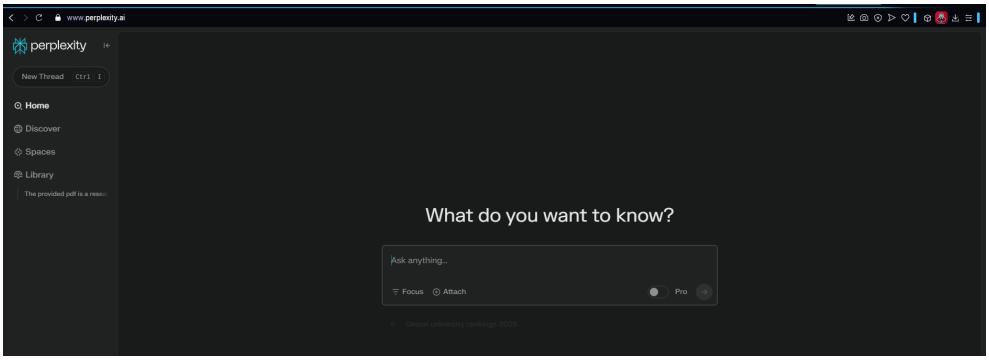
Practical 4

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

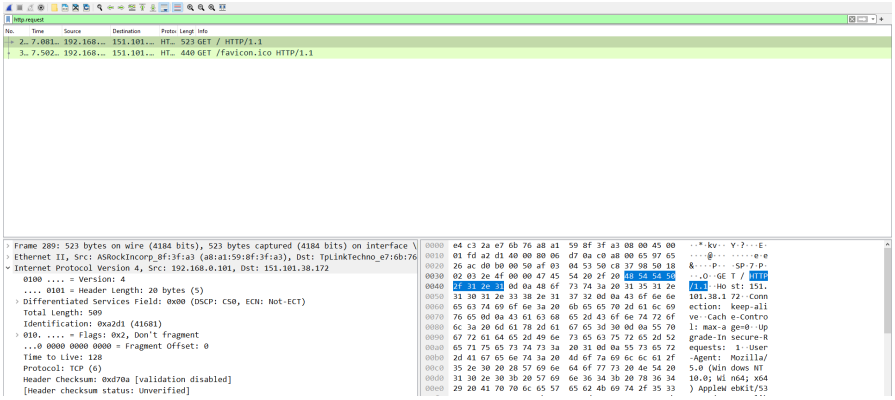
- Identification the live network
- Capture Packets
- Analyse the captured packets.

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.

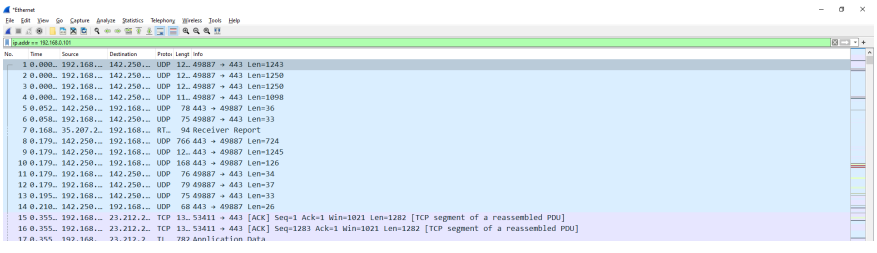


Step 3: Now come back to Wireshark and stop the recording and search for http.

