VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

BCSE308P-COMPUTER NETWORKS LAB

NAME : PATEL SWAPNILKUMAR C.

REG.NO : 22BAI1308

SEM : FALL 23-24

TOPIC : EXPERIMENT-1

1) NETWORKING COMMANDS:

Aim:To test various commands and their outputs

Procedure:

C:\>hostname: This is the simplest of all TCP/IP commands. It simply displays the name of your computer.

C:\>ipconfig: The ipconfig command displays information about the host (the computer your sitting at)computer TCP/IP configuration.

Command Prompt

```
C:\Users\student>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a961:712:60c6:9018%21
   IPv4 Address. . . . . . . . . . . : 172.16.15.60
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.15.2

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e0fa:ceae:fd10:7295%5
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e865:4796:f7fb:fed9%4
   IPv4 Address. . . . . . . . . . . : 192.168.203.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::54bd:2bc8:b6d7:391%13
   IPv4 Address. . . . . . . . . . . : 192.168.245.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\student>hostname
AB1311SCOPE60

C:\Users\student>_
```

C:\>ipconfig /all: This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP, and type of Ethernet adapter in your system.

Output:

Command Prompt

```
C:\Users\student>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : AB1311SCOPE60
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : A0-8C-FD-C9-9F-EB
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a961:712:60c6:9018%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.15.60(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.15.2
   DHCPv6 IAID . . . . . . . . . . . : 278957309
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-A7-80-9A-A0-8C-FD-C9-9F-EB
   DNS Servers . . . . . . . . . . . : 172.16.1.11
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-05
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e0fa:ceae:fd10:7295%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 436863015
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-A7-80-9A-A0-8C-FD-C9-9F-EB
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
```

Command Prompt

```
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter #4
   Physical Address. . . . . . . . . : 0A-00-27-00-00-04
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e865:4796:f7fb:fed9%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.203.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 638189607
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-A7-80-9A-A0-8C-FD-C9-9F-EB
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter #6
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::54bd:2bc8:b6d7:391%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.245.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 738852903
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-A7-80-9A-A0-8C-FD-C9-9F-EB
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\student>
```

C:\>ipconfig /flushdns: This command is only needed if you're having trouble with your networks DNS configuration. The best time to use this command is after network configuration frustration sets in, and you really need the computer to reply with flushed.

C:\>nbtstat –a: This command helps solve problems with NetBIOS name resolution. (Nbt stands for NetBIOS over TCP/IP) Output:

Command Prompt

```
C:\Users\student>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\student>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.


C:\Users\student>
```

C:\>netstat: Netstat displays a variety of statistics about a computers active TCP/IP connections. This tool is most useful when you're having trouble with TCP/IP applications such as HTTP, and FTP.

C:\>nslookup: Nslookup is used for diagnosing DNS problems. If you can access a resource by specifying an IP address but not it's DNS you have a DNS problem.

Output:

Command Prompt - nslookup

```
C:\Users\student>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.15.60:7680      AB1311SCOPE17:51786    TIME_WAIT
  TCP    172.16.15.60:53944     20.198.119.84:https    ESTABLISHED
  TCP    172.16.15.60:54261     a23-206-206-224:https  CLOSE_WAIT
  TCP    172.16.15.60:54320     40.70.161.7:https      ESTABLISHED
  TCP    172.16.15.60:54332     a23-59-175-96:https    CLOSE_WAIT
  TCP    172.16.15.60:54333     117.18.232.200:https   CLOSE_WAIT
  TCP    172.16.15.60:54339     13.107.246.254:https   CLOSE_WAIT
  TCP    172.16.15.60:54354     52.137.103.130:https   TIME_WAIT
  TCP    172.16.15.60:54356     20.189.173.11:https    TIME_WAIT
  TCP    [fe80::54bd:2bc8:b6d7:391%13]:1521  AB1311SCOPE60:49680    ESTABLISHED
  TCP    [fe80::54bd:2bc8:b6d7:391%13]:49680  AB1311SCOPE60:1521     ESTABLISHED

C:\Users\student>nslookup
Default Server:  vitccdns
Address:  172.16.1.11

>
```

C:\>arp –a: ARP is short form of address resolution protocol, It will show the IP address of your computer along with the IP address and MAC address of your router.

Output:

Command Prompt

```
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.

C:\Users\student>hostname
AB1311SCOPE60

C:\Users\student>_
```

C:\>pathping: Pathping is unique to Window's, and is basically a combination of the Ping and Tracert commands. Pathping traces the route to the destination address then launches a 25 second test of each router along the way, gathering statistics on the rate of data loss along each hop.

