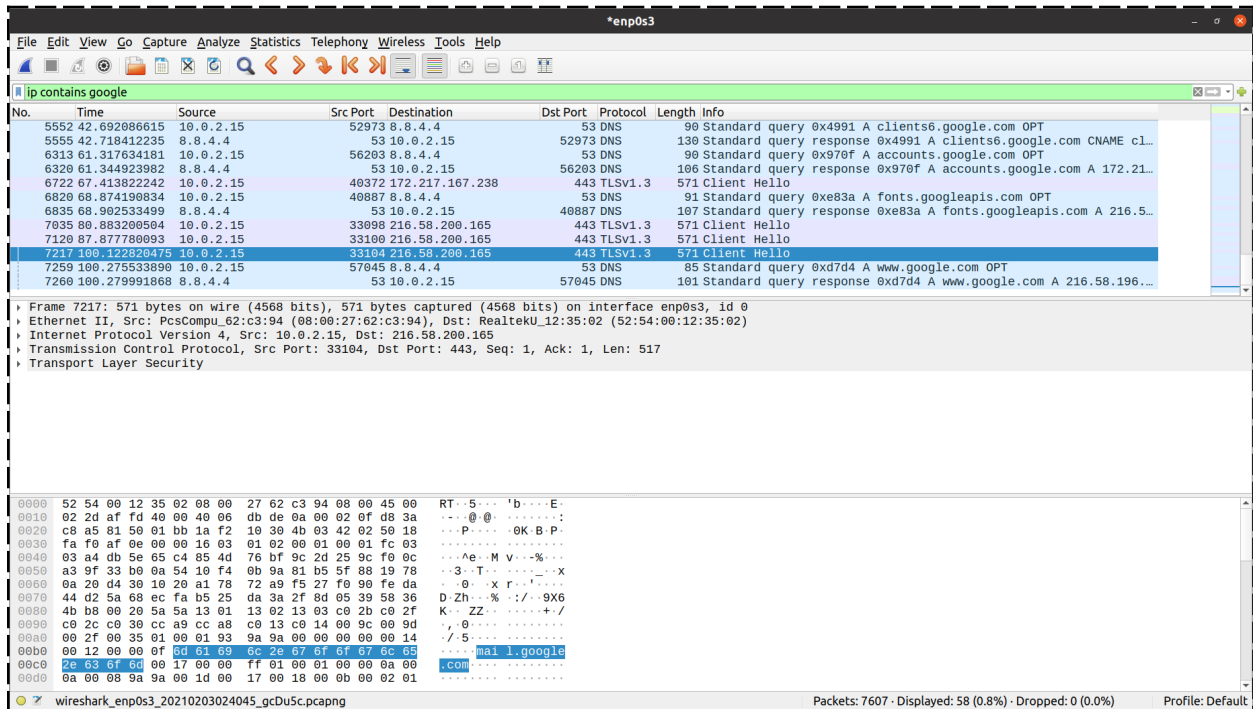


While the HTTPS POST messages can't be sniffed, thus we won't be able to sniff POST messages for Gmail and Facebook. (Screenshots attached below)

4) Could you sniff the credential information for all the websites? (Yes/No) Give reasons with substantiated result screenshot.

No, we couldn't sniff the credential information for Gmail and Facebook because they use HTTPS and get their data encrypted.

For mail.google.com



The image shows a Wireshark packet capture for the domain mail.google.com. The top pane displays a list of network packets. Packet 7217 is selected, showing a TLSv1.3 Client Hello. The middle pane shows the packet details, including the TLSv1.3 Client Hello structure. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates 7607 packets displayed, with 58 (0.8%) displayed and 0 (0.0%) dropped.

