

Lab Experiment No 8

Aim: Installation of Wireshark (Network protocol analyzer) and analyze the traffic.

Introduction:

1. What is Wireshark?

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.

Implementation:

1. TCP

Wireshark network traffic capture showing TCP segments. The packet list shows several TCP segments from 192.168.0.105 to 203.23.178.59. The packet details pane shows the structure of a TCP segment, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
88	1.676516	192.168.0.105	203.23.178.59	TCP	55	49677 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
99	1.772520	203.23.178.59	192.168.0.105	TCP	54	443 → 49677 [ACK] Seq=0 Ack=2 Win=11 Len=0
100	1.772548	192.168.0.105	203.23.178.59	TCP	54	[TCP Dup ACK 88#1] [TCP ACKed unseen segment] 49677 → 443 [ACK] Seq=2 Ack=1 Win=516 Len=0
101	1.801402	203.23.178.59	192.168.0.105	TCP	66	[TCP Previous segment not captured] 443 → 49677 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
150	2.325771	157.240.7.54	192.168.0.105	TLSv1.2	296	Application Data
151	2.326090	192.168.0.105	157.240.7.54	TLSv1.2	89	Application Data
152	2.326200	192.168.0.105	157.240.7.54	TLSv1.2	89	Application Data
153	2.374300	192.168.0.105	157.240.7.54	TLSv1.2	164	Application Data
154	2.385952	157.240.7.54	192.168.0.105	TCP	54	443 → 51818 [ACK] Seq=243 Ack=36 Win=2070 Len=0
155	2.385952	157.240.7.54	192.168.0.105	TCP	54	443 → 51818 [ACK] Seq=243 Ack=71 Win=2070 Len=0
158	2.435678	157.240.7.54	192.168.0.105	TCP	54	443 → 51818 [ACK] Seq=243 Ack=181 Win=2070 Len=0
183	2.768181	192.168.0.105	52.113.194.132	TCP	66	57450 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 88: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{924EC87C-D5E1-4DA5-91FE-58A92640CD3F}, id 0
 Ethernet II, Src: IntelCor_a3:43:f5 (a4:c3:f0:a3:43:f5), Dst: Tp-LinkT_a7:5f:3c (d8:07:b6:a7:5f:3c)
 Internet Protocol Version 4, Src: 192.168.0.105, Dst: 203.23.178.59
 Transmission Control Protocol, Src Port: 49677, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000 d8 07 b6 a7 5f 3c a4 c3 f0 a3 43 f5 08 00 45 00<...C...E
 0010 00 29 be 7d 40 00 06 00 00 c0 a8 00 69 cb 17 ...>]@...i..
 0020 b2 3b c2 0d 01 bb f2 7a 22 8a 54 19 45 4a 50 10 :.....z".T.EJP
 0030 02 04 3e 80 00 00 00 ..>....