C:\>ping: Ping is the most basic TCP/IP command, and it's the same as placing a phone call to your best friend. You pick up your telephone and dial a number, expecting your best friend to reply with "Hello" on the other end. Computers make phone calls to each other over a network by using a Ping command. The Ping commands main purpose is to place a phone call to another computer on the network, and request an answer. Ping has 2 options it can use to place a phone call to another computer on the network. It can use the computers name or IP address.

Output:

```
Command Prompt
C:\Users\student>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list      Loose source route along host-list.
    -h maximum_hops   Maximum number of hops to search for target.
    -i address        Use the specified source address.
    -n                Do not resolve addresses to hostnames.
    -p period         Wait period milliseconds between pings.
    -q num_queries    Number of queries per hop.
    -w timeout        Wait timeout milliseconds for each reply.
    -4                Force using IPv4.
    -6                Force using IPv6.

C:\Users\student>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
```

C:\>route: The route command displays the computers routing table. A typical computer, with a single network interface, connected to a LAN, with a router is fairly simple and generally doesn't pose any network problems. But if you're having trouble accessing other computers on your network, you can use the route command to make sure the entries in the routing table are correct.

Output:

Command Prompt

```
                    this header is used.
    -S srcaddr      Source address to use.
    -c compartment  Routing compartment identifier.
    -p              Ping a Hyper-V Network Virtualization provider address.
    -4              Force using IPv4.
    -6              Force using IPv6.


C:\Users\student>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f            Clears the routing tables of all gateway entries.  If this is
                used in conjunction with one of the commands, the tables are
                cleared prior to running the command.

  -p            When used with the ADD command, makes a route persistent across
                boots of the system. By default, routes are not preserved
                when the system is restarted. Ignored for all other commands,
                which always affect the appropriate persistent routes.

  -4            Force using IPv4.

  -6            Force using IPv6.

  command       One of these:
                  PRINT     Prints  a route
                  ADD       Adds    a route
                  DELETE    Deletes a route
                  CHANGE    Modifies an existing route
  destination   Specifies the host.
  MASK          Specifies that the next parameter is the 'netmask' value.
  netmask       Specifies a subnet mask value for this route entry.
                If not specified, it defaults to 255.255.255.255.
  gateway       Specifies gateway.
  interface     the interface number for the specified route.
  METRIC        specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.
```

Command Prompt

```
If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32

C:\Users\student>
```

C:\>tracert: The tracert command displays a list of all the routers that a packet has to go through to get from the computer where tracert is run to any other computer on the internet.

Output:

Command Prompt

```
C:\Users\student>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\student>_
```

C:\>Ipconfig /renew: Using this command will renew all your IP addresses that you are currently (leasing) borrowing from the DHCP server. This command is a quick problem solver if you are having connection issues, but does not work if you have been configured with a static IP address.

C:\>Ipconifg /release: This command allows you to drop the IP lease from the DHCP server.

C:\>ipconfig /flushdns: This command is only needed if you’re having trouble with your networks DNS configuration. The best time to use this command is after network configuration frustration sets in, and you really need the computer to reply with flushed.

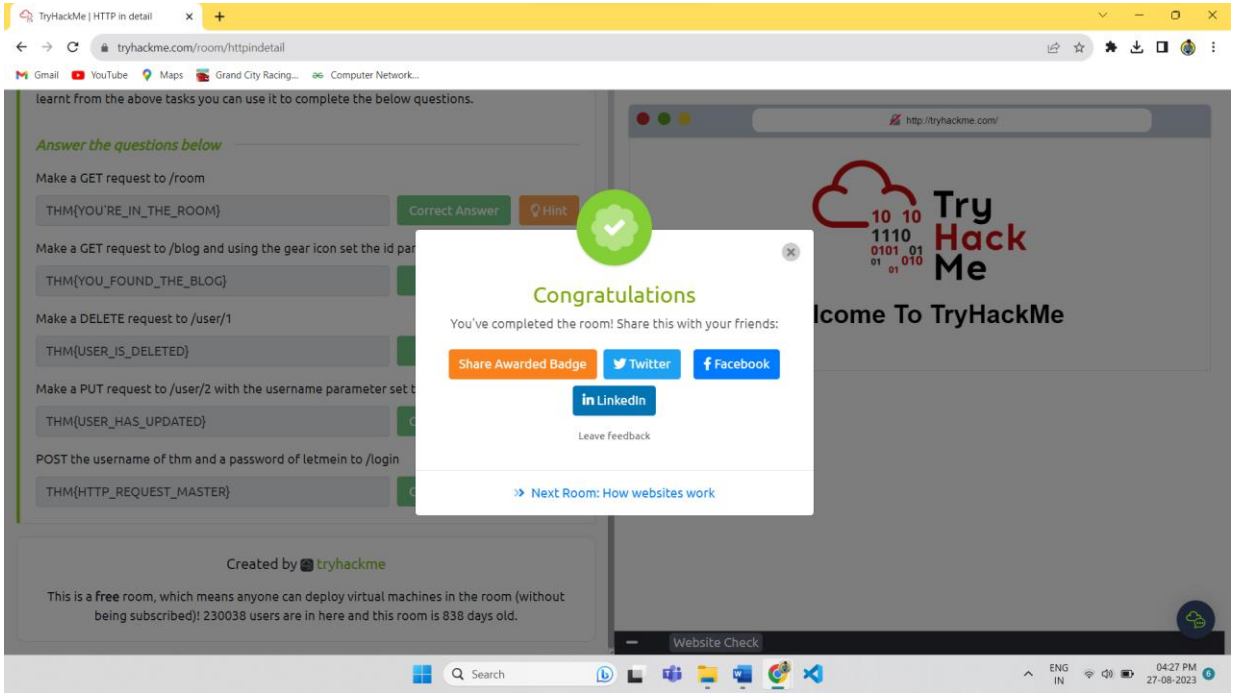
Output:

Command Prompt

```
C:\Users\student>Ipconfig/renew

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.

C:\Users\student>Ipconfig/release

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.

C:\Users\student>netdiag
'netdiag' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student>
```

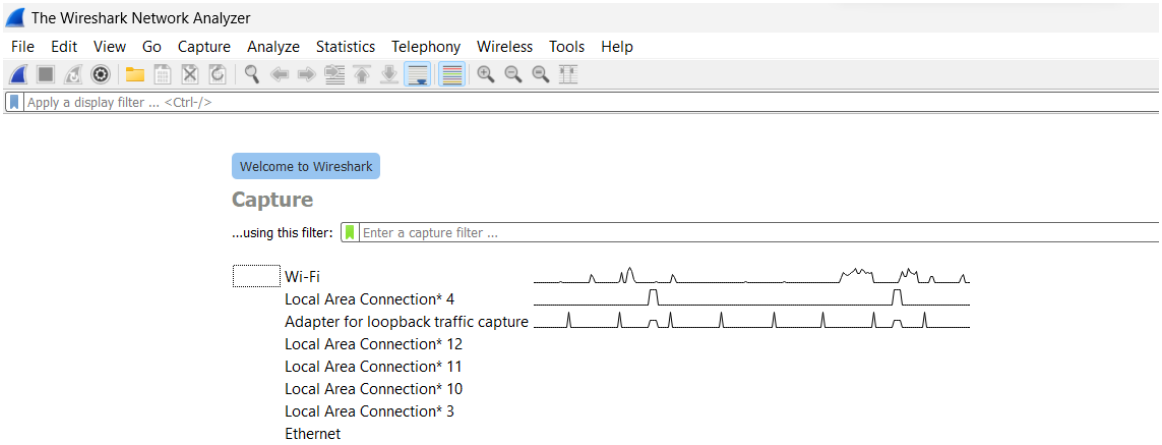
2) TRY HACK ME – 7 TASKS COMPLETED:

HTTP in Detail (under web fundamentals)



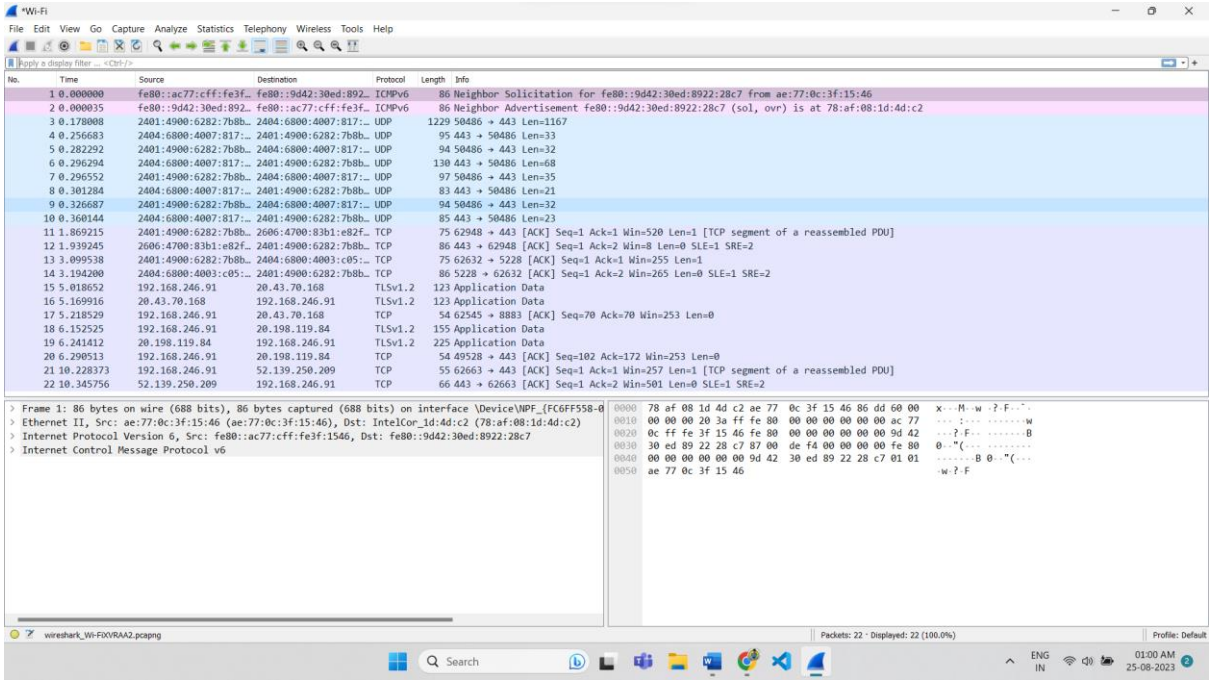
2) WIRESHARK :

