

Lab 8

Name- Adarsh Nandanwar
BITS ID- 2018A7PS0396G

Customizing Wireshark

Activities Wireshark - Apr 12 00:45

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

capture.pcapng

Apply a display filter... <Ctrl/>

Time	Source	Src. Port	Destination	Dest. Port	Protocol	Packet Len	IP	Len IP	He	TCP	TCP Tr	Info
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	183	169	20				Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _f...
2021-04-11 19:09:00	192.168.0.195	35773	192.168.0.1	53	DNS	92	78	20				Standard query 0xe913 A predator-pop-os.Dlink OPT
2021-04-11 19:09:00	192.168.0.195	60713	192.168.0.1	53	DNS	92	78	20				Standard query 0x8278 AAAA predator-pop-os.Dlink OPT
2021-04-11 19:09:00	192.168.0.1	53	192.168.0.195	35773	DNS	108	94	20				Standard query response 0xe913 A predator-pop-os.Dlink A 192.168...
2021-04-11 19:09:00	192.168.0.1	53	192.168.0.195	60713	DNS	92	78	20				Standard query response 0x8278 AAAA predator-pop-os.Dlink OPT
2021-04-11 19:09:00	Espresso_7f:33:08	Broadcast		ARP	42							ARP Announcement for 192.168.0.152
2021-04-11 19:09:00	192.168.0.192	49154	255.255.255.255	6667	UDP	230	216	20				49154 - 6667 Len=188
2021-04-11 19:09:00	192.168.0.195	68	192.168.0.1	67	DHCP	342	328	20				DHCP Release - Transaction ID 0x951fb2a
2021-04-11 19:09:00	0.0.0.0	68	255.255.255.255	67	DHCP	342	328	20				DHCP Discover - Transaction ID 0x3384e975
2021-04-11 19:09:00	192.168.0.1	67	192.168.0.195	68	DHCP	342	328	20				DHCP Offer - Transaction ID 0x3384e975
2021-04-11 19:09:00	0.0.0.0	68	255.255.255.255	67	DHCP	342	328	20				DHCP Request - Transaction ID 0x3384e975
2021-04-11 19:09:00	192.168.0.1	67	192.168.0.195	68	DHCP	358	344	20				DHCP ACK - Transaction ID 0x3384e975
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	183	169	20				Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _f...
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	259	245	20				Standard query 0x0000 ANY 3.1.7.9.8.9.2.6.8.4.0.2.5.f.b.c.0.0.0...
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	259	245	20				Standard query 0x0000 ANY 3.1.7.9.8.9.2.6.8.4.0.2.5.f.b.c.0.0.0...
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	259	245	20				Standard query 0x0000 ANY 3.1.7.9.8.9.2.6.8.4.0.2.5.f.b.c.0.0.0...
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	241	227	20				Standard query response 0x0000 PTR, cache flush predator-pop-os...
2021-04-11 19:09:00	192.168.0.152	49154	255.255.255.255	6667	UDP	230	216	20				49154 - 6667 Len=188
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	82	68	20				Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	82	68	20				Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2021-04-11 19:09:00	LiteonTe_b9:98:87	Broadcast		ARP	42							Who has 192.168.0.17 Tell 192.168.0.195
2021-04-11 19:09:00	D-LinkIn_45:a1:82	LiteonTe_b9:98:87		ARP	42							192.168.0.1 is at c4:e9:0a:45:a1:82
2021-04-11 19:09:00	192.168.0.195	33625	192.168.0.1	53	DNS	89	75	20				Standard query 0x3c5d A eyyrtdgpbntbl.Dlink OPT
2021-04-11 19:09:00	192.168.0.195	38683	192.168.0.1	53	DNS	90	76	20				Standard query 0xac11 A mimnvccielegcc.Dlink OPT
2021-04-11 19:09:00	192.168.0.195	59690	192.168.0.1	53	DNS	84	70	20				Standard query 0x9233 A eimshhh.Dlink OPT
2021-04-11 19:09:00	192.168.0.1	53	192.168.0.195	33625	DNS	164	150	20				Standard query response 0x3c5d No such name A eyyrtdgpbntbl.Dlink...
2021-04-11 19:09:00	192.168.0.195	33625	192.168.0.1	53	DNS	78	64	20				Standard query 0x3c5d A eyyrtdgpbntbl.Dlink
2021-04-11 19:09:00	192.168.0.1	53	192.168.0.195	33625	DNS	153	139	20				Standard query response 0x3c5d No such name A eyyrtdgpbntbl.Dlink...
2021-04-11 19:09:00	192.168.0.195	5353	224.0.0.251	5353	MDNS	183	169	20				Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _f...
2021-04-11 19:09:00	192.168.0.1	53	192.168.0.195	59690	MDNS	159	145	20				Standard query response 0x9233 No such name A eimshhh.Dlink SOA ...

Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface wlp2s0, id 0

Ethernet II, Src: LiteonTe_b9:98:87 (98:22:ef:b9:98:87), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)

Internet Protocol Version 4, Src: 192.168.0.195, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (query)

capture.pcapng

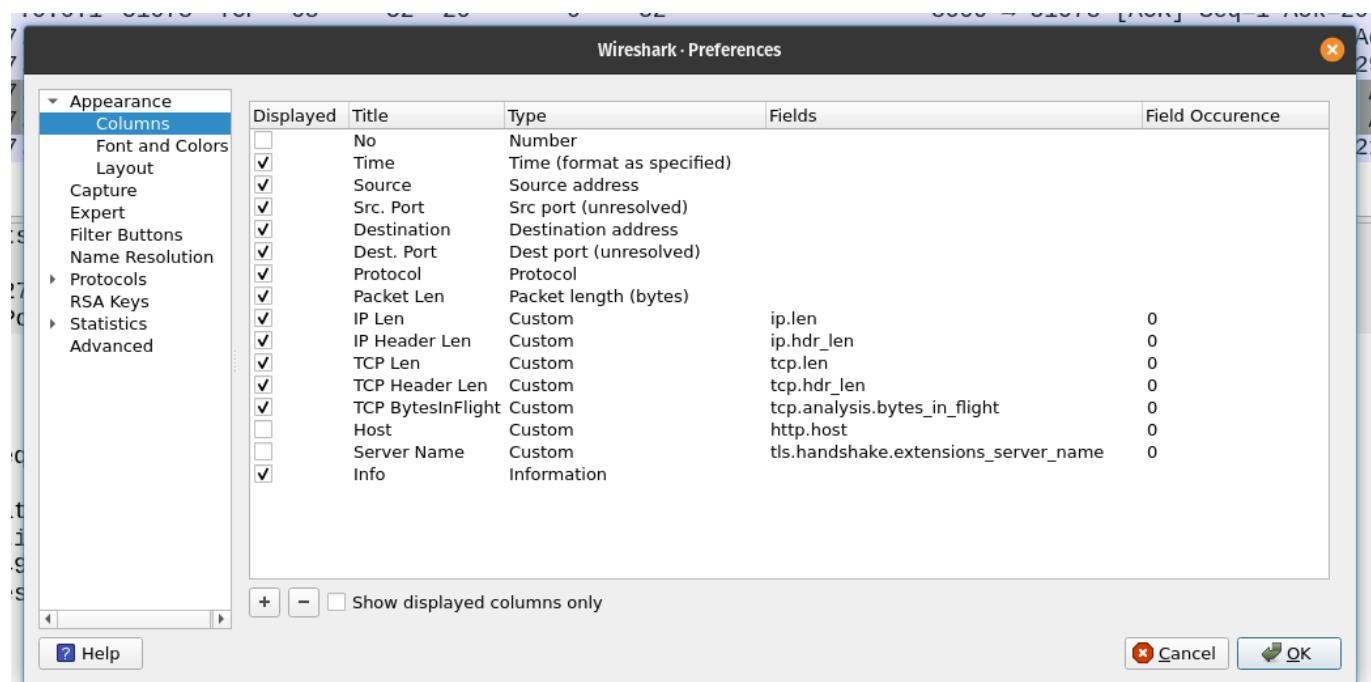
Packets: 177 - Displayed: 177 (100.0%) - Dropped: 0 (0.0%)

Profile: CS F303

Columns:

- No. (Hidden)
 - Date & time in UTC
 - Source IP
 - Source port
 - Destination IP
 - Destination port
 - Protocol
 - Packet Length
 - IP Length `ip.len`
 - IP Header Length `ip.hdr_len`
 - TCP Length `tcp.len`
 - TCP Header Length `tcp.hdr_len`
 - TCP Bytes in Flight `tcp.analysis.bytes_in_flight` - Tells bytes that are sent but not ACKed
 - HTTP host (Hidden) `http.host`
 - HTTPS server (Hidden) `tls.handshake.extensions_server_name`
 - Info

