Assignment 3

Dhiraj Kumar Chaurasiya

PAS078BEI012

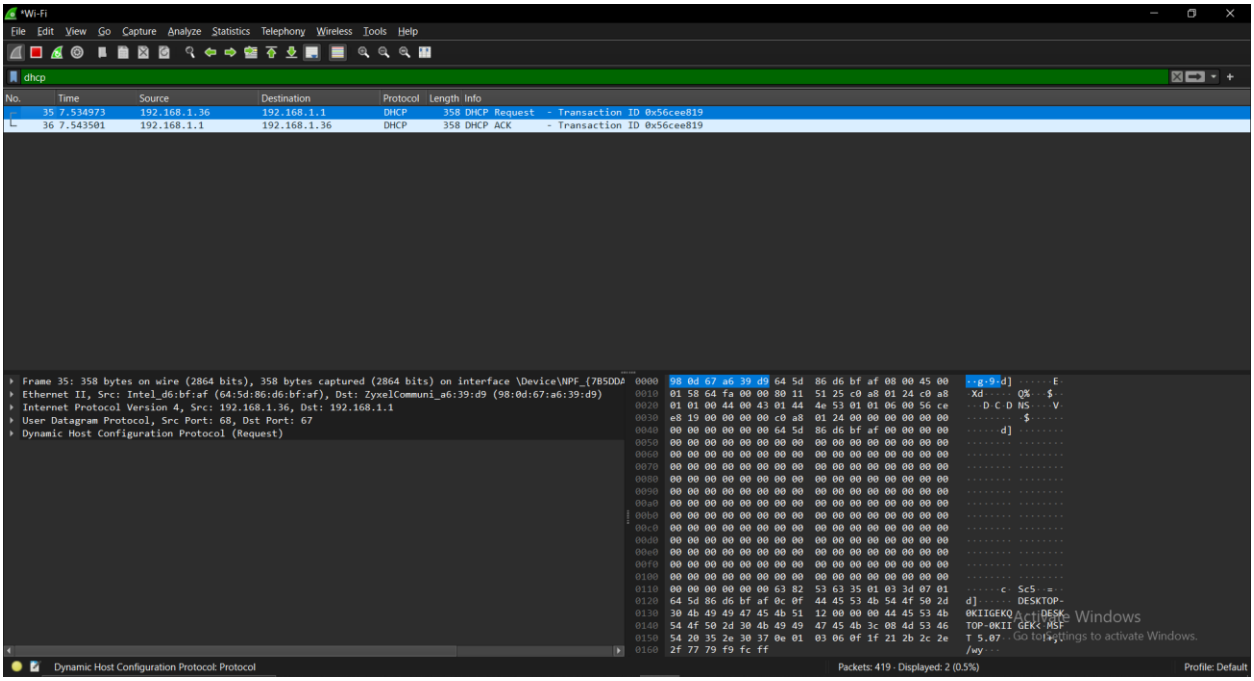
1. Trace DHCP Protocol On Wireshark

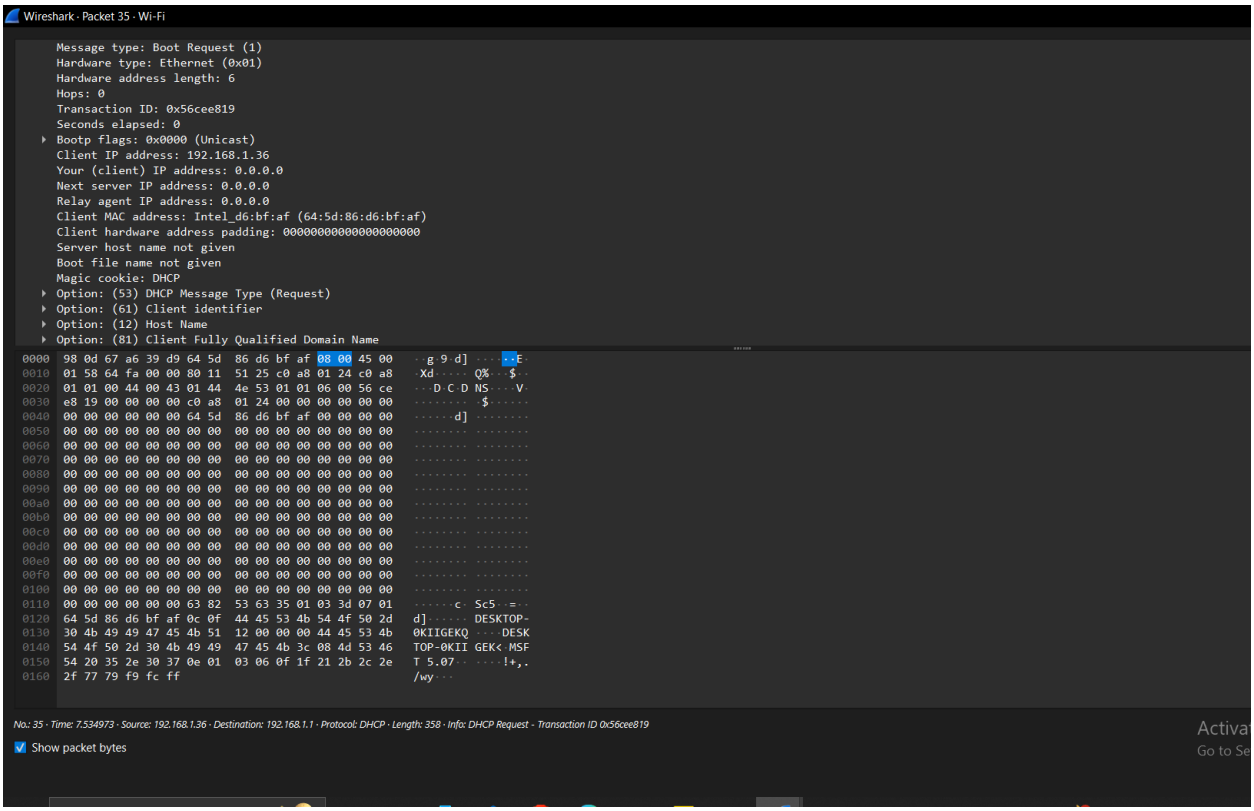
-> First went to Wireshark couldnot find anything when searched for dhcp