INTERFACE (Home Screen) :



In the main window, you'll see a list of available network interfaces. These are your network adapters through which Wireshark can capture packets. The above screen shows my adapters and the traffic on it.

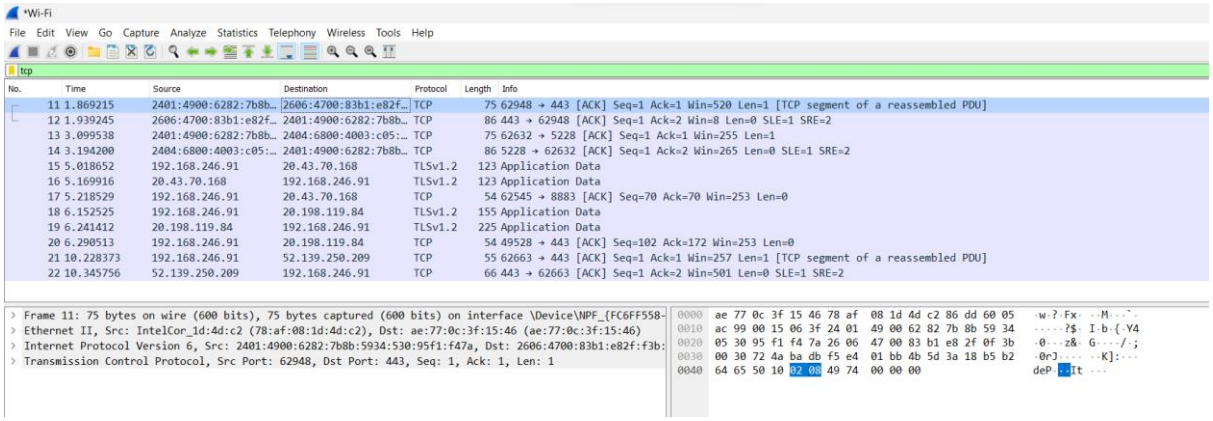
1. Here selecting Wifi adapter and **Capturing the packets for 5 sec.**



