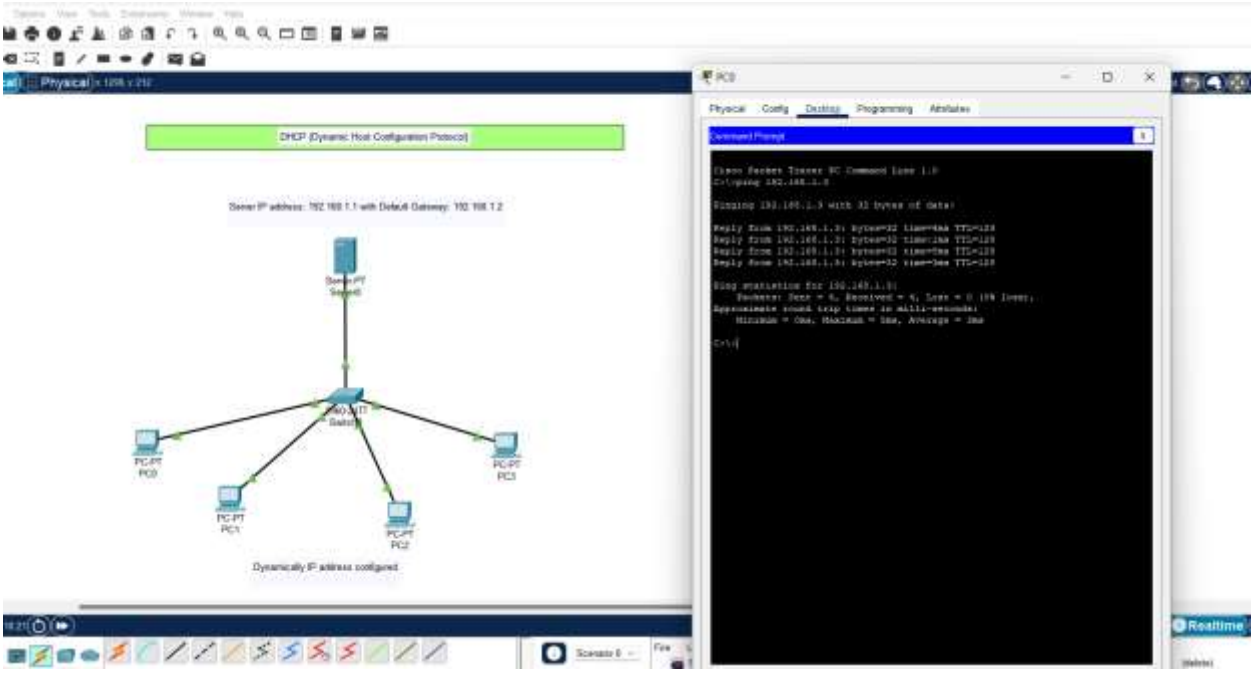
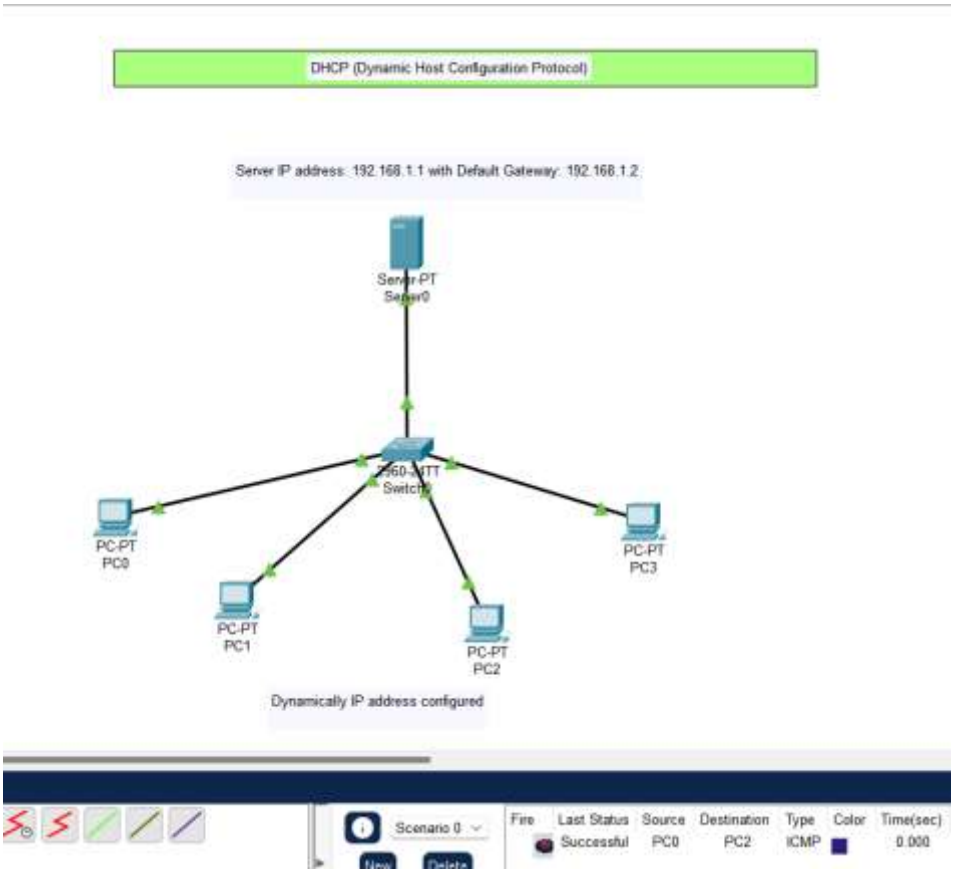
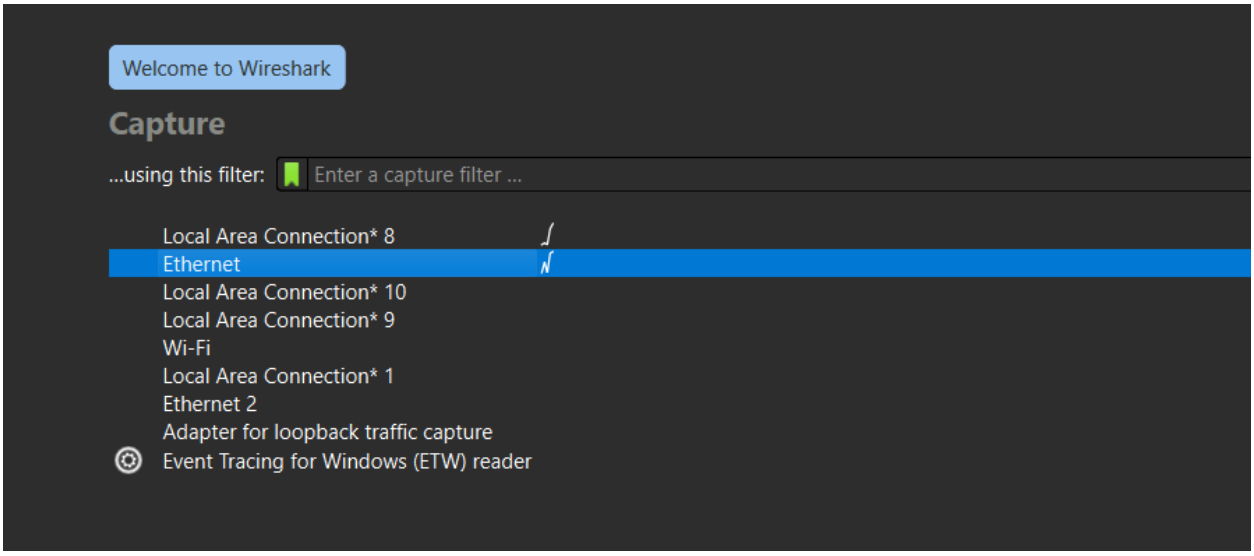
Q) Simulate DHCP server on packet tracer.
=> The .pkt file is attached to this assignment.