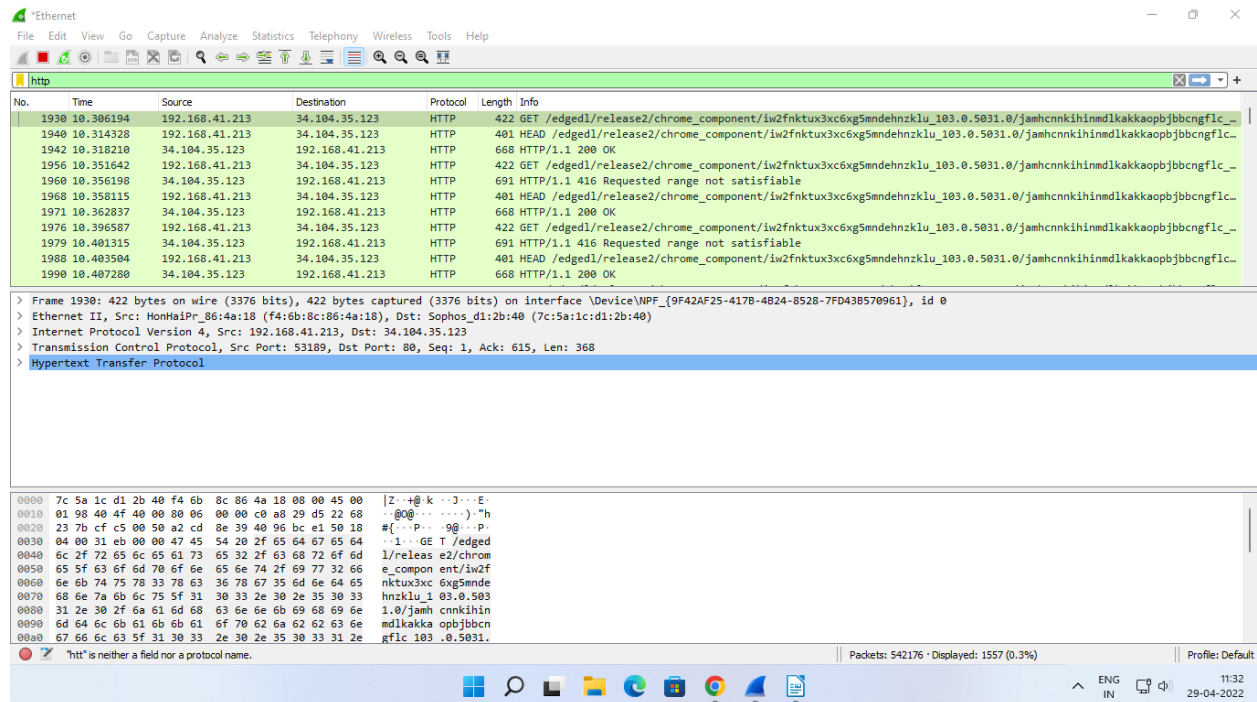
Transmission Control Protocol: Protocol

Packets: 399 · Displayed: 52 (13.0%) · Dropped: 0 (0.0%)