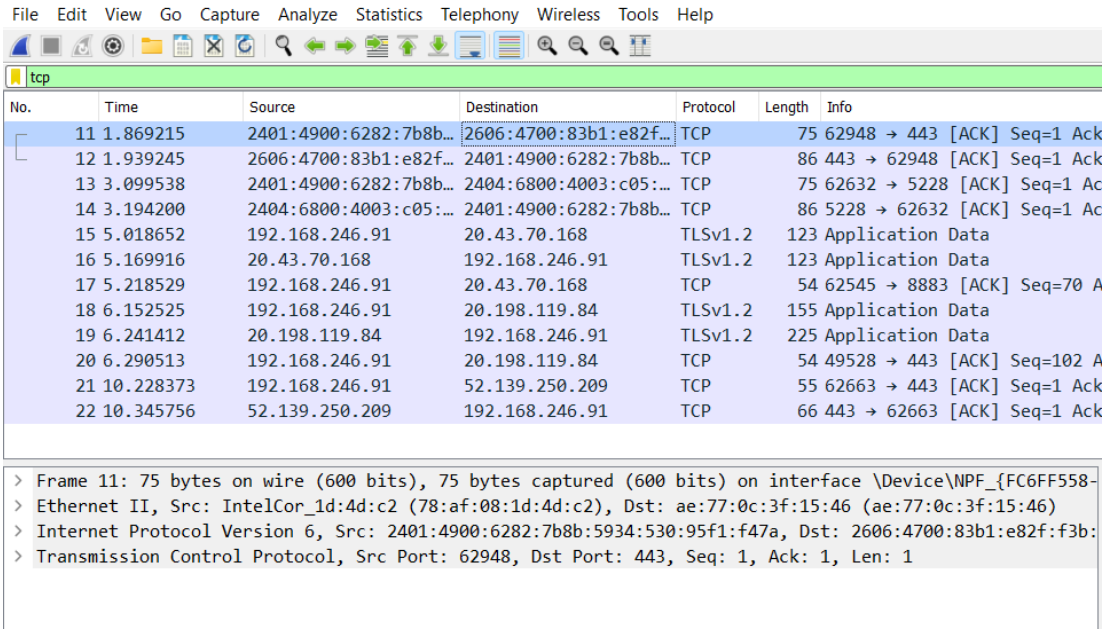
Locating TCP packet – packet no. 11

Locating UDP packet – packet no. 3

2. Applying filter to see only TCP packets.



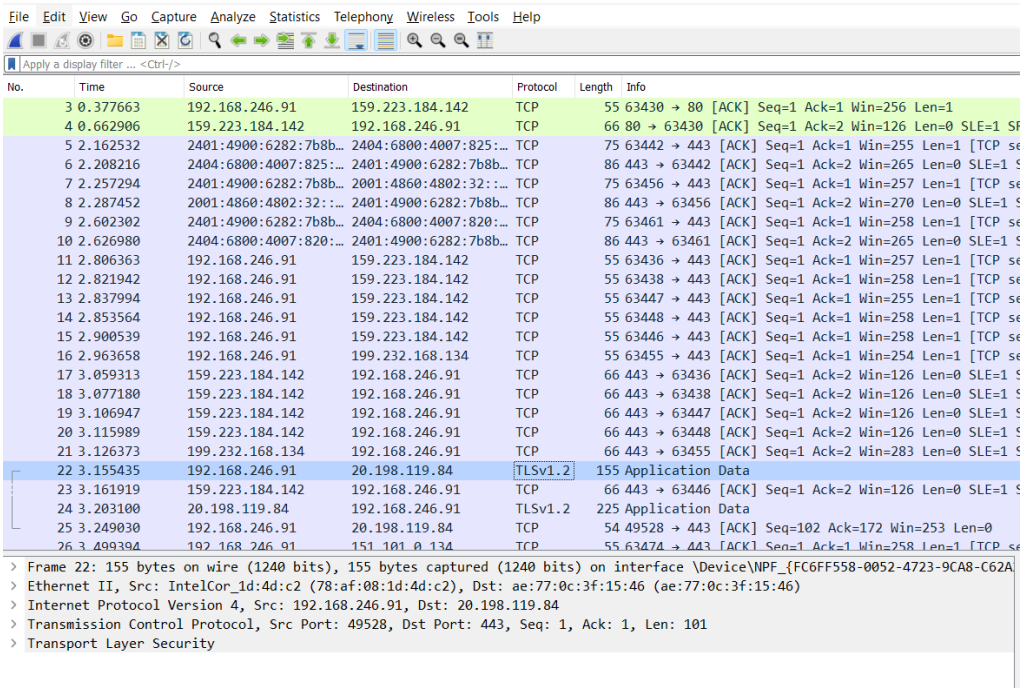
3. Locating a TCP packet and analyzing its layers.



Packet number – 11 (selected above)

No. of layers – 4 (layers details in lower window pane)

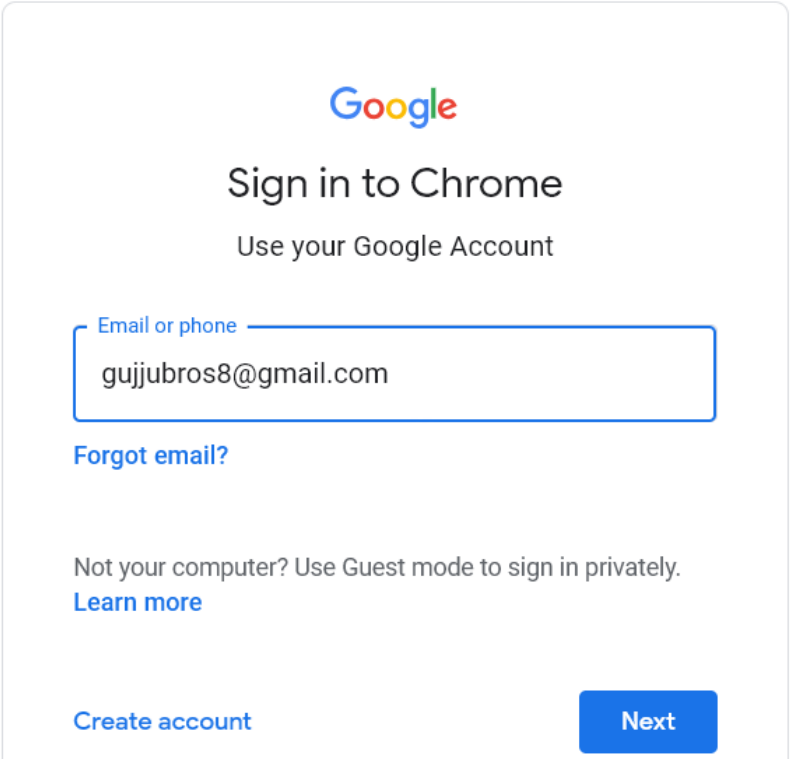
4. Locating a TLS packet and analyzing its layers.



