

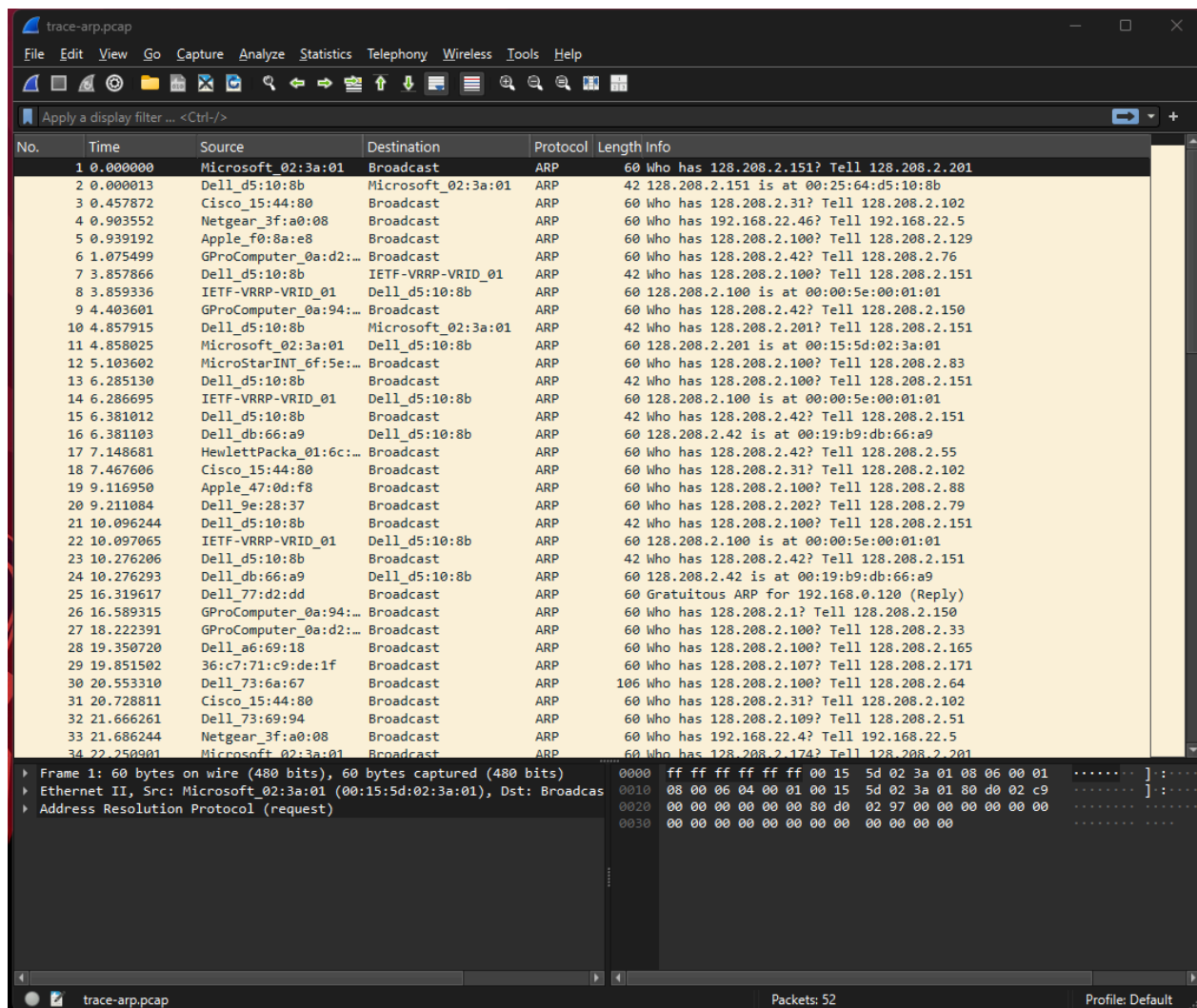
# Assignment

Name - *Aryan Thapliyal*

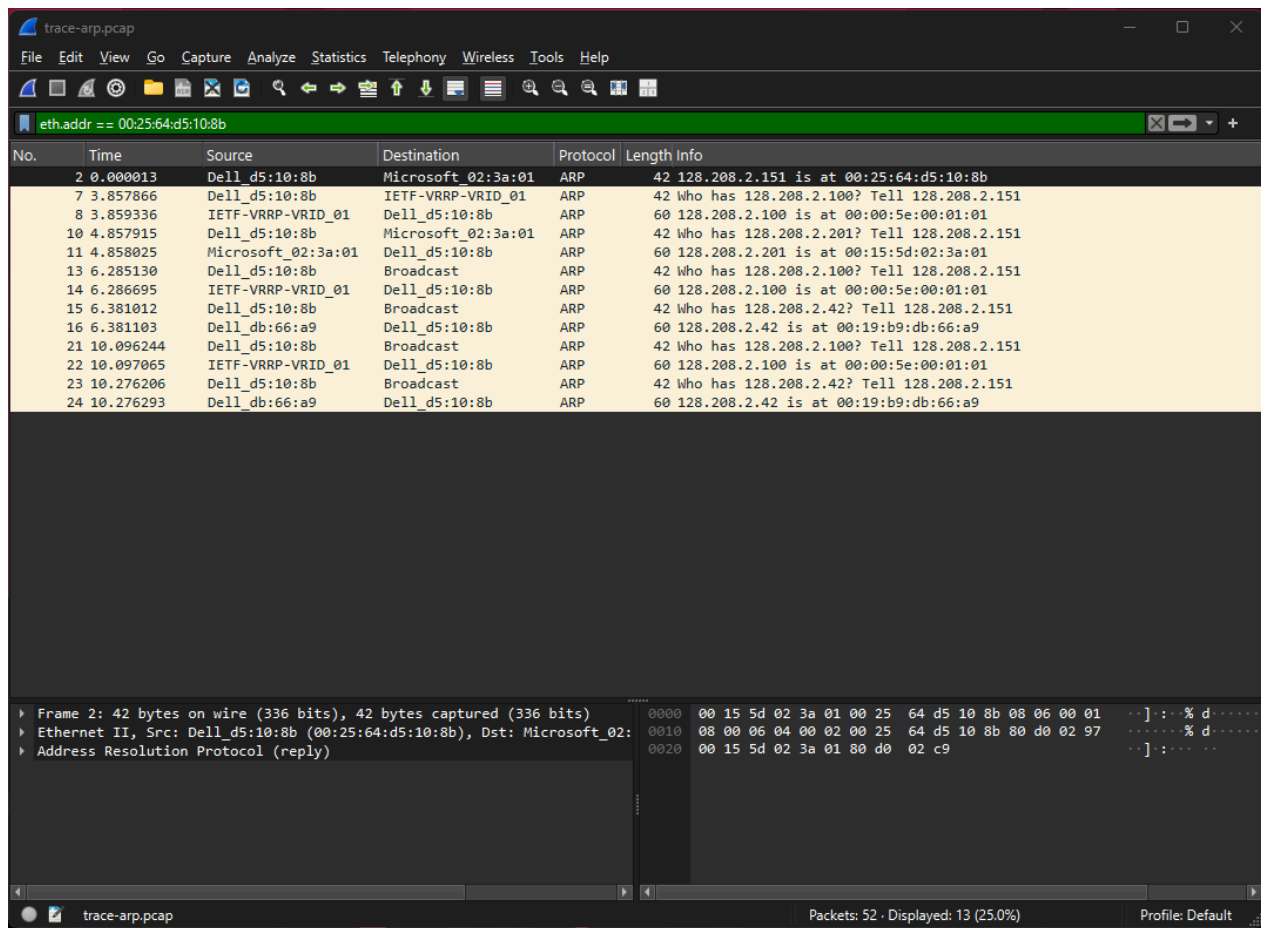
Roll No. - 13

Subject - *Internetworking with TCP/IP*

Step 2: Initial screenshot



## Step 3: Display filter



# Step 4: Request packet

The screenshot shows a Wireshark capture of an ARP request packet. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000013	Dell_d5:10:8b	Microsoft_02:3a:01	ARP	42	128.208.2.151 is at 00:25:64:d5:10:8b
7	3.857866	Dell_d5:10:8b	IETF-VRRP-VRID_01	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
8	3.859336	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
10	4.857915	Dell_d5:10:8b	Microsoft_02:3a:01	ARP	42	Who has 128.208.2.201? Tell 128.208.2.151
11	4.858025	Microsoft_02:3a:01	Dell_d5:10:8b	ARP	60	128.208.2.201 is at 00:15:5d:02:3a:01
13	6.285130	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
14	6.286695	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
15	6.381012	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.42? Tell 128.208.2.151

The packet details pane for Frame 7 shows:

- Ethernet II, Src: Dell\_d5:10:8b (00:25:64:d5:10:8b), Dst: IETF-VRRP-VRID\_01 (00:00:5e:00:01:01)
- Address Resolution Protocol (request)
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: Dell\_d5:10:8b (00:25:64:d5:10:8b)
- Sender IP address: 128.208.2.151
- Target MAC address: IETF-VRRP-VRID\_01 (00:00:5e:00:01:01)
- Target IP address: 128.208.2.100

The packet bytes pane shows the raw data of the ARP request.