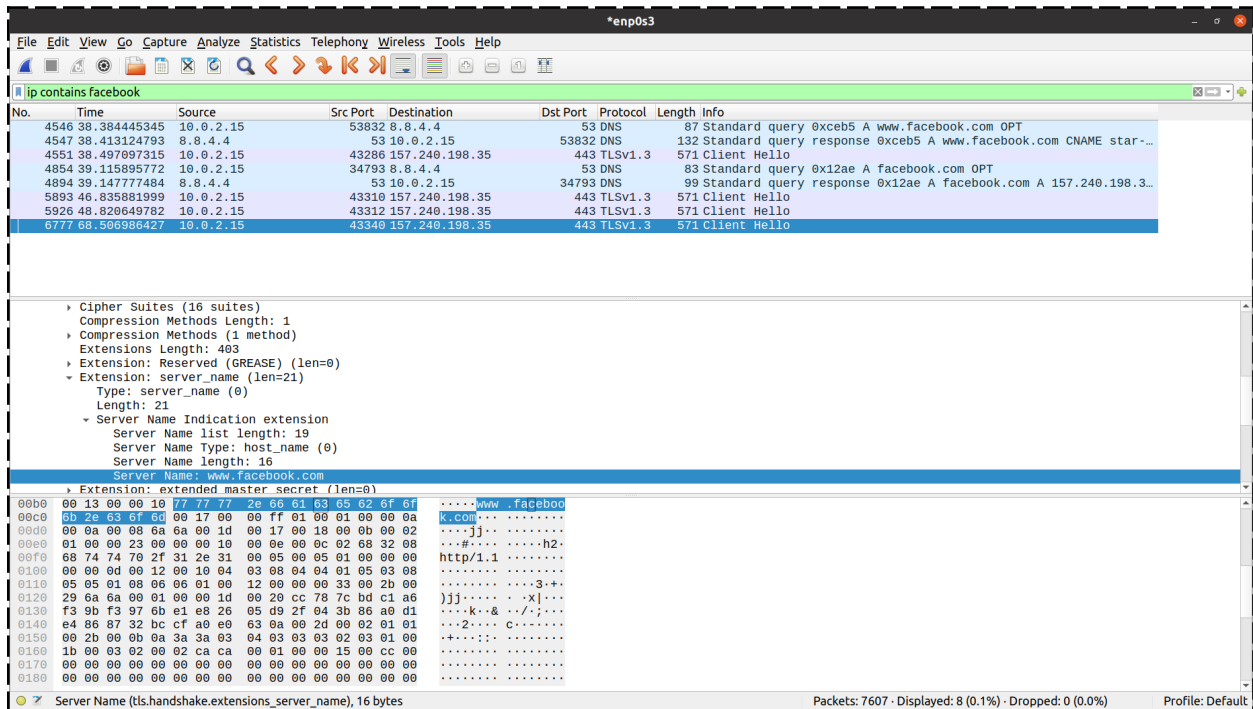
No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
5552	42.692086615	10.0.2.15	52973	8.8.4.4	53	DNS	90	Standard query 0x4991 A clients6.google.com OPT
5555	42.718412235	8.8.4.4	53	10.0.2.15	52973	DNS	130	Standard query response 0x4991 A clients6.google.com CNAME cl...
6313	61.317634181	10.0.2.15	56203	8.8.4.4	53	DNS	90	Standard query 0x970f A accounts.google.com OPT
6320	61.344923982	8.8.4.4	53	10.0.2.15	56203	DNS	106	Standard query response 0x970f A accounts.google.com A 172.21...
6722	67.413822242	10.0.2.15	40372	172.217.167.238	443	TLSv1.3	571	Client Hello
6820	68.874190834	10.0.2.15	40887	8.8.4.4	53	DNS	91	Standard query 0xe83a A fonts.googleapis.com OPT
6835	68.902533499	8.8.4.4	53	10.0.2.15	40887	DNS	107	Standard query response 0xe83a A fonts.googleapis.com A 216.5...
7035	88.883208504	10.0.2.15	33098	216.58.200.165	443	TLSv1.3	571	Client Hello
7120	87.877760993	10.0.2.15	33100	216.58.200.165	443	TLSv1.3	571	Client Hello
7217	100.612820475	10.0.2.15	33104	216.58.200.165	443	TLSv1.3	571	Client Hello
7259	100.275533890	10.0.2.15	57045	8.8.4.4	53	DNS	85	Standard query 0xd7d4 A www.google.com OPT
7260	100.279991868	8.8.4.4	53	10.0.2.15	57045	DNS	101	Standard query response 0xd7d4 A www.google.com A 216.58.196...

Frame 7217: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_62:c3:94 (08:00:27:62:c3:94), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.200.165
Transmission Control Protocol, Src Port: 33104, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security

0000 52 54 00 12 35 02 08 00 27 62 c3 94 08 00 45 00 RT...5... 'b....E:
0010 02 2d af fd 00 00 40 06 db de 0a 00 02 0f d8 3a ...@... ..
0020 c8 a5 81 50 01 bb 1a f2 10 30 4b 03 42 02 50 18 ...P... ..OK:B:P:
0030 fa f9 af 0e 00 00 10 03 01 02 00 01 00 01 fc 03
0040 03 04 db 5e 05 c4 05 4d 76 bf 9c 2d 25 9c f0 0c ...Ae..M...%..
0050 a3 9f 33 b0 0a 54 10 f4 0b 9a 81 b5 5f 88 19 78 ...3..T... ..x
0060 0a 20 d4 30 10 20 a1 78 72 a9 f5 27 f0 90 fe dax r... ..
0070 44 d2 5a 68 ec fa b5 25 da 3a 2f 8d 05 39 58 36 D.Zh...% :/- 9X6
0080 4b b8 00 20 5a 5a 13 01 13 02 13 03 c0 2b c0 2f K...ZZ... ..+/
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d
00a0 00 2f 00 35 01 00 01 93 9a 9a 00 00 00 00 14
00b0 00 12 00 00 0f 0d 01 03 6c 2e 07 0f 0f 07 0c 65 ...mai l.google
00c0 2e 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 ...com... ..
00d0 0a 00 08 9a 9a 00 1d 00 17 00 18 00 00 00 02 01

Wireshark - enp0s3_20210203024045_gcdUsc.pcapng Packets: 7607 - Displayed: 58 (0.8%) - Dropped: 0 (0.0%) Profile: Default

For www.facebook.com



The image shows a Wireshark packet capture for the domain www.facebook.com. The top pane displays a list of network packets. Packet 6777 is selected, showing a TLSv1.3 Client Hello. The middle pane shows the packet details, including the TLSv1.3 Client Hello structure. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates 7607 packets displayed, with 8 (0.1%) displayed and 0 (0.0%) dropped.