Q) Track DHCP packets on your local network using Wireshark.
=> In order to track DHCP packet on our local network using Wireshark, the steps to be followed are:

Step 1:
Go to wireshark and select the network interface (Ethernet in my case)



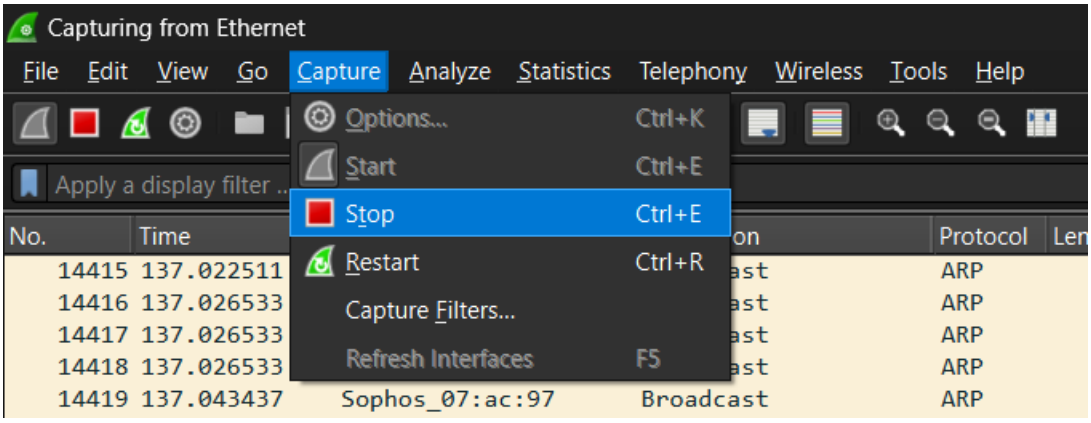
Step 2:
Then, Open the command prompt and run these two commands:

```
C:\Users\ACER>ipconfig /release
```

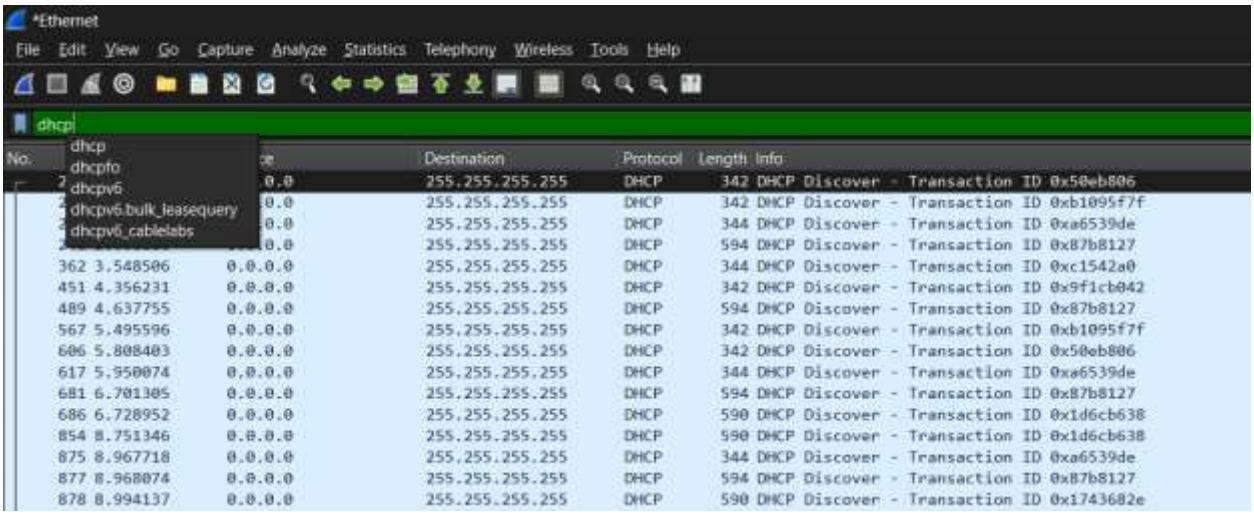
```
C:\Users\ACER>ipconfig/rebase
```

```
                              /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                      ... Show information
    > ipconfig /all                 ... Show detailed information
    > ipconfig /renew               ... renew all adapters
    > ipconfig /renew EL*           ... renew any connection that has its
                                        name starting with EL
    > ipconfig /release *Con*       ... release all matching connections,
                                        eg. "Wired Ethernet Connection 1" or
                                            "Wired Ethernet Connection 2"
    > ipconfig /allcompartments     ... Show information about all
                                        compartments
```

Step 3: Capture the packet on the wireshark.



