Computer Networks Lab (CS302)

Report Submission: CN Assignment Lab-4

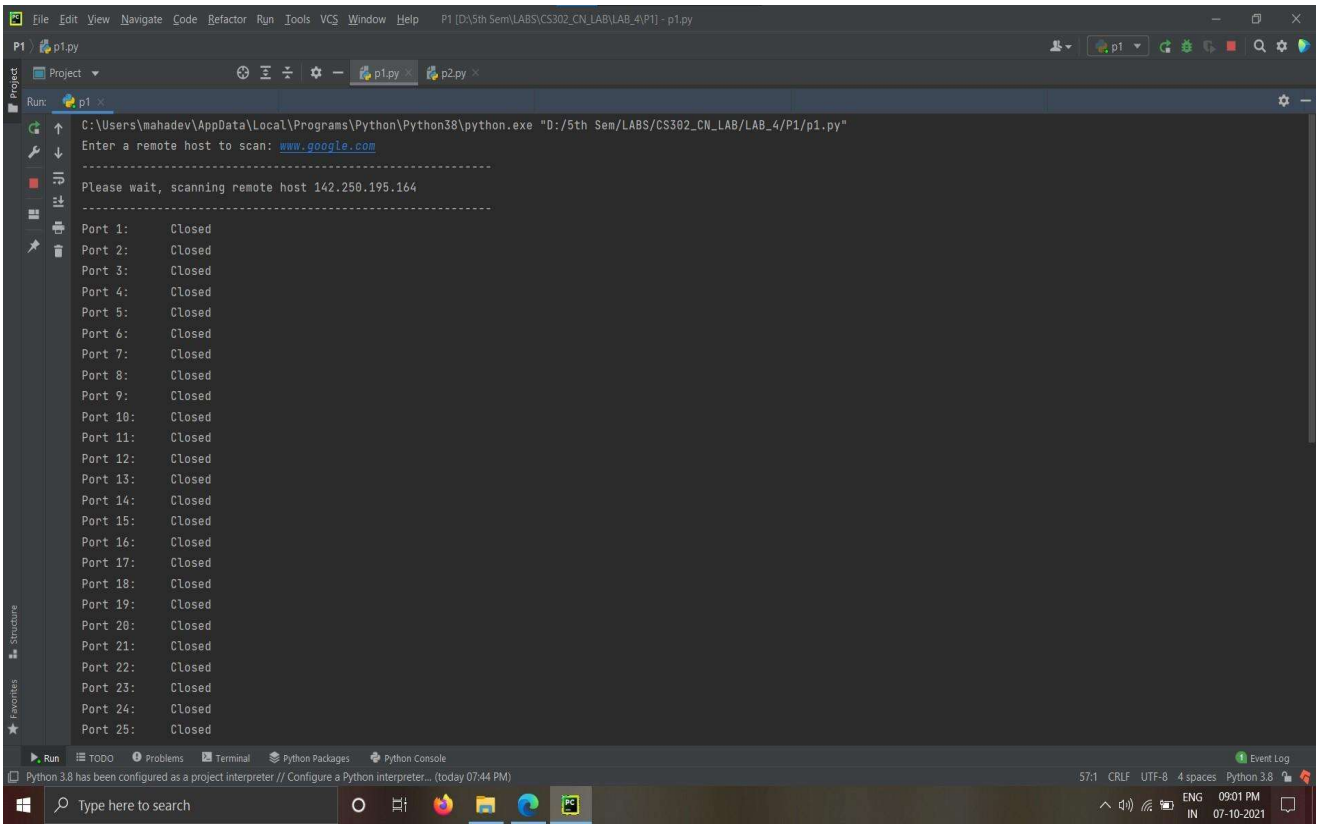
Group Member Details:

1. Mahadev M Hatti 191CS133
2. Darshan A V 191CS219

1.Develop a basic port scanner to check if particular ports are open or closed for an input remote host.

Code:

```
import socket
import sys
from distlib.compat import raw_input


# Ask for input
remoteServer    = raw_input("Enter a remote host to scan: ")
remoteServerIP  = socket.gethostbyname(remoteServer)

# Print a nice banner with information on which host we are about to scan
print("-" * 60)
print("Please wait, scanning remote host", remoteServerIP)
print("-" * 60)

# Using the range function to specify ports (here it will scans all ports between 1
and 1024)

# We also put in some error handling for catching errors

try:
    for port in range(1, 1025):
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        result = sock.connect_ex((remoteServerIP, port))
        if result != 0:
            print("Port {}:     Closed".format(port))
        else:
            print("Port {}:     Open".format(port))
        sock.close()

except socket.gaierror:
    print('Hostname could not be resolved. Exiting')
    sys.exit()

except socket.error:
    print("Couldn't connect to server")
    sys.exit()
```

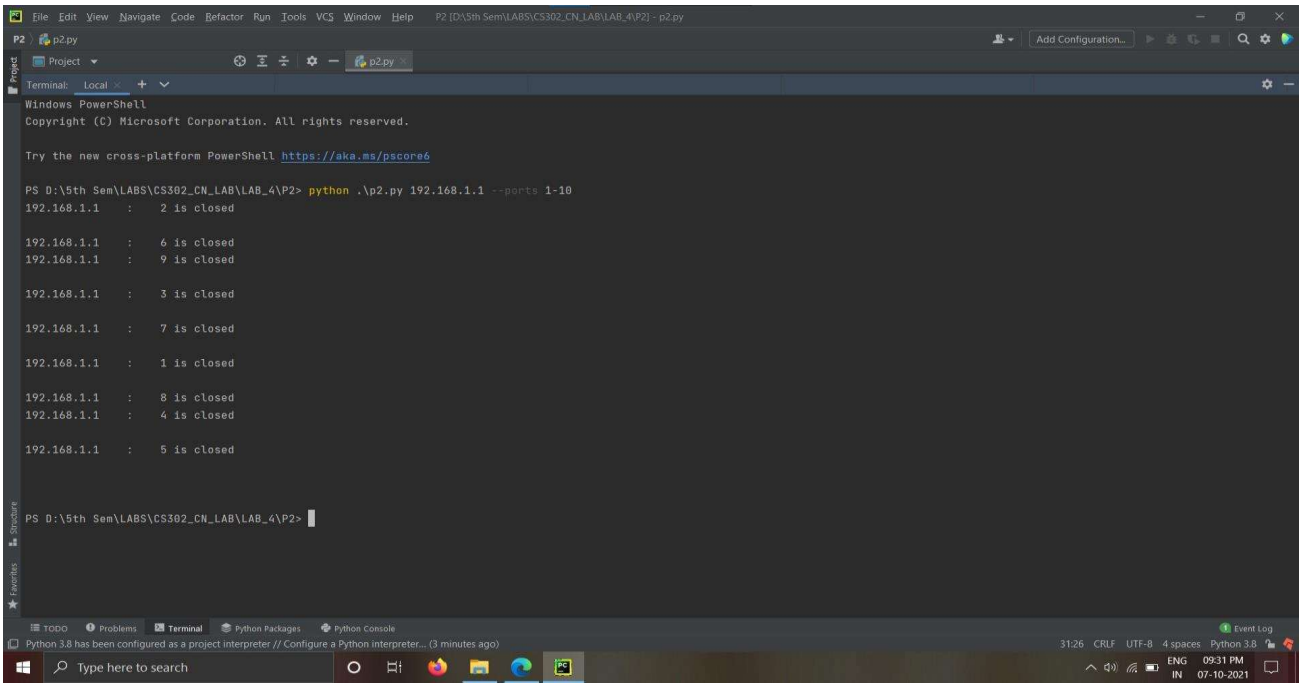


2.Develop a threaded port scanner to check if particular ports are open or closed for a remote host. Determine which Port scanner is efficient.

Code:

```
import argparse
import socket  # for connecting
from threading import Thread
from queue import Queue


# number of threads, feel free to tune this parameter as you wish
N_THREADS = 400
# thread queue
q = Queue()


def port_scan(port):
    try:
        s = socket.socket()
        s.connect((host, port))
```