Profile: Default

21:23
25-04-2022

2. HTTP

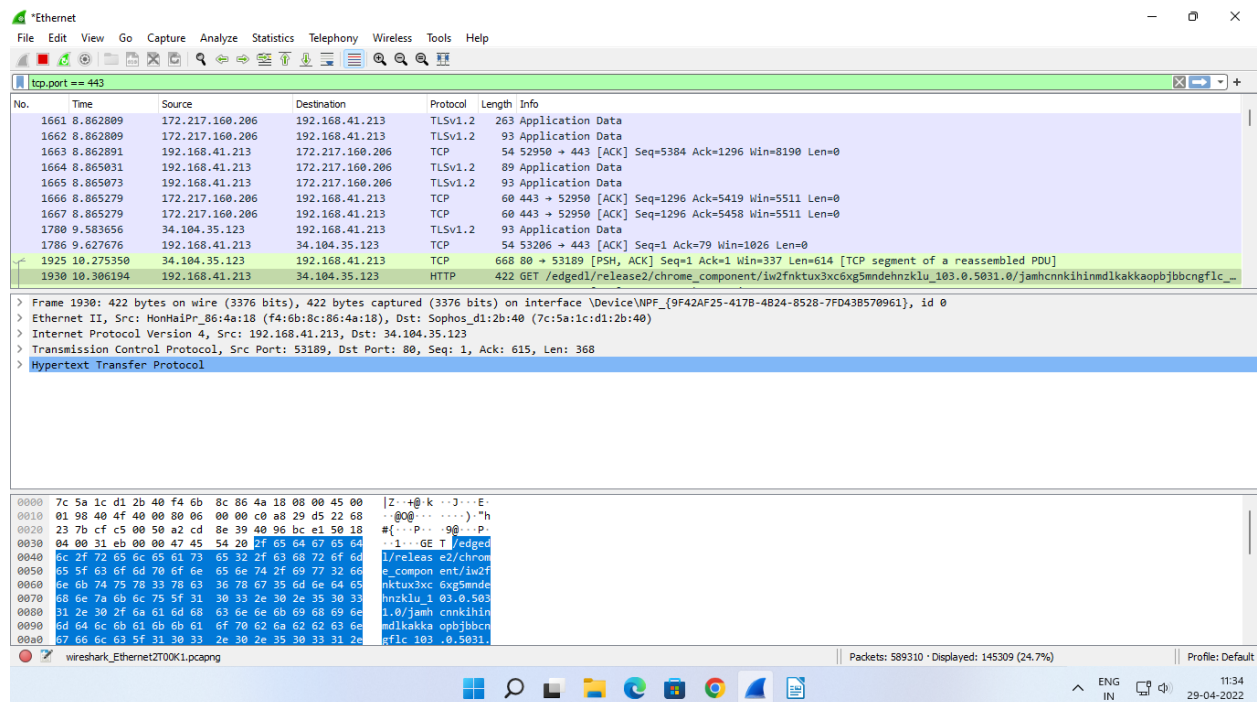


The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane displays a single packet (No. 1930) at time 10.386194, sourced from 192.168.41.213 and destined for 34.104.35.123. The protocol is HTTP, and the length is 422 bytes. The packet details pane shows the structure of the HTTP GET request, including the method (GET), the request URI (/edged1/release2/chrome_component/iw2fntux3xc6xg5mndehnzkl_u103.0.5031.0/jamhcnkkihnm1d1akkaopbjbbcnf1c...), and the status code (200 OK). The packet bytes pane shows the raw data of the request, including the GET method and the request URI.

No.	Time	Source	Destination	Protocol	Length	Info
1930	10.386194	192.168.41.213	34.104.35.123	HTTP	422	GET /edged1/release2/chrome_component/iw2fntux3xc6xg5mndehnzkl_u103.0.5031.0/jamhcnkkihnm1d1akkaopbjbbcnf1c...

Frame 1930: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface \Device\NPF_{9F42AF25-417B-4B24-8528-7FD438570961}, id 0
> Ethernet II, Src: HonHaiPr_86:4a:18 (f4:6b:8c:86:4a:18), Dst: Sophos_d1:2b:40 (7c:5a:1c:d1:2b:40)
> Internet Protocol Version 4, Src: 192.168.41.213, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 53189, Dst Port: 80, Seq: 1, Ack: 615, Len: 368
> Hypertext Transfer Protocol

3. tcp.port == 443



The screenshot shows a Wireshark capture of a TLSv1.2 connection. The packet list pane displays a single packet (No. 1930) at time 10.386194, sourced from 192.168.41.213 and destined for 34.104.35.123. The protocol is TLSv1.2, and the length is 422 bytes. The packet details pane shows the structure of the TLSv1.2 connection, including the version (TLSv1.2), the cipher suite (TLSv1.2), and the status code (200 OK). The packet bytes pane shows the raw data of the connection, including the TLSv1.2 header and the request URI.

No.	Time	Source	Destination	Protocol	Length	Info
1930	10.386194	192.168.41.213	34.104.35.123	TLSv1.2	422	GET /edged1/release2/chrome_component/iw2fntux3xc6xg5mndehnzkl_u103.0.5031.0/jamhcnkkihnm1d1akkaopbjbbcnf1c...

Frame 1930: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface \Device\NPF_{9F42AF25-417B-4B24-8528-7FD438570961}, id 0
> Ethernet II, Src: HonHaiPr_86:4a:18 (f4:6b:8c:86:4a:18), Dst: Sophos_d1:2b:40 (7c:5a:1c:d1:2b:40)
> Internet Protocol Version 4, Src: 192.168.41.213, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 53189, Dst Port: 80, Seq: 1, Ack: 615, Len: 368
> Hypertext Transfer Protocol

4. tcp.port == 80

Wireshark capture showing traffic filtered by `tcp.port == 80`. The capture shows several packets, including a GET request and its response. The packet list shows packets 1925 to 1939. The packet details pane shows the structure of the selected packet (1930), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers.