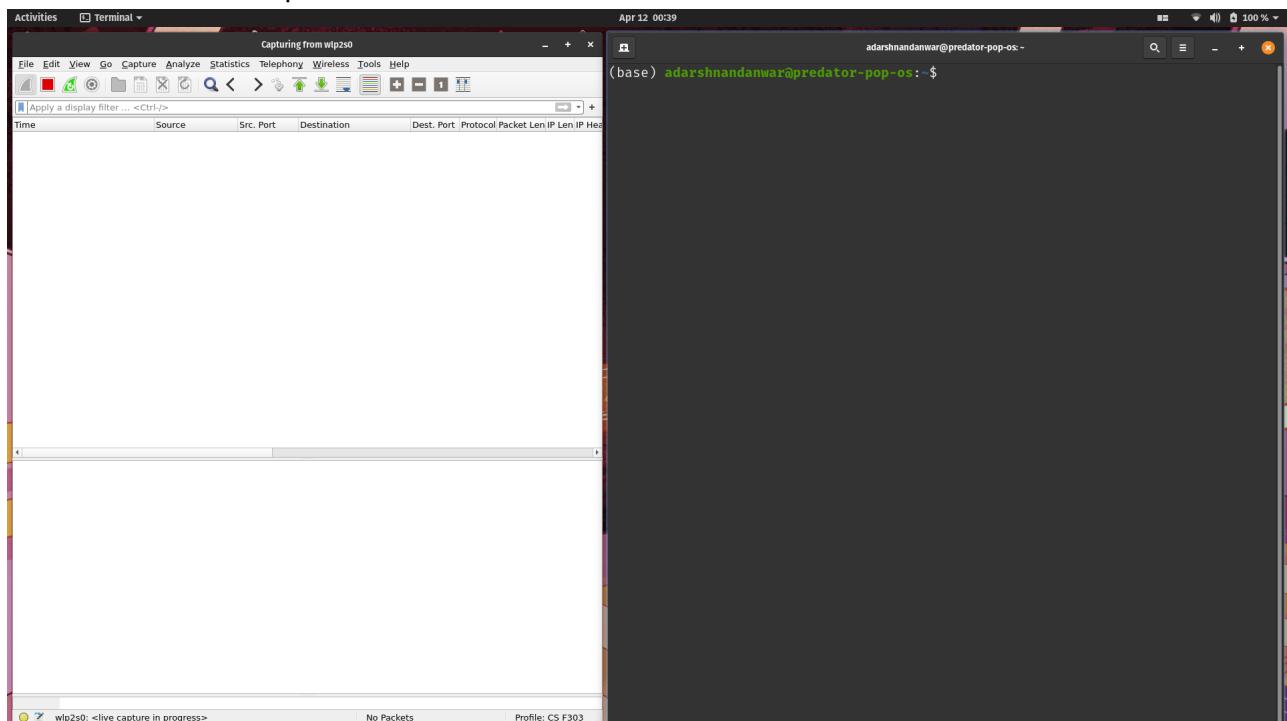
Column Preferences



Program Screenshots

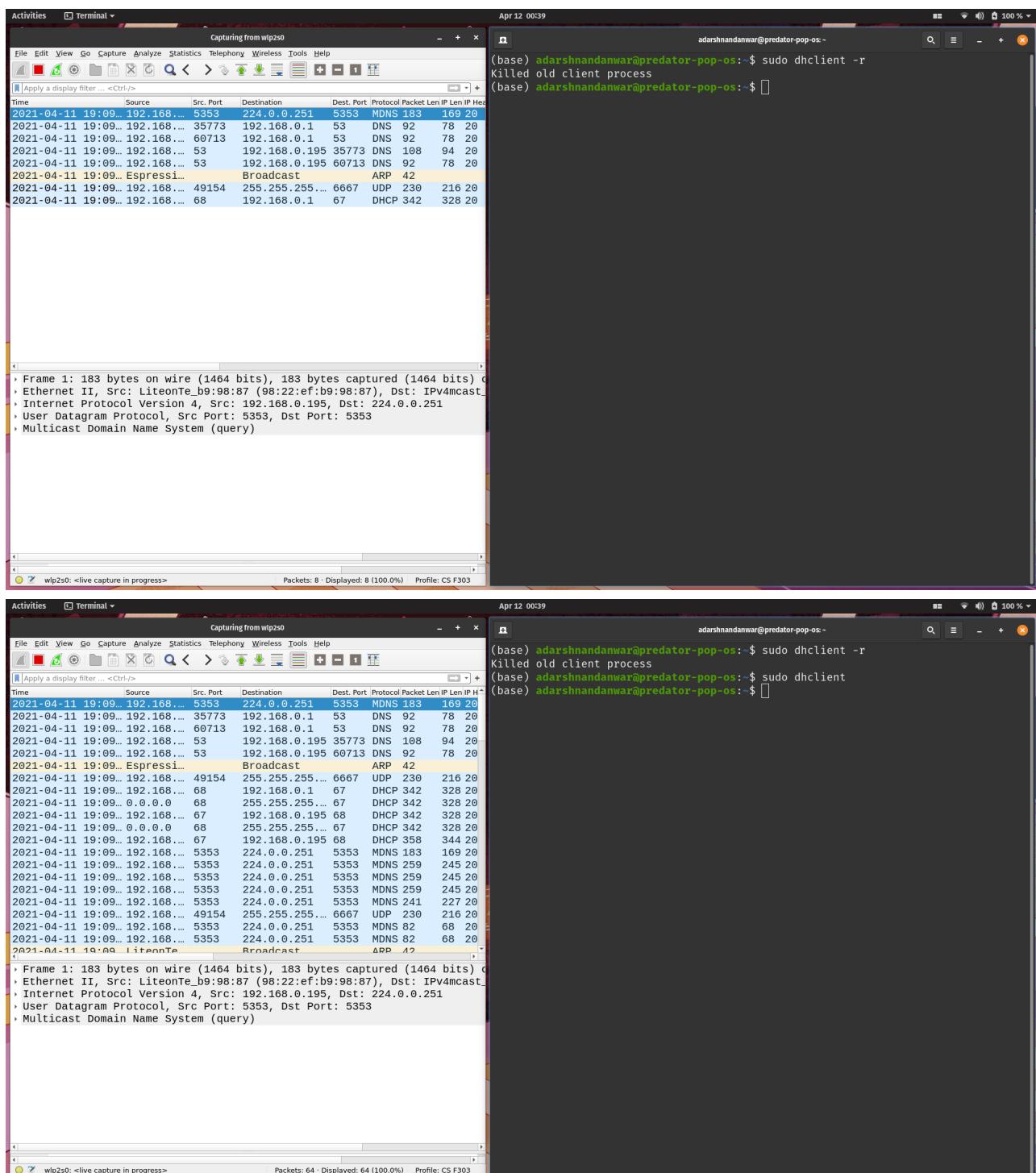
Capturing Packets

- Start the wireshark capture



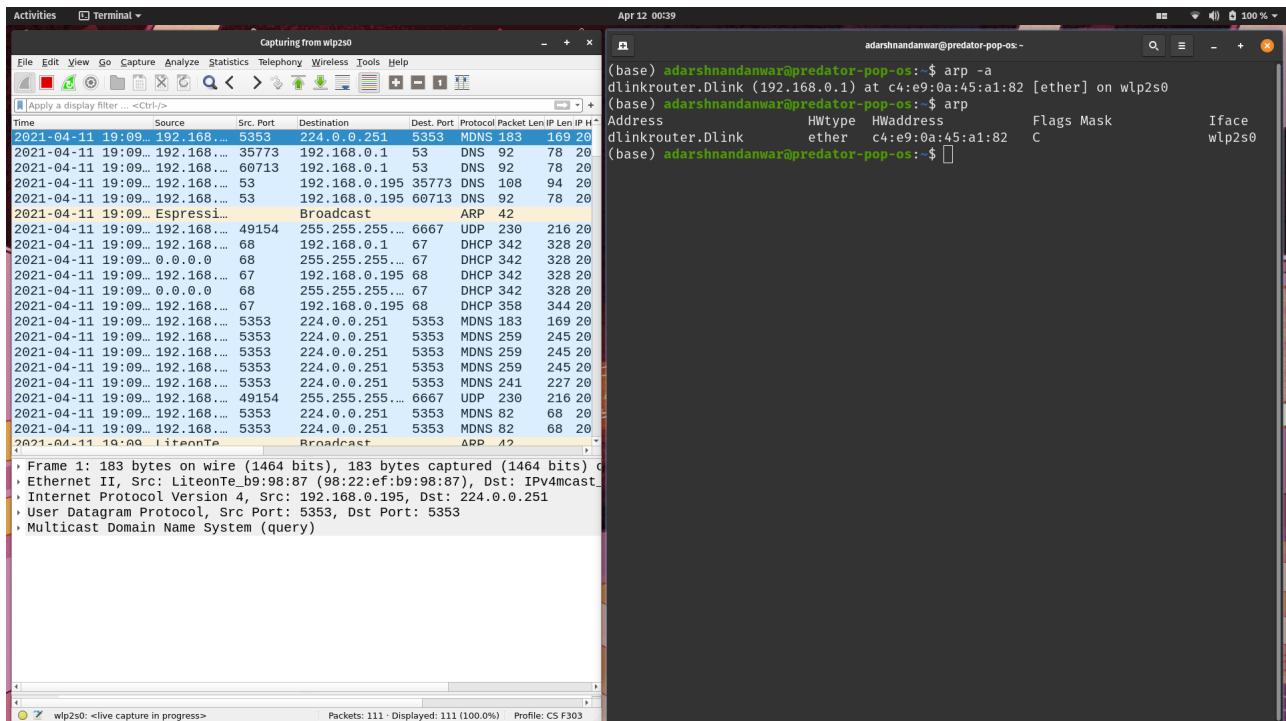
- To see DHCP in action, we must release the current IP address and obtain a new one. Use the following commands in the terminal

```
$ sudo dhclient -r
$ sudo dhclient
```