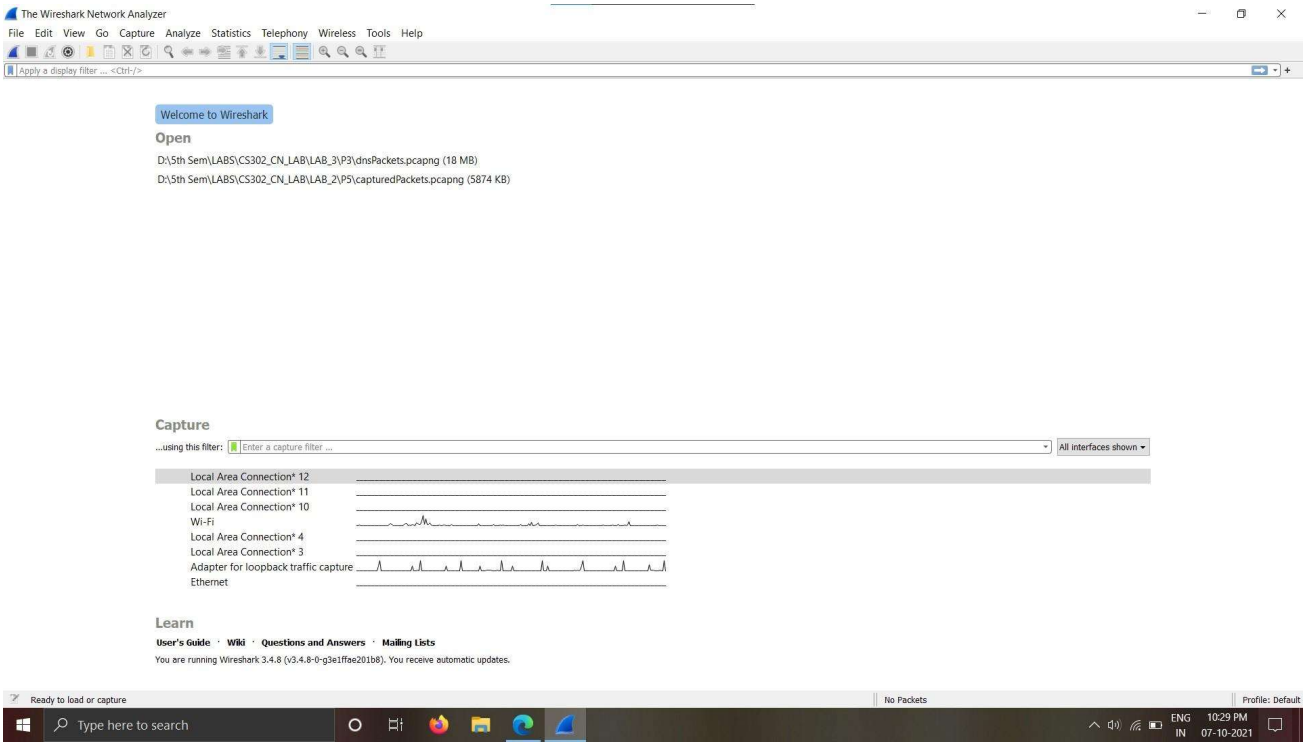
```
    except:
        print(f"{host:15}:{port:5} is closed\n")
    else:
        print(f"{host:15}:{port:5} is open\n")
    finally:
        s.close()


def scan_thread():
    global q
    while True:
        # get the port number from the queue
        worker = q.get()
        # scan that port number
        port_scan(worker)
        # tells the queue that the scanning for that port
        # is done
        q.task_done()


def main(host, ports):
    global q
    for t in range(N_THREADS):
        # for each thread, start it
        t = Thread(target=scan_thread)
        # when we set daemon to true, that thread will end when the main thread ends
        t.daemon = True
        # start the daemon thread
        t.start()
    for worker in ports:
        # for each port, put that port into the queue
        # to start scanning
        q.put(worker)
    # wait the threads ( port scanners ) to finish, wait until the queue is empty
before performing other operations
    q.join()


if __name__ == "__main__":
    # parse some parameters passed
    parser = argparse.ArgumentParser(description="Simple port scanner")
    parser.add_argument("host", help="Host to scan.")
    parser.add_argument("--ports", "-p", dest="port_range", default="1-65535",
                        help="Port range to scan, default is 1-65535 (all ports)")
    args = parser.parse_args()
    host, port_range = args.host, args.port_range

    start_port, end_port = port_range.split("-")
    start_port, end_port = int(start_port), int(end_port)

    ports = [p for p in range(start_port, end_port)]

    main(host, ports)
```



3. Capture UDP packets and with the help of the captured UDP Packets.

a. analyse UDP DHCP Packets

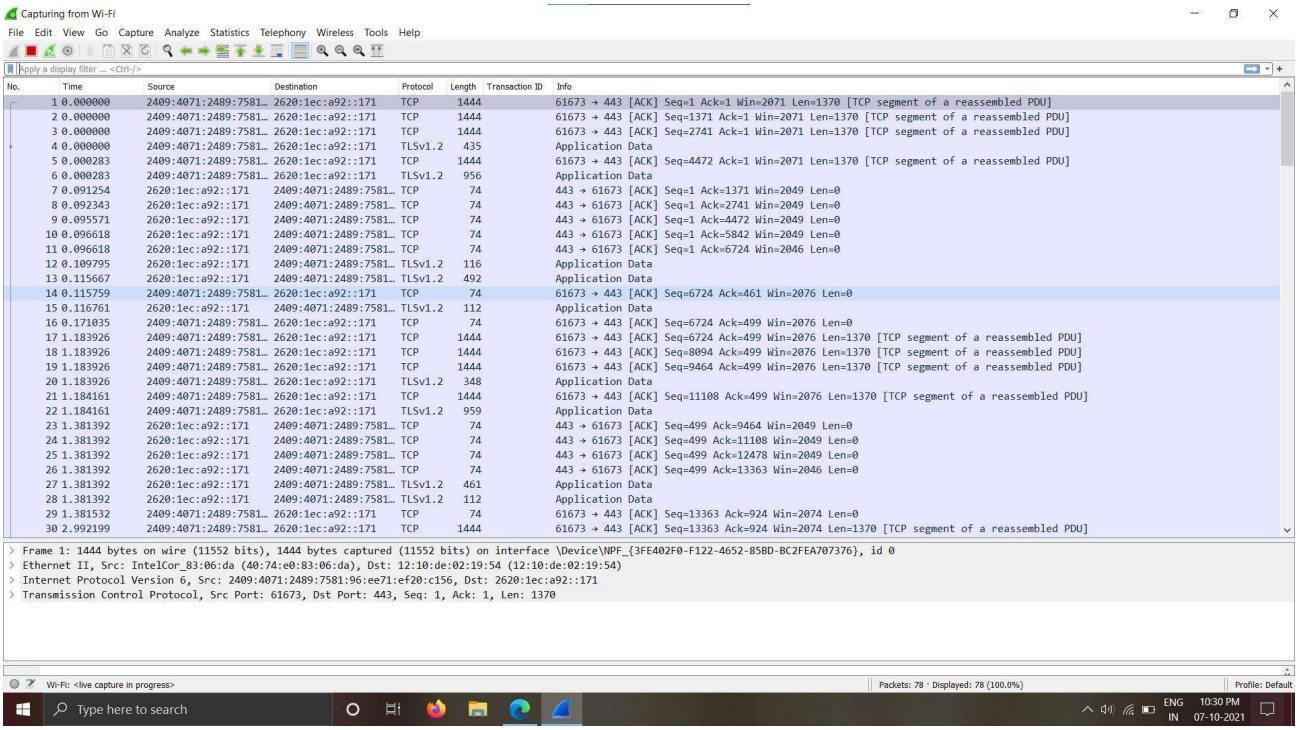
1. In the below fig. selects the Wi-Fi option from the Interface list options.



2. In the new window you can see all the current traffic on the network. (Clear cache – Before capturing the traffic, you need to clear your browser's cache.)

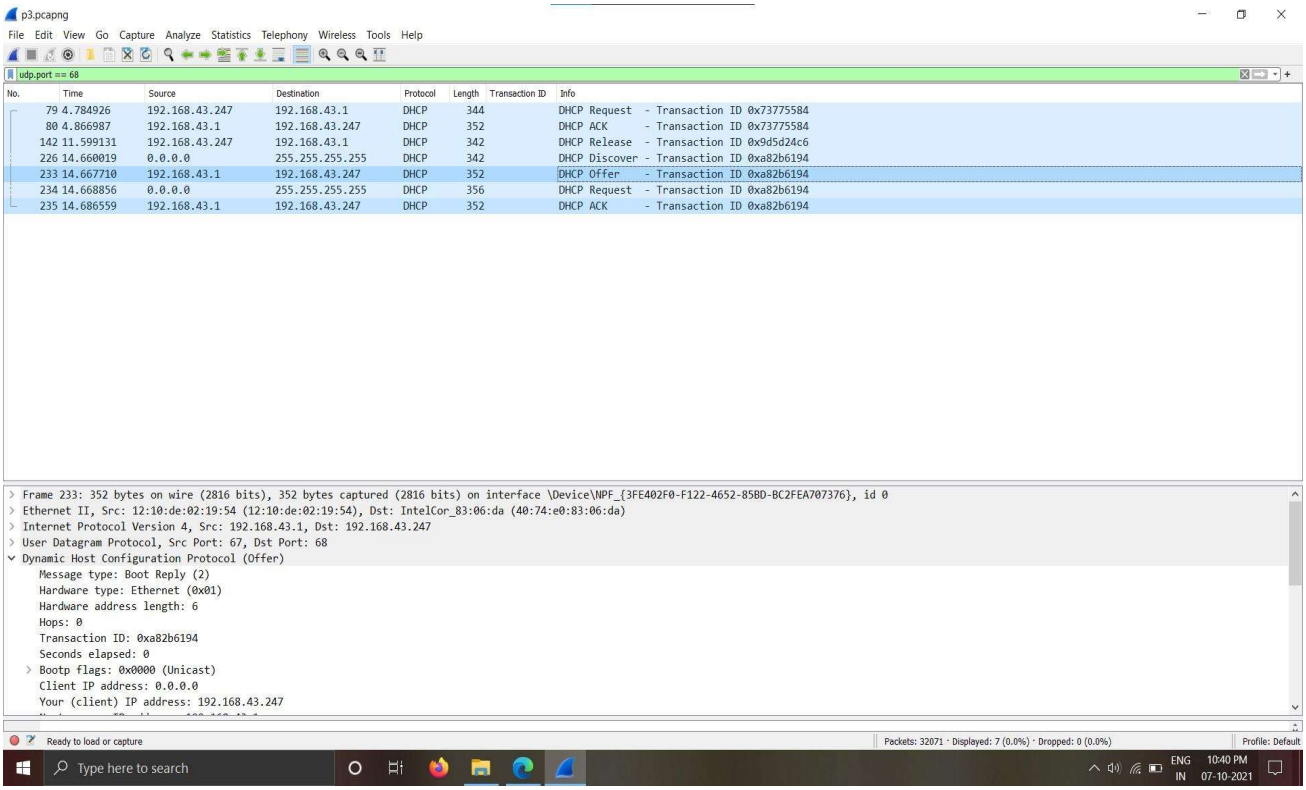
From this Pane you can observe:

- No. – The number of a captured packet.
- Time – This shows you when the packet was captured with regards to when you started capturing.
- Source – This is the origin of a captured packet in the form of an address.
- Destination – The destination address of a captured packet.
- Protocol – The type of a captured packet.
- Length – This shows you the length of a captured packet. This is expressed in bytes.