-> Then went to command prompt and searched for ipconfig/renew

```
C:\Users\suraj>ipconfig/renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : zyxel.com
   Link-local IPv6 Address . . . . . : fe80::2e9:fe1c:5e24:affa%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.36
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::9a0d:67ff:fea6:39d9%11
                                       192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\suraj>
```

Then observed Wireshark and got this.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
No. Time Source Destination Protocol Length Info
35 7.534973 192.168.1.36 192.168.1.1 DHCP 358 DHCP Request - Transaction ID 0x56cee819
36 7.543501 192.168.1.1 192.168.1.36 DHCP 358 DHCP ACK - Transaction ID 0x56cee819
Frame 35: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{7B5DDA
Ethernet II, Src: Intel_d6:bf:af (64:5d:86:d6:bf:af), Dst: ZyxelCommuni_a6:39:d9 (98:0d:67:a6:39:d9)
Internet Protocol Version 4, Src: 192.168.1.36, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
Dynamic Host Configuration Protocol: Protocol
Packets: 419 · Displayed: 2 (0.5%)
Profile: Default


Wireshark · Packet 35 · Wi-Fi
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x56cee819
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.36
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_d6:bf:af (64:5d:86:d6:bf:af)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
Option: (61) Client identifier
Option: (12) Host Name
Option: (81) Client Fully Qualified Domain Name
No.: 35 · Time: 7.534973 · Source: 192.168.1.36 · Destination: 192.168.1.1 · Protocol: DHCP · Length: 358 · Info: DHCP Request - Transaction ID 0x56cee819
Show packet bytes

2. What happens when you type Facebook.com on your browser and hit enter?

-> When you enter "facebook.com" in your browser's address box and press Enter, many things happen:
Domain Resolution: Your browser initially determines whether the domain name "facebook.com" is already in its cache or DNS cache. If not, it issues a DNS (Domain Name System) request to resolve the domain to its matching IP address.

DNS Lookup: Your browser searches a DNS server (often provided by your ISP or a public DNS provider such as Google DNS or Cloudflare) for the IP address associated with "facebook.com".

Connection Establishment: After obtaining the IP address, your browser establishes a TCP (Transmission Control Protocol) connection to the server at that IP address over port 80 for HTTP or 443 for HTTPS.

TLS Handshake (If HTTPS): If "facebook.com" uses HTTPS (which it does), a TLS (Transport Layer Security) handshake is performed to establish a secure encrypted connection. This entails exchanging encryption keys and authenticating the server's SSL/TLS certificate.

Request has been sent. Your browser sends an HTTP or HTTPS request to the server requesting the webpage. This request comprises information such as browser type, cookies, and URL path (typically "/").

Server answer: The server processes the request and returns either an HTTP or HTTPS answer. This often comprises the requested page's HTML content as well as links to other resources (CSS files, JavaScript files, pictures, and so on).

Rendering: Your browser begins rendering the page. It processes HTML, applies CSS styles, and runs JavaScript. Additional resources (such as photos or movies) are requested and loaded as required.

Page Displayed: Once all resources have been loaded and processed, the page appears on your screen. Throughout this process, several background actions including as caching, connection reuse, and security checks are carried out to guarantee that the page loads quickly and safely.