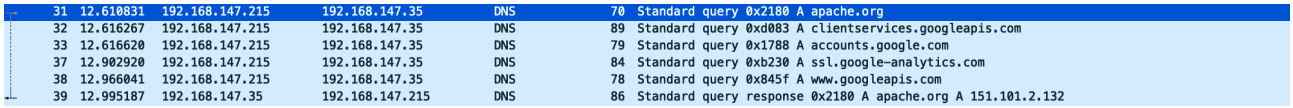
Assignment 1
COL334

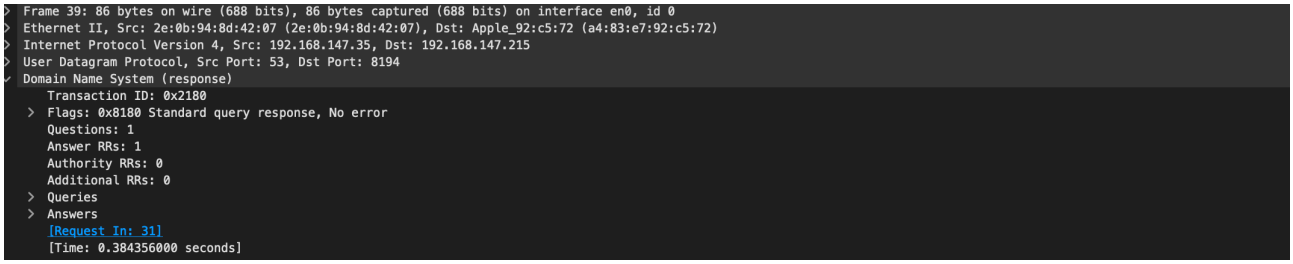
Name : Siddhesh Kalekar Entry No : 2019CS50436

Part 2. Packet Analysis

a)



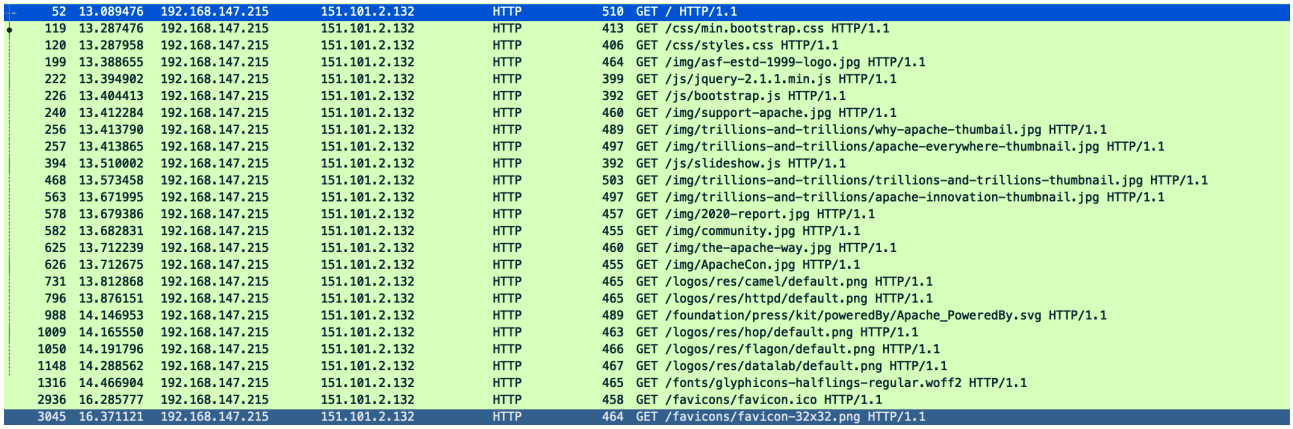
31	12.610831	192.168.147.215	192.168.147.35	DNS	70	Standard query 0x2180 A apache.org
32	12.616267	192.168.147.215	192.168.147.35	DNS	89	Standard query 0xd083 A clientservices.googleapis.com
33	12.616620	192.168.147.215	192.168.147.35	DNS	79	Standard query 0x1788 A accounts.google.com
37	12.902920	192.168.147.215	192.168.147.35	DNS	84	Standard query 0xb230 A ssl.google-analytics.com
38	12.966041	192.168.147.215	192.168.147.35	DNS	78	Standard query 0x845f A www.googleapis.com
39	12.995187	192.168.147.35	192.168.147.215	DNS	86	Standard query response 0x2180 A apache.org A 151.101.2.132



```
> Frame 39: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: 2e:0b:94:8d:42:07 (2e:0b:94:8d:42:07), Dst: Apple_92:c5:72 (a4:83:e7:92:c5:72)
> Internet Protocol Version 4, Src: 192.168.147.35, Dst: 192.168.147.215
> User Datagram Protocol, Src Port: 53, Dst Port: 8194
v Domain Name System (response)
    Transaction ID: 0x2180
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 31]
    [Time: 0.384356000 seconds]
```

