Ftp protocol

1) Sudo apt update
2) Sudo apt install vsftpd
3) Sudo service vsftpd status
4) Sudo nano /etc/vsftpd.conf
   *) anonymous_enable=YES
   *) local_enable = YES
   *) write_enable = YES
   *)optional pasv_min_port=10000
   pasv_max_port=10100
5) sudo systemctl restart vsftpd
6) Sudo ufw allow ftp
7) sudo useradd -m testuser
8) sudo passwd testuser (Abbas@110)
9) hostname
10) Sudo ftp abbasmakasarwala (your-server-name) - then put the name and password of another user.

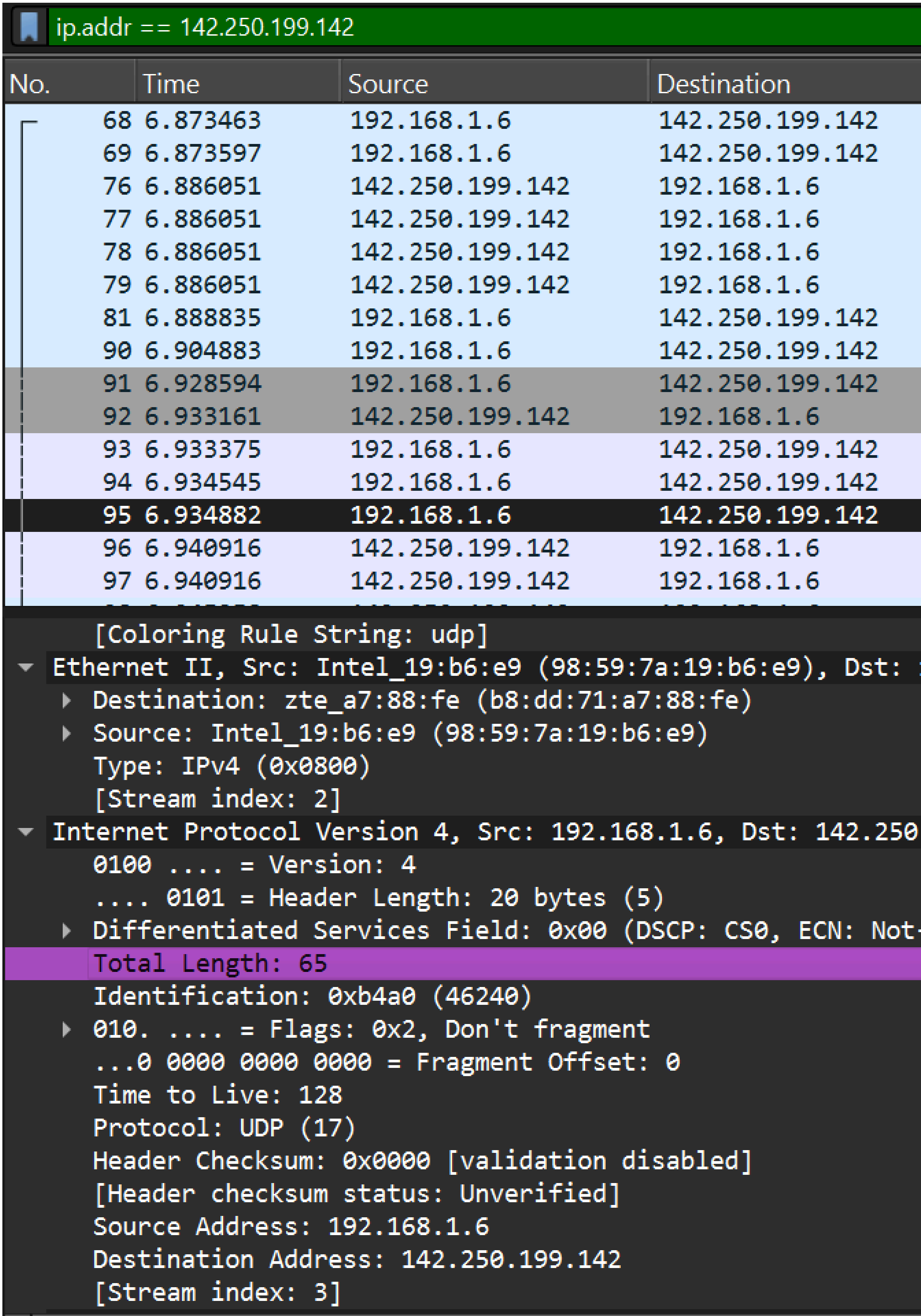
    If any error:
    Sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.back
    Sudo nano /etc/vsftpd.conf
    Pam_service =ftp
    Sudo service vsftpd restart .