No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
4546	38.384445345	10.0.2.15	53832	8.8.4.4	53	DNS	87	Standard query 0xceb5 A www.facebook.com OPT
4547	38.413124793	8.8.4.4	53	10.0.2.15	53832	DNS	132	Standard query response 0xceb5 A www.facebook.com CNAME star...
4551	38.497097315	10.0.2.15	43286	157.240.198.35	443	TLSv1.3	571	Client Hello
4854	39.115895772	10.0.2.15	34793	8.8.4.4	53	DNS	83	Standard query 0x12ae A facebook.com OPT
4894	39.147777484	8.8.4.4	53	10.0.2.15	34793	DNS	99	Standard query response 0x12ae A facebook.com A 157.240.198.3...
5893	46.835881999	10.0.2.15	43310	157.240.198.35	443	TLSv1.3	571	Client Hello
5926	48.820649782	10.0.2.15	43312	157.240.198.35	443	TLSv1.3	571	Client Hello
6777	68.506986427	10.0.2.15	43340	157.240.198.35	443	TLSv1.3	571	Client Hello

Cipher Suites (16 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 403
Extension: Reserved (GREASE) (len=0)
Extension: server_name (len=21)
Type: server_name (0)
Length: 21
Server Name Indication extension
Server Name list length: 19
Server Name Type: host_name (0)
Server Name length: 16
Server Name: www.facebook.com
Extension: extended_master_secret (len=0)

00b0 00 13 00 00 10 77 77 77 2e 66 61 03 65 62 6f 6f ...www .facebook
00c0 0b 2e 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a ...k.com... ..
00d0 00 0a 00 08 6a 6a 00 1d 00 17 00 18 00 0b 00 02 ...jj... ..
00e0 01 00 00 23 00 00 10 00 0e 00 0c 02 68 32 08 ...#... ..h2..
00f0 68 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 http/1.1
0100 00 00 00 00 12 00 10 04 03 08 04 04 01 05 03 08
0110 05 05 01 08 06 06 01 00 12 00 00 00 33 00 2b 00x+..
0120 29 6a 6a 00 01 00 00 1d 00 20 cc 78 7c bd c1 a6)jj... ..x|...
0130 f3 9b f3 97 6b e1 e8 26 05 d9 2f 04 3b 86 a0 d1 ...k...&... ..
0140 e4 86 87 32 bc cf a0 e0 63 0a 00 2d 00 02 01 01 ...2... ..c...
0150 00 2b 00 00 0a 3a 0a 03 04 03 03 03 02 03 01 00
0160 1b 00 03 02 00 02 ca 0a 00 01 00 00 15 00 cc 00
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Server Name (tls.handshake.extensions_server_name), 16 bytes Packets: 7607 - Displayed: 8 (0.1%) - Dropped: 0 (0.0%) Profile: Default

5) Name all the protocols which you have encountered during the sniffing operation. Explain their functionalities.

i) DNS

DNS stands for Domain Name System. DNS servers translate a human-friendly name, like "example.com", to a machine-friendly IP address, like 192.168.2.1.

ii) TLS

TLS stands for Transport Layer Security. It encrypts the data sent over the Internet to ensure data security.

iii) TCP

***TCP** (Transmission Control **Protocol**) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data.*

iv) IP

The Internet Protocol is the protocol which pretty much dictates how data(in form of datagrams) is transmitted to and from the internet.

v) UDP

Universal Datagram Protocol provides a connectionless service and without error recovery. It uses no acknowledgement, not resequence the messages and sets up no flow control.

vi) HTTP

HTTP: A client-server protocol which allows the fetching of resources and data exchange on the Web such as HTML.

(Screenshots attached below)

52300 UDP	254 443 → 52300
443 UDP	75 52300 → 443
80 HTTP	365 GET /edge
49644 TCP	60 80 → 49644
49644 TCP	1482 80 → 49644
80 TCP	54 49644 → 80
49644 TCP	2910 80 → 49644

36987 DNS	99 Sta
53 DNS	85 Sta
53 DNS	91 Sta
60696 DNS	135 Sta
51361 DNS	122 Sta
53 DNS	91 Sta
36131 DNS	138 Sta
53 DNS	96 Sta

37994 TLSv1.2	93 Application
443 TLSv1.2	93 Application
443 TLSv1.2	78 Application
40126 TLSv1.2	78 Application
51402 TLSv1.2	85 Encrypted A
51398 TLSv1.2	85 Encrypted A
53676 TLSv1.2	106 Application
53676 TLSv1.2	85 Application
53676 TLSv1.2	93 Application
443 TLSv1.2	93 Application