Packet number – 22 (selected above)

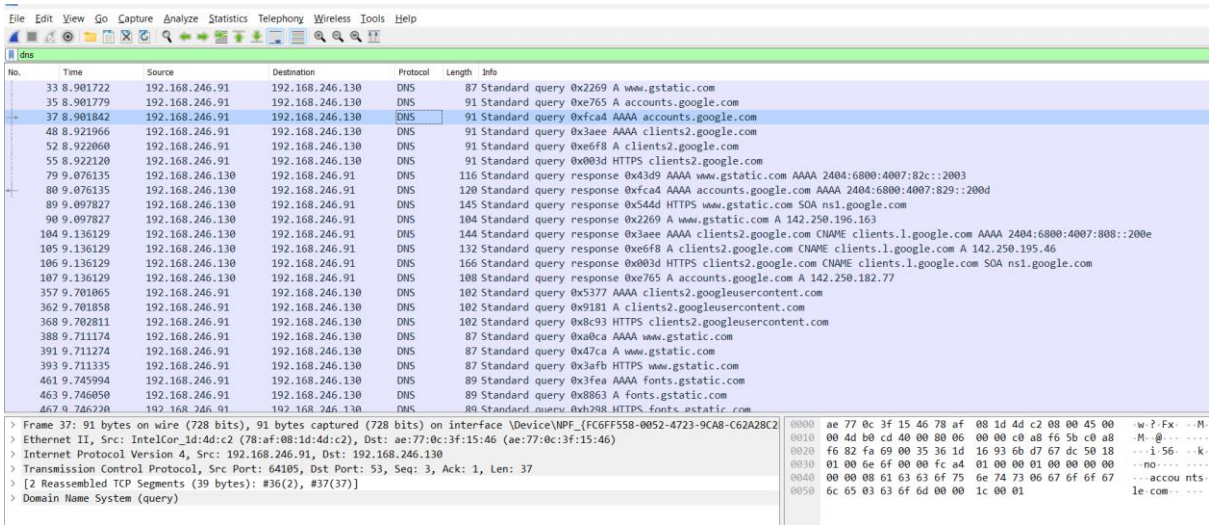
No. of layers – 5 (layers details in lower window pane)