Puts to puts
Gets
mputs - puts multiple files
mget -gets multiple files
Mkdir -make directory
Rmdir -remove directory.

Wire shark:

Filters:

1) tcp/udp
2) Tcp contains “youtube”
3) ip.addr == 142.250.199.142 (packages which contain ip address of youtube)
4) Different information of the packet like ipv entire header the udp entire header info of frames , src destination ports etc.

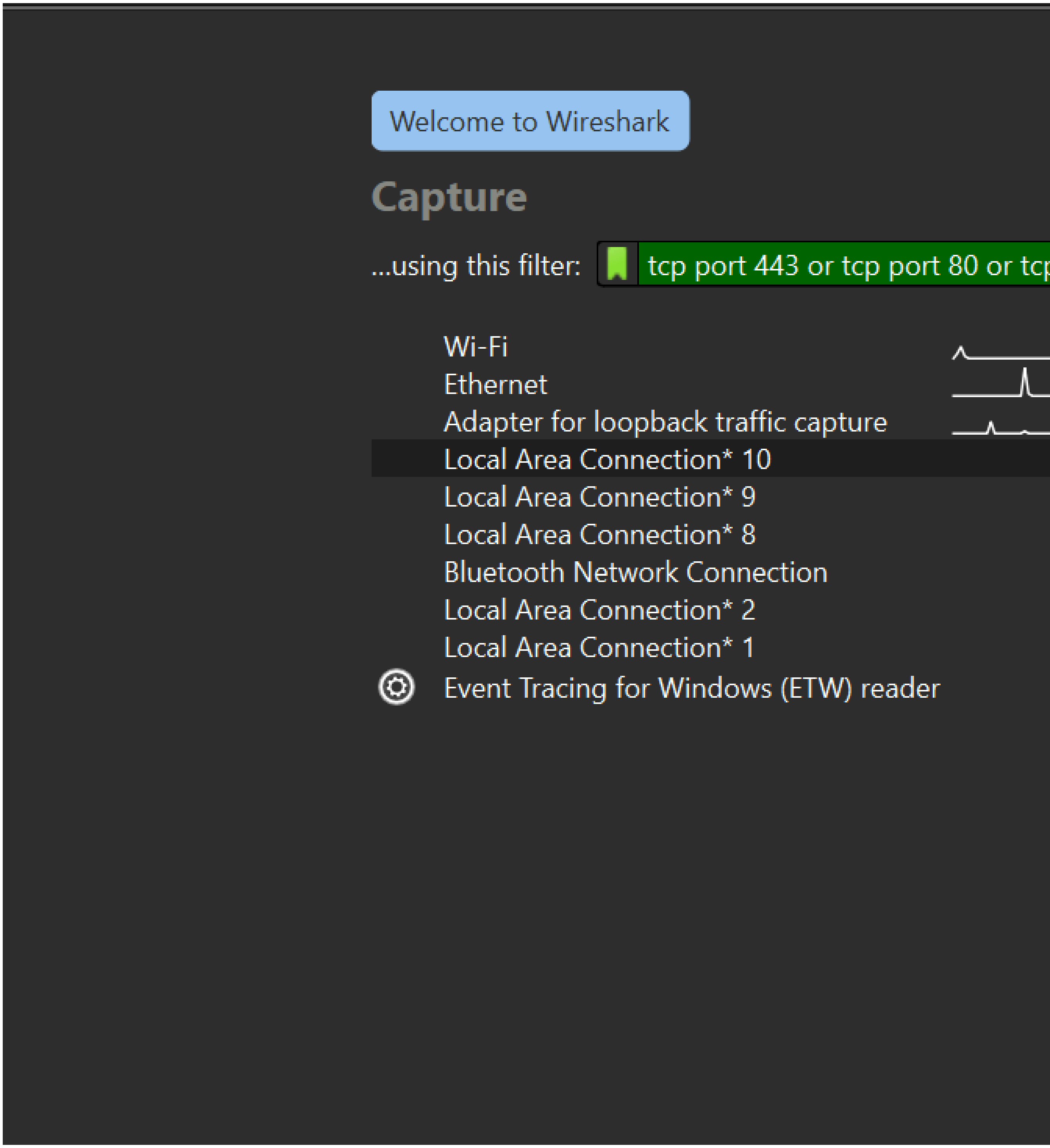


```
ip.addr == 142.250.199.142
```

```
No.   Time        Source            Destination
  68 6.873463    192.168.1.6       142.250.199.142
  69 6.873597    192.168.1.6       142.250.199.142
  76 6.886051    142.250.199.142   192.168.1.6
  77 6.886051    142.250.199.142   192.168.1.6
  78 6.886051    142.250.199.142   192.168.1.6
  79 6.886051    142.250.199.142   192.168.1.6
  81 6.888835    192.168.1.6       142.250.199.142
  90 6.904883    192.168.1.6       142.250.199.142
  91 6.928594    192.168.1.6       142.250.199.142
  92 6.933161    142.250.199.142   192.168.1.6
  93 6.933375    192.168.1.6       142.250.199.142
  94 6.934545    192.168.1.6       142.250.199.142
  95 6.934882    192.168.1.6       142.250.199.142
  96 6.940916    142.250.199.142   192.168.1.6
  97 6.940916    142.250.199.142   192.168.1.6
```

```
    [Coloring Rule String: udp]
Ethernet II, Src: Intel_19:b6:e9 (98:59:7a:19:b6:e9), Dst: 
    Destination: zte_a7:88:fe (b8:dd:71:a7:88:fe)
    Source: Intel_19:b6:e9 (98:59:7a:19:b6:e9)
    Type: IPv4 (0x0800)
    [Stream index: 2]
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 142.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-
    Total Length: 65
    Identification: 0xb4a0 (46240)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.6
    Destination Address: 142.250.199.142
    [Stream index: 3]
```

