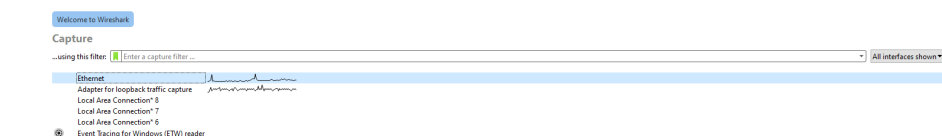


Practical 4

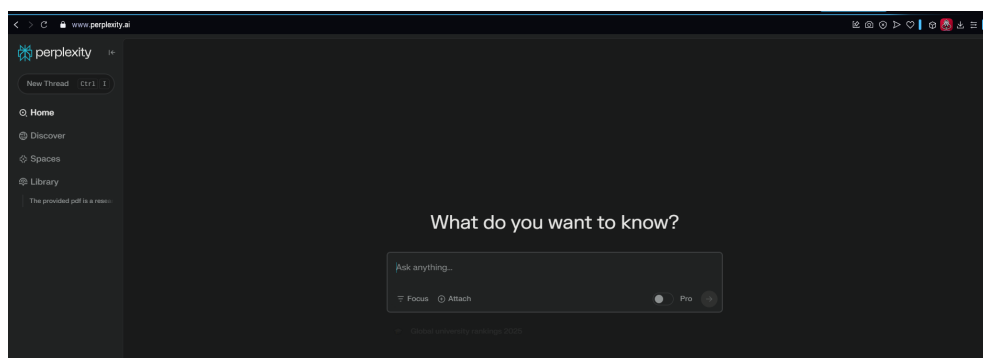
Aim: Capturing and analysing network packets using Wireshark (Fundamentals)

- Identification the live network
- Capture Packets
- Analyse the captured packets.

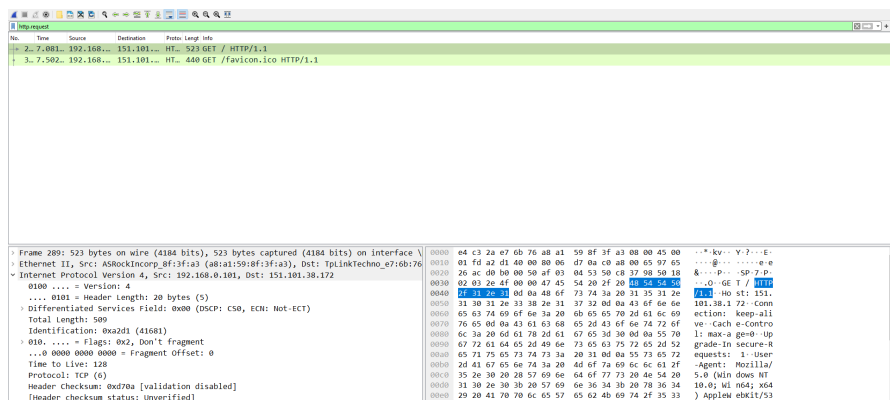
Step 1: Wireshark captures all the packets going in and out of our systems. To Capture traffic on your wireless network, Right click on your “Wi-Fi” interface and then click on “Start capture”.



Step 2: Go to any website in your browser and perform some actions.

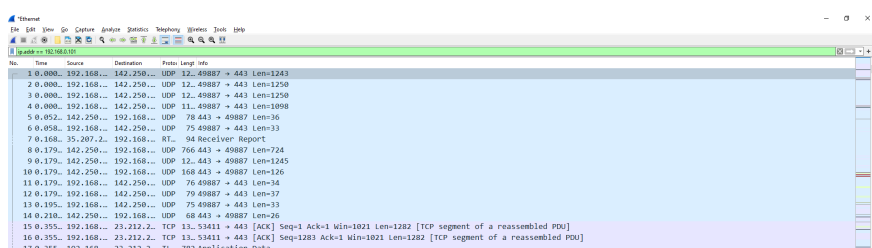


Step 3: Now come back to Wireshark and stop the recording and search for http.