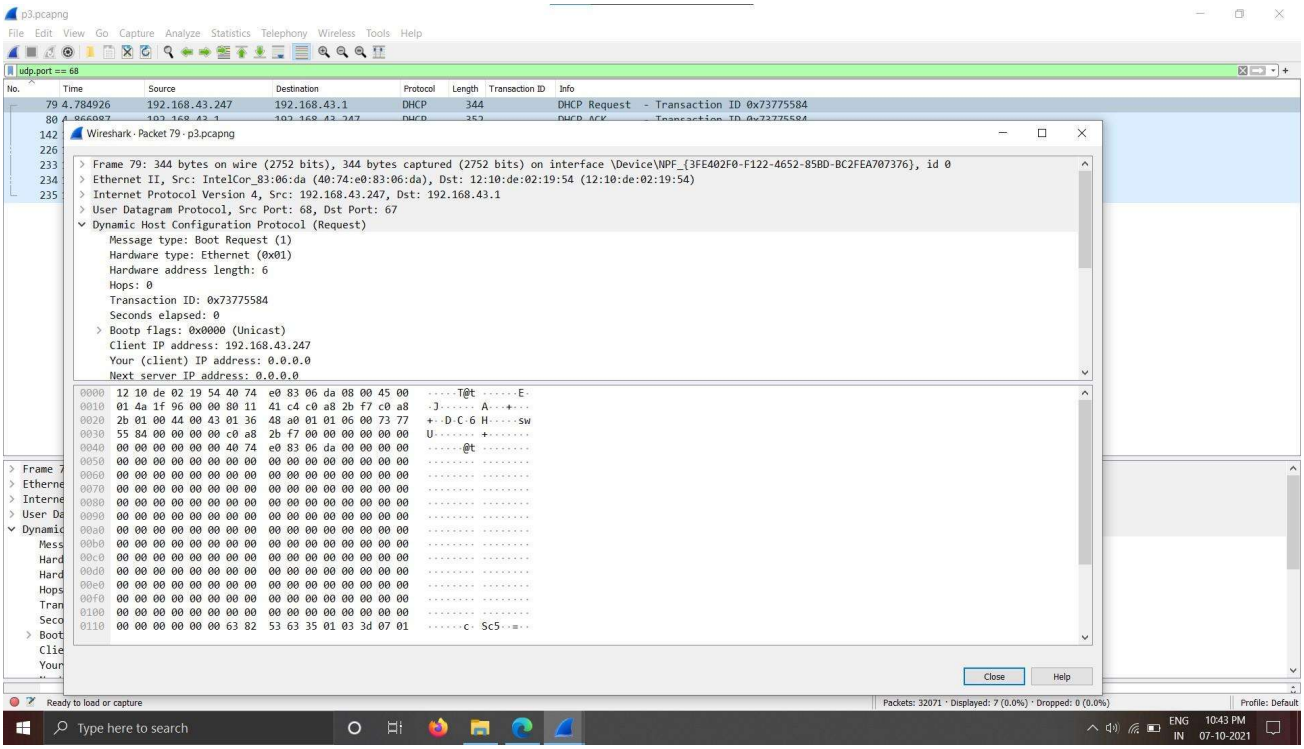


3. Use filter section to filter out Specific Packets related to dns Server.

- To view only DHCP traffic, type udp.port == 68 (lower case) in the Filter box and press Enter.



- **DHCP Request Traffic :**
- Select the first DHCP packet, labeled DHCP Request.



- I Noticed that there is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Bootstrap Protocol frame.
- Expanded Ethernet II to view Ethernet details.

- I observed that the destination is my DHCP server's MAC address and the source is my MAC address.

- I observed Internet Protocol Version 4 to view IP details.

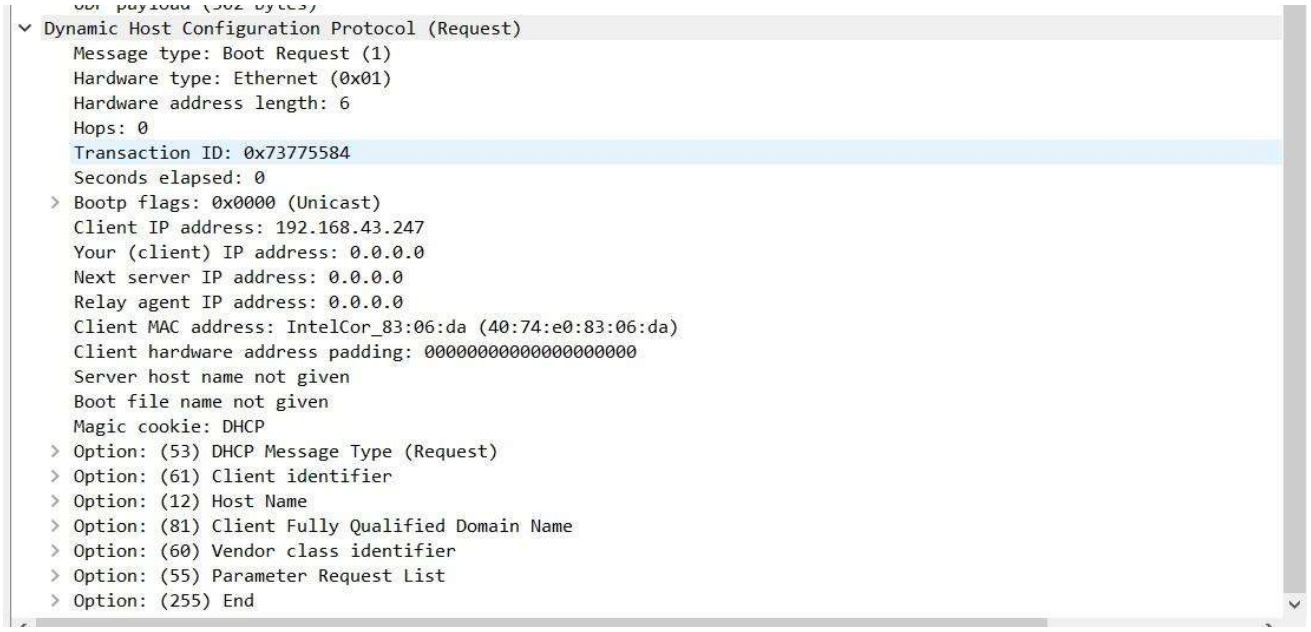
```
Internet Protocol Version 4, Src: 192.168.43.247, Dst: 192.168.43.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 330
    Identification: 0x1f96 (8086)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x41c4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.247
    Destination Address: 192.168.43.1
```

- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DHCP server.

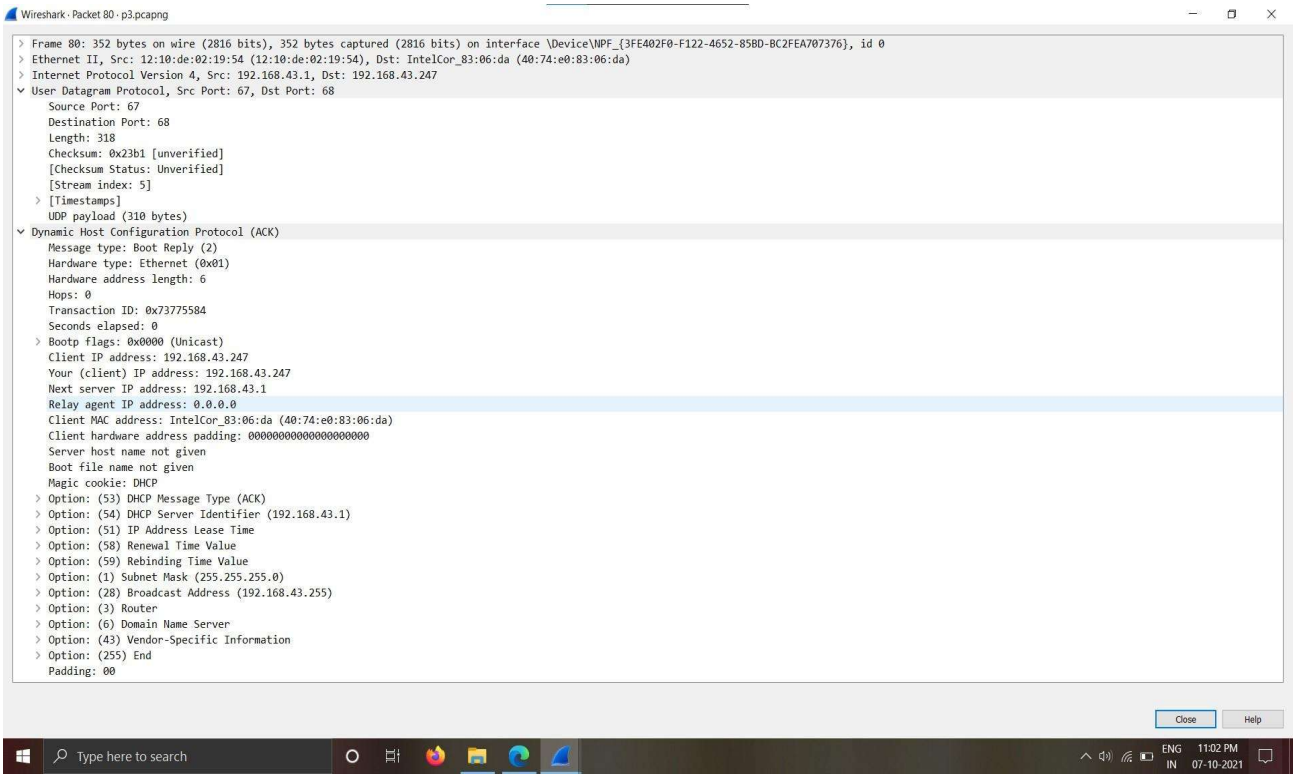
- Expanded User Datagram Protocol to view UDP details.

```
User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 310
    Checksum: 0x48a0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  > [Timestamps]
    UDP payload (302 bytes)
```

- Expanded Bootstrap Protocol to view BOOTP details.