5) (Not secure website) tcp contains ‘username”
6) Capture filter (capture packets based only on certain filter).
   Tcp port 443 or tcp port 80

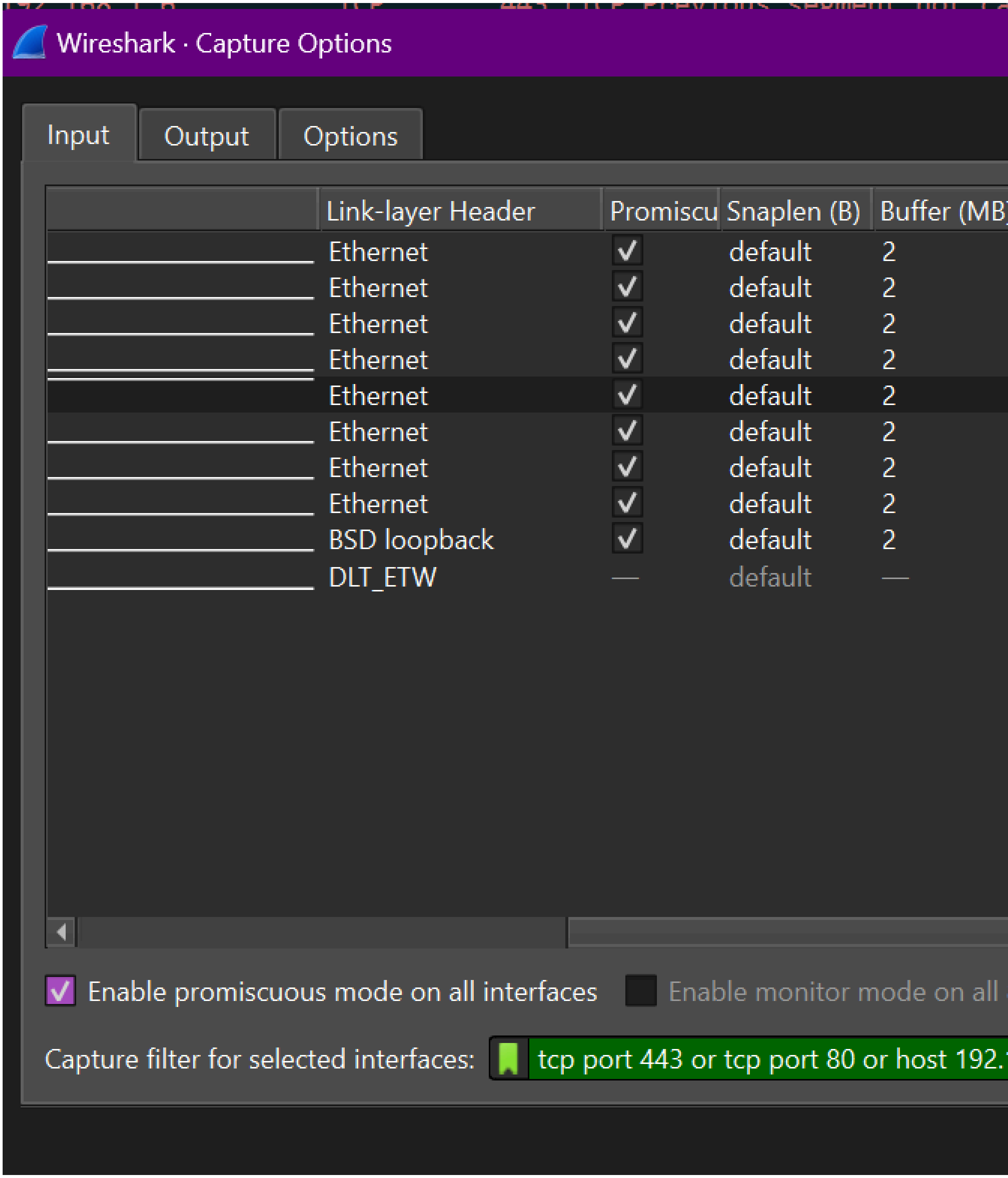


...using this filter: tcp port 443 or tcp port 80 or tcp

Wi-Fi
Ethernet
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Event Tracing for Windows (ETW) reader

7) Capture
   -> options

Can add more capture filters.



	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB
	Ethernet	☑	default	2
	Ethernet	☑	default	2
	Ethernet	☑	default	2
	Ethernet	☑	default	2
	Ethernet	☑	default	2
