COMPUTER NETWORKS LABORATORY

WIRESHARK

Mr
[COMPANY NAME]

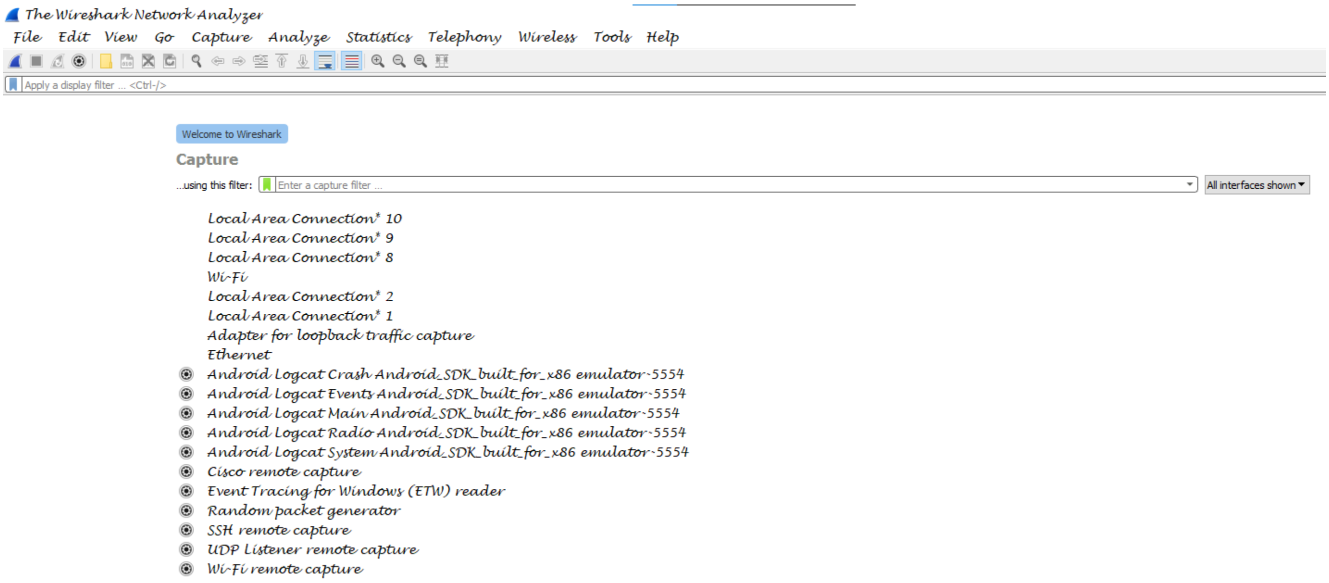
Questions

1. From your node please open the browser and do web surfing of your choice. Use “wireshark” to analyse the web traffic and show the communication from client to server in the application layer. Set the Ethernet card in promiscuous mode and capture all the packets that are transmitted through your node and do an analysis at each layer
2. From your node please open the browser and do web surfing of your choice. Use “wireshark” to analyse the web traffic and show the communication from client to server in the transport layer. Set the Ethernet card in promiscuous mode and capture all the packets that are transmitted through your node and do an analysis at each layer
3. Make a Google search for “apple”, use wireshark to analyse the web traffic and show the communication from client to server in the application layer
4. Analyze the web traffic which passes through port 21, transfer files and highlight the message transfer which is captured
5. Analyze the web traffic which passes through port 80, visit our college website and highlight the message transfer which is captured.

Steps to follow:

1. Use wireshark portable version (latest)
2. Use the internet with minimum speed of 200+ kb/s
3. Run wireshark as “Run as admin” mode only

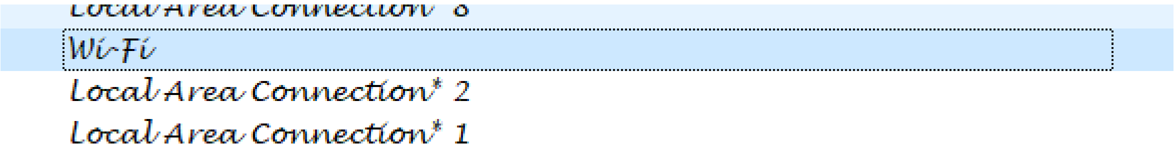
Interface of wireshark application


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
Android Logcat Crash Android_SDK_built_for_x86 emulator-5554
Android Logcat Events Android_SDK_built_for_x86 emulator-5554
Android Logcat Main Android_SDK_built_for_x86 emulator-5554
Android Logcat Radio Android_SDK_built_for_x86 emulator-5554
Android Logcat System Android_SDK_built_for_x86 emulator-5554
Cisco remote capture
Event Tracing for Windows (ETW) reader
Random packet generator
SSH remote capture
UDP Listener remote capture
Wi-Fi remote capture

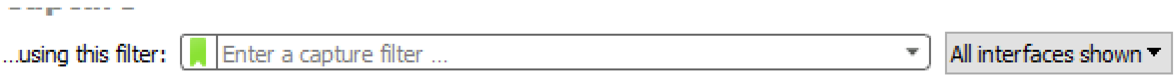
1. From your node please open the browser and do web surfing of your choice. Use “wireshark” to analyse the web traffic and show the communication from client to server in the application layer. Set the Ethernet card in promiscuous mode and capture all the packets that are transmitted through your node and do an analysis at each layer

   Steps:
   In application layer, we are going to capture the packets by using the http filter.
   First ensure that, the wireshark is run in admin mode or not
   Ensure the wifi is selected or not

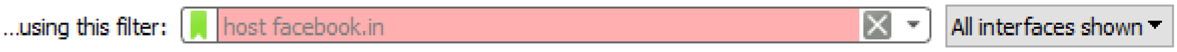


Local Area Connection* 8
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1

For college, ensure Ethernet is selected or not
Here we use facebook.in

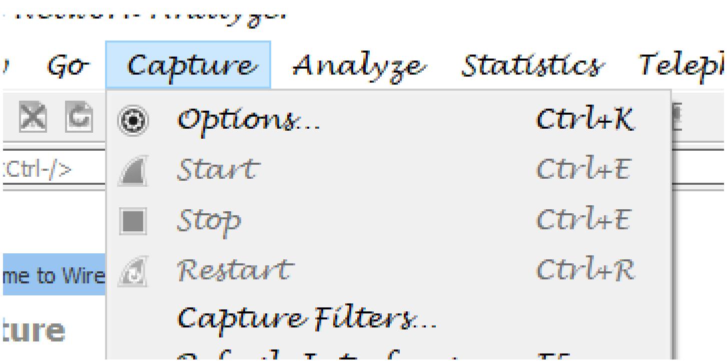


In this filter, type host facebook.in

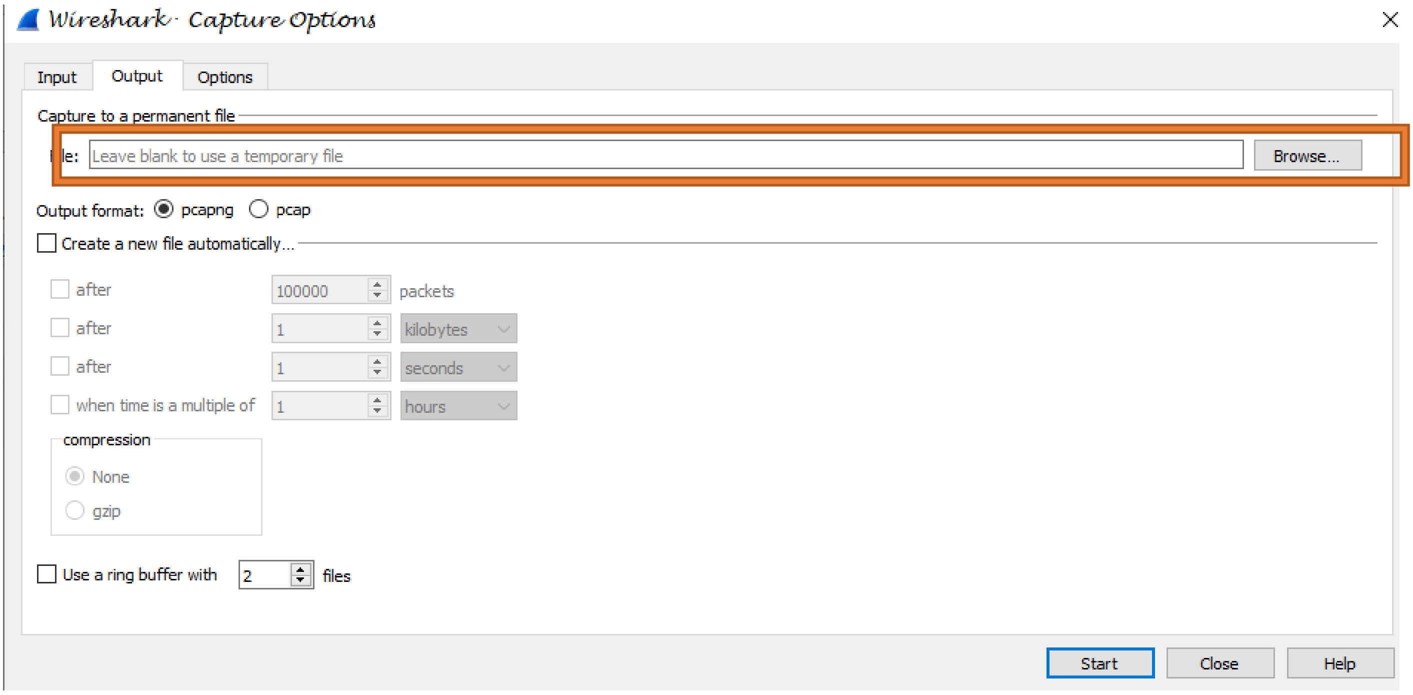


host facebook.in

Here, you see that the letters was in processing condition
After the background becomes green, you can choose the capture options from the top navbar



In this, browse the location to store the packets



Capture to a permanent file

File: Leave blank to use a temporary file

Output format: ● pcapng ○ pcap

□ Create a new file automatically...