5. Starting to collect the packets.
6. **Logging in to Google.**

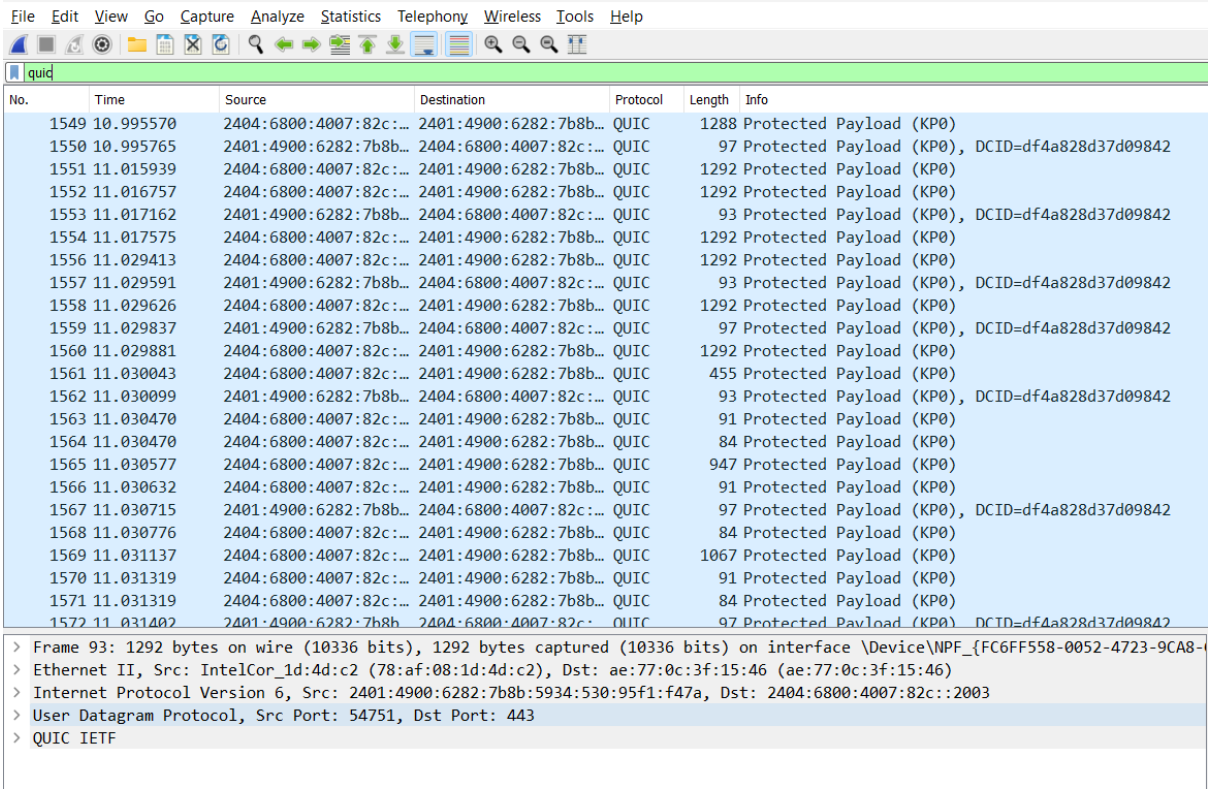


7. Stopping the packets capture.

Locating Request and Response of Gmail Login.



8. Packet 37 asking for **request**, and packet 79 onwards got the **response**.
9. Checking the presence of encrypted content.
10. Packets with description PROTECTED PAYLOAD.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

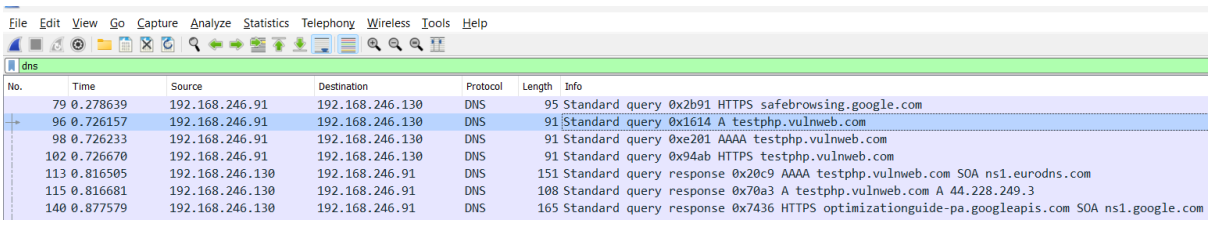
quic

No.	Time	Source	Destination	Protocol	Length	Info
1549	10.995570	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1288	Protected Payload (KP0)
1550	10.995765	2401:4900:6282:7b8b…	2404:6800:4007:82c:…	QUIC	97	Protected Payload (KP0), DCID=df4a828d37d09842
1551	11.015939	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1292	Protected Payload (KP0)
1552	11.016757	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1292	Protected Payload (KP0)
1553	11.017162	2401:4900:6282:7b8b…	2404:6800:4007:82c:…	QUIC	93	Protected Payload (KP0), DCID=df4a828d37d09842
1554	11.017575	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1292	Protected Payload (KP0)
1556	11.029413	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1292	Protected Payload (KP0)
1557	11.029591	2401:4900:6282:7b8b…	2404:6800:4007:82c:…	QUIC	93	Protected Payload (KP0), DCID=df4a828d37d09842
1558	11.029626	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1292	Protected Payload (KP0)
1559	11.029837	2401:4900:6282:7b8b…	2404:6800:4007:82c:…	QUIC	97	Protected Payload (KP0), DCID=df4a828d37d09842
1560	11.029881	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1292	Protected Payload (KP0)
1561	11.030043	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	455	Protected Payload (KP0)
1562	11.030099	2401:4900:6282:7b8b…	2404:6800:4007:82c:…	QUIC	93	Protected Payload (KP0), DCID=df4a828d37d09842
1563	11.030470	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	91	Protected Payload (KP0)
1564	11.030470	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	84	Protected Payload (KP0)
1565	11.030577	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	947	Protected Payload (KP0)
1566	11.030632	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	91	Protected Payload (KP0)
1567	11.030715	2401:4900:6282:7b8b…	2404:6800:4007:82c:…	QUIC	97	Protected Payload (KP0), DCID=df4a828d37d09842
1568	11.030776	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	84	Protected Payload (KP0)
1569	11.031137	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	1067	Protected Payload (KP0)
1570	11.031319	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	91	Protected Payload (KP0)
1571	11.031319	2404:6800:4007:82c:…	2401:4900:6282:7b8b…	QUIC	84	Protected Payload (KP0)
1572	11.031402	2401:4900:6282:7b8b…	2404:6800:4007:82c:…	QUIC	97	Protected Payload (KP0), DCID=df4a828d37d09842

```
> Frame 93: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{FC6FF558-0052-4723-9CA8-
> Ethernet II, Src: IntelCor_1d:4d:c2 (78:af:08:1d:4d:c2), Dst: ae:77:0c:3f:15:46 (ae:77:0c:3f:15:46)
> Internet Protocol Version 6, Src: 2401:4900:6282:7b8b:5934:530:95f1:f47a, Dst: 2404:6800:4007:82c::2003
> User Datagram Protocol, Src Port: 54751, Dst Port: 443
> QUIC IETF
```