	Ethernet	☑	default	2
	Ethernet	☑	default	2
	Ethernet	☑	default	2
	BSD loopback	☑	default	2
	DLT_ETW	—	default	—

☑ Enable promiscuous mode on all interfaces □ Enable monitor mode on all

Capture filter for selected interfaces: tcp port 443 or tcp port 80 or host 192.

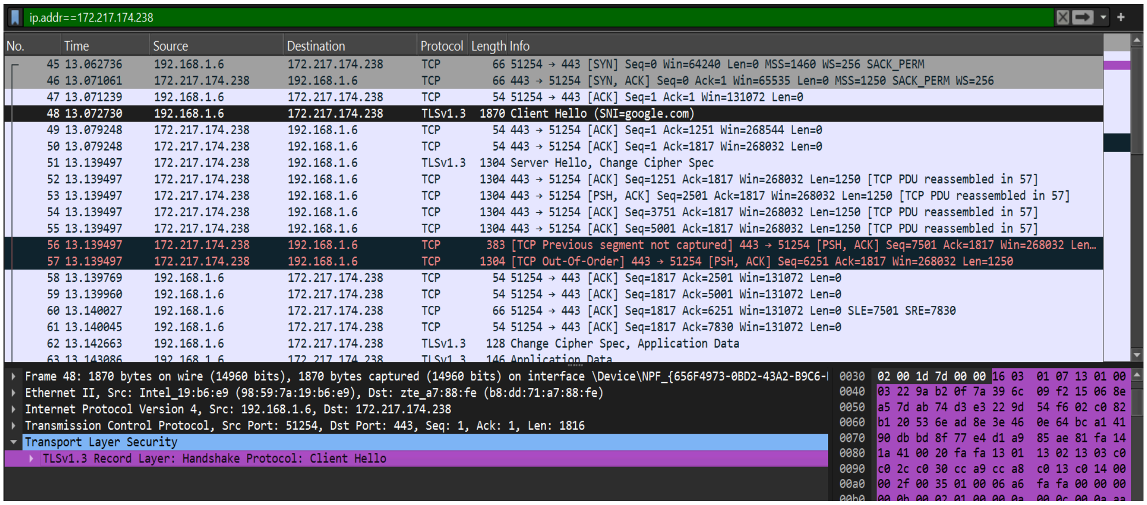
Handshake

Start capture

1) Start a incognito tab and search google.com
2) Then ping google.com to get ip

A cipher suite is a collection of cryptographic algorithms that are used to encrypt and decrypt data exchanged between a client and a server.