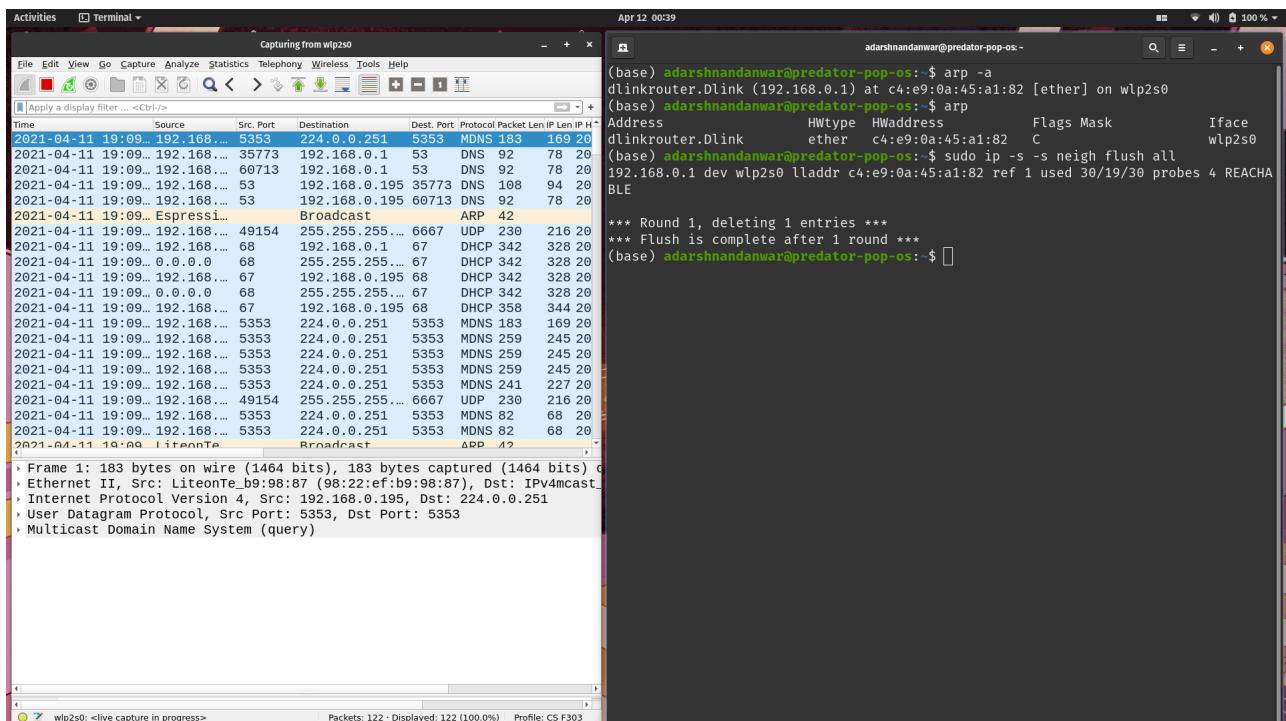
- To view the ARP table, use the following terminal commands:

```
arp -a
arp
```

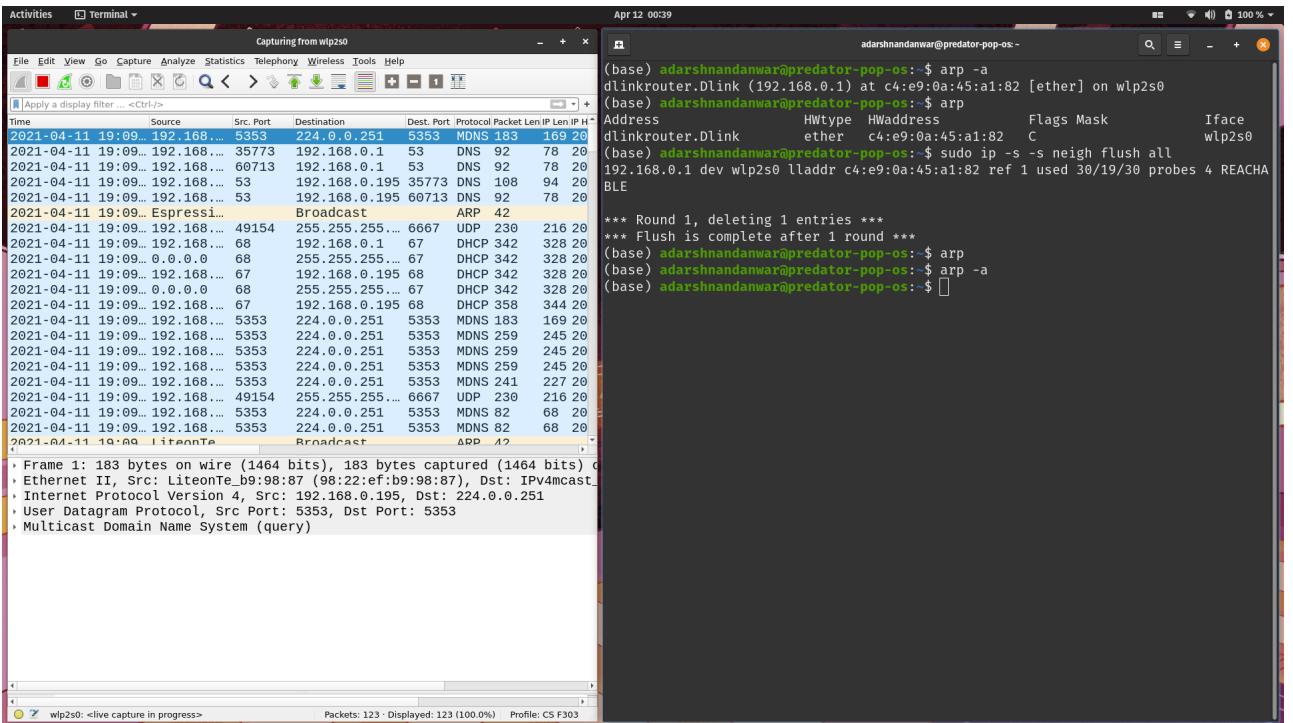


- To flush the ARP table, use:

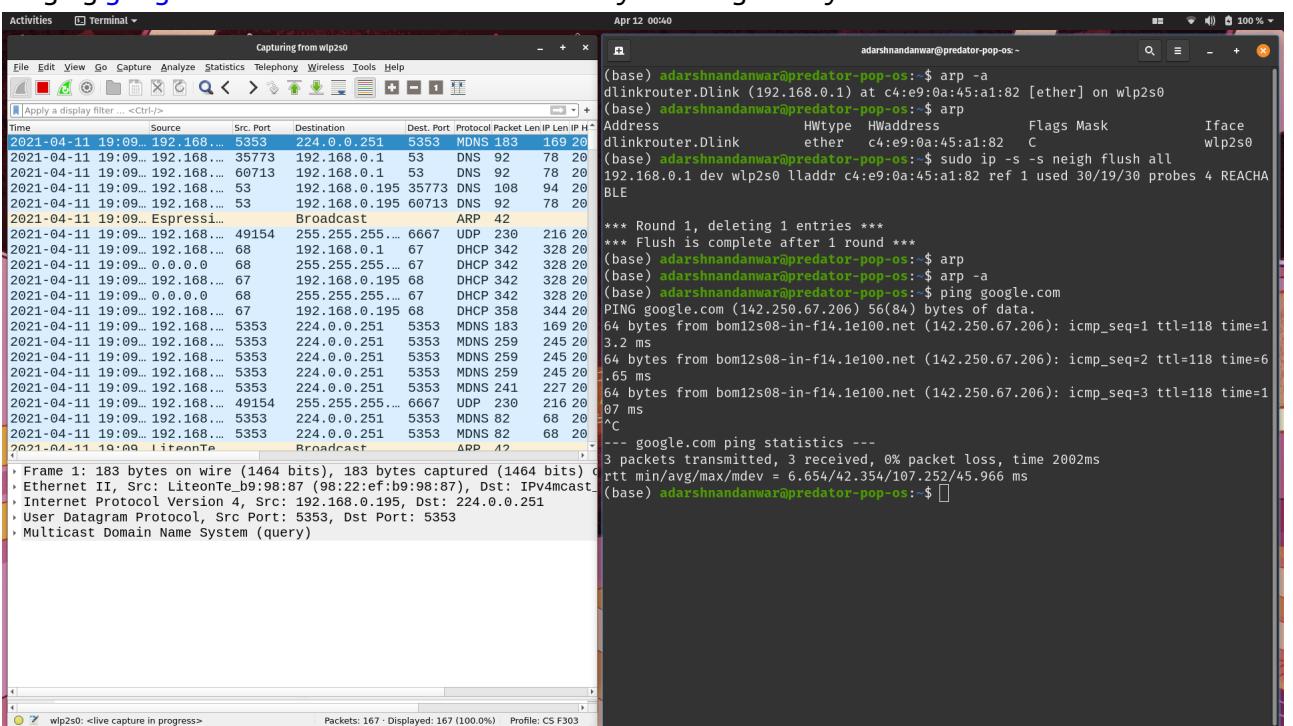
```
$ sudo ip -s -s neigh flush all
```



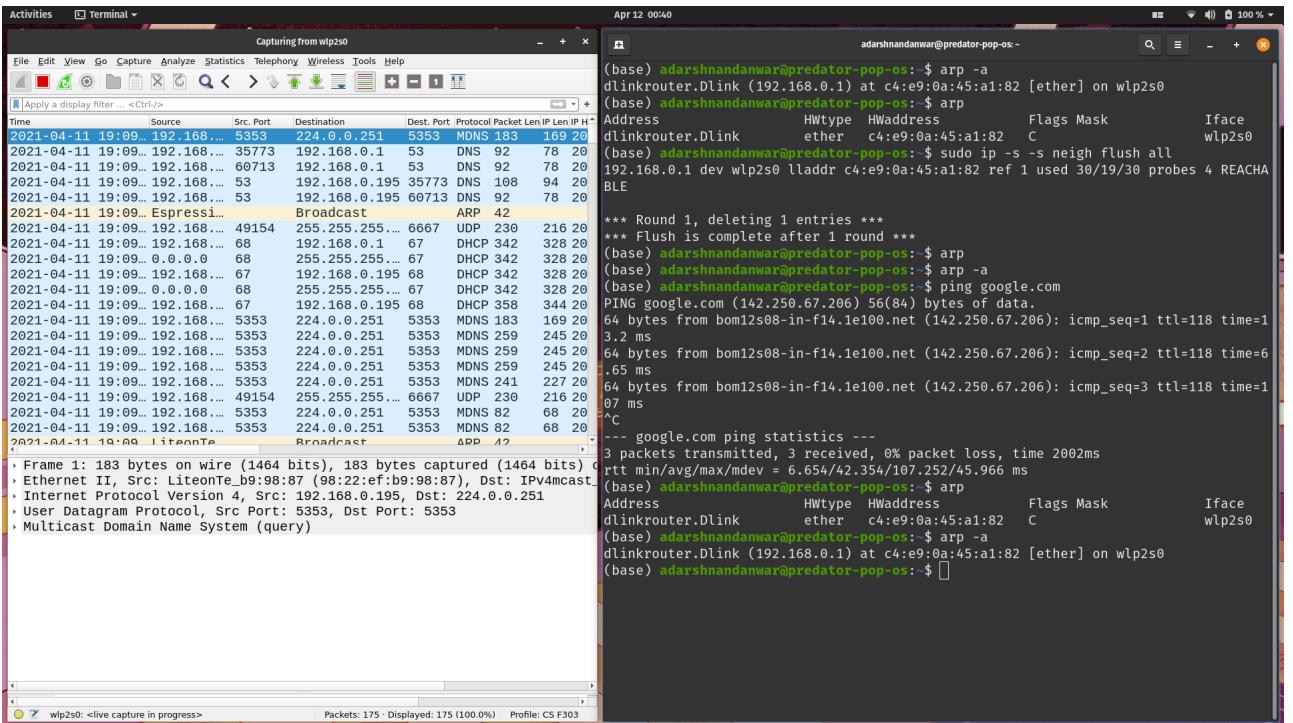
- The ARP table is now empty.



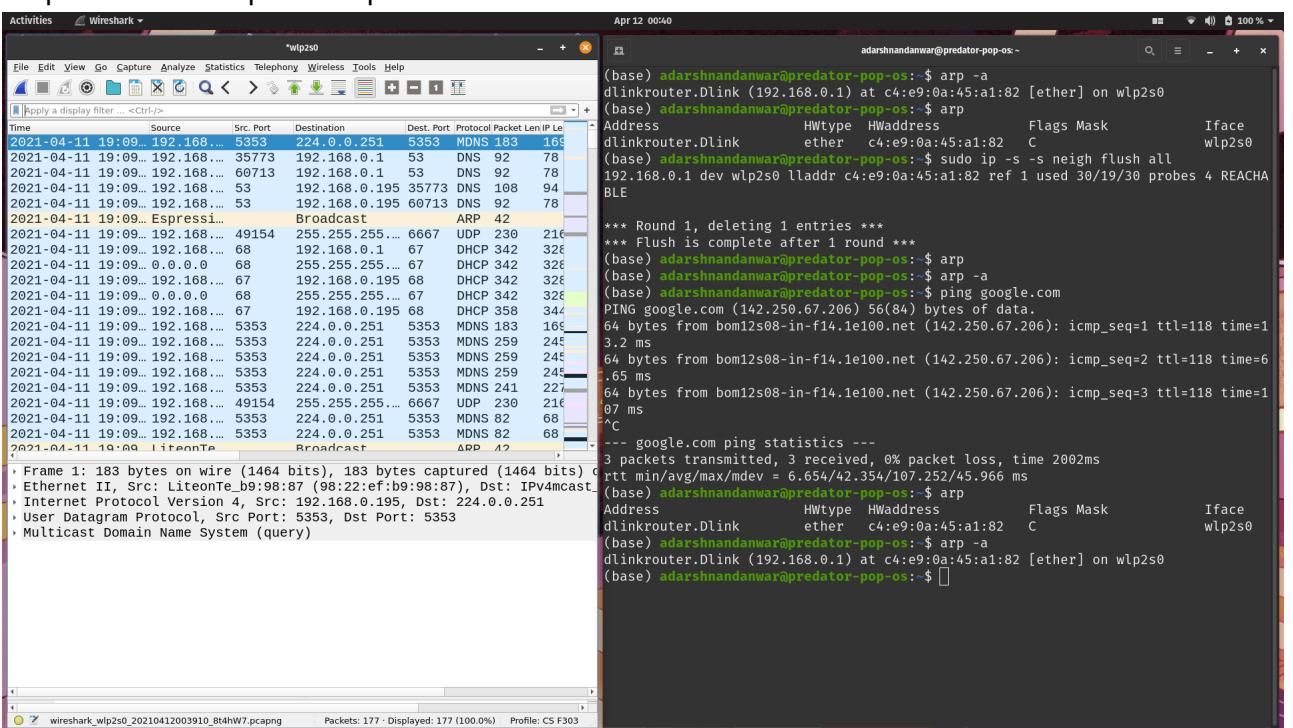
- Pinging google.com to create the ARP table entry for the gateway router.



- The ARP table now has the entry for the gateway router.