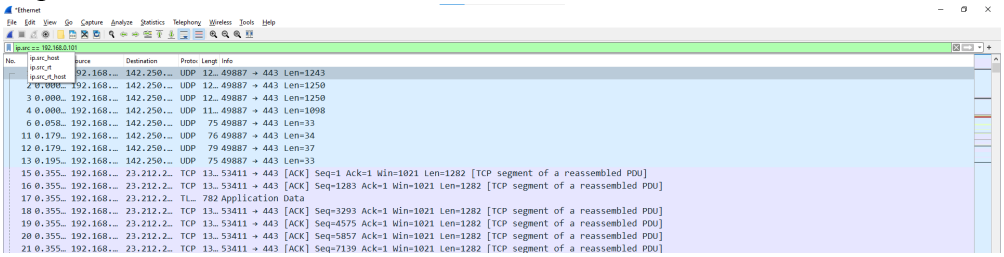


1. Display packets which are having specific IP-address

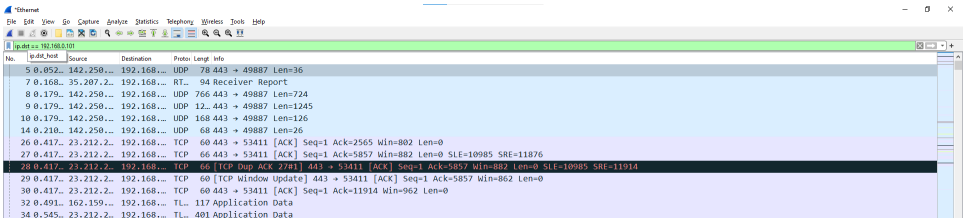
> ip.addr == 192.168.0.101



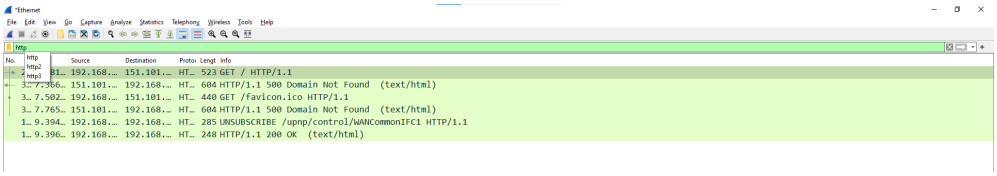
2. Display packets which are having specific IP-address source
> ip.src==192.168.211.1



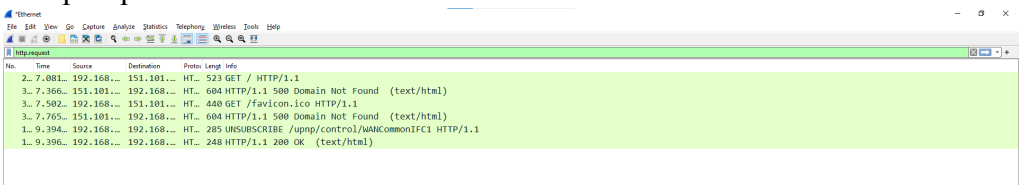
3. Display packets which are having specific IP-address destination
> ip.dst== 192.168.211.134



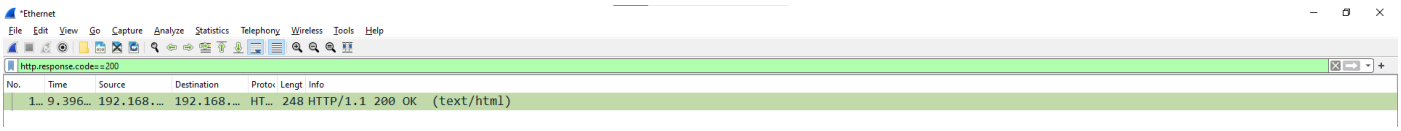
4. Display packets which are using http protocol
>http



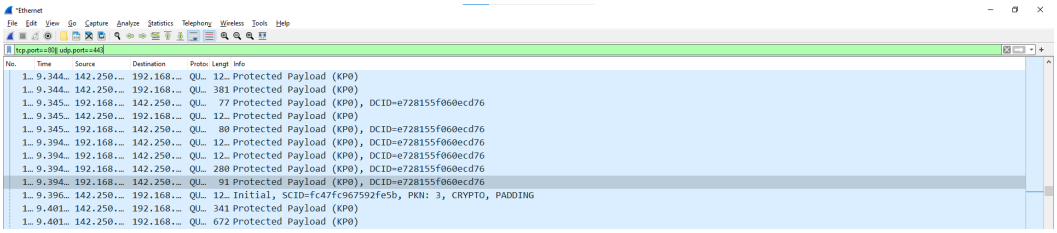
5. Display packets which are using http request
> http.request



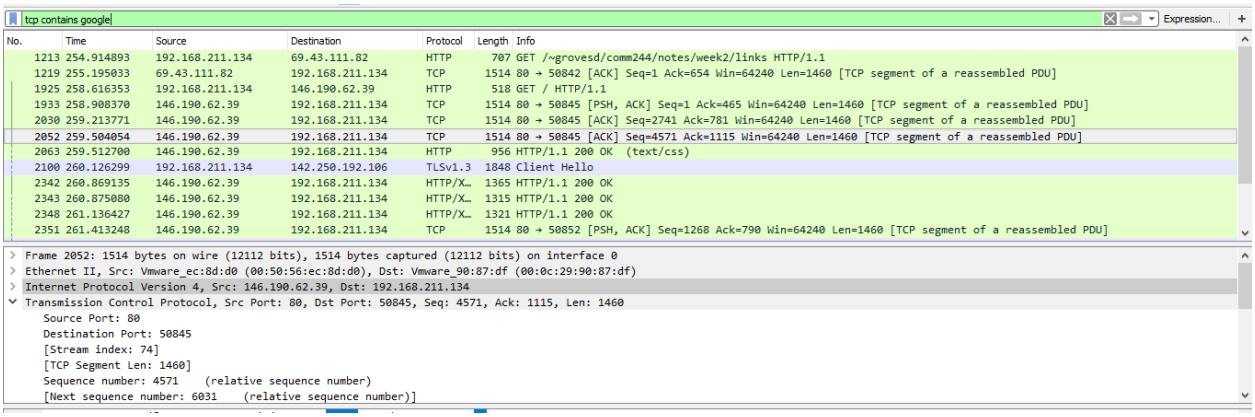
6. Display packets having no error connecting to server
>http.response.code==200



7. Display packets having port number 80 ,443
>tcp.port==80|| udp.port==443



8. Display packets which contains keyword Google.
>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 255.195033 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 260.875080 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)]