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.

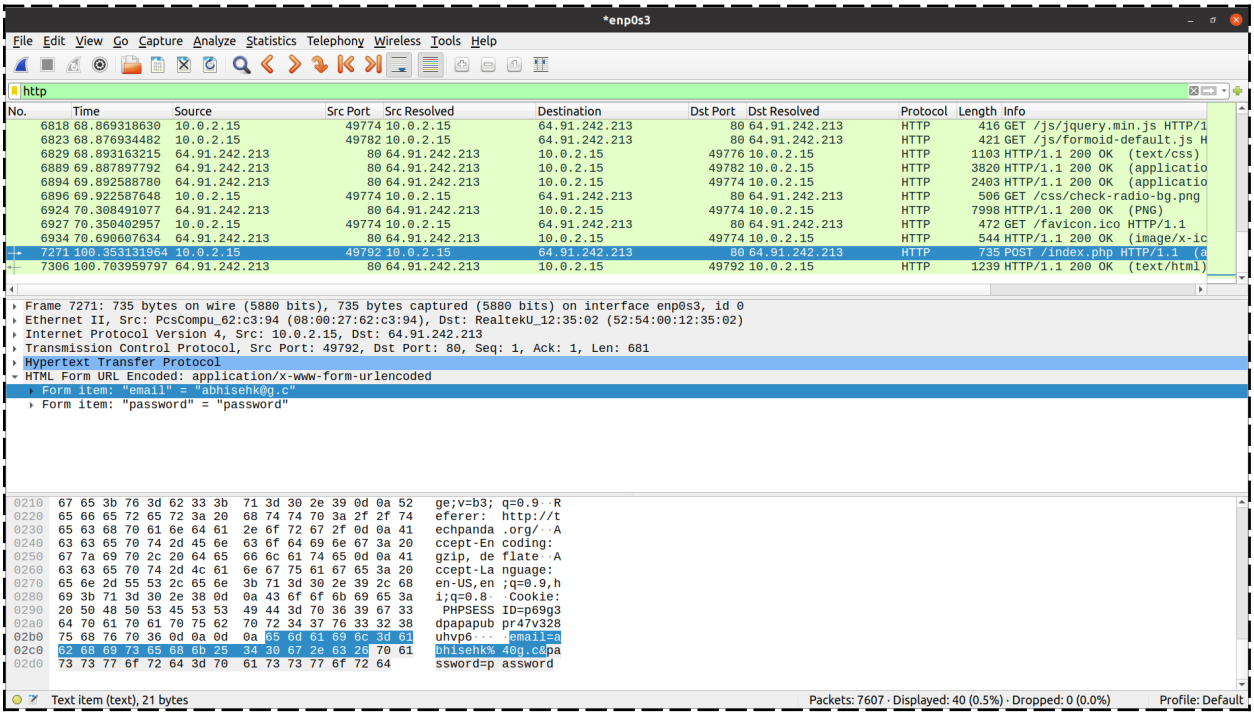
No.	Time	Src IP	Source	Src Port	Dst IP	Destination	Dst Port	Protocol	Length	Info
111	1.407280662	10.0.2.15	linux.local	37089	8.8.4.4	dns.google	53	DNS	93	Standard query 0x8e5b A stor
113	1.495050098	8.8.4.4	dns.google	53	10.0.2.15	linux.local	37089	DNS	301	Standard query response 0x8e
117	1.573198302	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/khaoiebndk
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`