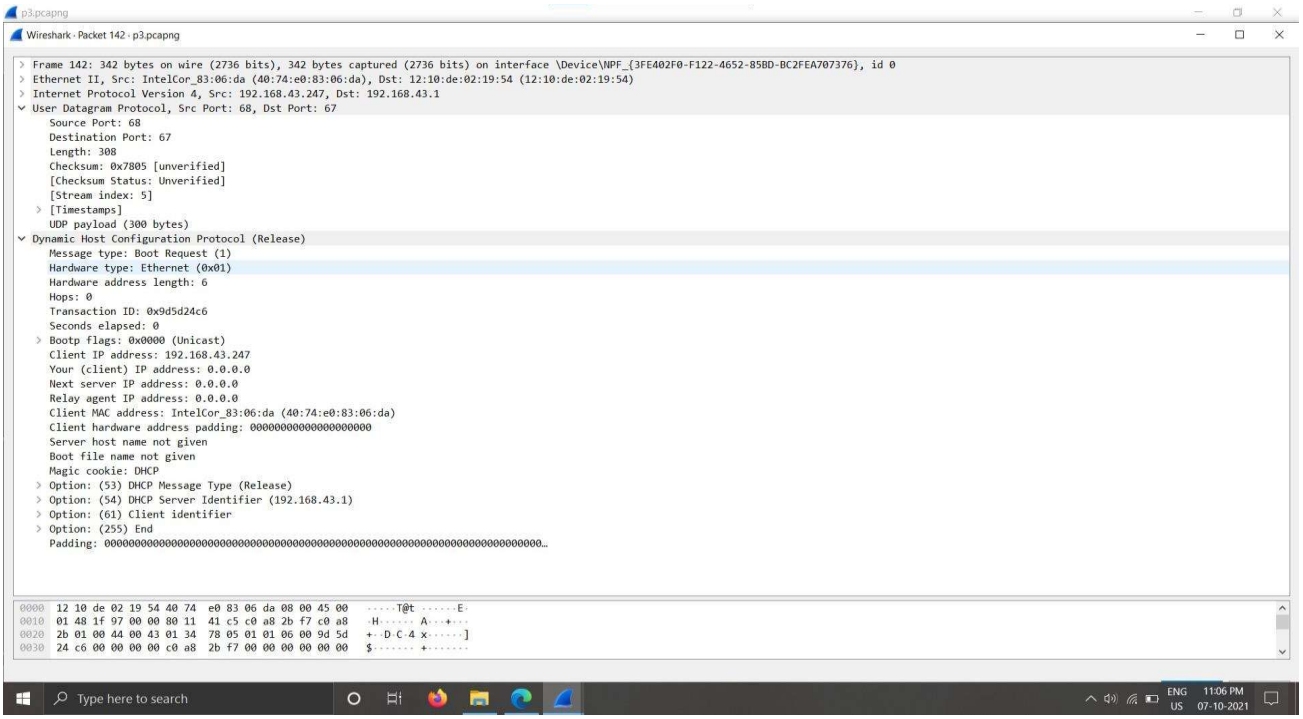


- **DHCP ACK Traffic:**
- Selected the second DHCP packet, labeled DHCP ACK



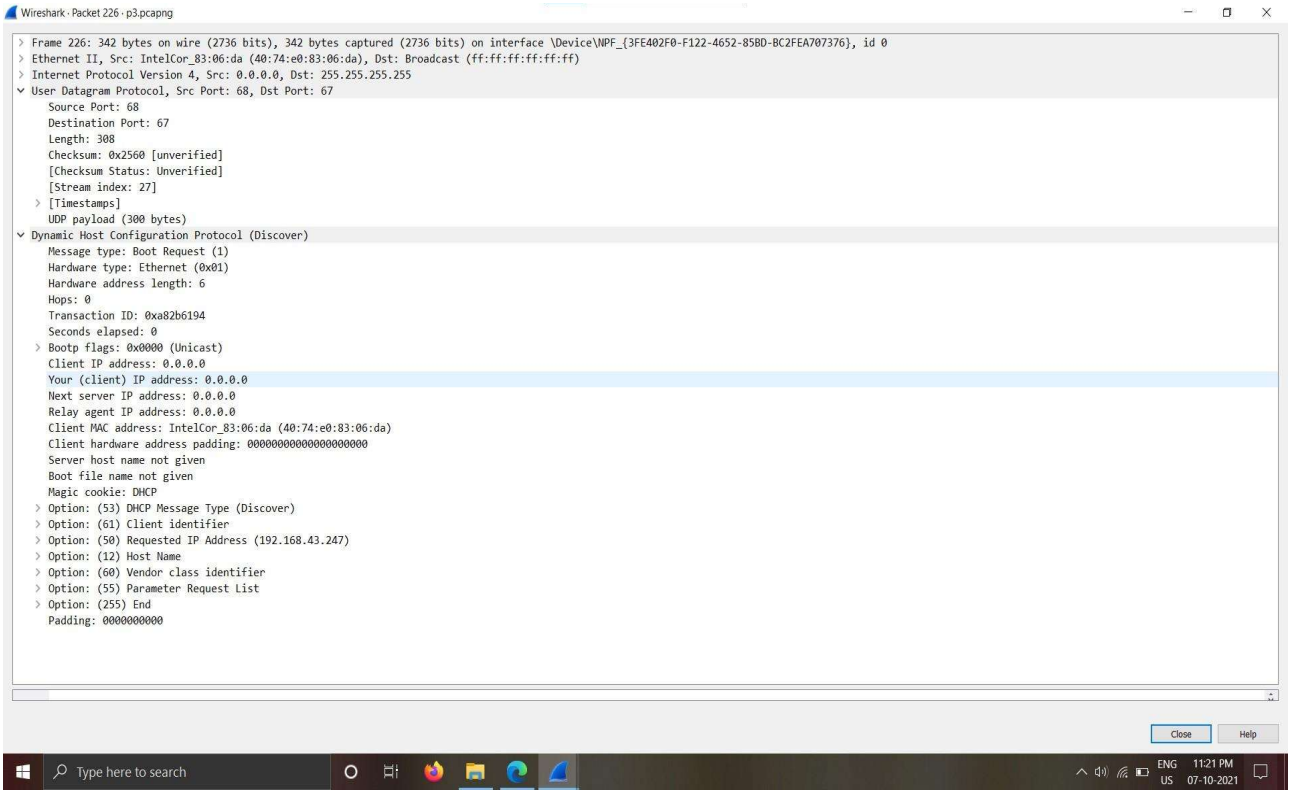
- I Noticed that there is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Bootstrap Protocol frame.
- Expanded Ethernet II to view Ethernet details.
- I observed that the destination is my DHCP server's MAC address and the source is my MAC address.
- I observed Internet Protocol Version 4 to view IP details.
- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DHCP server.
- Expanded User Datagram Protocol to view UDP details.
- Expanded Bootstrap Protocol to view BOOTP details.

- **DHCP Release Traffic:**
- Selected the third DHCP packet, labeled DHCP Release.



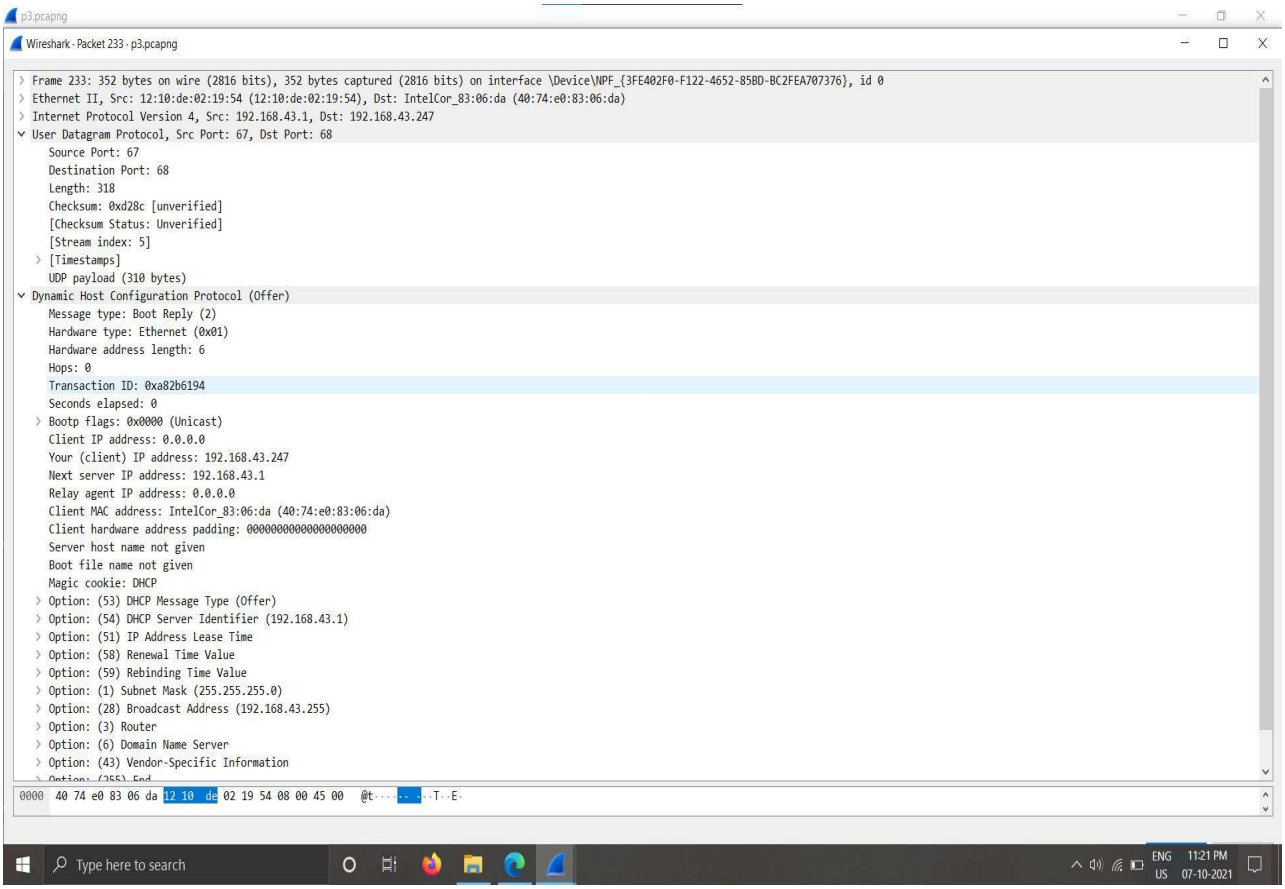
- I Noticed that there is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Bootstrap Protocol frame.
- Expanded Ethernet II to view Ethernet details.
- I observed that the destination is my DHCP server's MAC address and the source is my MAC address.
- I observed Internet Protocol Version 4 to view IP details.
- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DHCP server.
- Expanded User Datagram Protocol to view UDP details.
- Expanded Bootstrap Protocol to view BOOTP details.