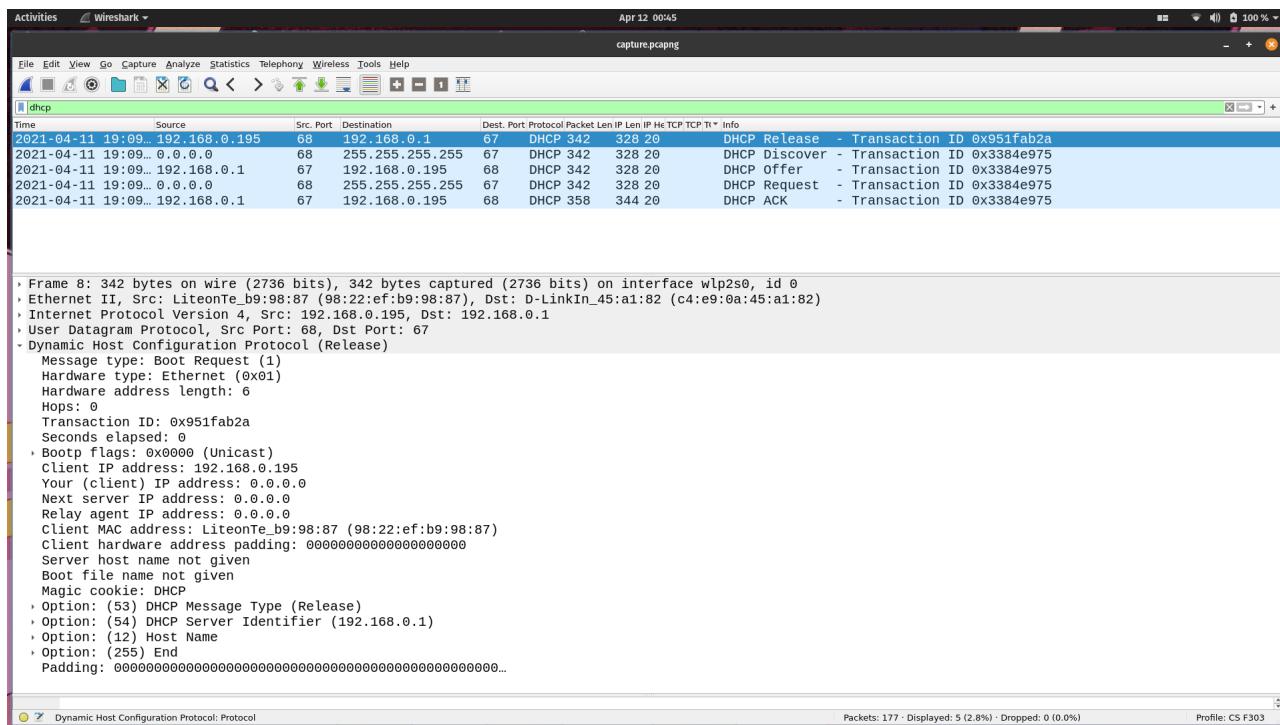
- Stop the wireshark packet capture.



DHCP Protocol

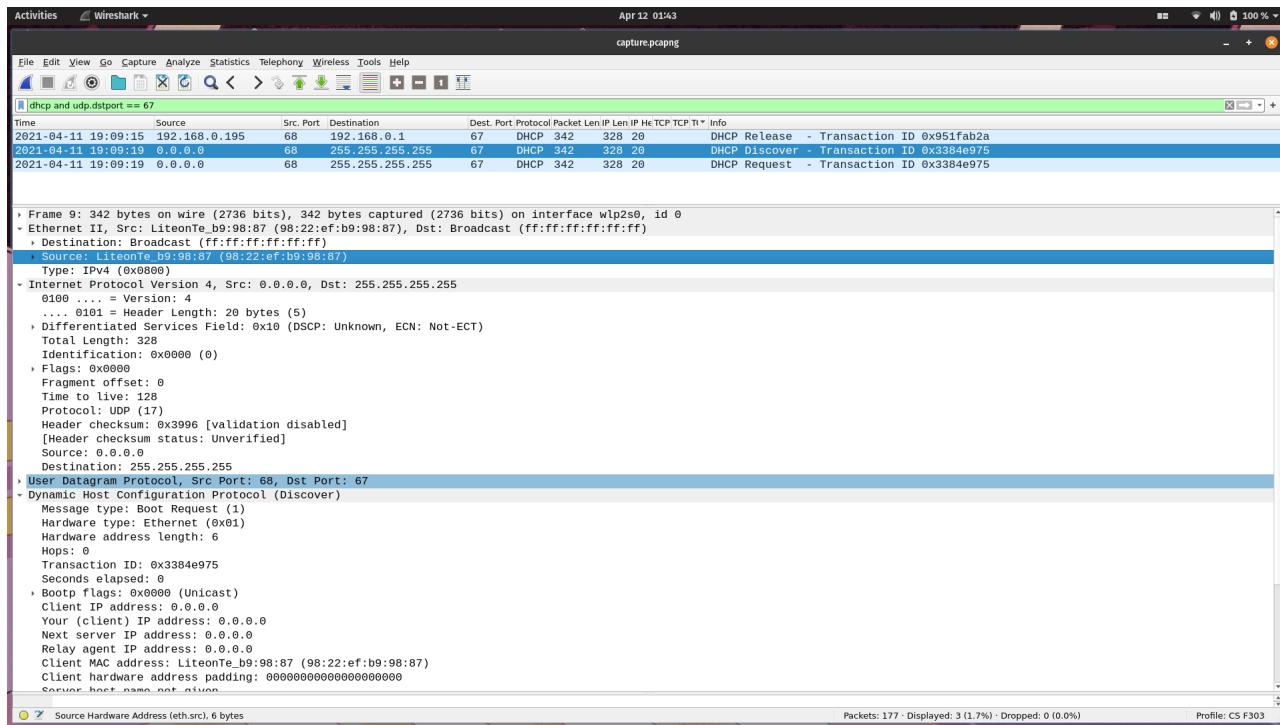
- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and gateway router.
- To see all the dhcp communication, use the following filter in wireshark

```
dhcp
```



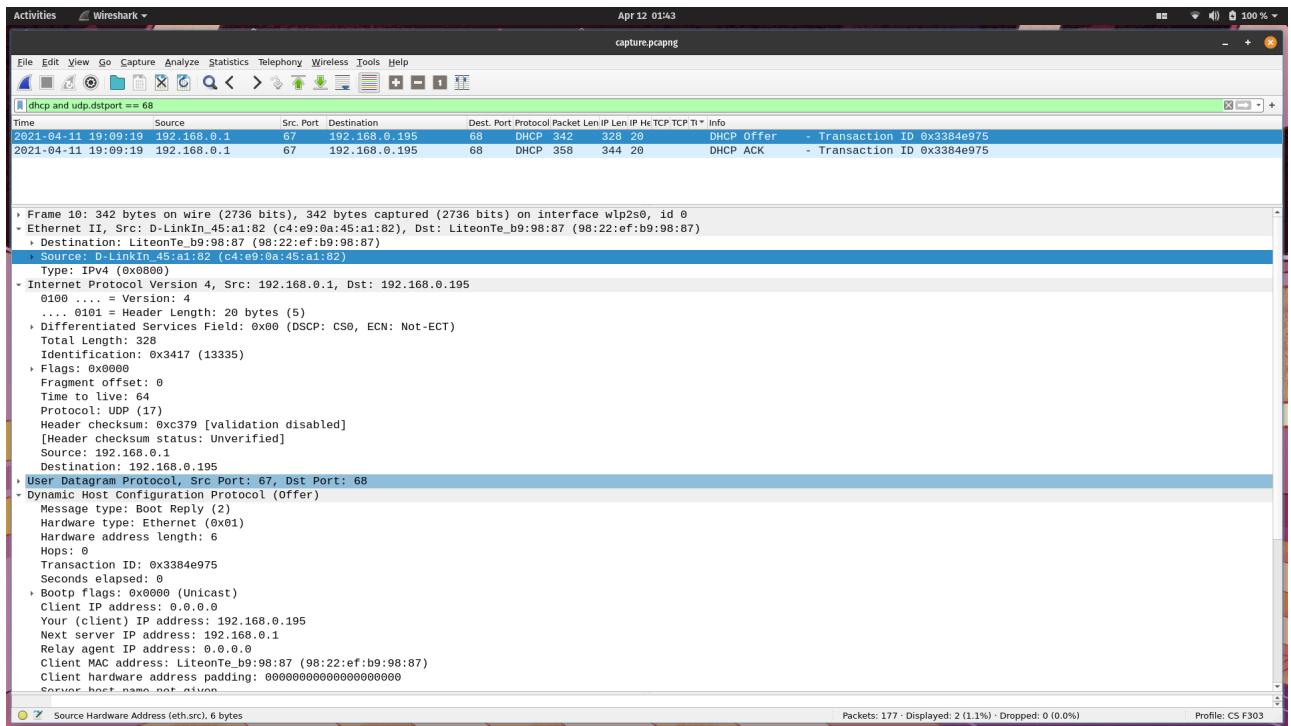
- Packets from client to server port uses port 67 (server port)