No.	Time	Source	Destination	Protocol	Length	Info
1925	10.275350	34.104.35.123	192.168.41.213	TCP	668	80 → 53189 [PSH, ACK] Seq=1 Ack=1 Win=337 Len=614 [TCP segment of a reassembled PDU]
1930	10.306194	192.168.41.213	34.104.35.123	HTTP	422	GET /edged1/release2/chrome_component/iw2fntux3xc6xg5mnde hnzkl u_103.0.5031.0/jamhcnk ihinmdlkakkaopbjbbcn gflc _
1931	10.306487	34.104.35.123	192.168.41.213	TCP	60	80 → 53189 [ACK] Seq=615 Ack=369 Win=346 Len=0
1932	10.310894	34.104.35.123	192.168.41.213	TCP	691	80 → 53189 [PSH, ACK] Seq=615 Ack=369 Win=346 Len=637 [TCP segment of a reassembled PDU]
1933	10.310894	34.104.35.123	192.168.41.213	TCP	60	80 → 53189 [FIN, ACK] Seq=1252 Ack=369 Win=0 Len=0
1934	10.310992	192.168.41.213	34.104.35.123	TCP	54	53189 → 80 [ACK] Seq=369 Ack=1253 Win=1021 Len=0
1935	10.311221	192.168.41.213	34.104.35.123	TCP	54	53189 → 80 [FIN, ACK] Seq=369 Ack=1253 Win=1021 Len=0
1936	10.311446	34.104.35.123	192.168.41.213	TCP	60	80 → 53189 [ACK] Seq=1253 Ack=370 Win=346 Len=0
1937	10.313564	192.168.41.213	34.104.35.123	TCP	66	53217 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1938	10.313949	34.104.35.123	192.168.41.213	TCP	66	80 → 53217 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1939	10.314064	192.168.41.213	34.104.35.123	TCP	54	53217 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0

Frame 1930: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface \Device\NPF_{9F42AF25-417B-4B24-8528-7FD438570961}, id 0
 Ethernet II, Src: HonHaiPr_86:4a:18 (f4:6b:8c:86:4a:18), Dst: Sophos_d1:2b:40 (7c:5a:1c:d1:2b:40)
 Internet Protocol Version 4, Src: 192.168.41.213, Dst: 34.104.35.123
 Transmission Control Protocol, Src Port: 53189, Dst Port: 80, Seq: 1, Ack: 615, Len: 368
 Hypertext Transfer Protocol

0000 7c 5a 1c d1 2b 40 f4 6b 8c 86 4a 18 00 00 45 00 | Z...@.k...J...E-
 0010 01 98 40 4f 40 00 00 06 00 00 c0 a8 29 d5 22 68 | .@0@... ..-).~h
 0020 23 7b cf c5 00 50 a2 cd 0e 39 40 96 bc e1 50 18 | #({-P...-9@...p
 0030 04 00 31 eb 00 00 47 45 54 20 2f 65 64 67 65 64 | .1...GE T /edged
 0040 6c 2f 72 65 6c 65 61 73 65 32 2f 63 68 72 6f 6d | l/releas e2/chrom
 0050 65 5f 63 6f 6d 70 6f 6e 65 6e 74 2f 69 77 32 66 | e_compon ent/iw2f
 0060 6e 6b 74 75 78 33 78 63 36 78 67 35 6d 6e 64 65 | nktux3xc 6xg5mnde
 0070 68 6e 7a 6b 6c 75 5f 31 30 33 2e 30 2e 35 30 33 | hnzkl u_1 03.0.503
 0080 31 2e 30 2f 6a 61 6d 68 63 6e 6e 6b 69 68 69 6e | 1.0/jamh cnkkih in
 0090 6d 64 6c 6b 61 6b 6b 61 6f 70 62 6a 62 62 63 6e | mdlk akka opbjbbcn
 00a0 67 6f 6c 63 5f 31 30 33 2e 30 2e 35 30 33 31 2e | gflc 103 .0.5031.