- **DHCP Discover Traffic:**
- Selected the fourth DHCP packet, labeled DHCP Discover.



- I Noticed that there is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Bootstrap Protocol frame.
- Expanded Ethernet II to view Ethernet details.
- I observed that the destination is my DHCP server's MAC address and the source is my MAC address.
- I observed Internet Protocol Version 4 to view IP details.
- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DHCP server.
- Expanded User Datagram Protocol to view UDP details.
- Expanded Bootstrap Protocol to view BOOTP details.

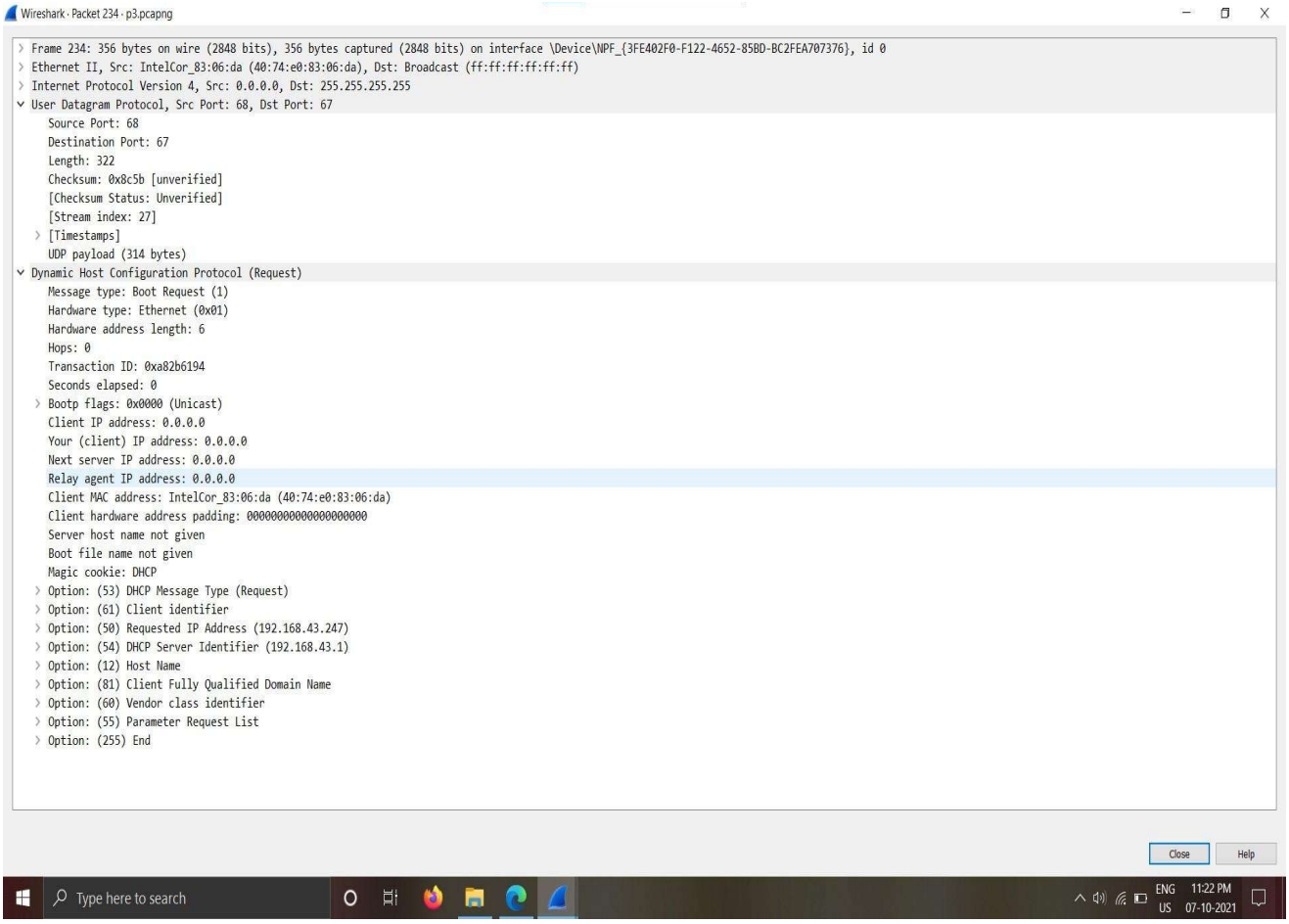
- **DHCP Offer Traffic:**
- Selected the fifth DHCP packet, labeled DHCP Offer.



- I Noticed that there is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Bootstrap Protocol frame.
- Expanded Ethernet II to view Ethernet details.
- I observed that the destination is my DHCP server's MAC address and the source is my MAC address.
- I observed Internet Protocol Version 4 to view IP details.

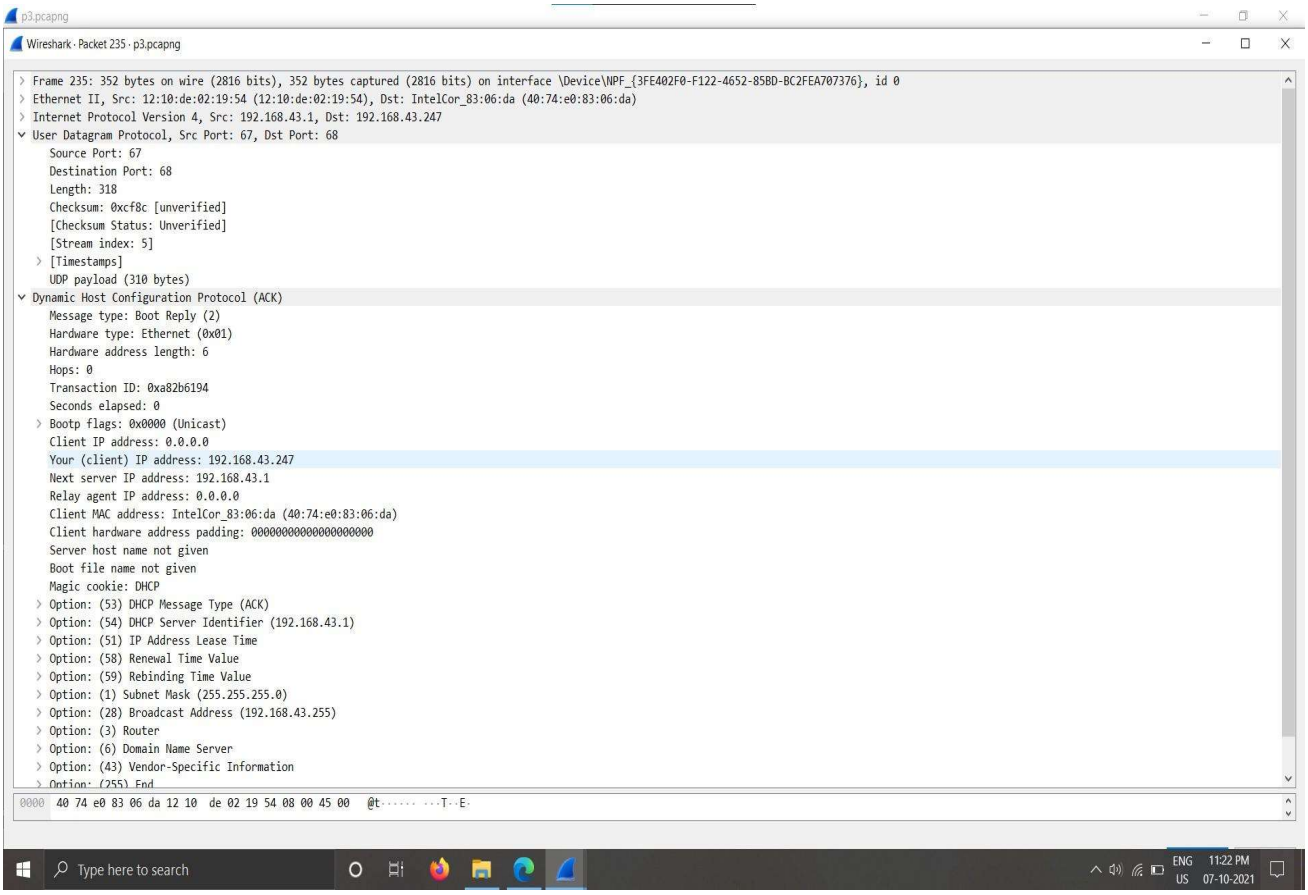
- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DHCP server.
- Expanded User Datagram Protocol to view UDP details.
- Expanded Bootstrap Protocol to view BOOTP details.

- **DHCP Request Traffic:**
- Selected the sixth DHCP packet, labeled DHCP Request.



- I Noticed that there is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Bootstrap Protocol frame.
- Expanded Ethernet II to view Ethernet details.
- I observed that the destination is my DHCP server's MAC address and the source is my MAC address.
- I observed Internet Protocol Version 4 to view IP details.
- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DHCP server.
- Expanded User Datagram Protocol to view UDP details.
- Expanded Bootstrap Protocol to view BOOTP details.