dhcp and udp.dstport == 67



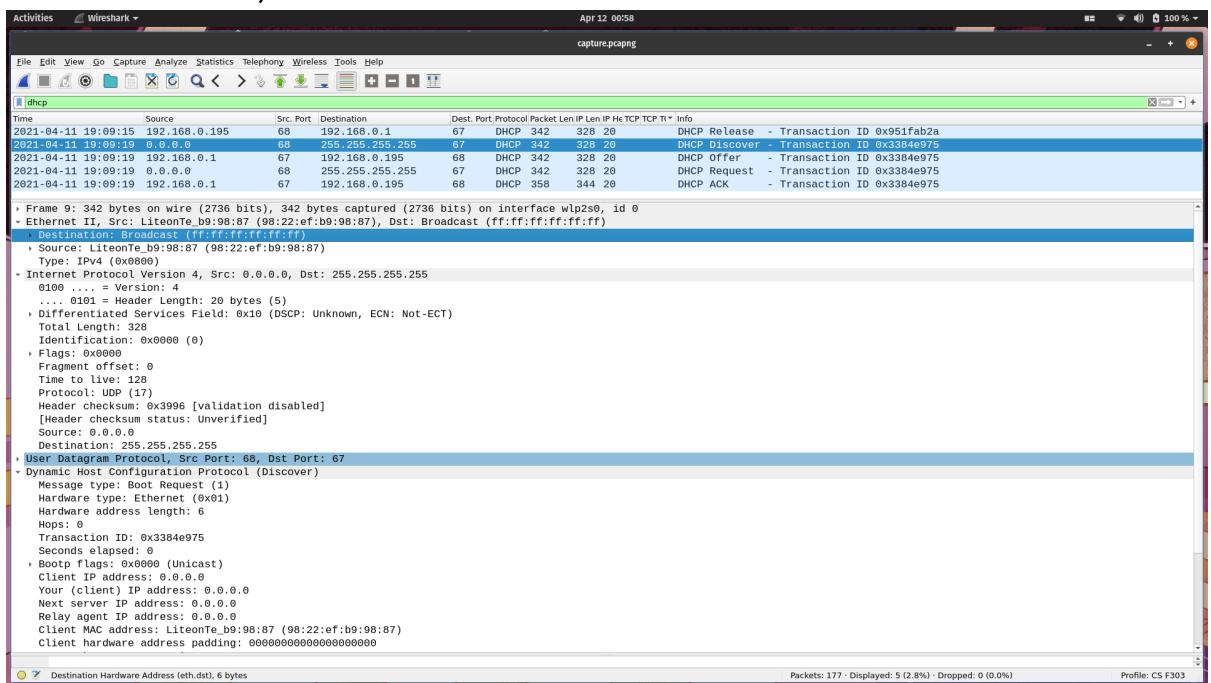
- Packets from server to client port uses port 68 (client port)

dhcp and udp.dstport == 68



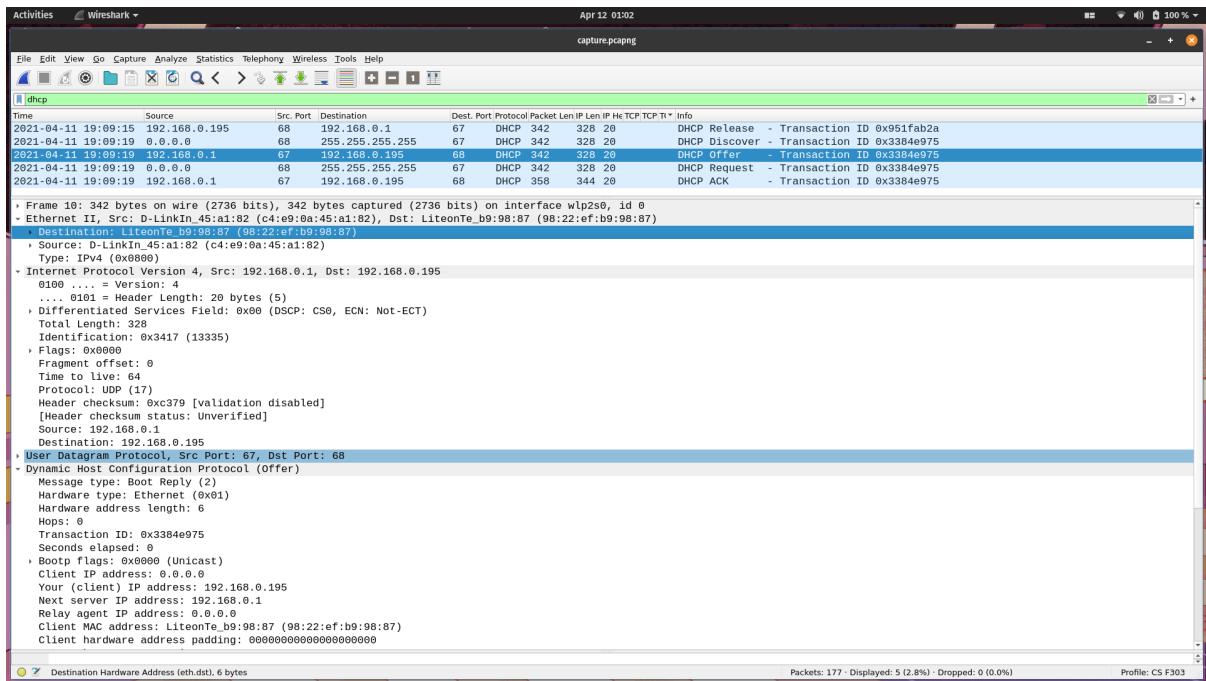
- DHCP is a 4 step protocol:

- DHCP Discover** (request) - whenever a device enters the network, it will not have IP address (source IP = **0.0.0.0**). So, it will ask if there is a DHCP server by broadcasting (destination IP = **255.255.255.255**)



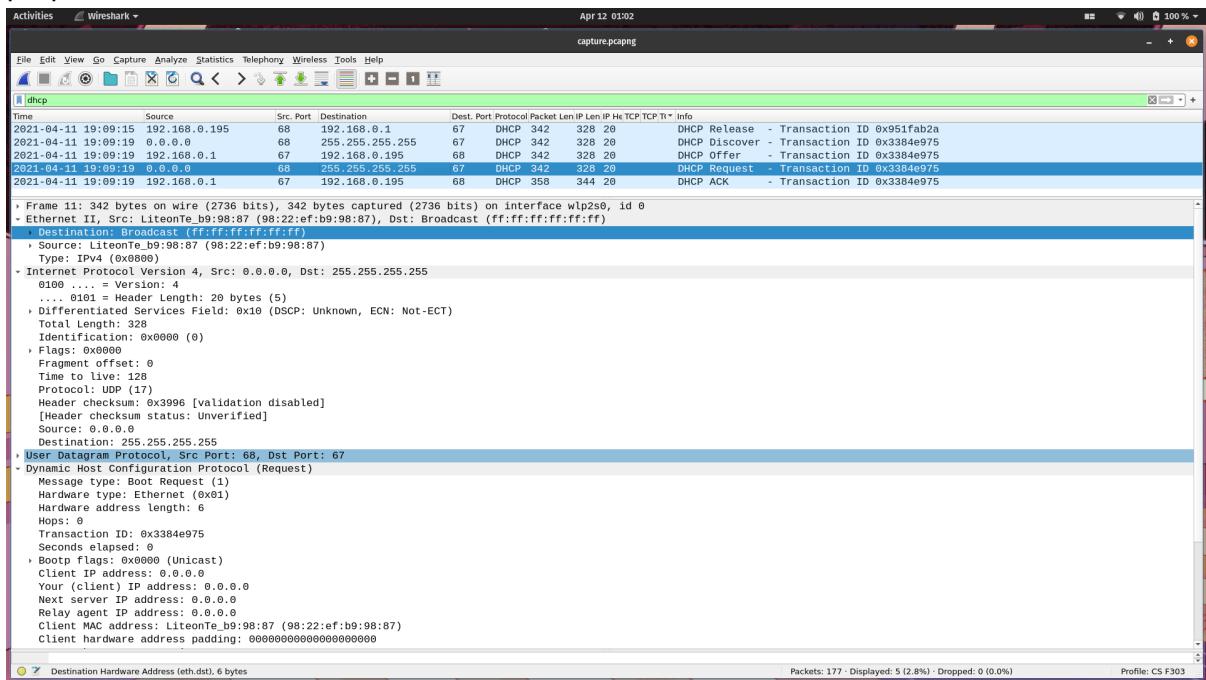
We can see that the destination address is broadcast, source IP address is **0.0.0.0**, source port is **68** and the destination port is **67**. DHCP uses UDP protocol.

- DHCP Offer** (reply) - On receiving the discovery, DHCP offers one of the available IP address to the client.