Wireshark_Ethernet2700K1.pcapng | Packets: 621237 · Displayed: 4154 (0.7%) | Profile: Default

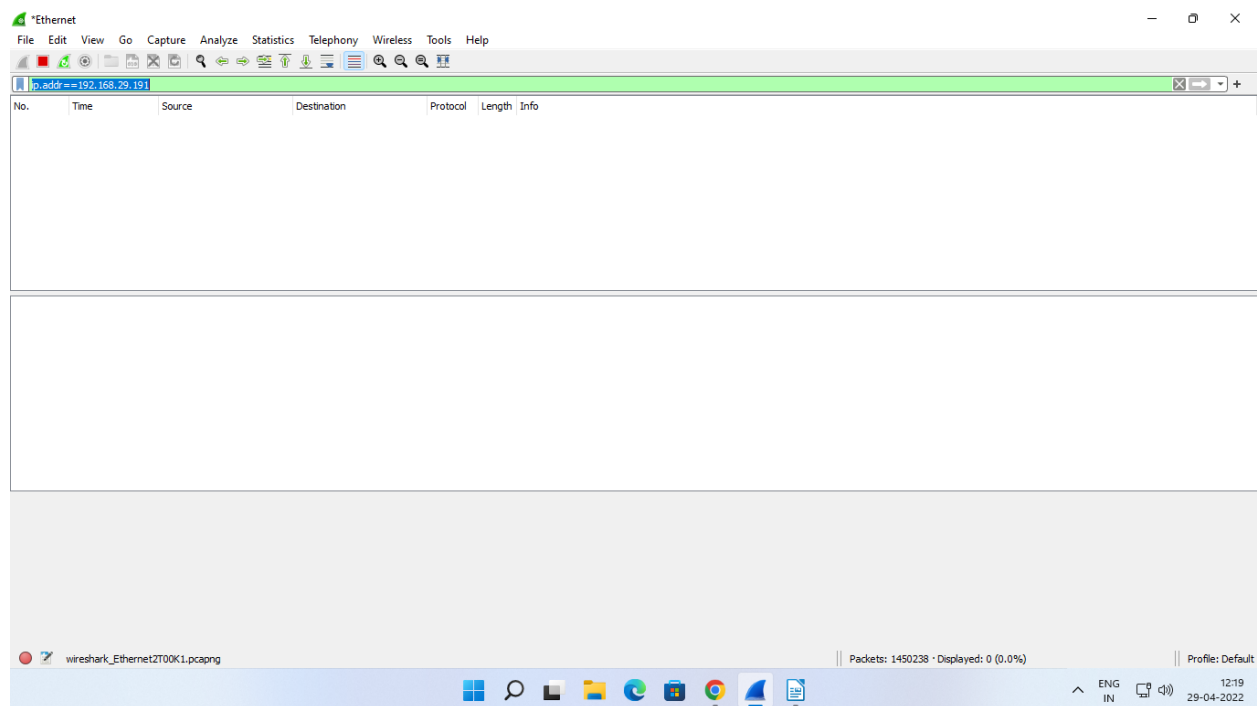
5. ip.src==192.168.29.191

Wireshark capture showing traffic filtered by `ip.src==192.168.29.191`. The capture shows a large number of packets, but the packet list is empty, indicating that no packets match the filter. The packet details pane is also empty.