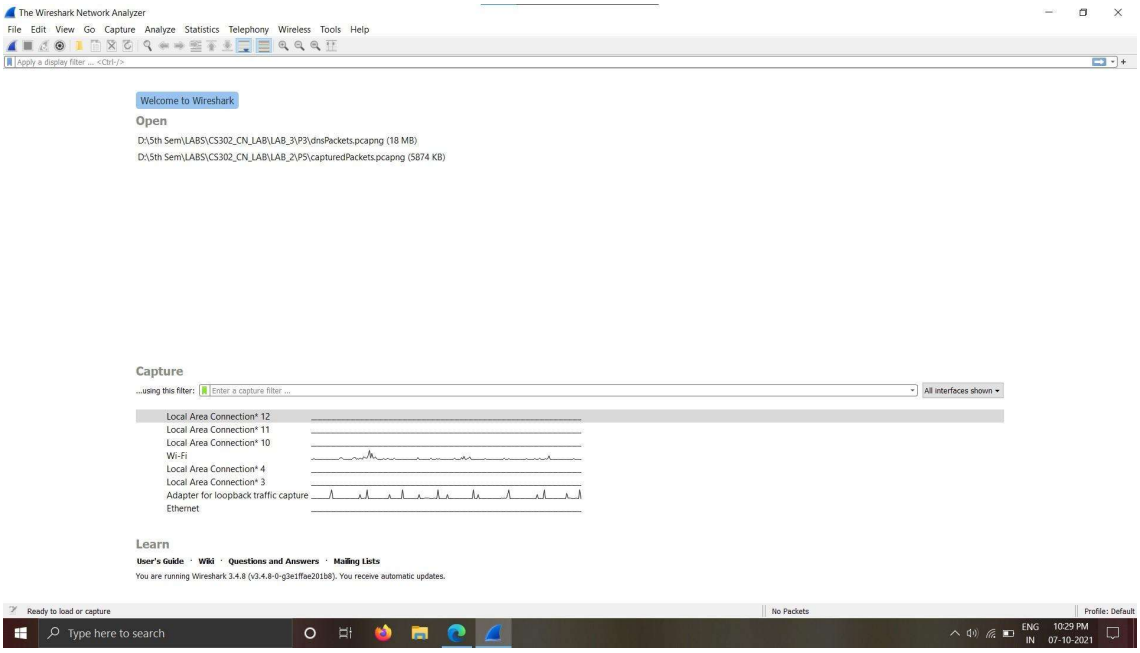
- **DHCP ACK Traffic:**
- Selected the seventh DHCP packet, labeled DHCP ACK.



- I Noticed that there is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Bootstrap Protocol frame.
- Expanded Ethernet II to view Ethernet details.
- I observed that the destination is my DHCP server's MAC address and the source is my MAC address.
- I observed Internet Protocol Version 4 to view IP details.
- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DHCP server.
- Expanded User Datagram Protocol to view UDP details.
- Expanded Bootstrap Protocol to view BOOTP details.

b. Analyse UDP DNS Packet

1.In the below fig. selects the Wi-Fi option from the Interface list options.

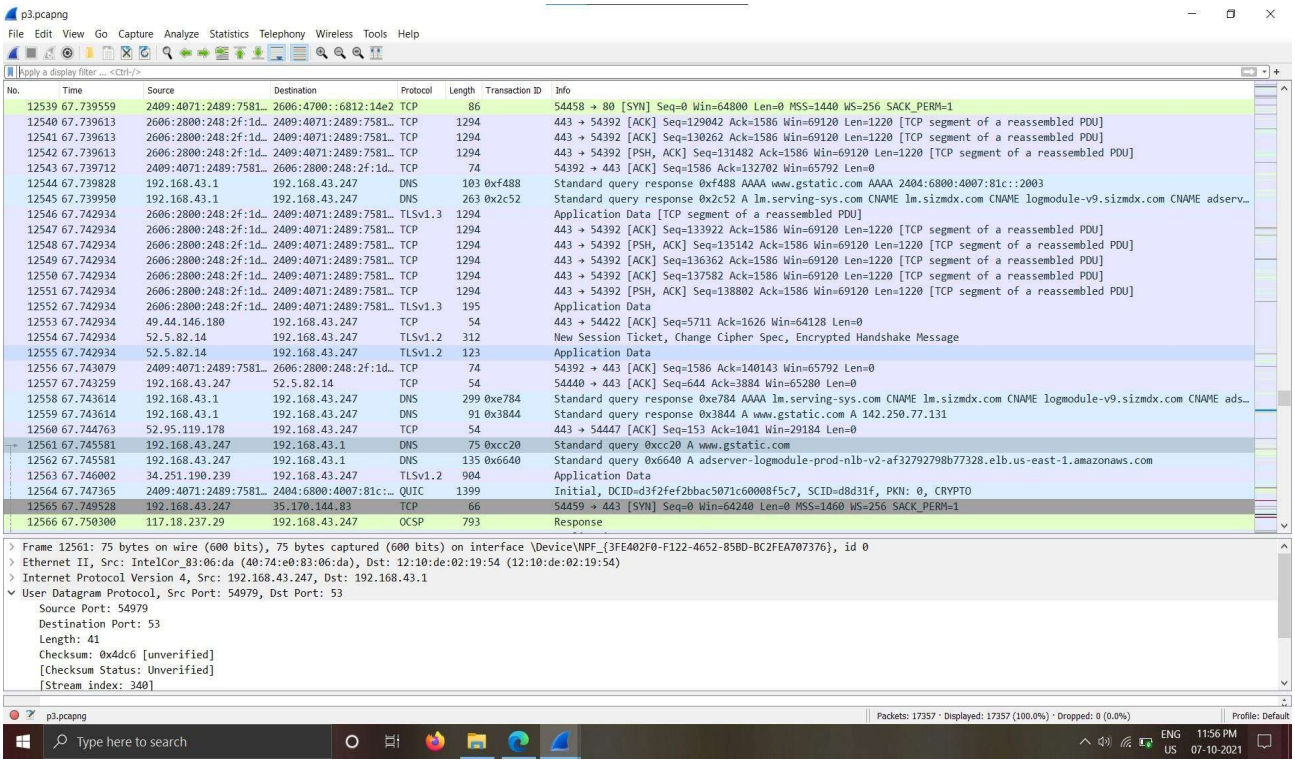


2.In the new window you can see all the current traffic on the network. (Clear cache – Before capturing the traffic, you need to clear your browser's cache.)

From this Pane you can observe:

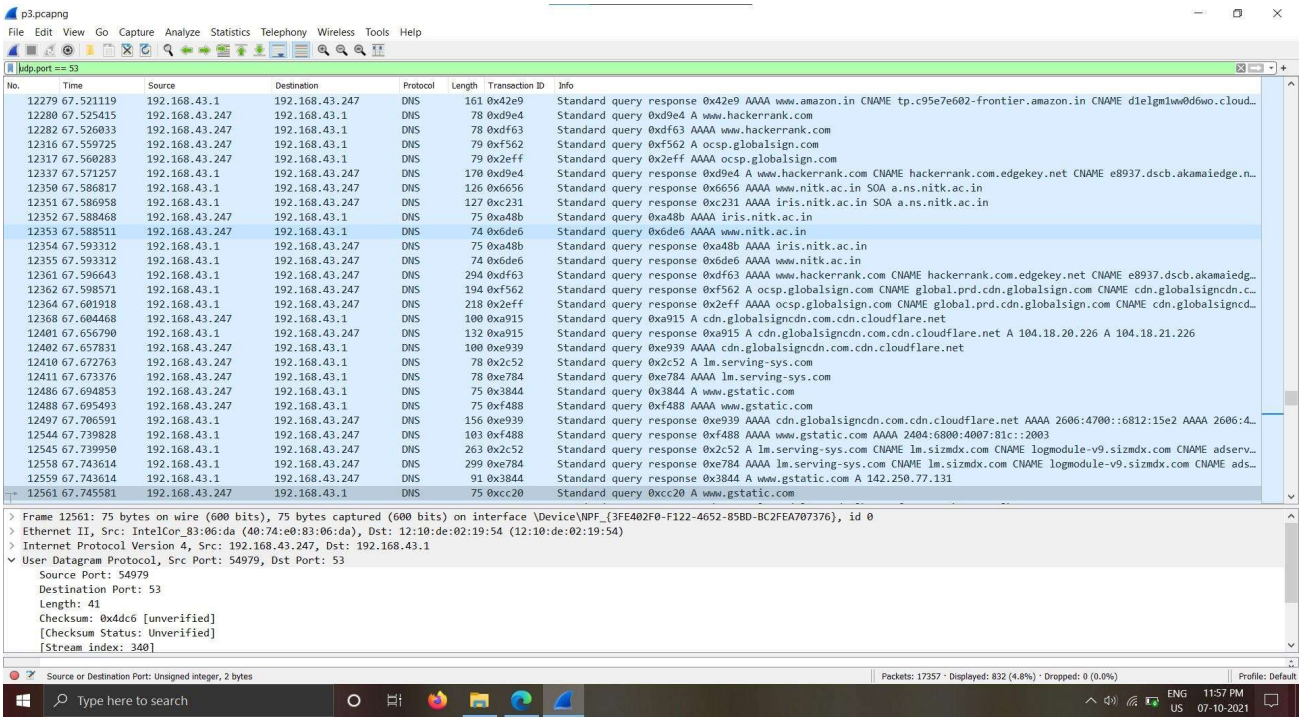
- No. – The number of a captured packet.
- Time – This shows you when the packet was captured with regards to when you started capturing.
- Source – This is the origin of a captured packet in the form of an address.
- Destination – The destination address of a captured packet.
- Protocol – The type of a captured packet.

- Length – This shows you the length of a captured packet. This is expressed in bytes.