□ after 100000 packets

□ after 1 kilobytes

□ after 1 seconds

□ when time is a multiple of 1 hours

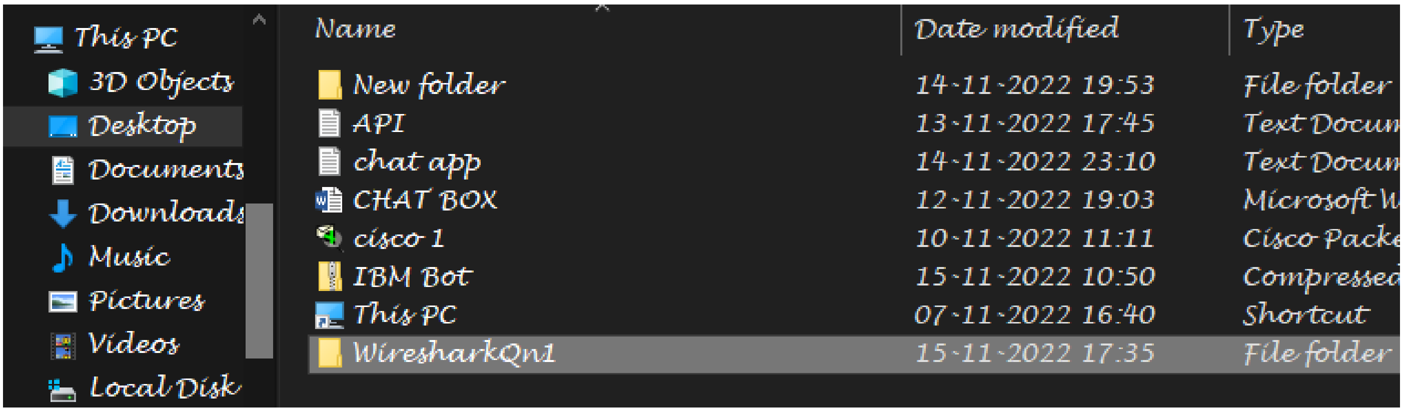
compression

● None

○ gzip

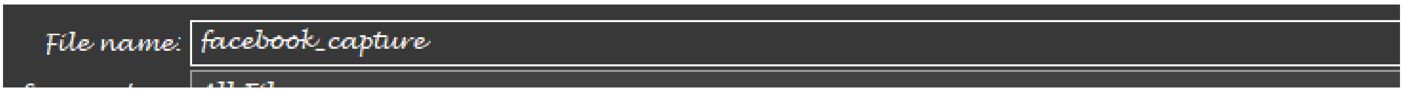
□ Use a ring buffer with 2 files

Create a new folder



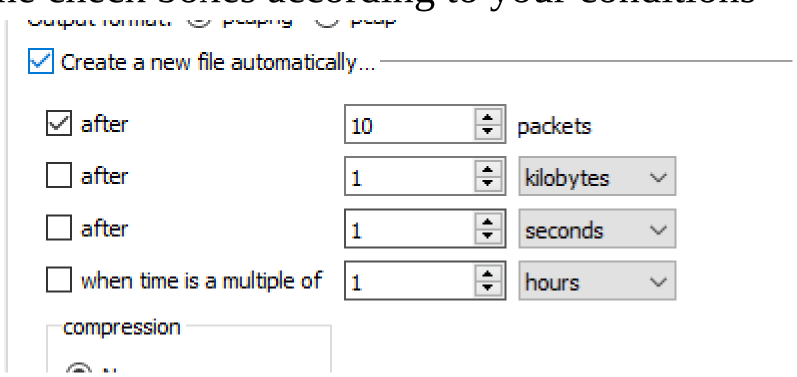
Name	Date modified	Type
New folder	14-11-2022 19:53	File folder
API	13-11-2022 17:45	Text Docum
chat app	14-11-2022 23:10	Text Docum
CHAT BOX	12-11-2022 19:03	Microsoft W
cisco 1	10-11-2022 11:11	Cisco Packe
IBM Bot	15-11-2022 10:50	Compressed
This PC	07-11-2022 16:40	Shortcut
WiresharkQn1	15-11-2022 17:35	File folder