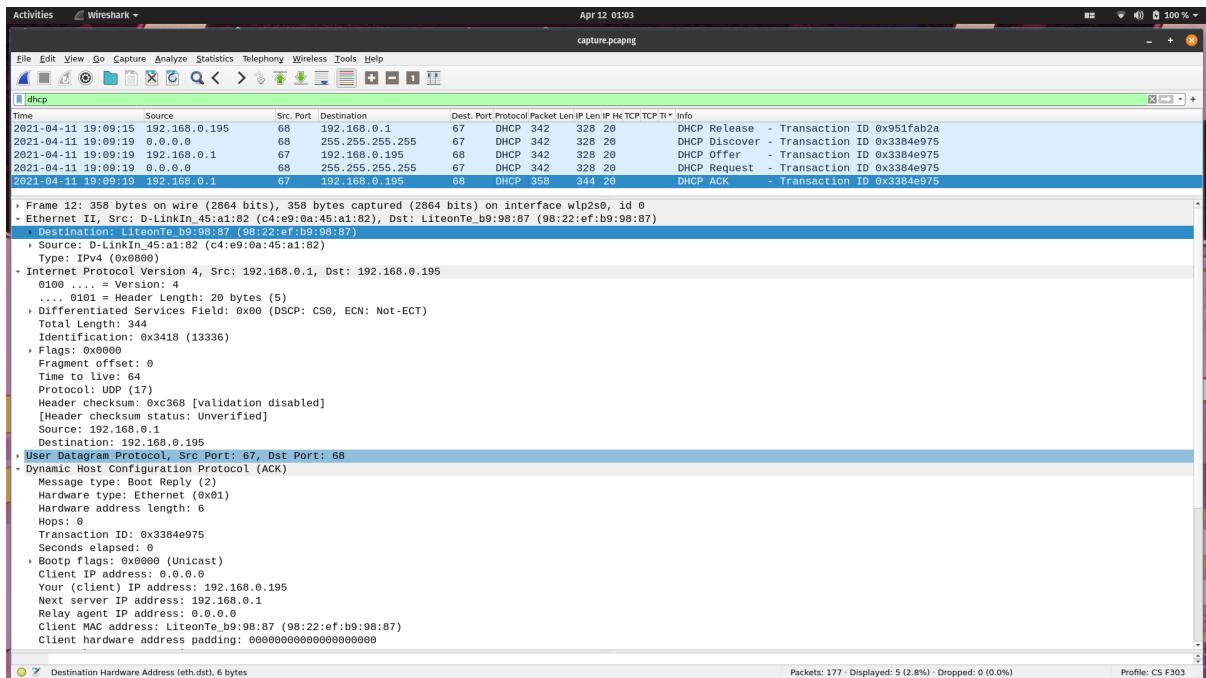


We can see that the source port is 67 and the destination port is 68. The IP address of the DHCP server is 192.168.0.1.

3. DHCP Request - Client confirms the offer that DHCP made and requests to accept the proposed IP address.



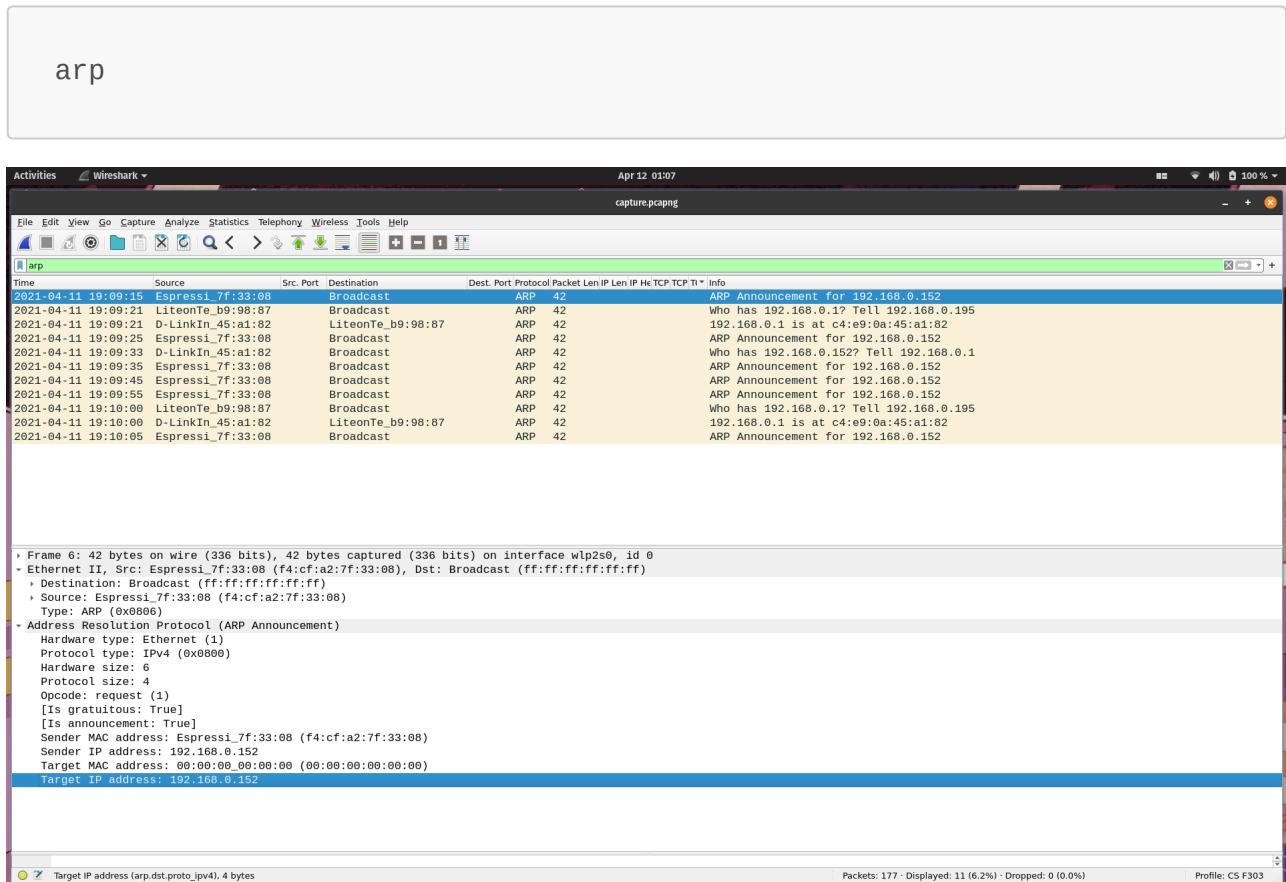
4. DHCP ACK (acknowledgment) - DHCP server acknowledges the client and allocates the IP to the new device.



The IP address allotted to the new client is **192.168.0.195**

ARP Protocol

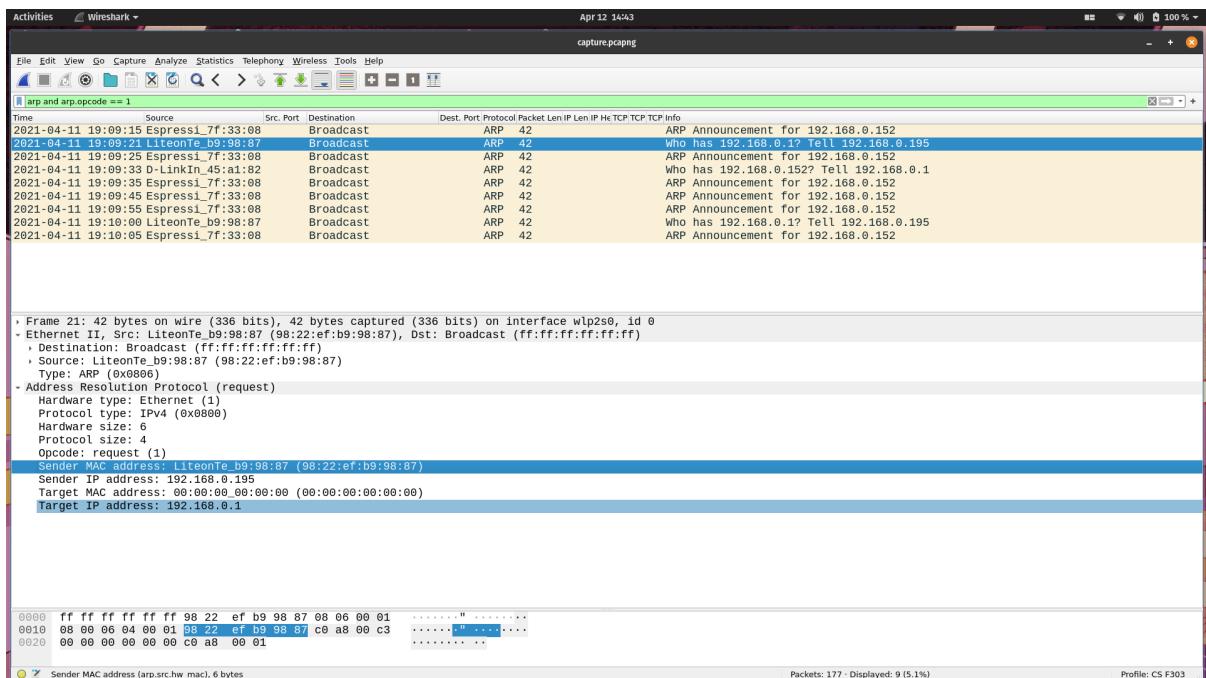
- Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN).
- Wireshark filter to see the ARP packets is