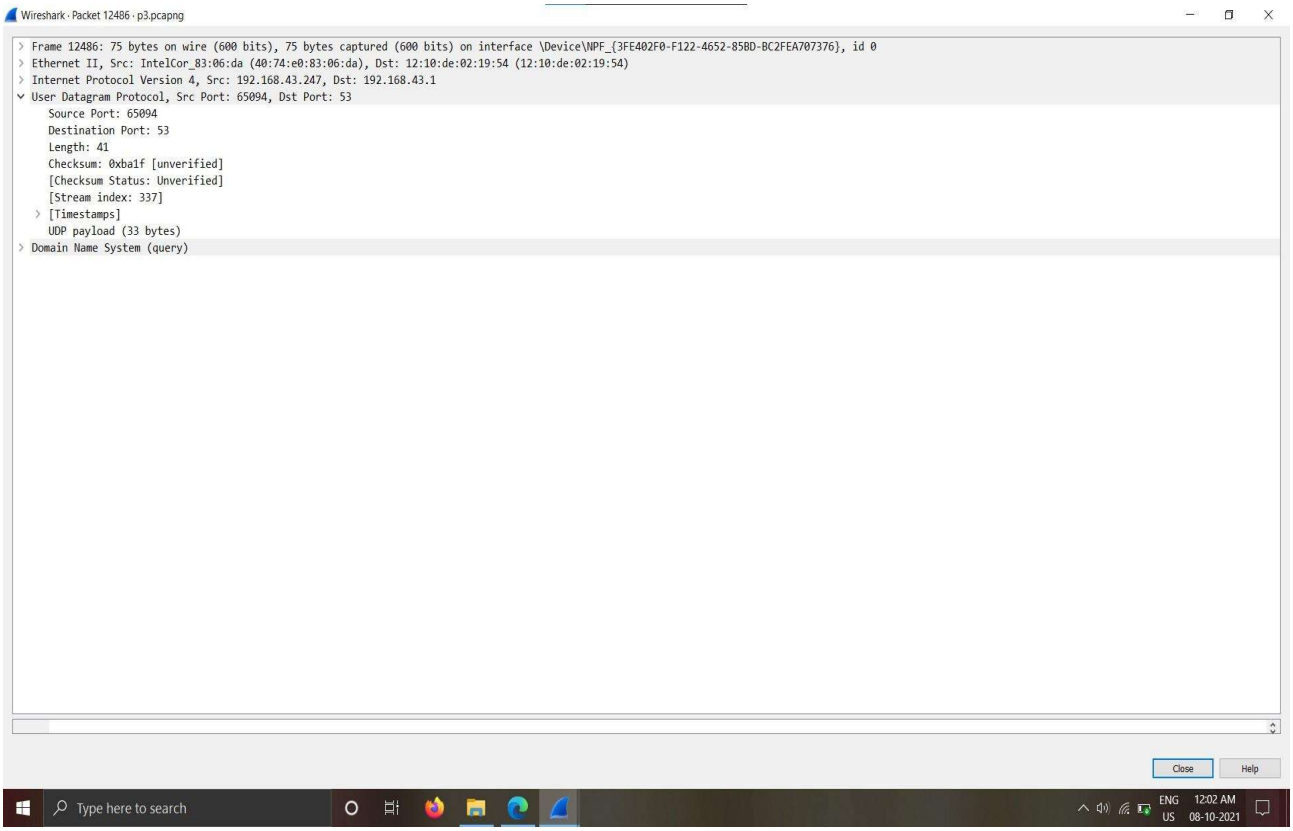
3.Use filter section to filter out Specific Packets related to dns Server.

- To view only DNS traffic, type udp.port == 53 (lower case) in the Filter box and press Enter.



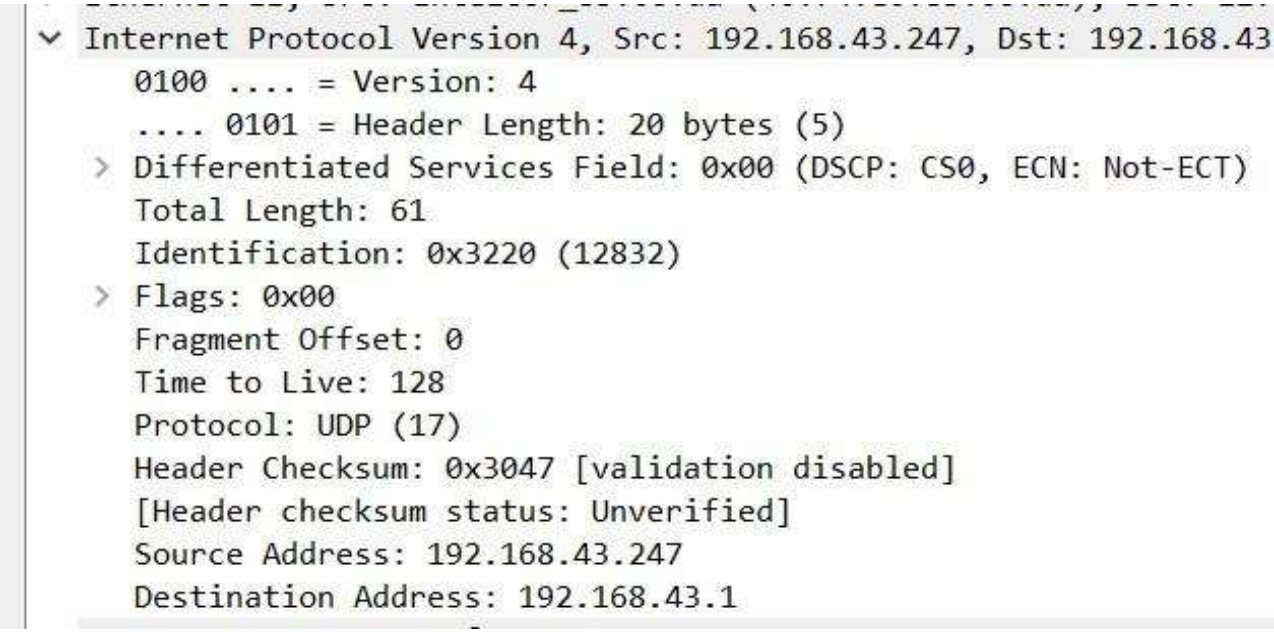
- **DNS Query Traffic:**
  - Selected the DNS packet labeled Standard query A www.gstatic.com.

  - Noticed the Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Domain Name System (query) frame.



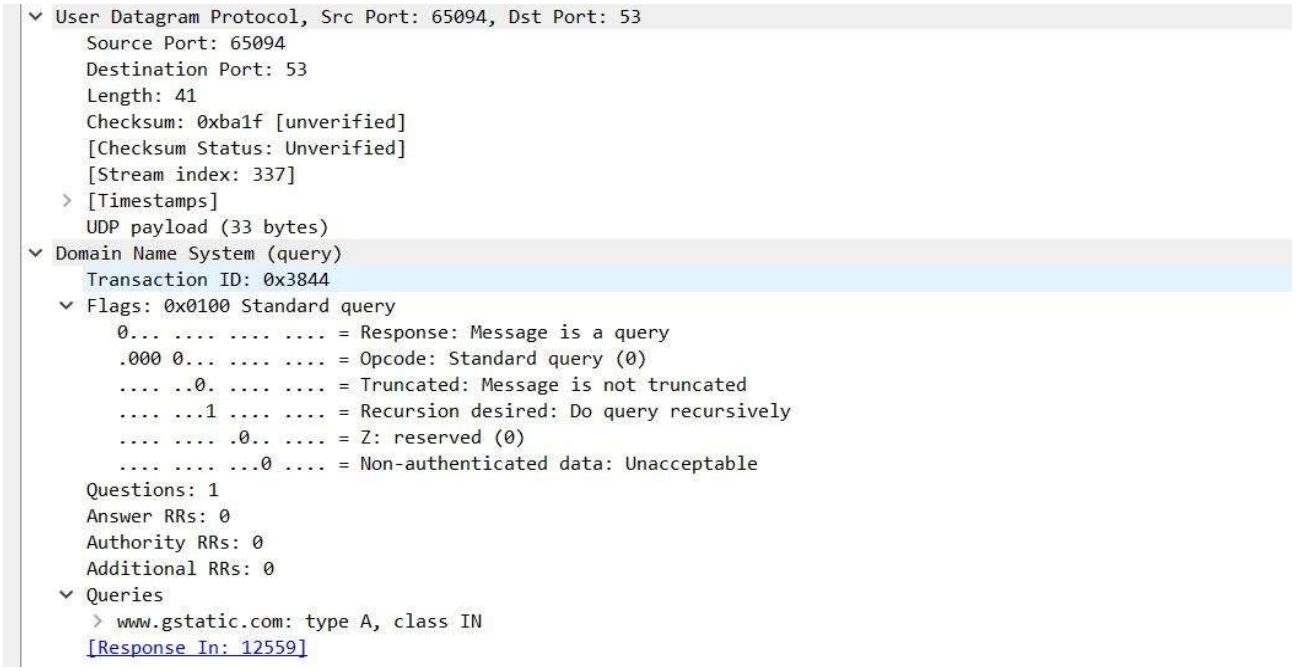
- Expanded Ethernet II to view Ethernet details.

- I observed Internet Protocol Version 4 to view IP details.