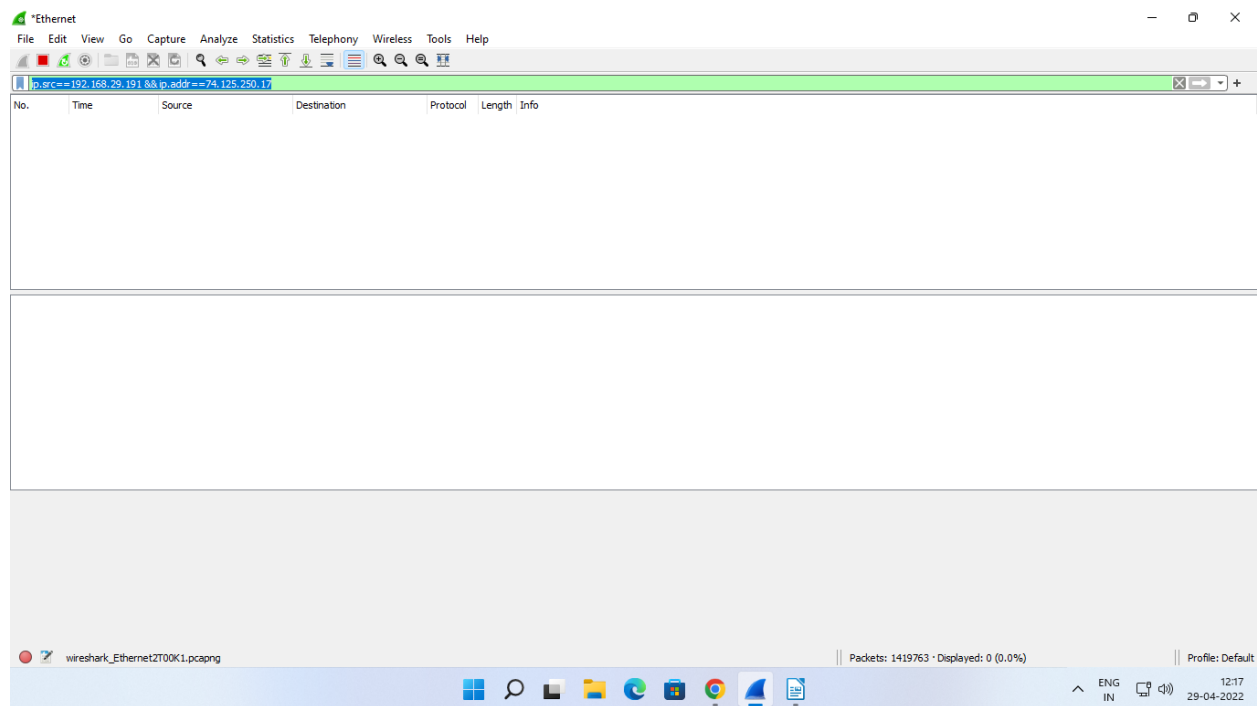
No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

Wireshark_Ethernet2700K1.pcapng | Packets: 1258360 · Displayed: 0 (0.0%) | Profile: Default