File name doesnot contains white spaces



File name: facebook_capture

Enable the check boxes according to your conditions



Output format: ○ pcapng ○ pcap

☑ Create a new file automatically…

☑ after 10 packets

□ after 1 kilobytes

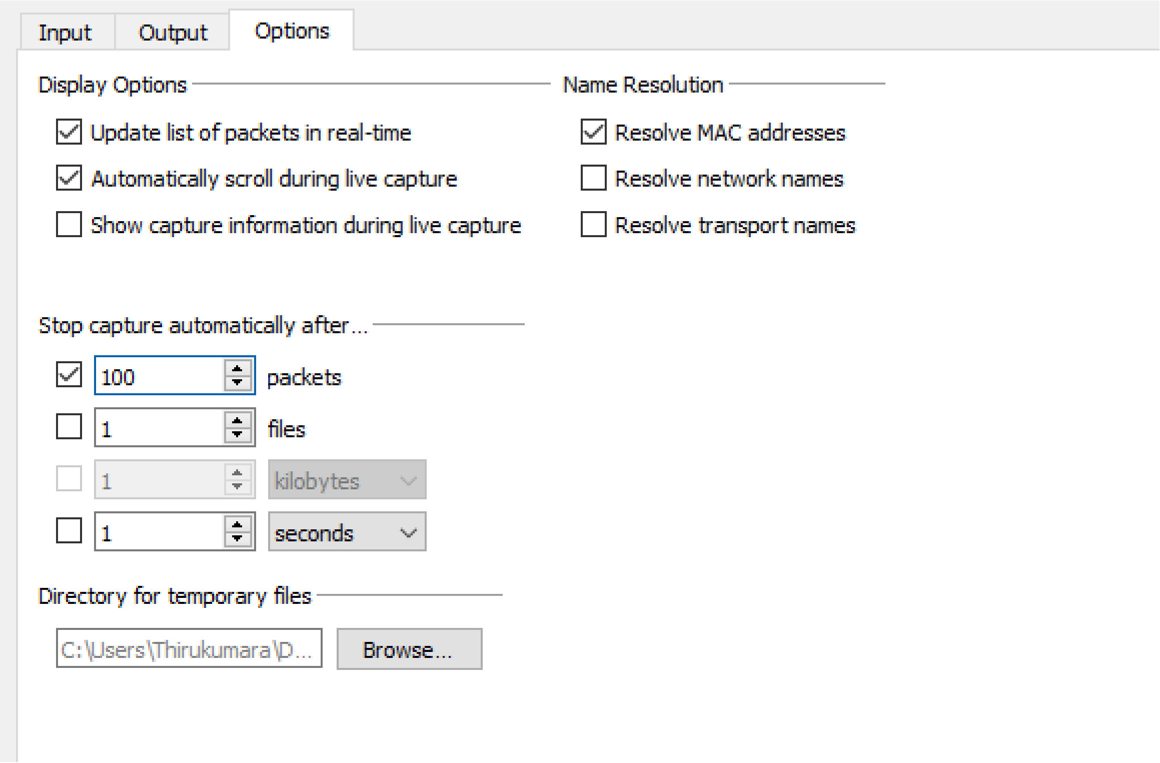
□ after 1 seconds

□ when time is a multiple of 1 hours

compression

Here, it is to ensure that how many files is to be created

In the options panel, you can set the limit of files



Display Options

☑ Update list of packets in real-time

☑ Automatically scroll during live capture

□ Show capture information during live capture

Name Resolution

☑ Resolve MAC addresses

□ Resolve network names

□ Resolve transport names

Stop capture automatically after…

☑ 100 packets

□ 1 files

□ 1 kilobytes

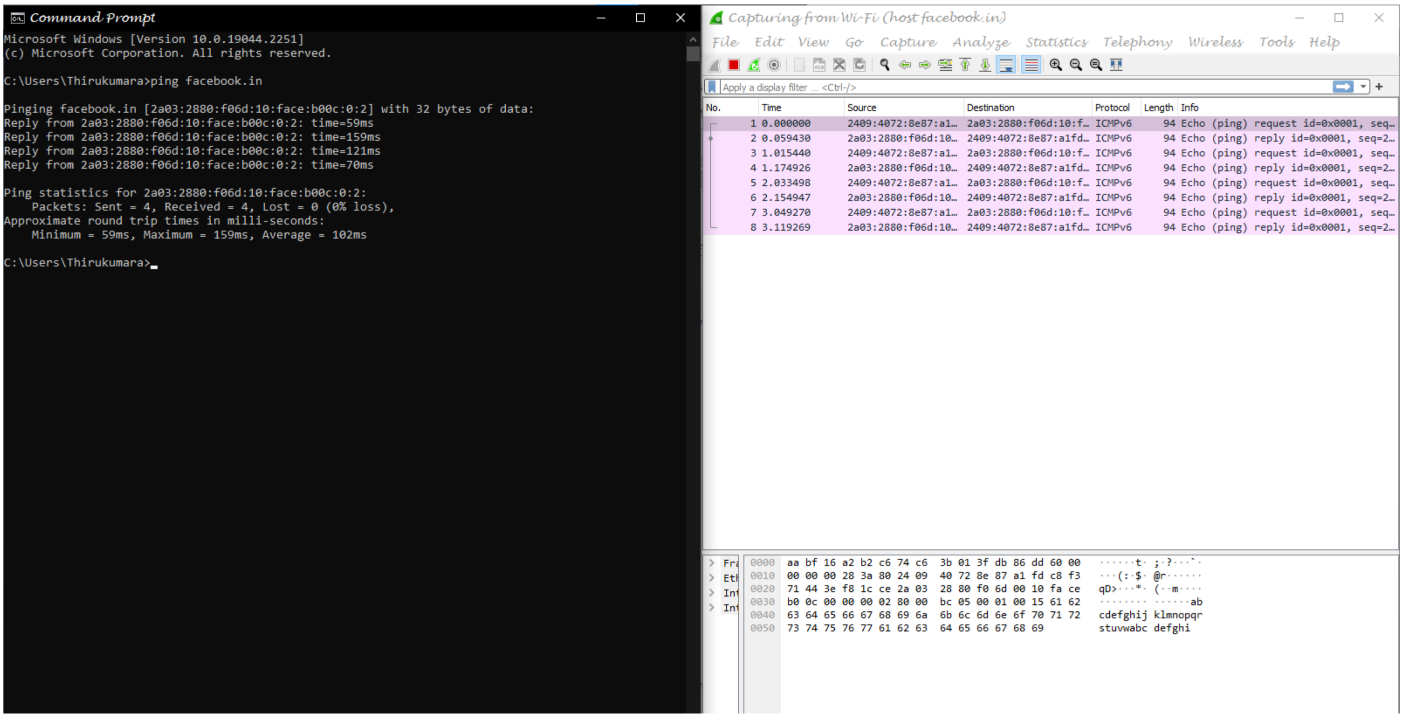
□ 1 seconds

Directory for temporary files

C:\Users\Thirukumara\D…

Start capturing

After this, you can get the empty screen. Go to cmd, type ping facebook.in



```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Thirukumara>ping facebook.in

Pinging facebook.in [2a03:2880:f06d:10:face:b00c:0:2] with 32 bytes of data:
Reply from 2a03:2880:f06d:10:face:b00c:0:2: time=59ms
Reply from 2a03:2880:f06d:10:face:b00c:0:2: time=159ms
Reply from 2a03:2880:f06d:10:face:b00c:0:2: time=121ms
Reply from 2a03:2880:f06d:10:face:b00c:0:2: time=70ms

Ping statistics for 2a03:2880:f06d:10:face:b00c:0:2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 59ms, Maximum = 159ms, Average = 102ms

C:\Users\Thirukumara>_
```

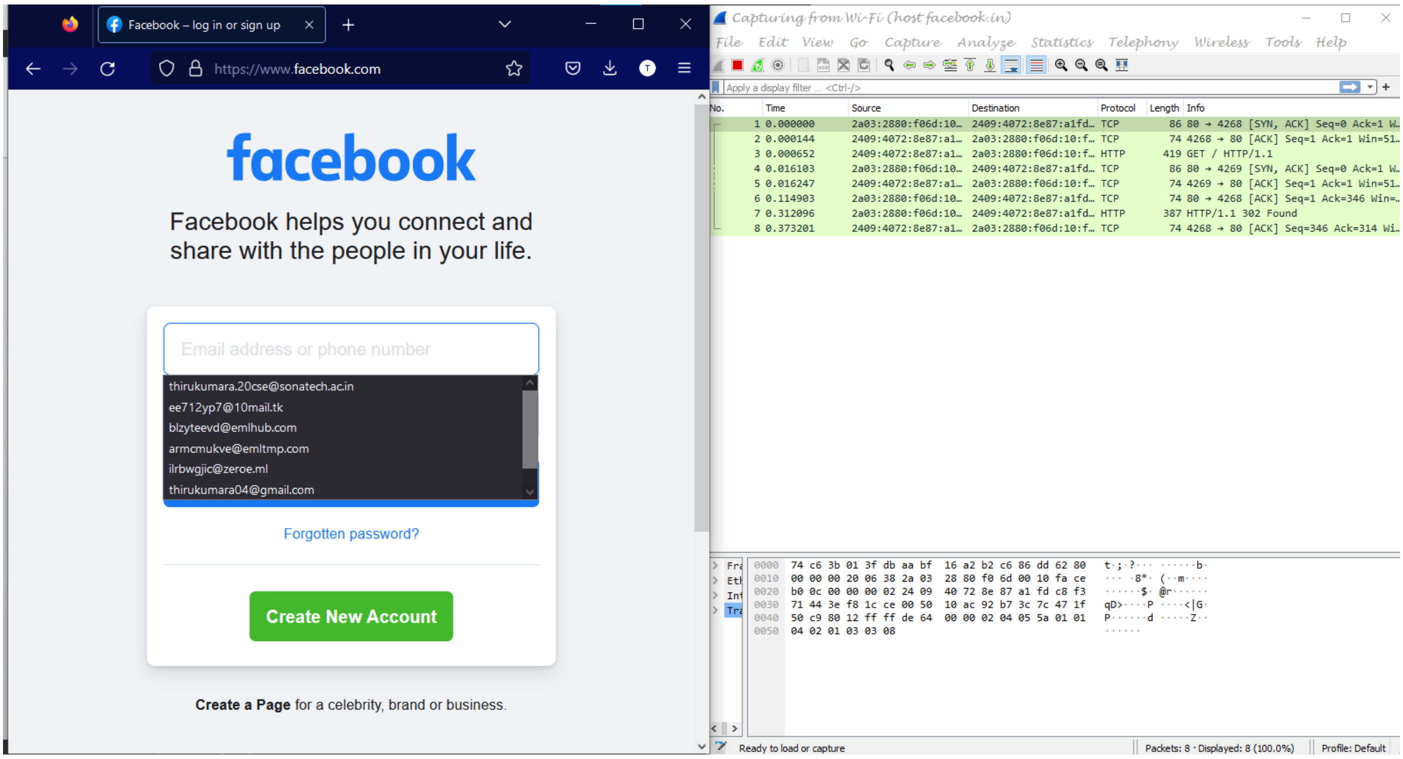
Capturing from Wi-Fi (host facebook.in)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source               Destination          Protocol Length Info
   1 0.000000  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… ICMPv6      94 Echo (ping) request id=0x0001, seq…
   2 0.059430  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… ICMPv6      94 Echo (ping) reply id=0x0001, seq=2…
   3 1.015440  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… ICMPv6      94 Echo (ping) request id=0x0001, seq…
   4 1.174926  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… ICMPv6      94 Echo (ping) reply id=0x0001, seq=2…
   5 2.033498  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… ICMPv6      94 Echo (ping) request id=0x0001, seq…
   6 2.154947  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… ICMPv6      94 Echo (ping) reply id=0x0001, seq=2…
   7 3.049270  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… ICMPv6      94 Echo (ping) request id=0x0001, seq…
   8 3.119269  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… ICMPv6      94 Echo (ping) reply id=0x0001, seq=2…
```

```
> Fra   0000  aa bf 16 a2 b2 c6 74 c6  3b 01 3f db 86 dd 60 00   ······t· ;·?···`·
> Eth   0010  00 00 00 28 3a 80 24 09  40 72 8e 87 a1 fd c8 f3   ···(:·$· @r······
> Int   0020  71 44 3e f8 1c ce 2a 03  28 80 f0 6d 00 10 fa ce   qD>···*· (··m····
> Int   0030  b0 0c 00 00 00 02 80 00  bc 05 00 01 00 15 61 62   ········ ······ab
        0040  63 64 65 66 67 68 69 6a  6b 6c 6d 6e 6f 70 71 72   cdefghij klmnopqr
        0050  73 74 75 76 77 61 62 63  64 65 66 67 68 69         stuvwabc defghi
```

.

Go to your browser and search for facebook.in



Facebook – log in or sign up
https://www.facebook.com
facebook

Facebook helps you connect and share with the people in your life.

Email address or phone number

thirukumara.20cse@sonatech.ac.in
ee712yp7@10mail.tk
blzyteevd@emlhub.com
armcmukve@emltmp.com
ilrbwgjic@zeroe.ml
thirukumara04@gmail.com

Forgotten password?
Create New Account

Create a Page for a celebrity, brand or business.

Capturing from Wi-Fi (host facebook.in)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source               Destination          Protocol Length Info
   1 0.000000  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… TCP         86 80 → 4268 [SYN, ACK] Seq=0 Ack=1 W…
   2 0.000144  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… TCP         74 4268 → 80 [ACK] Seq=1 Ack=1 Win=51…
   3 0.000652  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… HTTP       419 GET / HTTP/1.1
   4 0.016103  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… TCP         86 80 → 4269 [SYN, ACK] Seq=0 Ack=1 W…
   5 0.016247  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… TCP         74 4269 → 80 [ACK] Seq=1 Ack=1 Win=51…
   6 0.114903  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… TCP         74 80 → 4268 [ACK] Seq=1 Ack=346 Win=…
   7 0.312096  2a03:2880:f06d:10…   2409:4072:8e87:a1fd… HTTP       387 HTTP/1.1 302 Found
   8 0.373201  2409:4072:8e87:a1…   2a03:2880:f06d:10:f… TCP         74 4268 → 80 [ACK] Seq=346 Ack=314 Wi…
```