Client cipler suites ie which all suits are with the clien t

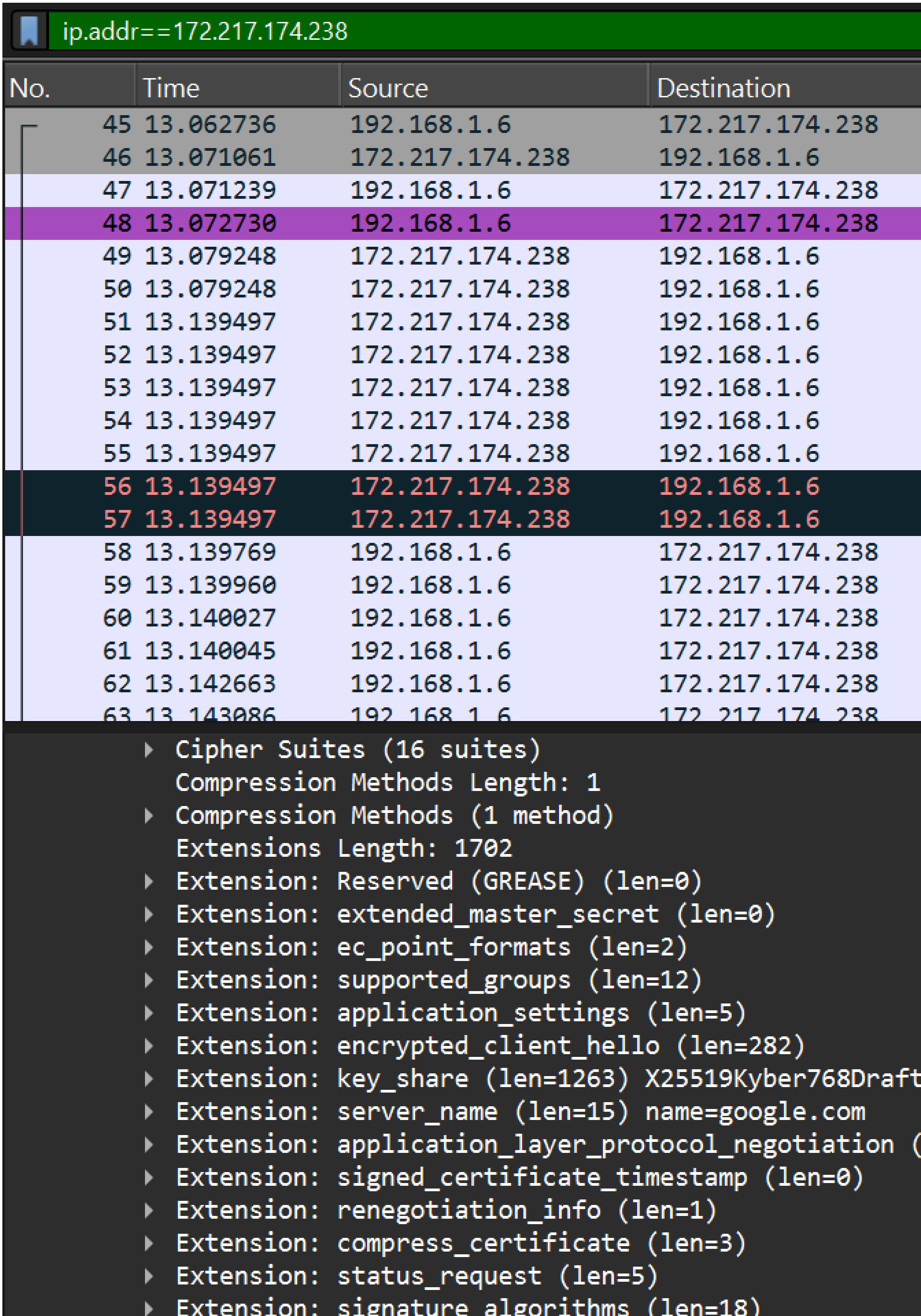


ip.addr==172.217.174.238

```
No.  Time       Source           Destination      Protocol Length Info
  45 13.062736  192.168.1.6      172.217.174.238  TCP        66 51254 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  46 13.071061  172.217.174.238  192.168.1.6      TCP        66 443 → 51254 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM WS=256
  47 13.071239  192.168.1.6      172.217.174.238  TCP        54 51254 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
  48 13.072730  192.168.1.6      172.217.174.238  TLSv1.3  1870 Client Hello (SNI=google.com)
  49 13.079248  172.217.174.238  192.168.1.6      TCP        54 443 → 51254 [ACK] Seq=1 Ack=1251 Win=268544 Len=0
  50 13.079248  172.217.174.238  192.168.1.6      TCP        54 443 → 51254 [ACK] Seq=1 Ack=1817 Win=268032 Len=0
  51 13.139497  172.217.174.238  192.168.1.6      TLSv1.3  1304 Server Hello, Change Cipher Spec
  52 13.139497  172.217.174.238  192.168.1.6      TCP      1304 443 → 51254 [ACK] Seq=1251 Ack=1817 Win=268032 Len=1250 [TCP PDU reassembled in 57]
  53 13.139497  172.217.174.238  192.168.1.6      TCP      1304 443 → 51254 [PSH, ACK] Seq=2501 Ack=1817 Win=268032 Len=1250 [TCP PDU reassembled in 57]
  54 13.139497  172.217.174.238  192.168.1.6      TCP      1304 443 → 51254 [ACK] Seq=3751 Ack=1817 Win=268032 Len=1250 [TCP PDU reassembled in 57]
  55 13.139497  172.217.174.238  192.168.1.6      TCP      1304 443 → 51254 [ACK] Seq=5001 Ack=1817 Win=268032 Len=1250 [TCP PDU reassembled in 57]
  56 13.139497  172.217.174.238  192.168.1.6      TCP       383 [TCP Previous segment not captured] 443 → 51254 [PSH, ACK] Seq=7501 Ack=1817 Win=268032 Len…