Step 4:
Filter the dhcp packets.

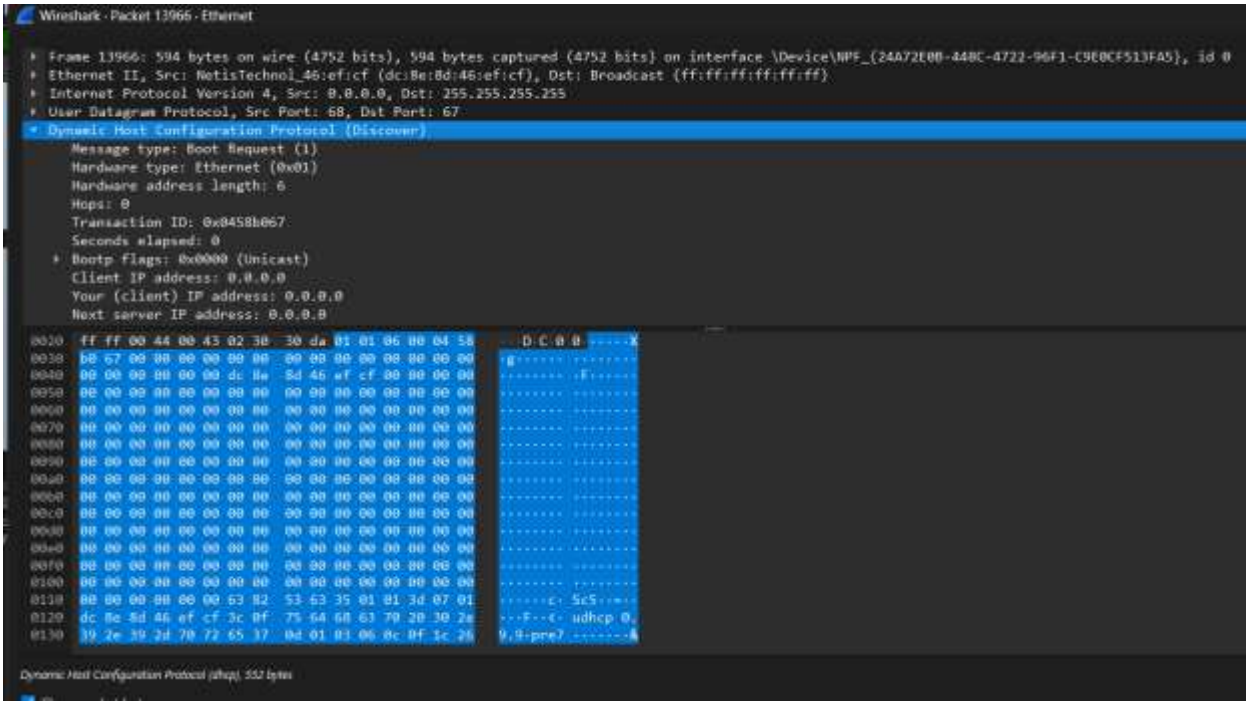


Step 5:

Look for DHCP packets in the capture such as:

DHCP Discover: Sent by a client to find available DHCP servers.
DHCP Offer: Sent by a server in response to a DHCP Discover, offering an IP address.
DHCP Request: Sent by a client to request the offered IP address.
DHCP Acknowledge: Sent by the server to acknowledge the client's request and confirm the IP address assignment.

This is what I got:


Wireshark · Packet 13966 · Ethernet
Frame 13966: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits) on interface \Device\NPF_{24A72E0B-448C-4722-96F1-C9E0CF513FA5}, id 0
Ethernet II, Src: NetisTechnol_46:ef:cf (dc:8e:8d:46:ef:cf), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x0458b067
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Dynamic Host Configuration Protocol (dhcp), 552 bytes