Protected content

11. Define Interface & Start collecting packets again
12. login with **guest account** in the webpage http://testphp.vulnweb.com/login.php



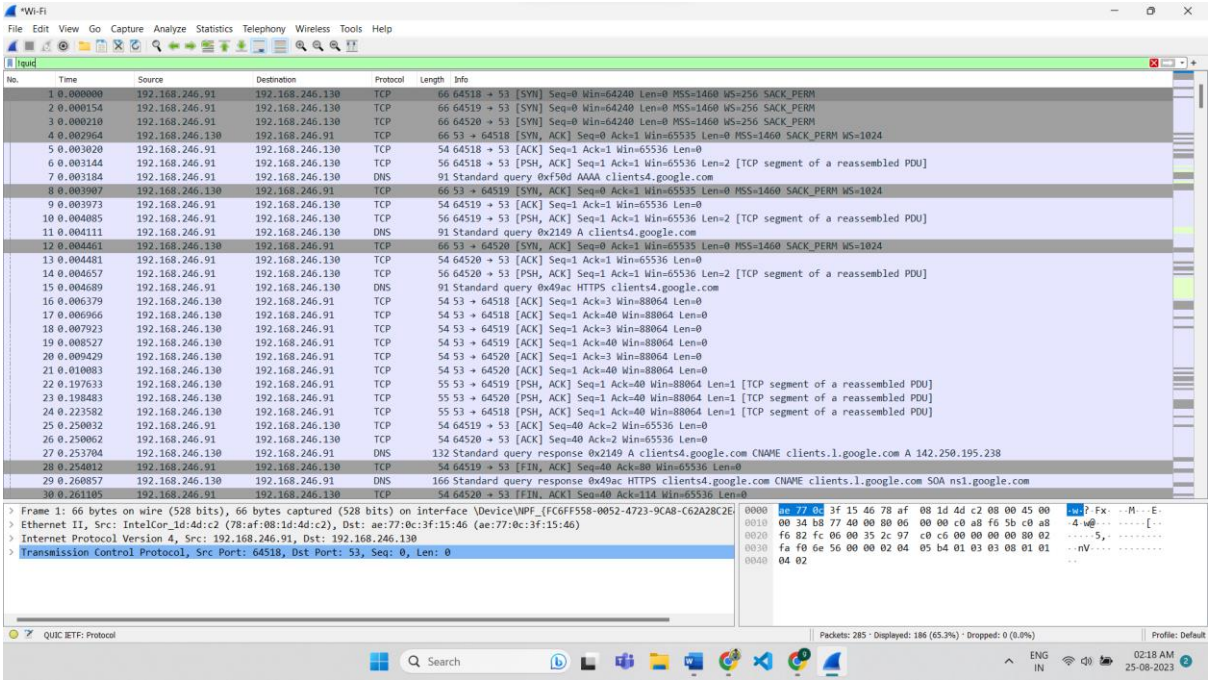
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
79	0.278639	192.168.246.91	192.168.246.130	DNS	95	Standard query 0x2b91 HTTPS safebrowsing.google.com
96	0.726157	192.168.246.91	192.168.246.130	DNS	91	Standard query 0x1614 A testphp.vulnweb.com
98	0.726233	192.168.246.91	192.168.246.130	DNS	91	Standard query 0xe201 AAAA testphp.vulnweb.com
102	0.726670	192.168.246.91	192.168.246.130	DNS	91	Standard query 0x94ab HTTPS testphp.vulnweb.com
113	0.816505	192.168.246.130	192.168.246.91	DNS	151	Standard query response 0x20c9 AAAA testphp.vulnweb.com SOA ns1.eurodns.com
115	0.816681	192.168.246.130	192.168.246.91	DNS	108	Standard query response 0x70a3 A testphp.vulnweb.com A 44.228.249.3
140	0.877579	192.168.246.130	192.168.246.91	DNS	165	Standard query response 0x7436 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com

- Packet 102 asking for **request**, and Packet 113 **response** in above image.

13. Checking the presence of **unencrypted content.**
14. Type “!QUIC” under filters and click on apply.



Unprotected content

OVER

------X-----X-----X-----X-----X-----X-----X-----X-----X-----X-----X-----X------X-----X-----X-----X-----X----

!! . THANK YOU . !!