1. Display packets which are having specific IP-address

> ip.addr == 192.168.0.101



```
> ip.src==192.168.211.1
```

No.	src_ip	src_port	destination	protocol	length	info
1	192.168...	...	142.250...	UDP	12	49887 → 443 Len=1243
2	192.168...	...	142.250...	UDP	12	49887 → 443 Len=1250
3	192.168...	...	142.250...	UDP	12	49887 → 443 Len=1250
4	192.168...	...	142.250...	UDP	11	49887 → 443 Len=1098
5	192.168...	...	142.250...	UDP	75	49887 → 443 Len=33
6	192.168...	...	142.250...	UDP	76	49887 → 443 Len=34
7	192.168...	...	142.250...	UDP	79	49887 → 443 Len=37
8	192.168...	...	142.250...	UDP	75	49887 → 443 Len=33
9	192.168...	...	212.212.21...	TCP	13	53411 + 443 [ACK] Seq=1-Ack1 Win=1021 Len=1282 [TCP segment of a reassembled PDU]
10	192.168...	...	212.212.21...	TCP	13	53411 + 443 [ACK] Seq=1283-Ack1 Win=1021 Len=1282 [TCP segment of a reassembled PDU]
11	192.168...	...	212.212.21...	TCP	782	Application Data
12	192.168...	...	212.212.21...	TCP	13	53411 + 443 [ACK] Seq=3293-Ack1 Win=1021 Len=1282 [TCP segment of a reassembled PDU]
13	192.168...	...	212.212.21...	TCP	13	53411 + 443 [ACK] Seq=573-Ack1 Win=1021 Len=1282 [TCP segment of a reassembled PDU]
14	192.168...	...	212.212.21...	TCP	13	53411 + 443 [ACK] Seq=587-Ack1 Win=1021 Len=1282 [TCP segment of a reassembled PDU]
15	192.168...	...	212.212.21...	TCP	13	53411 + 443 [ACK] Seq=7139-Ack1 Win=1021 Len=1282 [TCP segment of a reassembled PDU]

```
> ip.dst== 192.168.211.134
```

No.	Time	Source	Destination	Protocol	Length	Info
5	0.052.142.250...	192.168.1.105	192.168.1.106	UDP	78	443 → 49887 Len=36
7	0.168.35.207.2...	192.168.1.105	RT.	94	Receiver Report	
8	0.179.142.250...	192.168.1.105	192.168.1.106	UDP	76	443 → 49887 Len=74
9	0.179.142.250...	192.168.1.105	192.168.1.106	UDP	12	443 → 49887 Len=1245
10	0.179.142.250...	192.168.1.105	192.168.1.106	UDP	16	443 → 49887 Len=126
14	0.210.142.250...	192.168.1.105	192.168.1.106	UDP	68	443 → 49887 Len=26
26	0.417.23.212.2...	192.168.1.105	192.168.1.106	TCP	60	443 → 53111 [ACK] Seq=1 Acl=2565 Min=802 Len=0
27	0.417.23.212.2...	192.168.1.105	192.168.1.106	TCP	66	443 → 53111 [ACK] Seq=1 Acl=5857 Min=802 Len=0 SLE=10985 SRE=11876
28	0.417.23.212.2...	192.168.1.105	192.168.1.106	TCP	66	[TCP Dup ACK 2781] 443 → 53111 [ACK] Seq=1 Acl=5857 Min=802 Len=0 SLE=10985 SRE=11914
29	0.417.23.212.2...	192.168.1.105	192.168.1.106	TCP	60	[TCP Window Update] 443 → 53111 [ACK] Seq=1 Acl=5857 Min=802 Len=0
30	0.417.23.212.2...	192.168.1.105	192.168.1.106	TCP	60	443 → 53111 [ACK] Seq=1 Acl=11914 Min=962 Len=0
38	0.491.162.159...	192.168.1.105	192.168.1.106	TLS	117	Application Data
36	0.545.23.212.2...	192.168.1.105	192.168.1.106	TLS	491	Application Data

>http

[illegible]

```
> http.request
```

The screenshot shows the Wireshark interface with a packet capture of HTTP traffic. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions like opening files, saving, zooming, and filtering.

