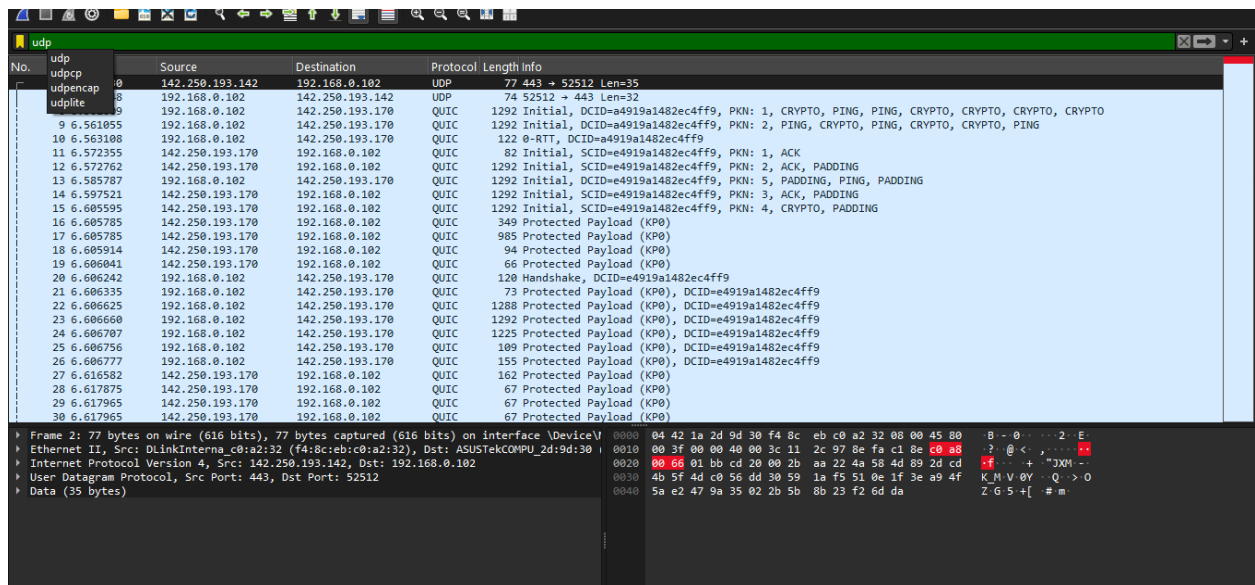
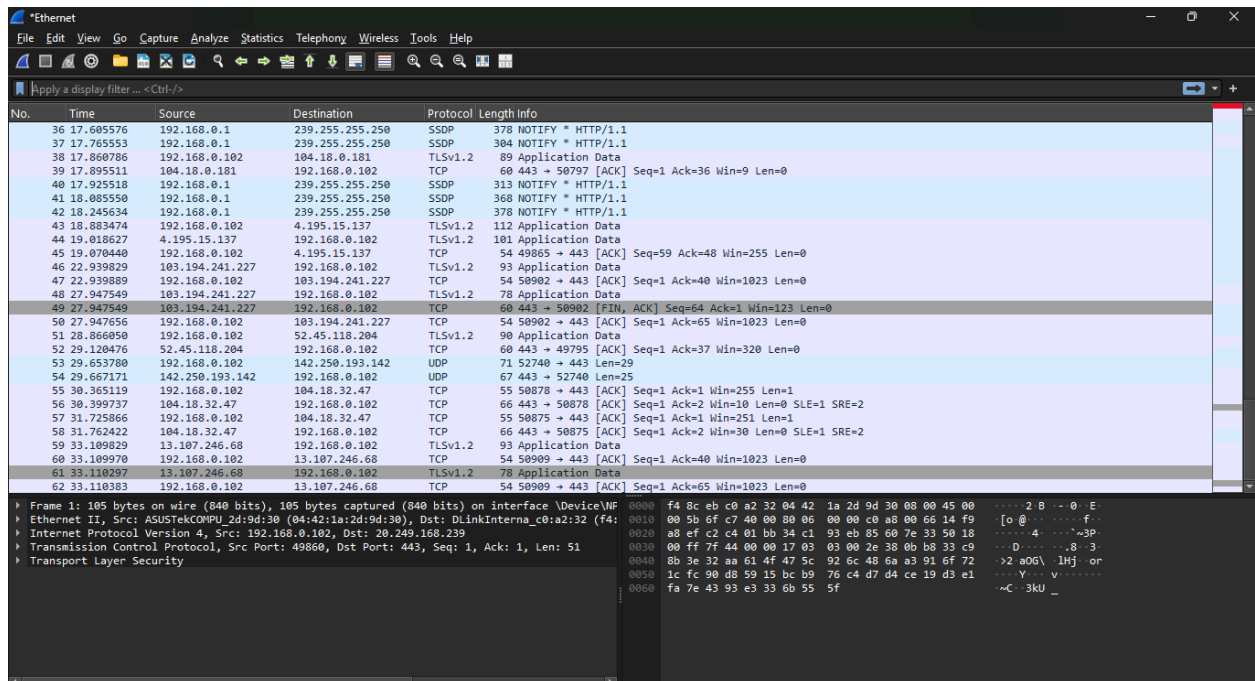