  57 13.139497  172.217.174.238  192.168.1.6      TCP      1304 [TCP Out-Of-Order] 443 → 51254 [PSH, ACK] Seq=6251 Ack=1817 Win=268032 Len=1250
  58 13.139769  192.168.1.6      172.217.174.238  TCP        54 51254 → 443 [ACK] Seq=1817 Ack=2501 Win=131072 Len=0
  59 13.139960  192.168.1.6      172.217.174.238  TCP        54 51254 → 443 [ACK] Seq=1817 Ack=5001 Win=131072 Len=0
  60 13.140027  192.168.1.6      172.217.174.238  TCP        66 51254 → 443 [ACK] Seq=1817 Ack=6251 Win=131072 Len=0 SLE=7501 SRE=7830
  61 13.140045  192.168.1.6      172.217.174.238  TCP        54 51254 → 443 [ACK] Seq=1817 Ack=7830 Win=131072 Len=0
  62 13.142663  192.168.1.6      172.217.174.238  TLSv1.3   128 Change Cipher Spec, Application Data
  63 13.143086  192.168.1.6      172.217.174.238  TLSv1.3   146 Application Data
```

```
▸ Frame 48: 1870 bytes on wire (14960 bits), 1870 bytes captured (14960 bits) on interface \Device\NPF_{656F4973-0BD2-43A2-B9C6-
▸ Ethernet II, Src: Intel_19:b6:e9 (98:59:7a:19:b6:e9), Dst: zte_a7:88:fe (b8:dd:71:a7:88:fe)
▸ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.217.174.238
▸ Transmission Control Protocol, Src Port: 51254, Dst Port: 443, Seq: 1, Ack: 1, Len: 1816
▾ Transport Layer Security
    ▸ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
```

```
0030  02 00 1d 7d 00 00 16 03  01 07 13 01 00
0040  03 22 9a b2 0f 7a 39 6c  09 f2 15 06 8e
0050  a5 7d ab 74 d3 e3 22 9d  54 f6 02 c0 82
0060  b1 20 53 6e ad 8e 3e 46  0e 64 bc a1 41
0070  90 db bd 8f 77 e4 d1 a9  85 ae 81 fa 14
0080  1a 41 00 20 fa fa 13 01  13 02 13 03 c0
0090  c0 2c c0 30 cc a9 cc a8  c0 13 c0 14 00
00a0  00 2f 00 35 01 00 06 a6  fa fa 00 00 00
00b0  00 0b 00 02 01 00 00 0a  00 0c 00 0a aa
```