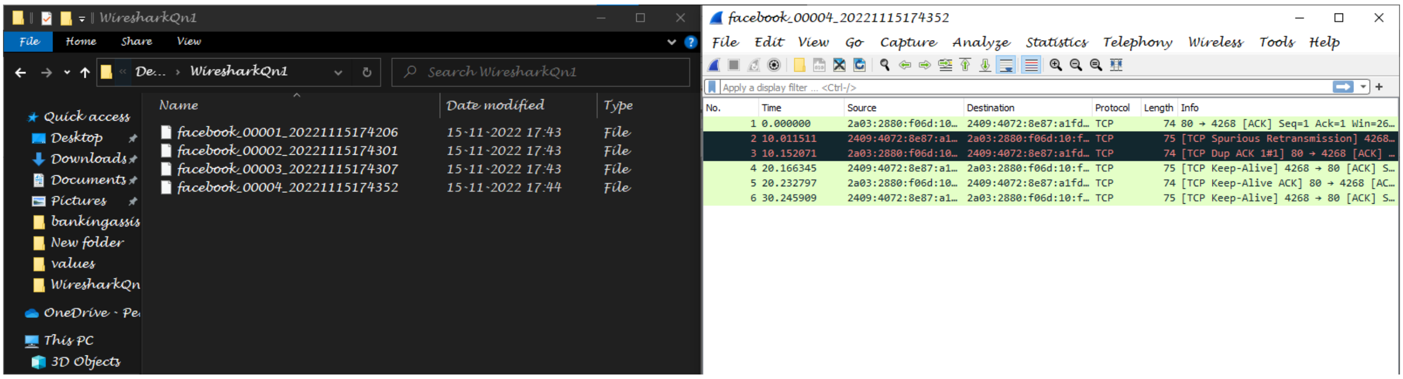
```
> Fra   0000  74 c6 3b 01 3f db aa bf  16 a2 b2 c6 86 dd 62 80   t·;·?··· ······b·
> Eth   0010  00 00 00 20 06 38 2a 03  28 80 f0 6d 00 10 fa ce   ··· ·8*· (··m····
> Int   0020  b0 0c 00 00 00 02 24 09  40 72 8e 87 a1 fd c8 f3   ······$· @r······
> Tra   0030  71 44 3e f8 1c ce 00 50  10 ac 92 b7 3c 7c 47 1f   qD>····P ····<|G·
        0040  50 c9 80 12 ff ff de 64  00 00 02 04 05 5a 01 01   P······d ·····Z··
        0050  04 02 01 03 03 08                                   ······

Ready to load or capture        Packets: 8 · Displayed: 8 (100.0%)        Profile: Default
```

Here you can see that some packets are captured and contains some protocols like tcp, udp, http and so on

In this, for our question 1, we need to capture the packets on application layer

So I use the filter called http

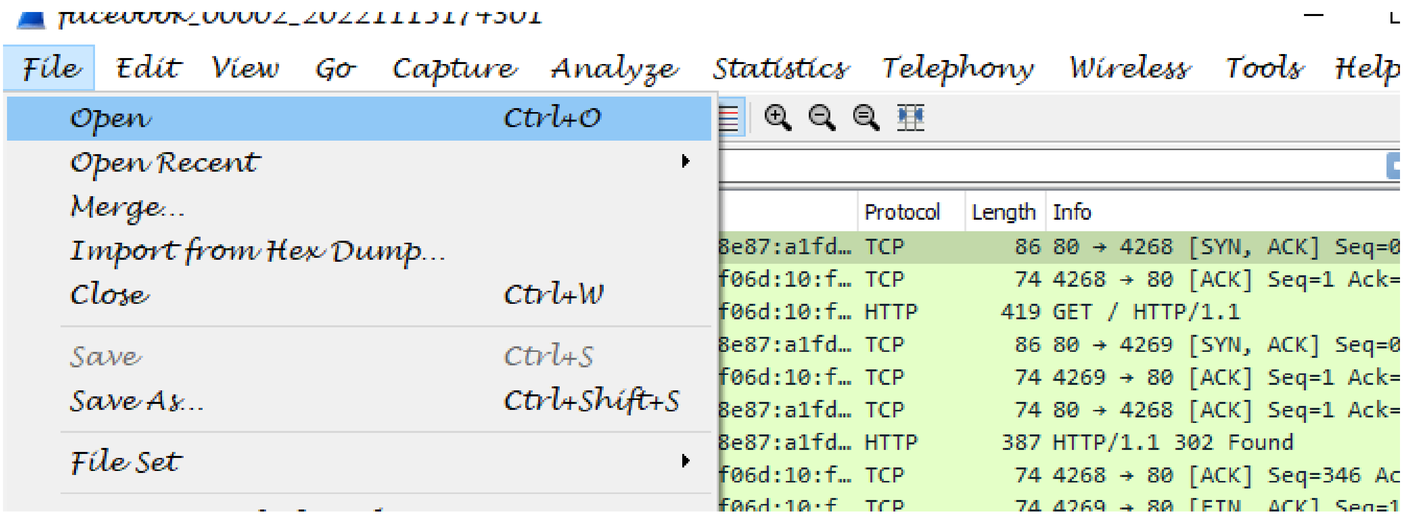
And you can see our packets are captured in the folder



Name	Date modified	Type
facebook_00001_20221115174206	15-11-2022 17:43	File
facebook_00002_20221115174301	15-11-2022 17:43	File
facebook_00003_20221115174307	15-11-2022 17:43	File
facebook_00004_20221115174352	15-11-2022 17:44	File

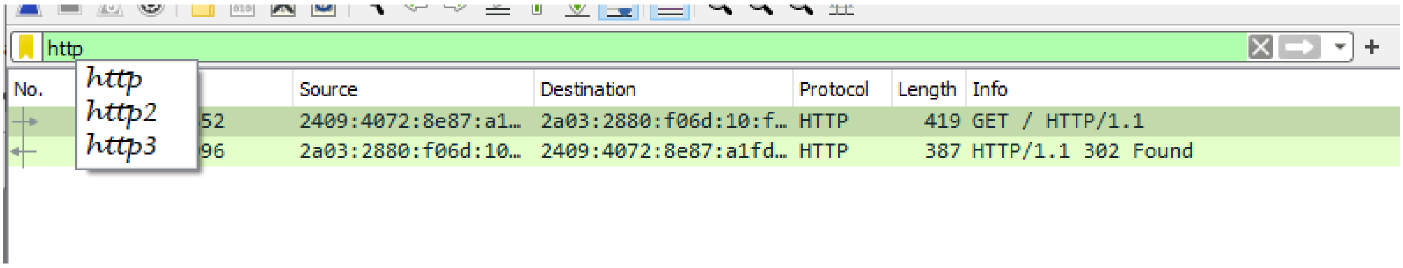
facebook_00004_20221115174352
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	TCP	74	80 → 4268 [ACK] Seq=1 Ack=1 Win=26…
2	10.011511	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	TCP	75	[TCP Spurious Retransmission] 4268…
3	10.152071	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	TCP	74	[TCP Dup ACK 1#1] 80 → 4268 [ACK] …
4	20.166345	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	TCP	75	[TCP Keep-Alive] 4268 → 80 [ACK] S…
5	20.232797	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	TCP	74	[TCP Keep-Alive ACK] 80 → 4268 [AC…
6	30.245909	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	TCP	75	[TCP Keep-Alive] 4268 → 80 [ACK] S…



	Protocol	Length	Info
8e87:a1fd…	TCP	86	80 → 4268 [SYN, ACK] Seq=0
f06d:10:f…	TCP	74	4268 → 80 [ACK] Seq=1 Ack=
f06d:10:f…	HTTP	419	GET / HTTP/1.1
8e87:a1fd…	TCP	86	80 → 4269 [SYN, ACK] Seq=0
f06d:10:f…	TCP	74	4269 → 80 [ACK] Seq=1 Ack=
8e87:a1fd…	TCP	74	80 → 4268 [ACK] Seq=1 Ack=
8e87:a1fd…	HTTP	387	HTTP/1.1 302 Found
f06d:10:f…	TCP	74	4268 → 80 [ACK] Seq=346 Ac
f06d:10:f	TCP	74	4269 → 80 [FIN, ACK] Seq=1

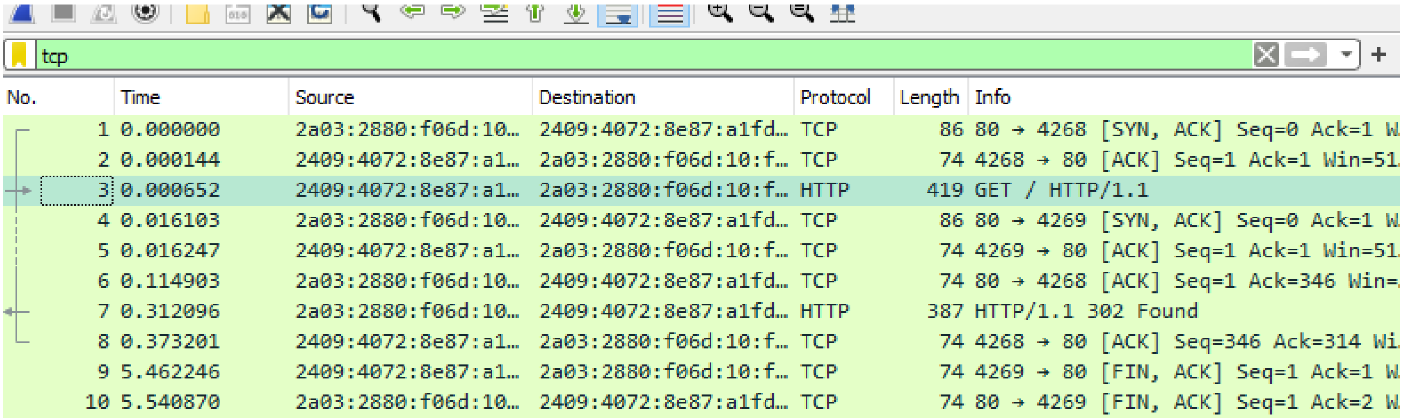
Use the http filter and we can capture the packets



No.		Source	Destination	Protocol	Length	Info
	52	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	HTTP	419	GET / HTTP/1.1
	96	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	HTTP	387	HTTP/1.1 302 Found

2. From your node please open the browser and do web surfing of your choice. Use “wireshark” to analyse the web traffic and show the communication from client to server in the transport layer. Set the Ethernet card in promiscuous mode and capture all the packets that are transmitted through your node and do an analysis at each layer