Wireshark Tool Usage :

Starting to capture and filter based on UDP protocol is done here.



Using “tcpdump” command in Linux :

Capturing packets passing in Ethernet 0:

```
Other Linux 6.x kernel 64-bit ...
makunochiippo@makunochi: ~
File Actions Edit View Help
(makunochiippo@makunochi)-[~]
$ sudo tcpdump -i eth0
[sudo] password for makunochiippo:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:25:35.708036 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:25:35.737772 IP 192.168.32.136.37191 > 192.168.32.2.domain: 27493+ PTR? 2.32.168.192.in-addr.arpa. (43)
14:25:35.786080 IP 192.168.32.2.domain > 192.168.32.136.37191: 27493- 0/0/0 (43)
14:25:35.786233 IP 192.168.32.136.39935 > 192.168.32.2.domain: 27493+ PTR? 2.32.168.192.in-addr.arpa. (43)
14:25:35.834706 IP 192.168.32.2.domain > 192.168.32.136.39935: 27493- 0/0/0 (43)
14:25:35.834877 IP 192.168.32.136.38235 > 192.168.32.2.domain: 50923+ PTR? 1.32.168.192.in-addr.arpa. (43)
14:25:35.887446 IP 192.168.32.2.domain > 192.168.32.136.38235: 50923- 0/0/0 (43)
14:25:35.887585 IP 192.168.32.136.45513 > 192.168.32.2.domain: 50923+ PTR? 1.32.168.192.in-addr.arpa. (43)
14:25:36.738605 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:25:37.689392 IP 192.168.32.2.domain > 192.168.32.136.45513: 50923- 0/0/0 (43)
14:25:37.690476 IP 192.168.32.136.56349 > 192.168.32.2.domain: 12546+ PTR? 136.32.168.192.in-addr.arpa. (45)
14:25:37.707054 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:25:37.736306 IP 192.168.32.2.domain > 192.168.32.136.56349: 12546- 0/0/0 (45)
14:25:37.736429 IP 192.168.32.136.48877 > 192.168.32.2.domain: 12546+ PTR? 136.32.168.192.in-addr.arpa. (45)
14:25:37.781187 IP 192.168.32.2.domain > 192.168.32.136.48877: 12546- 0/0/0 (45)
```