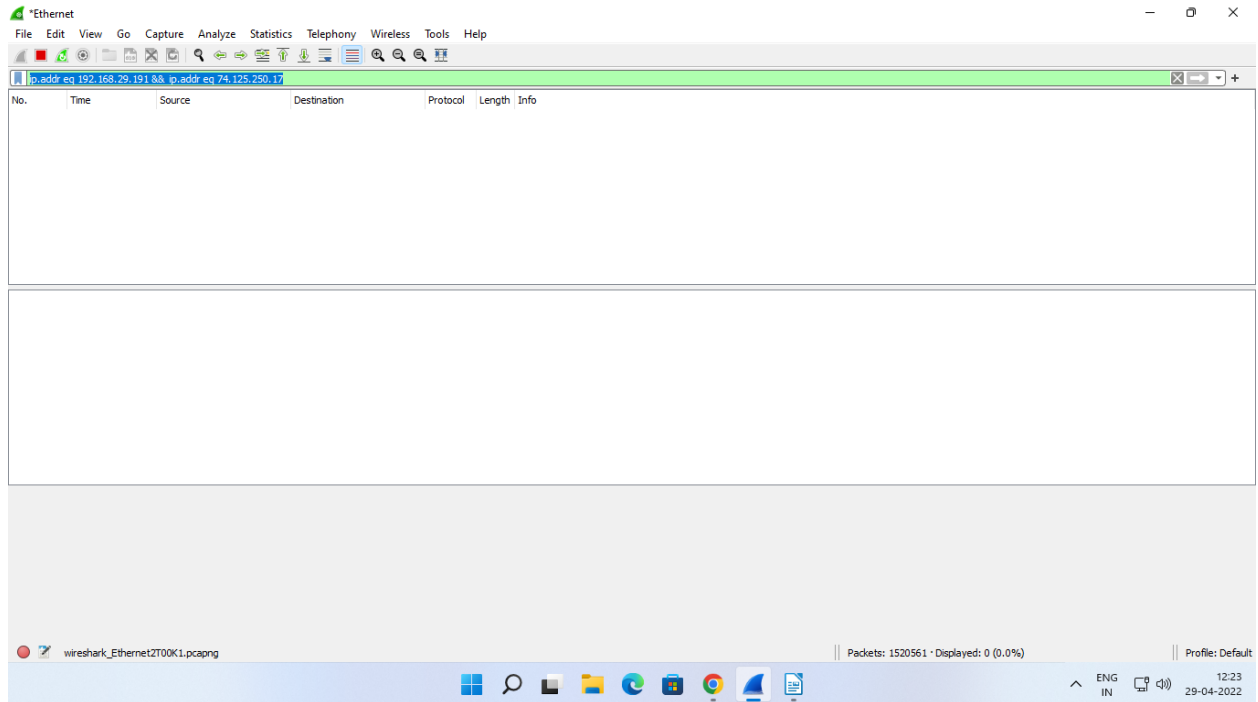
6. ip.addr==192.168.29.191



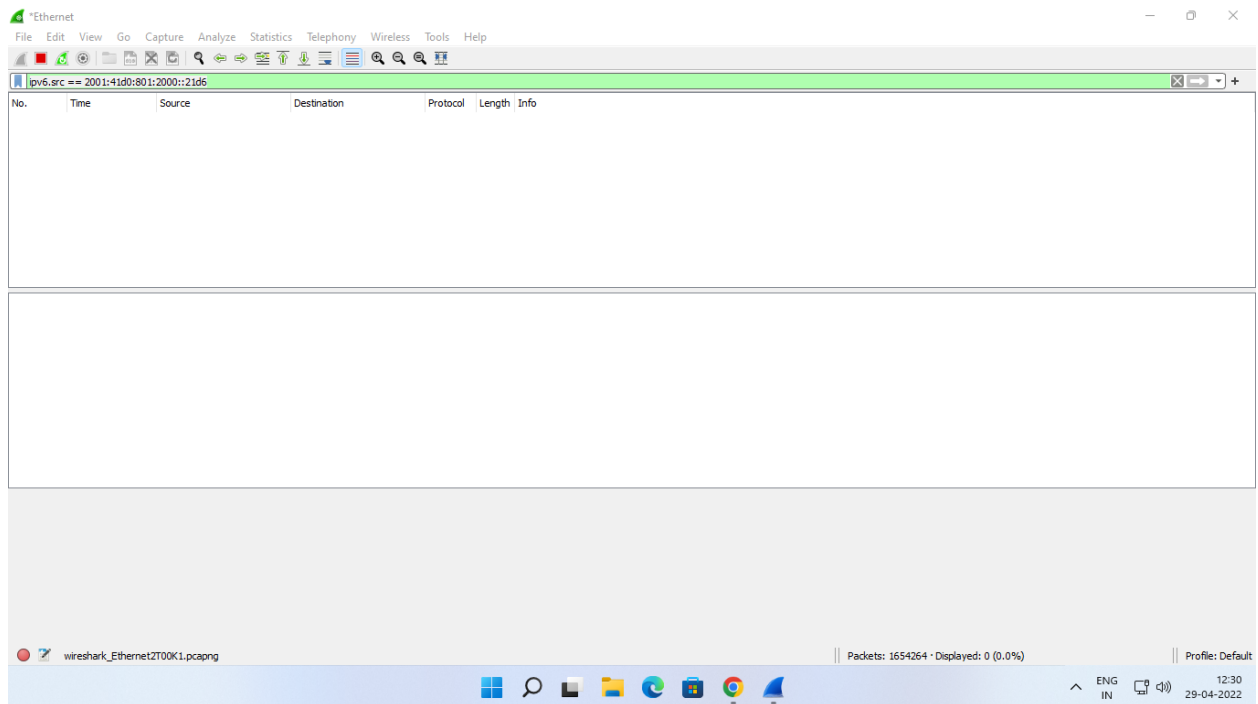
7. ip.src==192.168.29.191 && ip.addr==74.125.250.17