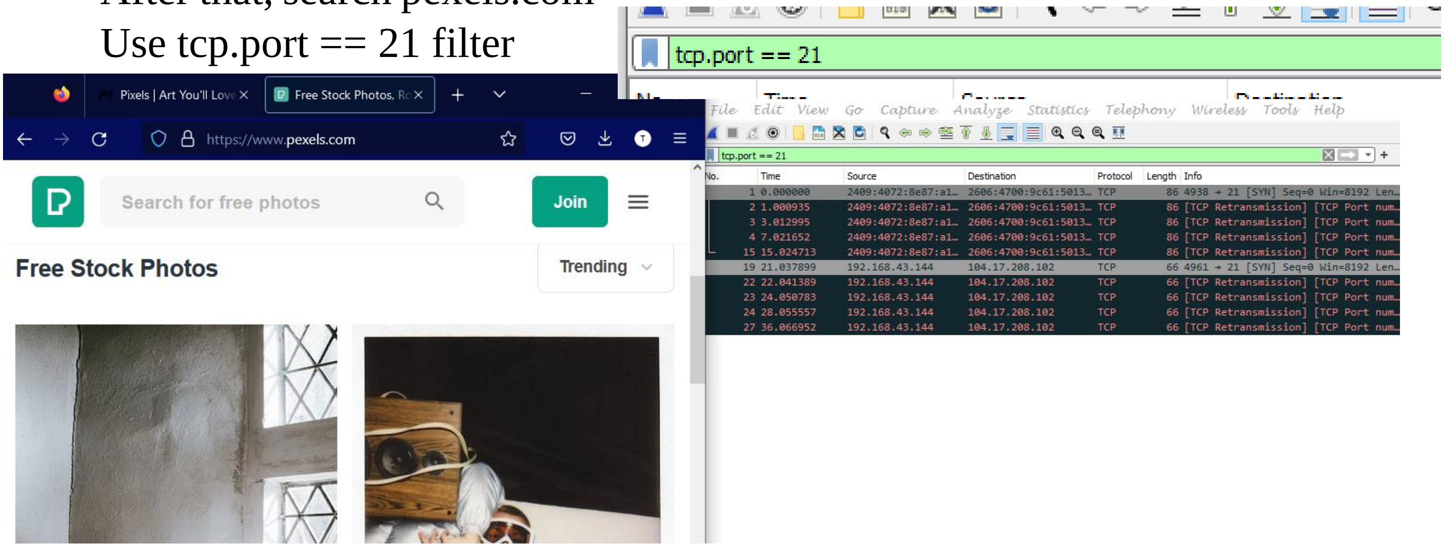
   Steps:
   The second question is same as like this
   Here we use tcp or udp filter
   Repeat all the process as same as first qn
   Use tcp or udp in the filter option
   Capture the packets



tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	TCP	86	80 → 4268 [SYN, ACK] Seq=0 Ack=1 W
2	0.000144	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	TCP	74	4268 → 80 [ACK] Seq=1 Ack=1 Win=51
3	0.000652	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	HTTP	419	GET / HTTP/1.1
4	0.016103	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	TCP	86	80 → 4269 [SYN, ACK] Seq=0 Ack=1 W
5	0.016247	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	TCP	74	4269 → 80 [ACK] Seq=1 Ack=1 Win=51
6	0.114903	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	TCP	74	80 → 4268 [ACK] Seq=1 Ack=346 Win=
7	0.312096	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	HTTP	387	HTTP/1.1 302 Found
8	0.373201	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	TCP	74	4268 → 80 [ACK] Seq=346 Ack=314 Wi
9	5.462246	2409:4072:8e87:a1…	2a03:2880:f06d:10:f…	TCP	74	4269 → 80 [FIN, ACK] Seq=1 Ack=1 W
10	5.540870	2a03:2880:f06d:10…	2409:4072:8e87:a1fd…	TCP	74	80 → 4269 [FIN, ACK] Seq=1 Ack=2 W

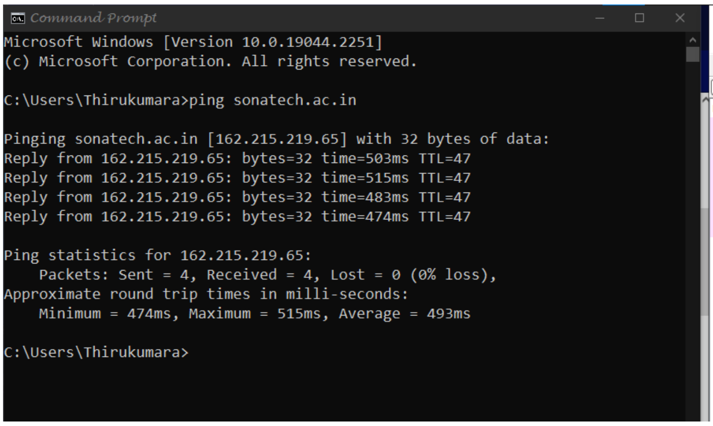
4. Analyze the web traffic which passes through port 21, transfer files and highlight the message transfer which is captured
   Here we use the ftp protocol, okay.
   So we use pexels.com and
   Use ftp pexels.com in cmd
   After that, search pexels.com
   Use tcp.port == 21 filter



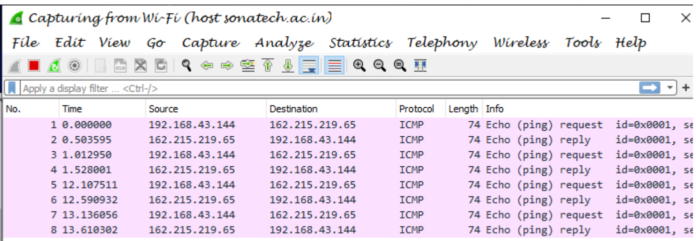
tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2409:4072:8e87:a1…	2606:4700:9c61:5013…	TCP	86	4938 → 21 [SYN] Seq=0 Win=8192 Len…
2	1.000935	2409:4072:8e87:a1…	2606:4700:9c61:5013…	TCP	86	[TCP Retransmission] [TCP Port num…
3	3.012995	2409:4072:8e87:a1…	2606:4700:9c61:5013…	TCP	86	[TCP Retransmission] [TCP Port num…
4	7.021652	2409:4072:8e87:a1…	2606:4700:9c61:5013…	TCP	86	[TCP Retransmission] [TCP Port num…
15	15.024713	2409:4072:8e87:a1…	2606:4700:9c61:5013…	TCP	86	[TCP Retransmission] [TCP Port num…
19	21.037899	192.168.43.144	104.17.208.102	TCP	66	4961 → 21 [SYN] Seq=0 Win=8192 Len…
22	22.041389	192.168.43.144	104.17.208.102	TCP	66	[TCP Retransmission] [TCP Port num…
23	24.050783	192.168.43.144	104.17.208.102	TCP	66	[TCP Retransmission] [TCP Port num…
24	28.055557	192.168.43.144	104.17.208.102	TCP	66	[TCP Retransmission] [TCP Port num…
27	36.066952	192.168.43.144	104.17.208.102	TCP	66	[TCP Retransmission] [TCP Port num…

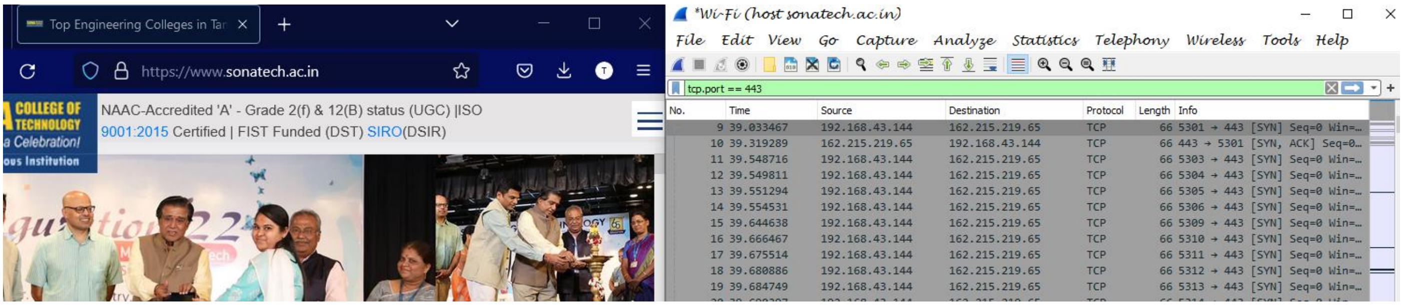
5. Analyze the web traffic which passes through port 80, visit our college website and highlight the message transfer which is captured.
   Here, while using port 80 for our college website, there is less number of network traffic. Sometimes we couldn't able to capture the traffics. So we use port 443



```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Thirukumara>ping sonatech.ac.in

Pinging sonatech.ac.in [162.215.219.65] with 32 bytes of data:
Reply from 162.215.219.65: bytes=32 time=503ms TTL=47
Reply from 162.215.219.65: bytes=32 time=515ms TTL=47
Reply from 162.215.219.65: bytes=32 time=483ms TTL=47
Reply from 162.215.219.65: bytes=32 time=474ms TTL=47

Ping statistics for 162.215.219.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 474ms, Maximum = 515ms, Average = 493ms

C:\Users\Thirukumara>
```


Capturing from Wi-Fi (host sonatech.ac.in)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.144	162.215.219.65	ICMP	74	Echo (ping) request id=0x0001, se
2	0.503595	162.215.219.65	192.168.43.144	ICMP	74	Echo (ping) reply id=0x0001, se
3	1.012950	192.168.43.144	162.215.219.65	ICMP	74	Echo (ping) request id=0x0001, se
4	1.528001	162.215.219.65	192.168.43.144	ICMP	74	Echo (ping) reply id=0x0001, se
5	12.107511	192.168.43.144	162.215.219.65	ICMP	74	Echo (ping) request id=0x0001, se
6	12.590932	162.215.219.65	192.168.43.144	ICMP	74	Echo (ping) reply id=0x0001, se
7	13.136056	192.168.43.144	162.215.219.65	ICMP	74	Echo (ping) request id=0x0001, se
8	13.610302	162.215.219.65	192.168.43.144	ICMP	74	Echo (ping) reply id=0x0001, se