The main pane displays a list of captured packets:

No.	Time	Source	Destination	Protocol Length Info
2.	7.081..	192.168.0.1	151.101.1..	HT- 523 GET / HTTP/1.1
7.	7.366..	192.168.0.1	192.168.0.10	HT- 604 HTTP/1.1 500 Domain Not Found (text/html)
7.	7.507..	192.168.0.1	151.101.1..	444 GET /favicon.ico HTTP/1.1
3.	7.765..	192.168.0.1	192.168.0.10	HT- 604 HTTP/1.1 500 Domain Not Found (text/html)
1.	9.394..	192.168.0.1	192.168.0.10	HT- 285 UNSUBSCRIBE /upnp/control/WANCommonIFc1 HTTP/1.1
1.	9.396..	192.168.0.1	192.168.0.10	HT- 248 HTTP/1.1 200 OK (text/html)

The bottom pane shows the details of the selected packet (No. 1), which is an HTTP 200 OK response. It lists the Ethernet II frame, Internet Protocol Version 4, and Hypertext Transfer Protocol layers.

```
>http.response.code==200
```

A screenshot of the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, packet selection, and analysis. The main display area shows a single captured packet, number 1, which is an HTTP response. The packet details pane on the left indicates it's an 'http.response.code==200'. The packet bytes pane on the right displays the raw data as a hex string: '1... 9.396... 192.168... 192.168... HT.. 248 HTTP/1.1 200 OK (text/html)'. The status bar at the bottom shows the current packet selected.

```
>tcp.port==80|| udp.port==443
```

The image shows a Wireshark packet capture of a series of protected payloads (KDP) sent from 1.9.344 to 1.9.394. The destination is 192.168.1.100. The payloads are protected using a key derived from the source IP and a padding of 3 bytes. The payloads are listed in the packet list pane, showing the source IP, destination IP, protocol, length, and the protected payload (KDP). The payloads are protected using a key derived from the source IP and a padding of 3 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
1.9.344	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		
1.9.344	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		
1.9.345	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.345	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		
1.9.345	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...	142.250...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	142.250...	192.168...	192.168.1.100	Protected Payload (KDP)		DCID=e728155f060ecd76
1.9.346	192.168...					

```
>tcp contains google
```

tcp contains google						Expression...
No.	Time	Source	Destination	Protocol	Length Info	
1213	254.914893	192.168.211.134	69.43.111.82	HTTP	707 GET /~grovesd/comm244/notes/week2/links HTTP/1.1	
1219	255.195933	69.43.111.82	192.168.211.134	TCP	1514 80 → 50842 [ACK] Seq=1 Ack=654 Win=64240 Len=1460 [TCP segment of a reassembled PDU]	
1925	258.616353	192.168.211.134	146.190.62.39	HTTP	518 GET / HTTP/1.1	
1933	258.908370	146.190.62.39	192.168.211.134	TCP	1514 80 → 50845 [PSH, ACK] Seq=1 Ack=465 Win=64240 Len=1460 [TCP segment of a reassembled PDU]	
2030	259.213771	146.190.62.39	192.168.211.134	TCP	1514 80 → 50845 [ACK] Seq=2741 Ack=781 Win=64240 Len=1460 [TCP segment of a reassembled PDU]	
2052	259.504054	146.190.62.39	192.168.211.134	TCP	1514 80 → 50845 [ACK] Seq=4571 Ack=1115 Win=64240 Len=1460 [TCP segment of a reassembled PDU]	
2063	259.512700	146.190.62.39	192.168.211.134	HTTP	956 HTTP/1.1 200 OK (text/css)	
2100	260.126299	192.168.211.134	142.250.192.106	TLSv1.3	1848 Client Hello	
2342	260.869135	146.190.62.39	192.168.211.134	HTTP/X.	1365 HTTP/1.1 200 OK	
2343	260.875000	146.190.62.39	192.168.211.134	HTTP/X.	1315 HTTP/1.1 200 OK	
2348	261.136427	146.190.62.39	192.168.211.134	HTTP/X.	1321 HTTP/1.1 200 OK	
2351	261.413248	146.190.62.39	192.168.211.134	TCP	1514 80 → 50852 [PSH, ACK] Seq=1268 Ack=790 Win=64240 Len=1460 [TCP segment of a reassembled PDU]	
> Frame 2052: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0						
> Ethernet II, Src: Vmware_ec:8d:d0 (00:50:56:ec:8d:d0), Dst: Vmware_90:87:df (00:0c:29:90:87:df)						
> Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.211.134						
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 50845, Seq: 4571, Ack: 1115, Len: 1460						
Source Port: 80						
Destination Port: 50845						
[Stream index: 74]						
[TCP Segment Len: 1460]						
Sequence number: 4571 (relative sequence number)						
[Next sequence number: 6031 (relative sequence number)]						