- Now the ARP table is empty. When the client needs to access the internet, it will need MAC address of the gateway router. So it will make an ARP request
- The ARP process consists of:

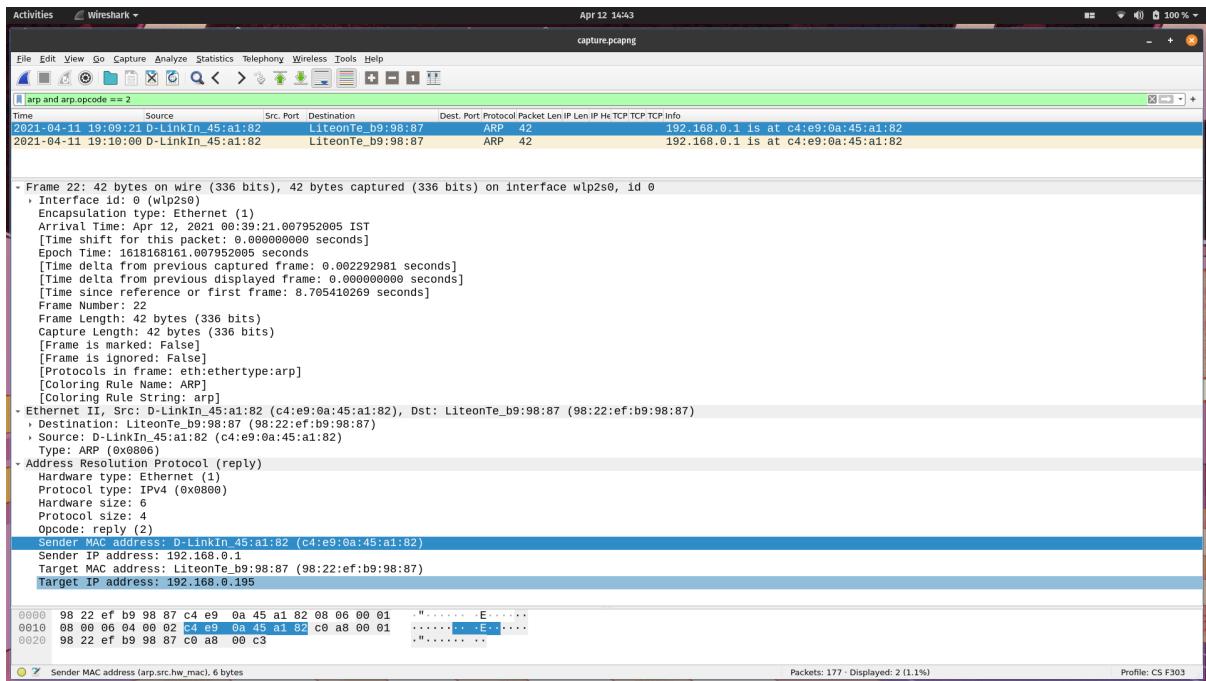
- o **ARP request** - The client broadcasts in the network and asks for the MAC address of the given IP address and asks to tell it to the client. As we can see, the client IP is the source, the destination is broadcast and the Target IP contains the IP for which the client wants to know the MAC address. To filter ARP requests, use:

```
arp and arp.opcode == 1
```



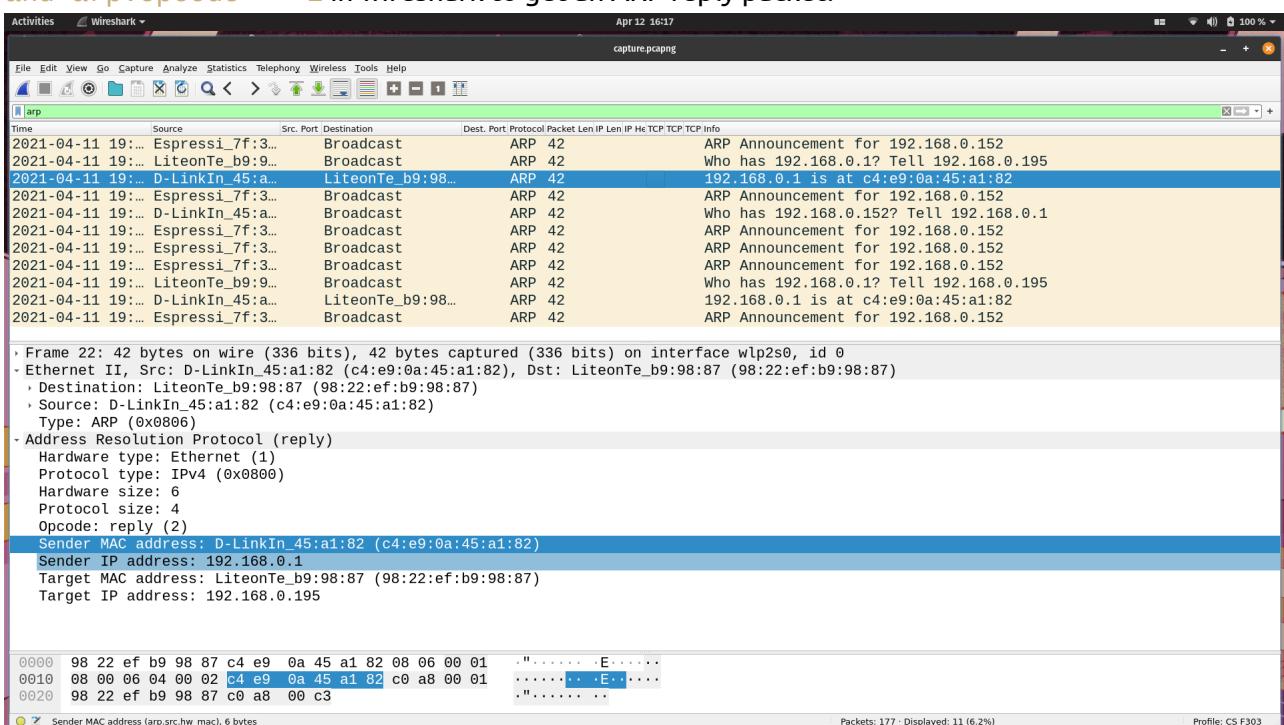
- o **ARP reply** - Only the host with the matching IP address will reply with its MAC address and others will ignore. Source is the host with the requested IP address (which is in this case the gateway router) and the destination is the host who requested the MAC address (client IP address = 192.168.0.195)

```
arp and arp.opcode == 2
```



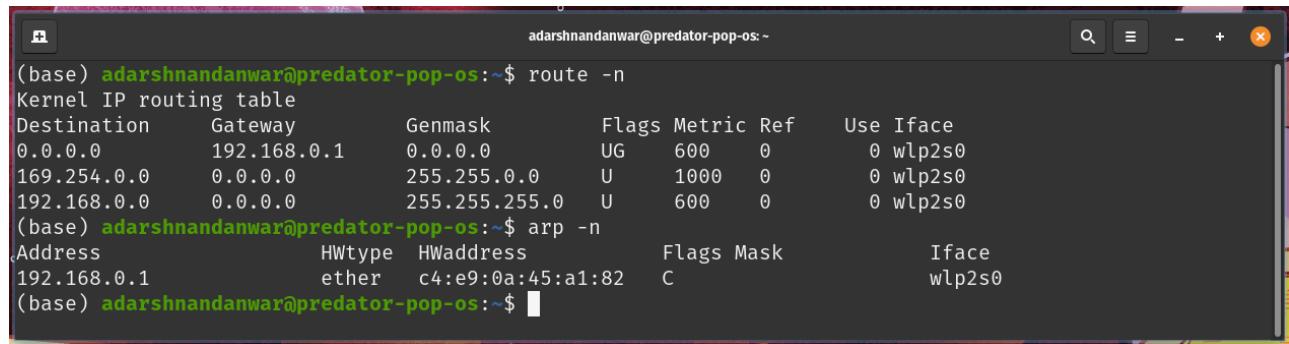
MAC Address of Gateway Router

- To get the MAC address and the IP address of the gateway router, use the same filter arp or arp and arp.opcode == 2 in wireshark to get an ARP reply packet.



- The MAC address and the IP address of the gateway router is highlighted in the screenshot.
 - MAC Address of gateway router = c4:e9:0a:45:a1:82
 - IP Address of gateway router = 192.168.0.1

- MAC address and IP address of the gateway router can also be found using terminal commands:



The screenshot shows a terminal window titled "adarshnandanwar@predator-pop-os:~". It displays two command outputs: the output of the "route -n" command and the output of the "arp -n" command.

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.0.1	0.0.0.0	UG	600	0	0	wlp2s0
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	wlp2s0
192.168.0.0	0.0.0.0	255.255.255.0	U	600	0	0	wlp2s0

arp -n

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.0.1	ether	c4:e9:0a:45:a1:82	C		wlp2s0