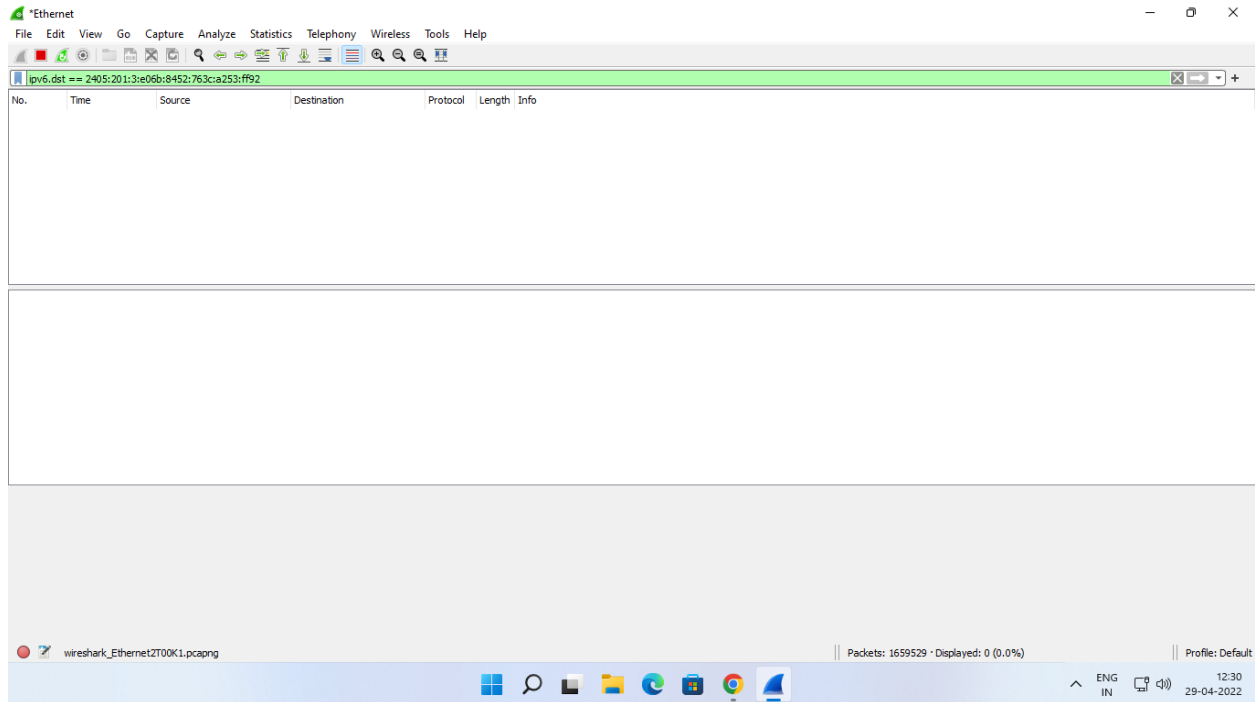
8. ip.addr eq 192.168.29.191 && ip.addr eq 74.125.250.17



9. ipv6.src == 2001:41d0:801:2000::21d6



10. ipv6.dst == 2405:201:3:e06b:8452:763c:a253:ff92



Conclusion:

We have successfully performed the aim of the experiment.