Filtering using IP address

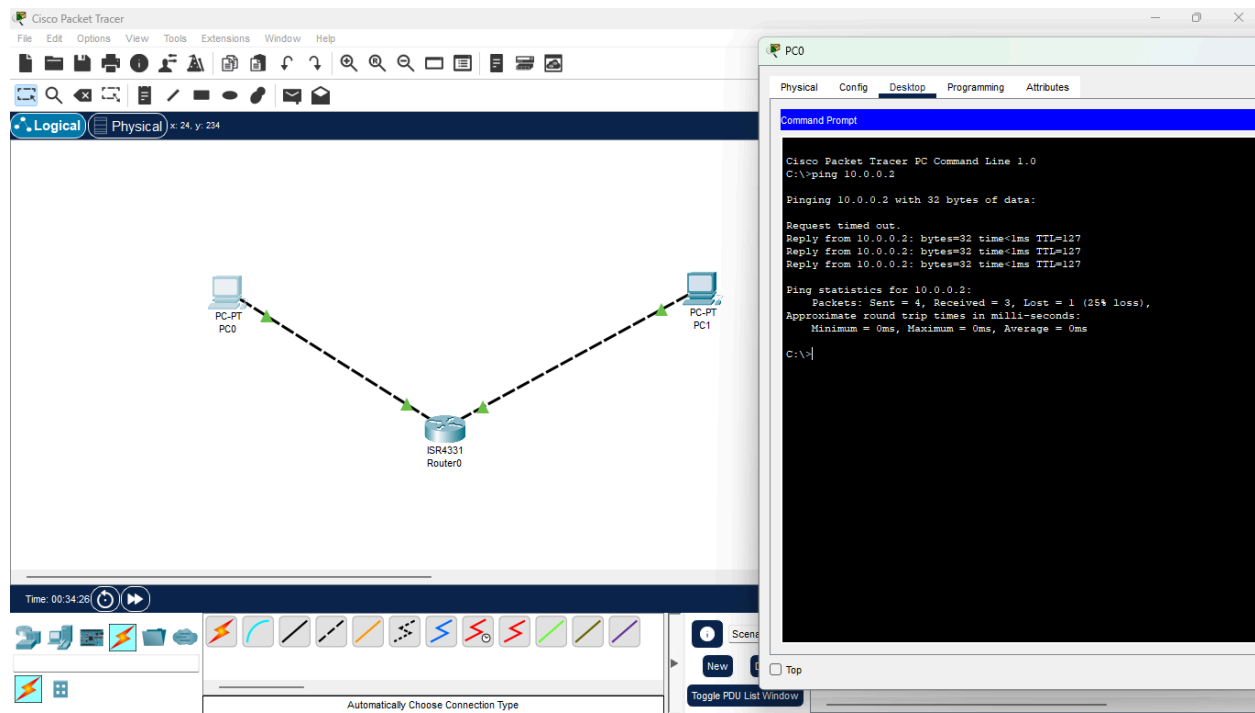
```
(makunochiippo@makunochi)-[~]
$ sudo tcpdump -i eth0 -w capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C36 packets captured
36 packets received by filter
0 packets dropped by kernel
(makunochiippo@makunochi)-[~]
$ tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
14:31:35.679207 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:36.740918 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:37.678836 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:38.680139 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:44.294587 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:45.191397 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:46.179056 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:47.318495 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:48.183359 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:49.186168 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:53.364621 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:54.183876 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:55.186752 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:56.381610 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:57.184163 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:57.389255 IP 192.168.32.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/2 PTR DESKTOP-PKPBI5I._dosvc._tcp.local. (300)
14:31:57.390699 IP6 fe80::4d0b:fd6:e710:cf13.mdns > ff02::fb.mdns: 0*- [0q] 1/0/2 PTR DESKTOP-PKPBI5I._dosvc._tcp.local. (300)
14:31:57.391301 IP 192.168.32.1.mdns > mdns.mcast.net.mdns: 0 ANY (QM)? DESKTOP-PKPBI5I._dosvc._tcp.local. (51)
```

Reading Captured packets in a file for further analysis:

```
(makunochiippo@makunochi)-[~]
$ sudo tcpdump -i eth0 -w capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C36 packets captured
36 packets received by filter
0 packets dropped by kernel
(makunochiippo@makunochi)-[~]
$ tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
14:31:35.679207 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:36.740918 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:37.678836 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:38.680139 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:44.294587 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:45.191397 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:46.179056 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:47.318495 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:48.183359 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:49.186168 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:53.364621 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:54.183876 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:55.186752 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:56.381610 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:57.184163 ARP, Request who-has 192.168.32.2 tell 192.168.32.1, length 46
14:31:57.389255 IP 192.168.32.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/2 PTR DESKTOP-PKPBI5I._dosvc._tcp.local. (300)
14:31:57.390699 IP6 fe80::4d0b:fd6:e710:cf13.mdns > ff02::fb.mdns: 0*- [0q] 1/0/2 PTR DESKTOP-PKPBI5I._dosvc._tcp.local. (300)
14:31:57.391301 IP 192.168.32.1.mdns > mdns.mcast.net.mdns: 0 ANY (QM)? DESKTOP-PKPBI5I._dosvc._tcp.local. (51)
```

Using Cisco Packet Tracer tool :

Providing a connection for 2 PC's through router and establishing the network



ICMP packets receiving access is provided using router configuring:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#access-list 100 permit icmp any any
```

```
Router(config)#access-list 100 deny icmp any any
```

```
Router(config)#interface GigabitEthernet 0/0/0
```

```
Router(config-if)#ip access-group 100 in
```

```
Router(config-if)#exit
```

```
Router(config)#exit
```

```
Router#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#write memory
```

```
Building configuration...
```

```
[OK]
```

```
Router#
```

```
Router#
```