Top Engineering Colleges in Tar

https://www.sonatech.ac.in

NAAC-Accredited 'A' - Grade 2(f) & 12(B) status (UGC) |ISO 9001:2015 Certified | FIST Funded (DST) SIRO(DSIR)

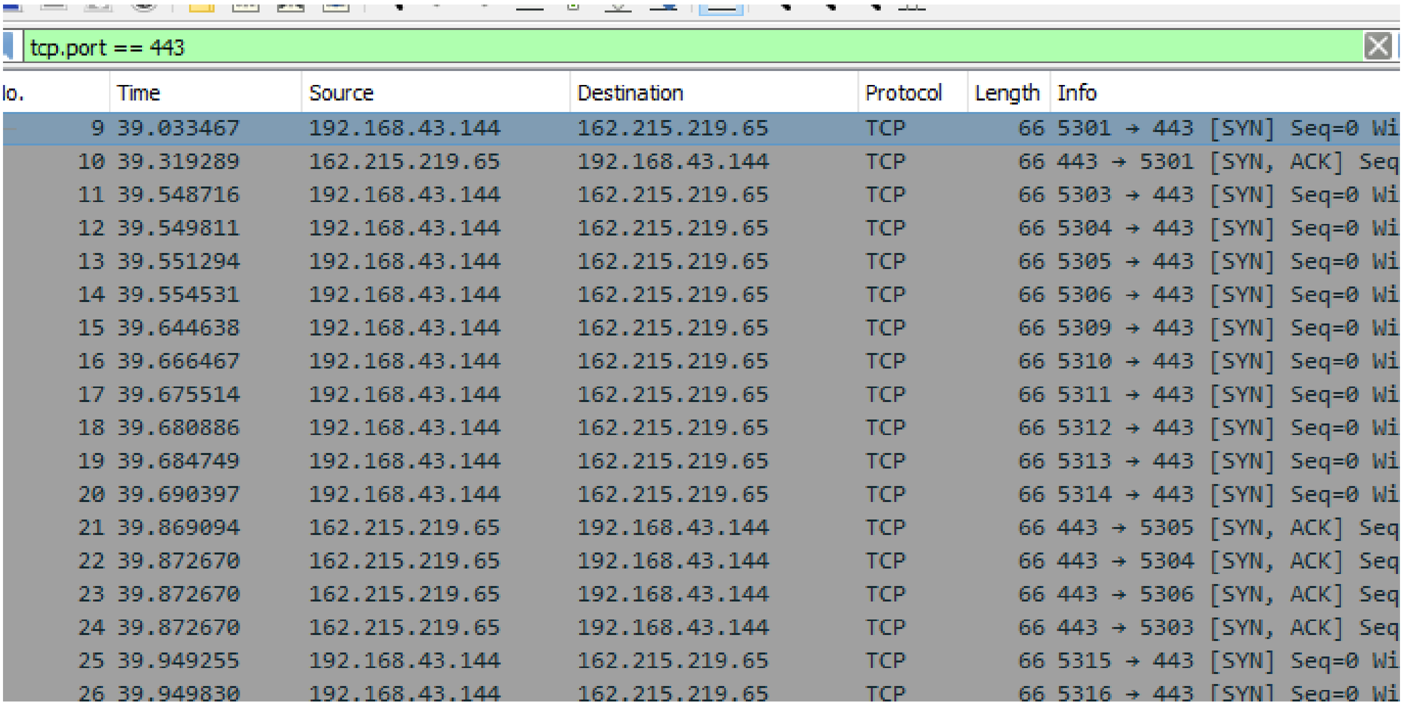
*Wi-Fi (host sonatech.ac.in)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

```
No.  Time       Source          Destination     Protocol Length Info
   9 39.033467  192.168.43.144  162.215.219.65  TCP      66 5301 → 443 [SYN] Seq=0 Win=…
  10 39.319289  162.215.219.65  192.168.43.144  TCP      66 443 → 5301 [SYN, ACK] Seq=0…
  11 39.548716  192.168.43.144  162.215.219.65  TCP      66 5303 → 443 [SYN] Seq=0 Win=…
  12 39.549811  192.168.43.144  162.215.219.65  TCP      66 5304 → 443 [SYN] Seq=0 Win=…
  13 39.551294  192.168.43.144  162.215.219.65  TCP      66 5305 → 443 [SYN] Seq=0 Win=…
  14 39.554531  192.168.43.144  162.215.219.65  TCP      66 5306 → 443 [SYN] Seq=0 Win=…
  15 39.644638  192.168.43.144  162.215.219.65  TCP      66 5309 → 443 [SYN] Seq=0 Win=…
  16 39.666467  192.168.43.144  162.215.219.65  TCP      66 5310 → 443 [SYN] Seq=0 Win=…
  17 39.675514  192.168.43.144  162.215.219.65  TCP      66 5311 → 443 [SYN] Seq=0 Win=…
  18 39.680886  192.168.43.144  162.215.219.65  TCP      66 5312 → 443 [SYN] Seq=0 Win=…
  19 39.684749  192.168.43.144  162.215.219.65  TCP      66 5313 → 443 [SYN] Seq=0 Win=…
```

.

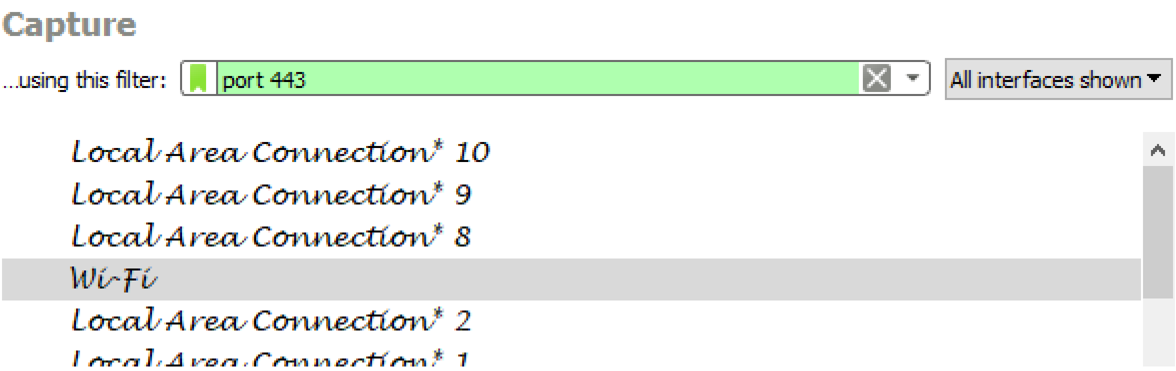


tcp.port == 443

```
lo.  Time       Source          Destination     Protocol  Length Info
   9 39.033467  192.168.43.144  162.215.219.65  TCP           66 5301 → 443 [SYN] Seq=0 Wi
  10 39.319289  162.215.219.65  192.168.43.144  TCP           66 443 → 5301 [SYN, ACK] Seq
  11 39.548716  192.168.43.144  162.215.219.65  TCP           66 5303 → 443 [SYN] Seq=0 Wi
  12 39.549811  192.168.43.144  162.215.219.65  TCP           66 5304 → 443 [SYN] Seq=0 Wi
  13 39.551294  192.168.43.144  162.215.219.65  TCP           66 5305 → 443 [SYN] Seq=0 Wi
  14 39.554531  192.168.43.144  162.215.219.65  TCP           66 5306 → 443 [SYN] Seq=0 Wi
  15 39.644638  192.168.43.144  162.215.219.65  TCP           66 5309 → 443 [SYN] Seq=0 Wi
  16 39.666467  192.168.43.144  162.215.219.65  TCP           66 5310 → 443 [SYN] Seq=0 Wi
  17 39.675514  192.168.43.144  162.215.219.65  TCP           66 5311 → 443 [SYN] Seq=0 Wi
  18 39.680886  192.168.43.144  162.215.219.65  TCP           66 5312 → 443 [SYN] Seq=0 Wi
  19 39.684749  192.168.43.144  162.215.219.65  TCP           66 5313 → 443 [SYN] Seq=0 Wi
  20 39.690397  192.168.43.144  162.215.219.65  TCP           66 5314 → 443 [SYN] Seq=0 Wi
  21 39.869094  162.215.219.65  192.168.43.144  TCP           66 443 → 5305 [SYN, ACK] Seq
  22 39.872670  162.215.219.65  192.168.43.144  TCP           66 443 → 5304 [SYN, ACK] Seq
  23 39.872670  162.215.219.65  192.168.43.144  TCP           66 443 → 5306 [SYN, ACK] Seq
  24 39.872670  162.215.219.65  192.168.43.144  TCP           66 443 → 5303 [SYN, ACK] Seq
  25 39.949255  192.168.43.144  162.215.219.65  TCP           66 5315 → 443 [SYN] Seq=0 Wi
  26 39.949830  192.168.43.144  162.215.219.65  TCP           66 5316 → 443 [SYN] Seq=0 Wi
```

Alternative method

port 443 in filter option
in cmd -> nmap –p ‘port number’ ‘website’
nmap –p 443 sonatech.ac.in
For this, ensure that u install the nmap or not