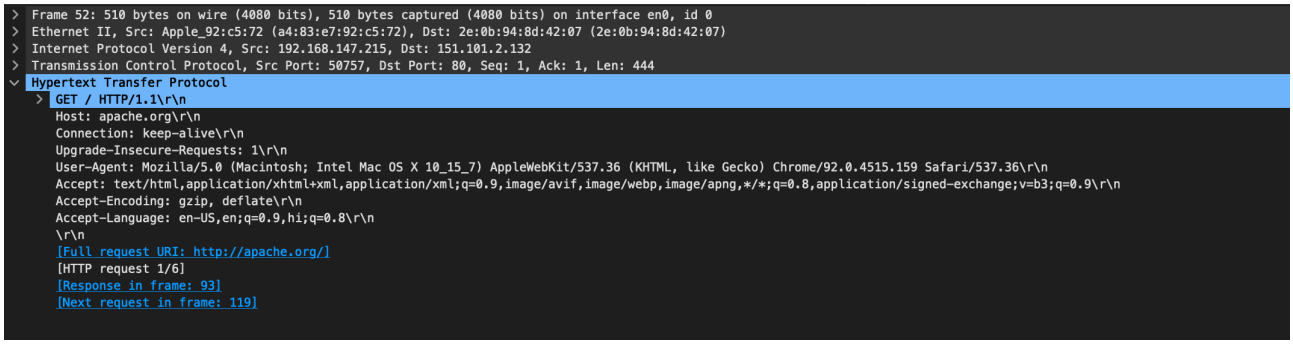
[Time: 0.384356000 seconds]

b)