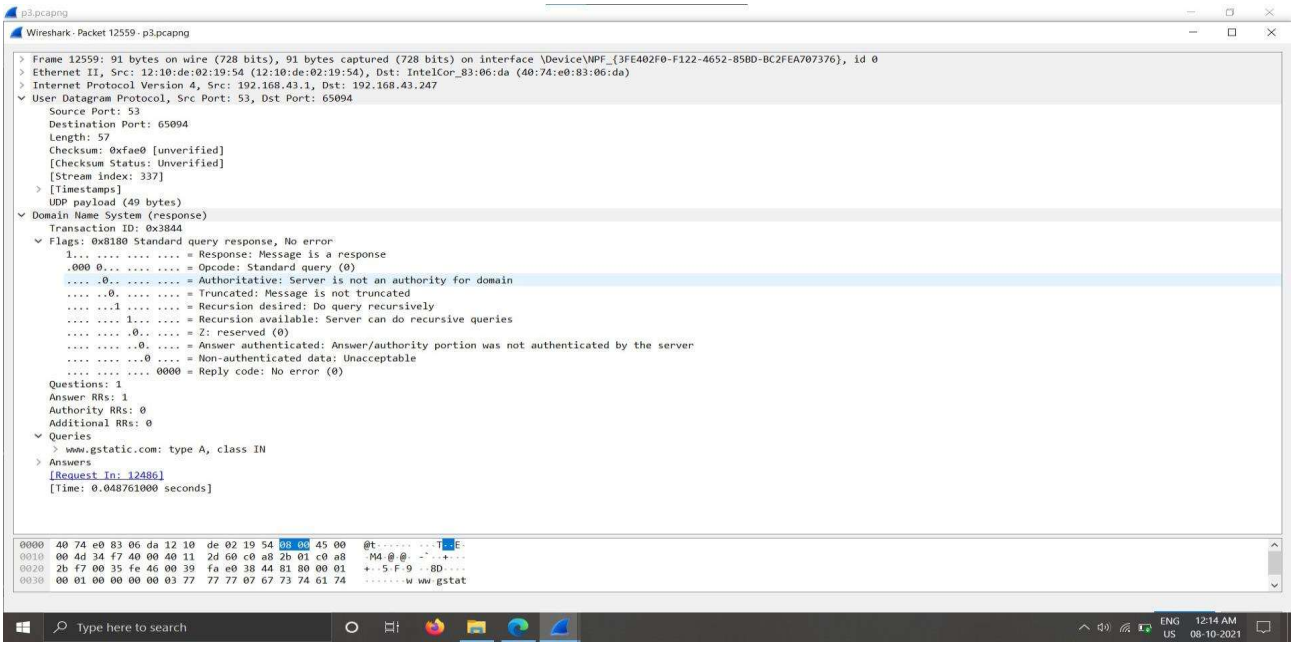
- Noticed that the source address is my IP address
- Noticed that the destination address is the IP address of the DNS server.

- Expanded User Datagram Protocol to view UDP details.
- Expanded Domain Name System (query) to view DNS details.
- Expanded Flags to view flags details.
- Expanded Queries to view query details.
- Observed the query for www.gstatic.com.

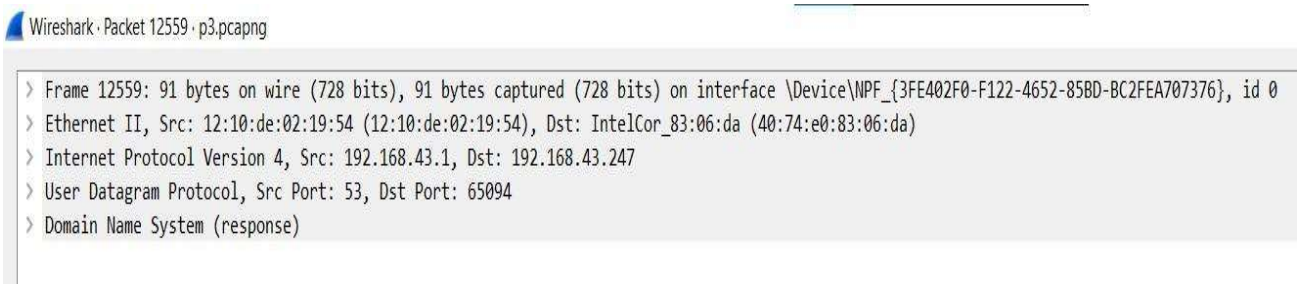


- **DNS Response Traffic:**

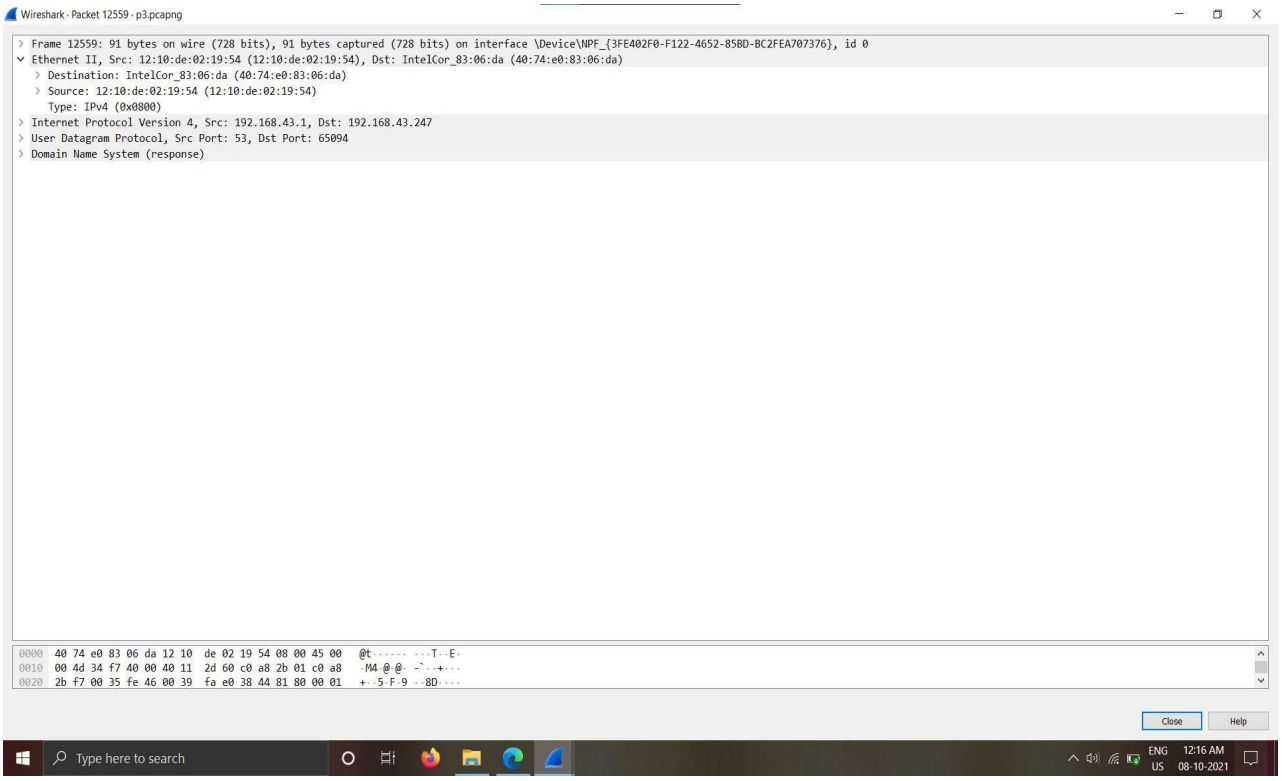
- Selected the next DNS packet, labeled Standard query response 0x3844 A www.gstatic.com A 142.250.77.131



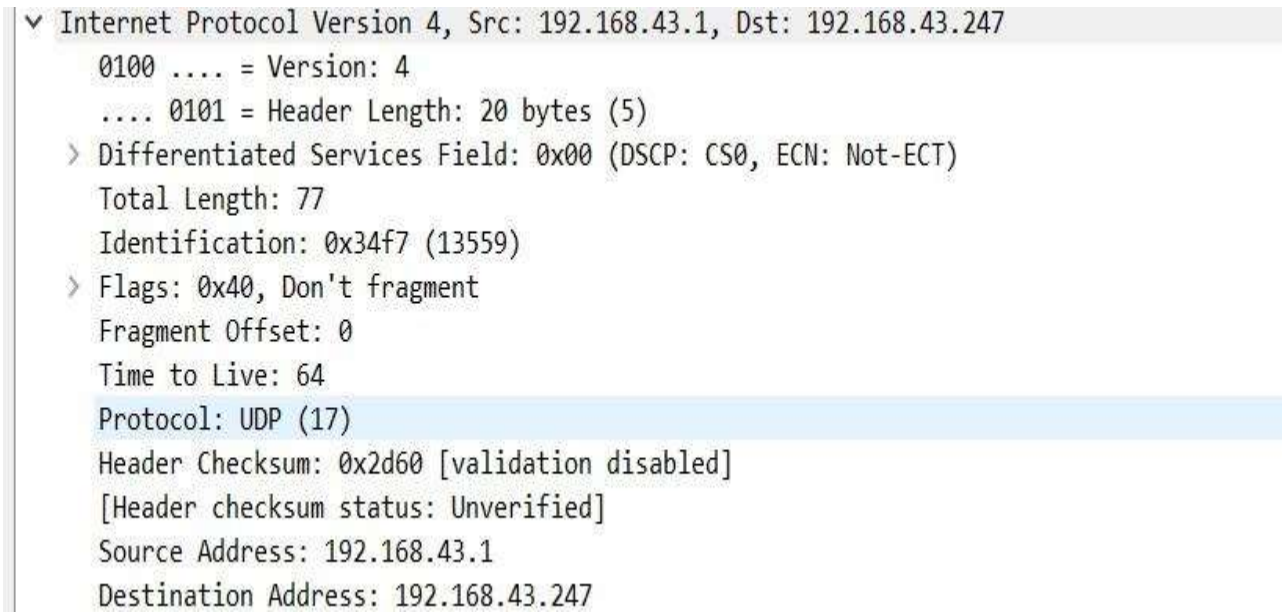
- Noticed the Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Domain Name System (query) frame.



- Expanded Ethernet II to view Ethernet details.



- I observed Internet Protocol Version 4 to view IP details.



- Noticed that the source address is my IP address

- Noticed that the destination address is the IP address of the DNS server.

- Expanded User Datagram Protocol to view UDP details.
- Expanded Domain Name System (query) to view DNS details.
- Expanded Flags to view flags details.
- Expanded Queries to view query details.
- Observed the query for www.gstatic.com.
- Expanded Answers to view answer details.