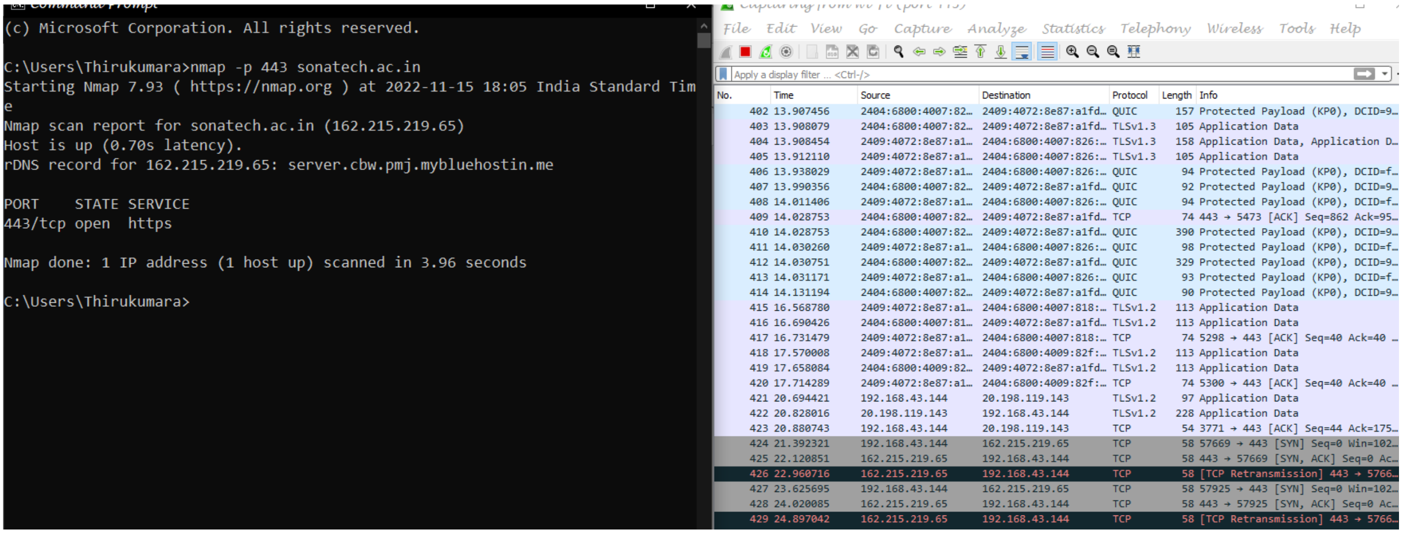


Capture

...using this filter: port 443

All interfaces shown

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1



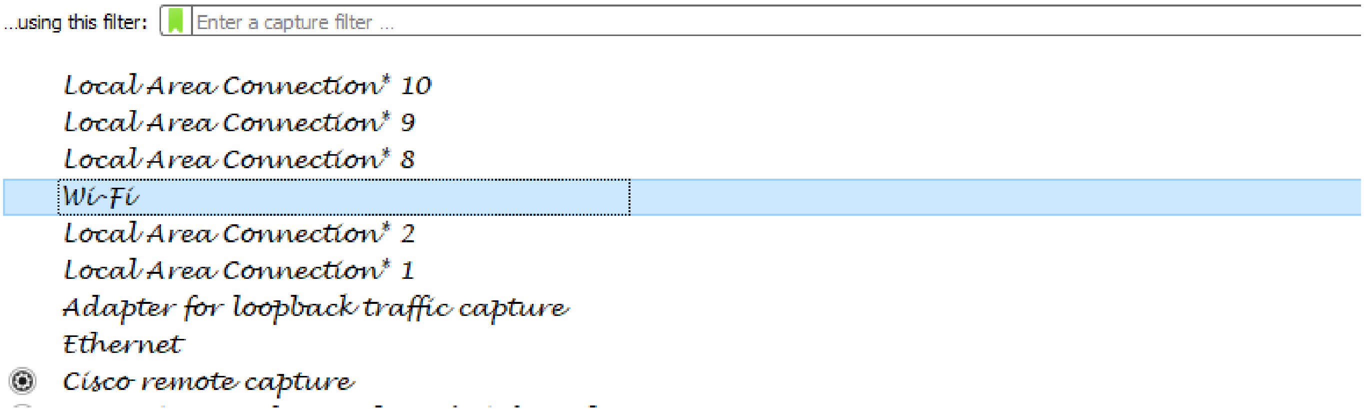
```
(c) Microsoft Corporation. All rights reserved.

C:\Users\Thirukumara>nmap -p 443 sonatech.ac.in
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 18:05 India Standard Tim
e
Nmap scan report for sonatech.ac.in (162.215.219.65)
Host is up (0.70s latency).
rDNS record for 162.215.219.65: server.cbw.pmj.mybluehostin.me

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 3.96 seconds

C:\Users\Thirukumara>
```

No.	Time	Source	Destination	Protocol	Length	Info
402	13.907456	2404:6800:4007:82…	2409:4072:8e87:a1fd…	QUIC	157	Protected Payload (KP0), DCID=9…
403	13.908079	2404:6800:4007:82…	2409:4072:8e87:a1fd…	TLSv1.3	105	Application Data
404	13.908454	2409:4072:8e87:a1…	2404:6800:4007:826:…	TLSv1.3	158	Application Data, Application D…
405	13.912110	2409:4072:8e87:a1…	2404:6800:4007:826:…	TLSv1.3	105	Application Data
406	13.938029	2409:4072:8e87:a1…	2404:6800:4007:826:…	QUIC	94	Protected Payload (KP0), DCID=f…
407	13.990356	2404:6800:4007:82…	2409:4072:8e87:a1fd…	QUIC	92	Protected Payload (KP0), DCID=9…
408	14.011406	2409:4072:8e87:a1…	2404:6800:4007:826:…	QUIC	94	Protected Payload (KP0), DCID=f…
409	14.028753	2404:6800:4007:82…	2409:4072:8e87:a1fd…	TCP	74	443 → 5473 [ACK] Seq=862 Ack=95…
410	14.028753	2404:6800:4007:82…	2409:4072:8e87:a1fd…	QUIC	390	Protected Payload (KP0), DCID=9…
411	14.030260	2409:4072:8e87:a1…	2404:6800:4007:826:…	QUIC	98	Protected Payload (KP0), DCID=f…
412	14.030751	2404:6800:4007:82…	2409:4072:8e87:a1fd…	QUIC	329	Protected Payload (KP0), DCID=9…
413	14.031171	2409:4072:8e87:a1…	2404:6800:4007:826:…	QUIC	93	Protected Payload (KP0), DCID=f…
414	14.131194	2404:6800:4007:82…	2409:4072:8e87:a1fd…	QUIC	90	Protected Payload (KP0), DCID=9…
415	16.568780	2409:4072:8e87:a1…	2404:6800:4007:818:…	TLSv1.2	113	Application Data
416	16.690426	2404:6800:4007:81…	2409:4072:8e87:a1fd…	TLSv1.2	113	Application Data
417	16.731479	2409:4072:8e87:a1…	2404:6800:4007:818:…	TCP	74	5298 → 443 [ACK] Seq=40 Ack=40 …
418	17.570008	2409:4072:8e87:a1…	2404:6800:4009:82f:…	TLSv1.2	113	Application Data
419	17.658084	2404:6800:4009:82…	2409:4072:8e87:a1fd…	TLSv1.2	113	Application Data
420	17.714289	2409:4072:8e87:a1…	2404:6800:4009:82f:…	TCP	74	5300 → 443 [ACK] Seq=40 Ack=40 …
421	20.694421	192.168.43.144	20.198.119.143	TLSv1.2	97	Application Data
422	20.828016	20.198.119.143	192.168.43.144	TLSv1.2	228	Application Data
423	20.880743	192.168.43.144	20.198.119.143	TCP	54	3771 → 443 [ACK] Seq=44 Ack=175…
424	21.392321	192.168.43.144	162.215.219.65	TCP	58	57669 → 443 [SYN] Seq=0 Win=102…
425	22.120851	162.215.219.65	192.168.43.144	TCP	58	443 → 57669 [SYN, ACK] Seq=0 Ac…
426	22.960716	162.215.219.65	192.168.43.144	TCP	58	[TCP Retransmission] 443 → 5766…
427	23.625695	192.168.43.144	162.215.219.65	TCP	58	57925 → 443 [SYN] Seq=0 Win=102…
428	24.020085	162.215.219.65	192.168.43.144	TCP	58	443 → 57925 [SYN, ACK] Seq=0 Ac…
429	24.897042	162.215.219.65	192.168.43.144	TCP	58	[TCP Retransmission] 443 → 5766…

Here the third question is little bit complicated

3. Make a Google search for “apple”, use wireshark to analyse the web traffic and show the communication from client to server in the application layer

Step 1

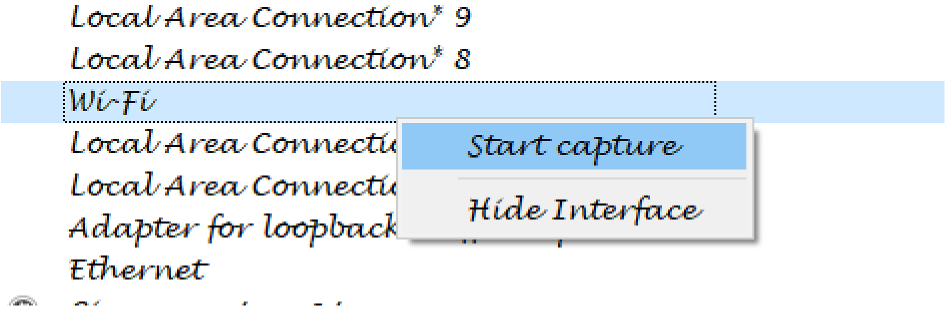


...using this filter: Enter a capture filter ...