52	13.089476	192.168.147.215	151.101.2.132	HTTP	510	GET / HTTP/1.1
119	13.287476	192.168.147.215	151.101.2.132	HTTP	413	GET /css/min.bootstrap.css HTTP/1.1
120	13.287958	192.168.147.215	151.101.2.132	HTTP	406	GET /css/styles.css HTTP/1.1
199	13.388655	192.168.147.215	151.101.2.132	HTTP	464	GET /img/asf-estd-1999-logo.jpg HTTP/1.1
222	13.394902	192.168.147.215	151.101.2.132	HTTP	399	GET /js/jquery-2.1.1.min.js HTTP/1.1
226	13.404413	192.168.147.215	151.101.2.132	HTTP	392	GET /js/bootstrap.js HTTP/1.1
240	13.412284	192.168.147.215	151.101.2.132	HTTP	460	GET /img/support-apache.jpg HTTP/1.1
256	13.413790	192.168.147.215	151.101.2.132	HTTP	489	GET /img/trillions-and-trillions/why-apache-thumbail.jpg HTTP/1.1
257	13.413865	192.168.147.215	151.101.2.132	HTTP	497	GET /img/trillions-and-trillions/apache-everywhere-thumbnail.jpg HTTP/1.1
394	13.510002	192.168.147.215	151.101.2.132	HTTP	392	GET /js/slideshow.js HTTP/1.1
468	13.573458	192.168.147.215	151.101.2.132	HTTP	503	GET /img/trillions-and-trillions/trillions-and-trillions-thumbnail.jpg HTTP/1.1
563	13.671995	192.168.147.215	151.101.2.132	HTTP	497	GET /img/trillions-and-trillions/apache-innovation-thumbnail.jpg HTTP/1.1
578	13.679386	192.168.147.215	151.101.2.132	HTTP	457	GET /img/2020-report.jpg HTTP/1.1
582	13.682831	192.168.147.215	151.101.2.132	HTTP	455	GET /img/community.jpg HTTP/1.1
625	13.712239	192.168.147.215	151.101.2.132	HTTP	460	GET /img/the-apache-way.jpg HTTP/1.1
626	13.712675	192.168.147.215	151.101.2.132	HTTP	455	GET /img/ApacheCon.jpg HTTP/1.1
731	13.812868	192.168.147.215	151.101.2.132	HTTP	465	GET /logos/res/camel/default.png HTTP/1.1
796	13.876151	192.168.147.215	151.101.2.132	HTTP	465	GET /logos/res/httpd/default.png HTTP/1.1
988	14.146953	192.168.147.215	151.101.2.132	HTTP	489	GET /foundation/press/kit/poweredBy/Apache_PoweredBy.svg HTTP/1.1
1009	14.165550	192.168.147.215	151.101.2.132	HTTP	463	GET /logos/res/hop/default.png HTTP/1.1
1050	14.191796	192.168.147.215	151.101.2.132	HTTP	466	GET /logos/res/flagon/default.png HTTP/1.1
1148	14.288562	192.168.147.215	151.101.2.132	HTTP	467	GET /logos/res/datalab/default.png HTTP/1.1
1316	14.466904	192.168.147.215	151.101.2.132	HTTP	465	GET /fonts/glyphicons-halflings-regular.woff2 HTTP/1.1
2936	16.285777	192.168.147.215	151.101.2.132	HTTP	458	GET /favicons/favicon.ico HTTP/1.1
3045	16.371121	192.168.147.215	151.101.2.132	HTTP	464	GET /favicons/favicon-32x32.png HTTP/1.1

25 HTTP requests were generated. Webpage is constructed by using various layers. Those layers are sent as packets one by one.
Example in the above requests : HTTP -> CSS -> js -> imp -> logos -> fonts -> icons, these are the layers involved.

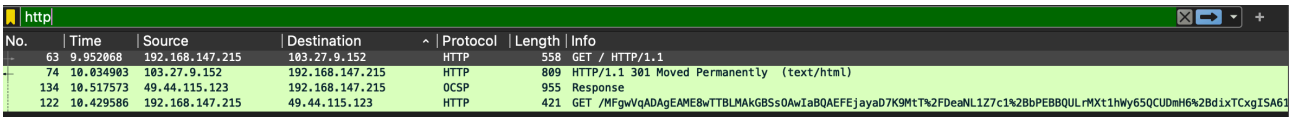


c)

31.	12.610831sec	192.168.147.215	192.168.147.35	DNS	70	Standard query 0x2180 A apache.org
3045.	16.371121 sec	192.168.147.215.	151.101.2.132	HTTP	464	GET /favicons/favicon-32x32.png HTTP/1.1

Total time taken = 16.371121 - 12.610831 = 3.760290 seconds

d)



No HTTP traffic found compared to apache.org .
https://www.cse.iitd.ac.in/ uses https .

The S in HTTPS stands for "secure." HTTPS uses TLS (or SSL) to encrypt HTTP requests and responses, so in the example above, instead of the text, an attacker would see a bunch of seemingly random characters.

Hence, there is no http traffic as it's encrypted(secure).