Address Resolution Protocol (arp), 28 bytes

Packets: 52 · Displayed: 13 (25.0%)

Profile: Default

# Step 4: Reply packet

The screenshot shows a Wireshark capture of an ARP reply packet. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
36	22.408728	Vmware_ae:e2:24	Broadcast	ARP	60	Who has 128.208.2.1? Tell 128.208.2.40
37	22.455669	Apple_72:d6:d9	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.99
38	22.952622	Dell_9c:c4:10	Broadcast	ARP	60	Gratuitous ARP for 192.168.22.53 (Reply)
39	23.328013	36:c7:71:c9:de:1f	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.171
40	23.668665	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102
41	23.862735	d6:f5:47:92:d2:18	Broadcast	ARP	60	Who has 128.208.2.106? Tell 128.208.2.107
42	24.632531	Apple_55:ba:b8	Broadcast	ARP	60	Who has 128.208.2.62? Tell 128.208.2.28
43	24.949656	Apple_f0:8a:e8	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.129
44	25.705728	Dell_43:2b:2e	Broadcast	ARP	60	Gratuitous ARP for 192.168.22.42 (Reply)
45	26.026224	Dell_fd:62:46	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.122
46	27.323847	HewlettPacka_cf:fe:...	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.91
47	27.633080	Apple_55:ba:b8	Broadcast	ARP	60	Who has 128.208.2.62? Tell 128.208.2.28
48	28.134624	HonHaiPrecis_54:ce:...	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.193
49	28.140365	Dell_c3:3a:4c	Broadcast	ARP	60	Who has 128.208.2.193? Tell 128.208.2.62
50	28.140726	HonHaiPrecis_54:ce:...	Broadcast	ARP	60	Who has 128.208.2.62? Tell 128.208.2.193
51	28.834255	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.11? Tell 128.208.2.102
52	29.692144	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102

The packet details pane for Frame 44 shows:

- Ethernet II, Src: Dell\_43:2b:2e (00:26:b9:43:2b:2e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (reply/gratuitous ARP)
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- [Is gratuitous: True]
- Sender MAC address: Dell\_43:2b:2e (00:26:b9:43:2b:2e)
- Sender IP address: 192.168.22.42
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.22.42

The packet bytes pane shows the raw data of the ARP reply.

Address Resolution Protocol (arp), 28 bytes

Packets: 52

Profile: Default

**Examine an ARP request and ARP reply to answer these questions: share screenshots to justify your answers.**

1. What opcode is used to indicate a request? What about a reply?

Ans. ARP request uses opcode 1, and ARP reply uses opcode 2.

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Apple_f0:8a:e8 (00:25:00:f0)
```

```
▼ Address Resolution Protocol (reply/gratui
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  [Is gratuitous: True]
```

2. What value is carried on a request for the unknown target MAC address?

Ans. **00:00:00:00:00:00** indicates an unknown MAC address.

```
Sender MAC address: Dell_43:2b:2e (00:26:b9:43:2b:2e)
Sender IP address: 192.168.22.42
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.22.42
```

3. What Ethernet Type value indicates that ARP is the higher layer protocol?

Ans. The Ethernet Type for ARP is **0x0806**.

```
▶ Frame 42: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▼ Ethernet II, Src: Apple_55:ba:b8 (10:9a:dd:55:ba:b8), Dst: Broadcast (f
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Apple_55:ba:b8 (10:9a:dd:55:ba:b8)
    Type: ARP (0x0806)
    [Stream index: 25]
```

4. *Is the ARP reply broadcast (like the ARP request) or not?*

**Ans.** ARP replies are unicast sent directly to the requester's MAC.

```

▼ Ethernet II, Src: Cisco_15:44:80 (00:18:74:15:44:80), Dst: Broadcast
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Cisco_15:44:80 (00:18:74:15:44:80)
  Type: ARP (0x0806)
  [Stream index: 2]
  Padding: 0000000000000000000000000000000000000000
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
▼ Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: Dell_d5
  ▶ Destination: Dell_d5:10:8b (00:25:64:d5:10:8b)
  ▶ Source: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
  Type: ARP (0x0806)
  [Stream index: 6]
  Padding: 0000000000000000000000000000000000000000
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)

```