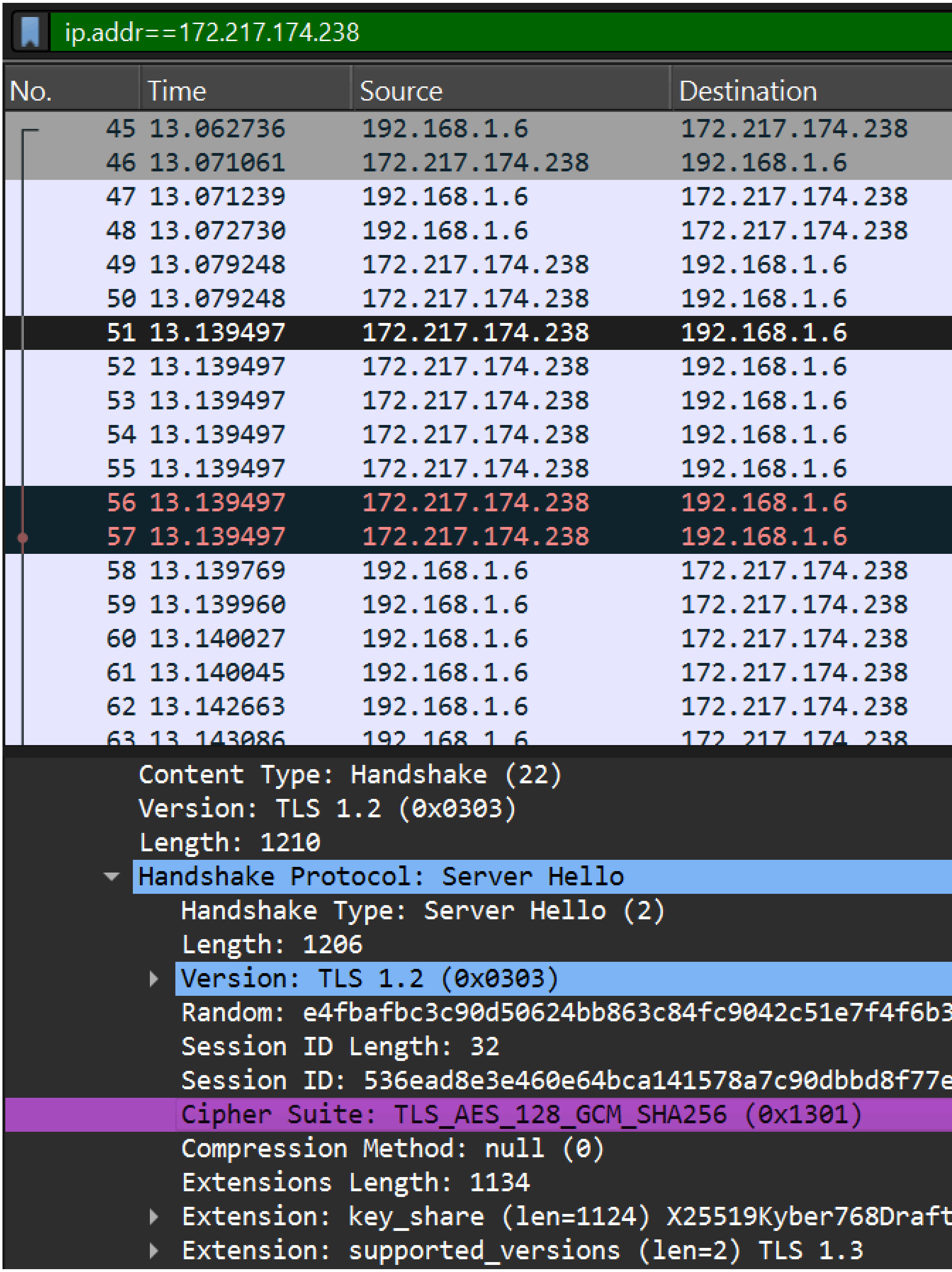


```
ip.addr==172.217.174.238

No.    Time        Source           Destination
    45 13.062736   192.168.1.6      172.217.174.238
    46 13.071061   172.217.174.238  192.168.1.6
    47 13.071239   192.168.1.6      172.217.174.238
    48 13.072730   192.168.1.6      172.217.174.238
    49 13.079248   172.217.174.238  192.168.1.6
    50 13.079248   172.217.174.238  192.168.1.6
    51 13.139497   172.217.174.238  192.168.1.6
    52 13.139497   172.217.174.238  192.168.1.6
    53 13.139497   172.217.174.238  192.168.1.6
    54 13.139497   172.217.174.238  192.168.1.6
    55 13.139497   172.217.174.238  192.168.1.6
    56 13.139497   172.217.174.238  192.168.1.6
    57 13.139497   172.217.174.238  192.168.1.6
    58 13.139769   192.168.1.6      172.217.174.238
    59 13.139960   192.168.1.6      172.217.174.238
    60 13.140027   192.168.1.6      172.217.174.238
    61 13.140045   192.168.1.6      172.217.174.238
    62 13.142663   192.168.1.6      172.217.174.238
    63 13.143086   192.168.1.6      172.217.174.238
```

```
      ▸ Cipher Suites (16 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 1702
      ▸ Extension: Reserved (GREASE) (len=0)
      ▸ Extension: extended_master_secret (len=0)
      ▸ Extension: ec_point_formats (len=2)
      ▸ Extension: supported_groups (len=12)
      ▸ Extension: application_settings (len=5)
      ▸ Extension: encrypted_client_hello (len=282)
      ▸ Extension: key_share (len=1263) X25519Kyber768Draft
      ▸ Extension: server_name (len=15) name=google.com
      ▸ Extension: application_layer_protocol_negotiation (
      ▸ Extension: signed_certificate_timestamp (len=0)
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: compress_certificate (len=3)
      ▸ Extension: status_request (len=5)
      ▸ Extension: signature_algorithms (len=18)
```