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
Cisco remote capture

Right click on the wifi or Ethernet

Start capture



Local Area Connection* 9
Local Area Connection* 8
Wi-Fi
Local Area Connecti
Local Area Connecti
Adapter for loopback
Ethernet

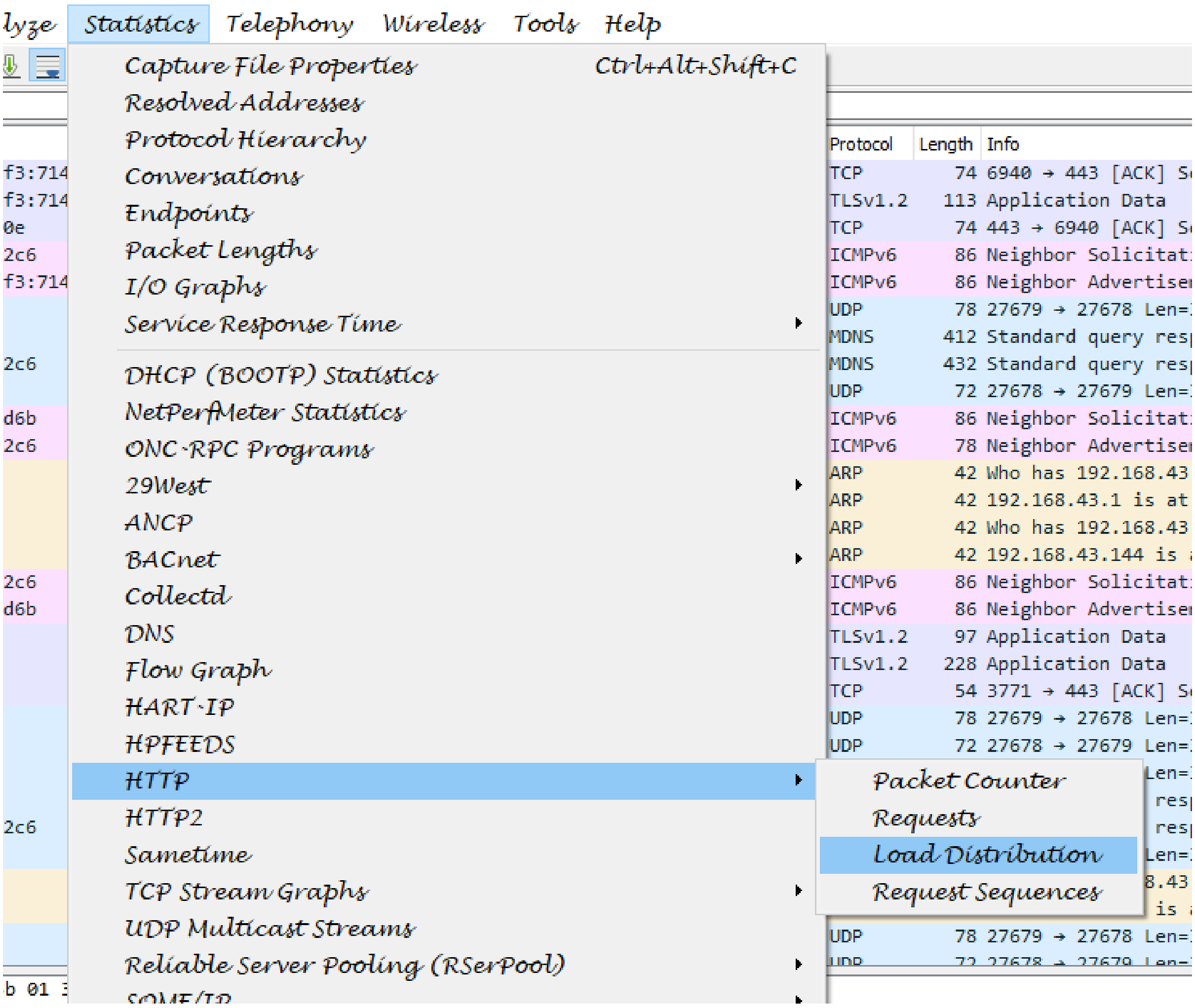
Go to browser

Search google

Search apple

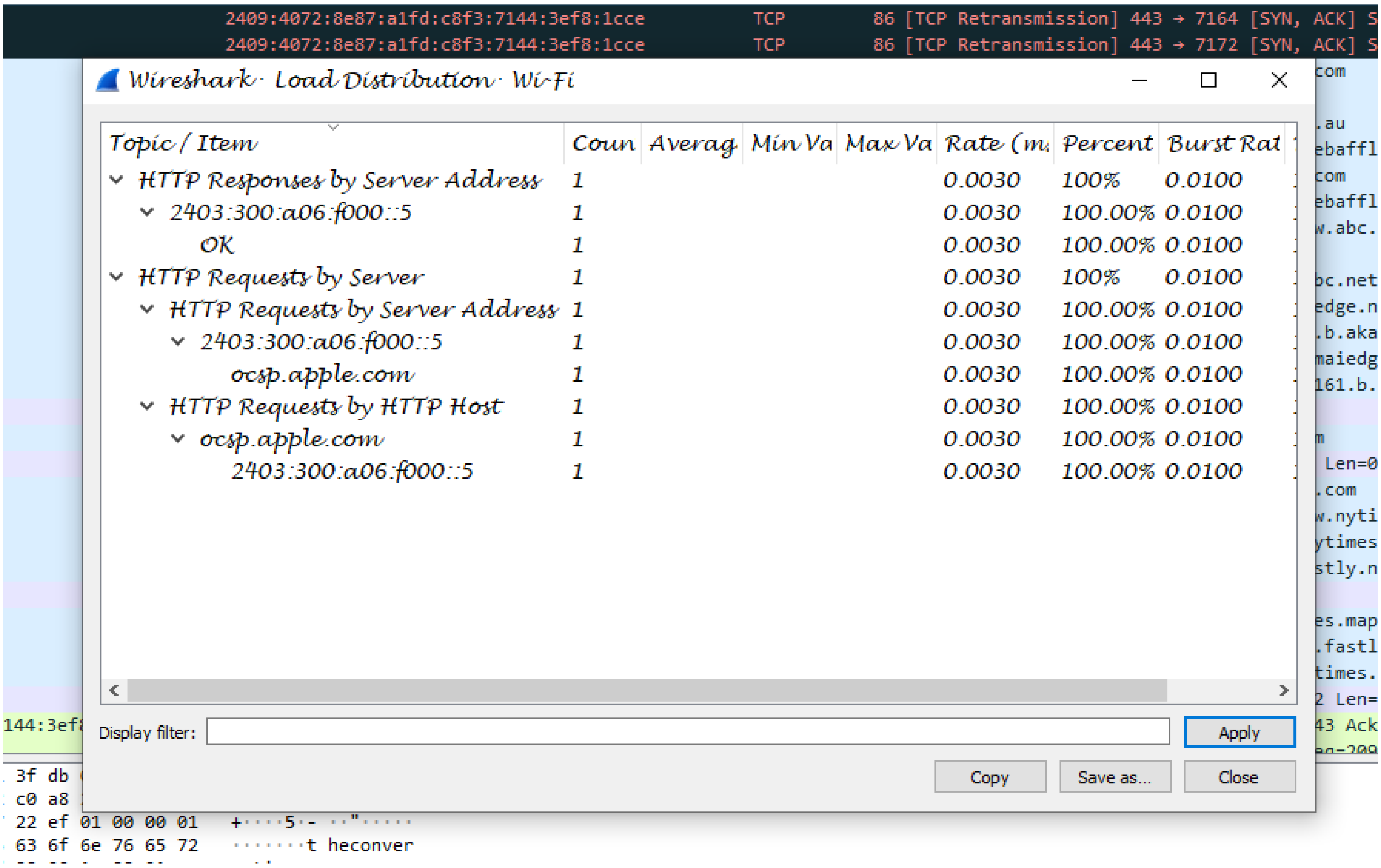
Then come to wireshark

Choose statistics, and select http



```
f3:714   TCP       74 6940 → 443 [ACK] S
f3:714   TLSv1.2  113 Application Data
0e       TCP       74 443 → 6940 [ACK] S
2c6      ICMPv6    86 Neighbor Solicitat
f3:714   ICMPv6    86 Neighbor Advertise
         UDP       78 27679 → 27678 Len=
         MDNS     412 Standard query res
2c6      MDNS     432 Standard query res
         UDP       72 27678 → 27679 Len=
d6b      ICMPv6    86 Neighbor Solicitat
2c6      ICMPv6    78 Neighbor Advertise
         ARP       42 Who has 192.168.43
         ARP       42 192.168.43.1 is at
         ARP       42 Who has 192.168.43
         ARP       42 192.168.43.144 is
2c6      ICMPv6    86 Neighbor Solicitat
d6b      ICMPv6    86 Neighbor Advertise
         TLSv1.2   97 Application Data
         TLSv1.2  228 Application Data
         TCP       54 3771 → 443 [ACK] S
         UDP       78 27679 → 27678 Len=
         UDP       72 27678 → 27679 Len=
```

In this ,we can see the results



```
2409:4072:8e87:a1fd:c8f3:7144:3ef8:1cce    TCP    86 [TCP Retransmission] 443 → 7164 [SYN, ACK] S
2409:4072:8e87:a1fd:c8f3:7144:3ef8:1cce    TCP    86 [TCP Retransmission] 443 → 7172 [SYN, ACK] S
```

Wireshark · Load Distribution · Wi-Fi

Topic / Item	Coun	Averag	Min Va	Max Va	Rate (m	Percent	Burst Rat
HTTP Responses by Server Address	1				0.0030	100%	0.0100
2403:300:a06:f000::5	1				0.0030	100.00%	0.0100
OK	1				0.0030	100.00%	0.0100
HTTP Requests by Server	1				0.0030	100%	0.0100
HTTP Requests by Server Address	1				0.0030	100.00%	0.0100
2403:300:a06:f000::5	1				0.0030	100.00%	0.0100
ocsp.apple.com	1				0.0030	100.00%	0.0100
HTTP Requests by HTTP Host	1				0.0030	100.00%	0.0100
ocsp.apple.com	1				0.0030	100.00%	0.0100
2403:300:a06:f000::5	1				0.0030	100.00%	0.0100

Display filter:

.

Apple’a kandu pudichaachu nanbargalee!!