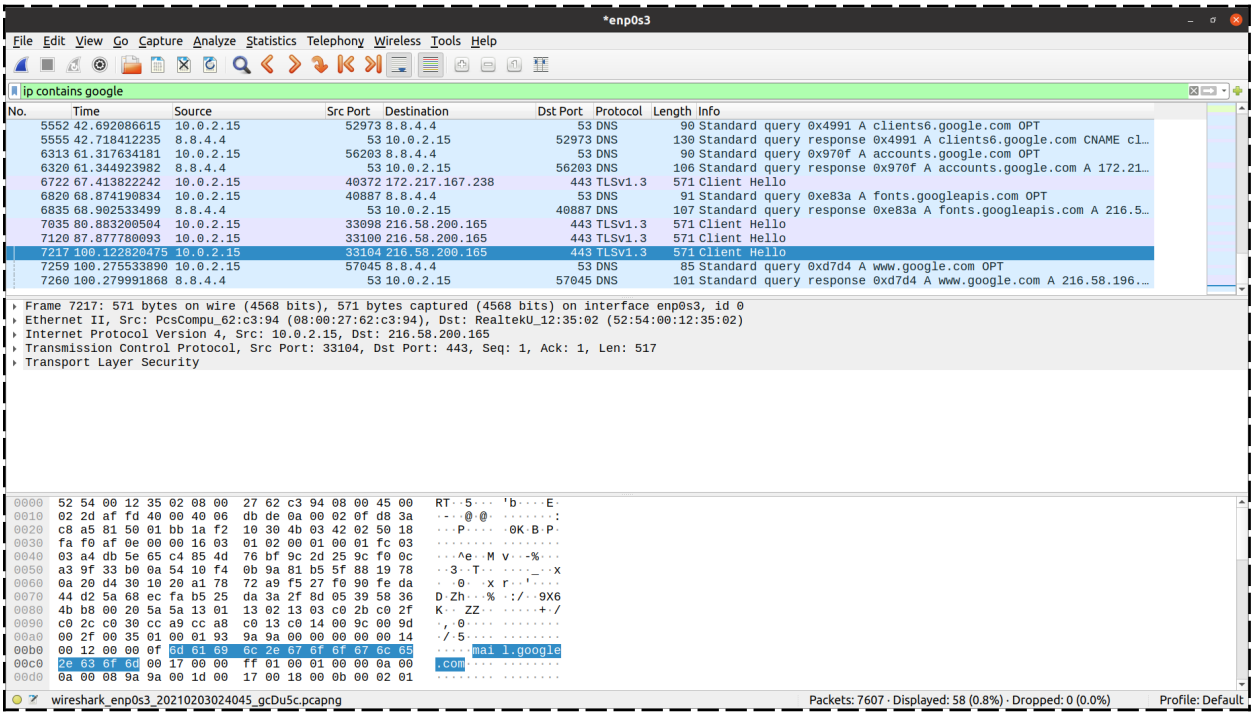


While the HTTPS POST messages can't be sniffed, thus we won't be able to sniff POST messages for Gmail and Facebook. (Screenshots attached below)

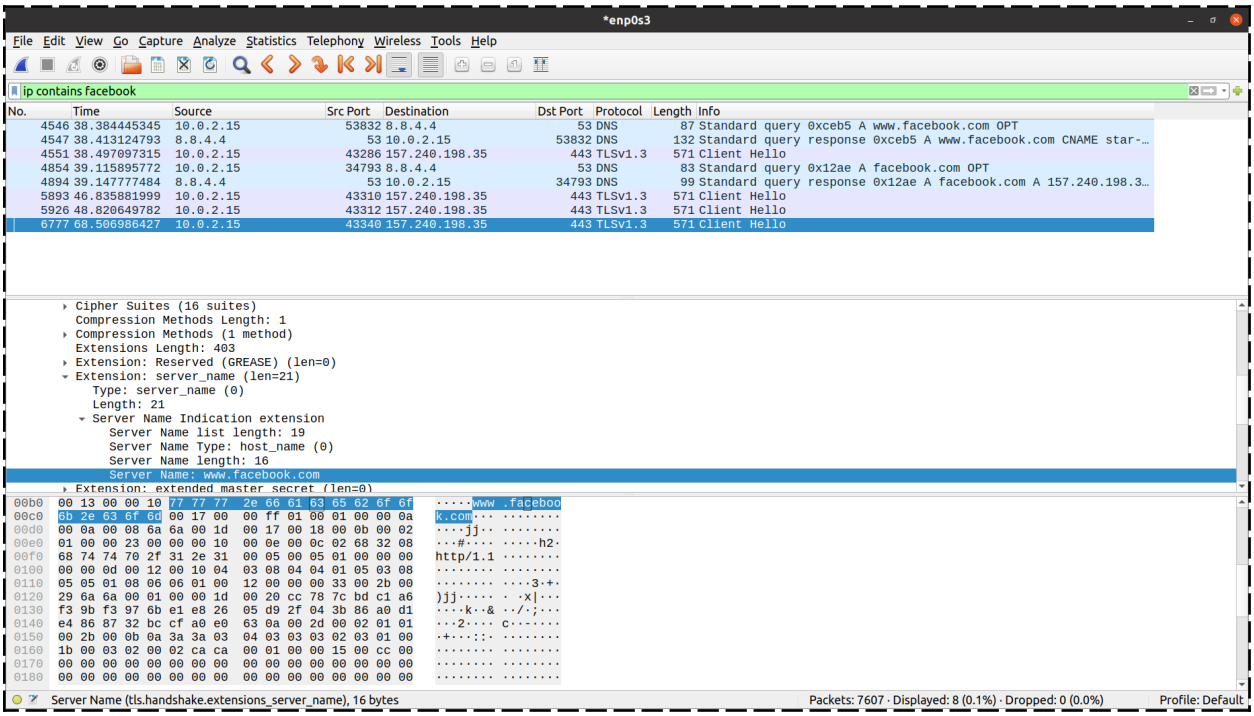
4) Could you sniff the credential information for all the websites? (Yes/No) Give reasons with substantiated result screenshot.

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



For www.facebook.com



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 → 52
443	UDP	75	52300 →
80	HTTP	365	GET /edg
49644	TCP	60	80 → 496
49644	TCP	1482	80 → 496
80	TCP	54	49644 →
49644	TCP	2910	80 → 496

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 Al
51398	TLSv1.2	85	Encrypted Al
53676	TLSv1.2	106	Application
53676	TLSv1.2	85	Application
53676	TLSv1.2	93	Application
443	TLSv1.2	93	Application