Which suit server used



```
ip.addr==172.217.174.238

No.   Time        Source            Destination
   45 13.062736   192.168.1.6       172.217.174.238
   46 13.071061   172.217.174.238   192.168.1.6
   47 13.071239   192.168.1.6       172.217.174.238
   48 13.072730   192.168.1.6       172.217.174.238
   49 13.079248   172.217.174.238   192.168.1.6
   50 13.079248   172.217.174.238   192.168.1.6
   51 13.139497   172.217.174.238   192.168.1.6
   52 13.139497   172.217.174.238   192.168.1.6
   53 13.139497   172.217.174.238   192.168.1.6
   54 13.139497   172.217.174.238   192.168.1.6
   55 13.139497   172.217.174.238   192.168.1.6
   56 13.139497   172.217.174.238   192.168.1.6
   57 13.139497   172.217.174.238   192.168.1.6
   58 13.139769   192.168.1.6       172.217.174.238
   59 13.139960   192.168.1.6       172.217.174.238
   60 13.140027   192.168.1.6       172.217.174.238
   61 13.140045   192.168.1.6       172.217.174.238
   62 13.142663   192.168.1.6       172.217.174.238
   63 13.143086   192.168.1.6       172.217.174.238
```

```
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1210
  ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 1206
      ▸ Version: TLS 1.2 (0x0303)
        Random: e4fbafbc3c90d50624bb863c84fc9042c51e7f4f6b3
        Session ID Length: 32
        Session ID: 536ead8e3e460e64bca141578a7c90dbbd8f77e
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 1134
      ▸ Extension: key_share (len=1124) X25519Kyber768Draft
      ▸ Extension: supported_versions (len=2) TLS 1.3
```

Encrypted data which the server sends can be viewed only using the Encryption key.

Location of the connection.

Edit -> preferences -> tick resolve ip address -> Apply.

Telenet

1) Sudo apt install telnetd
2) To check service active
   sudo systemctl status inetd

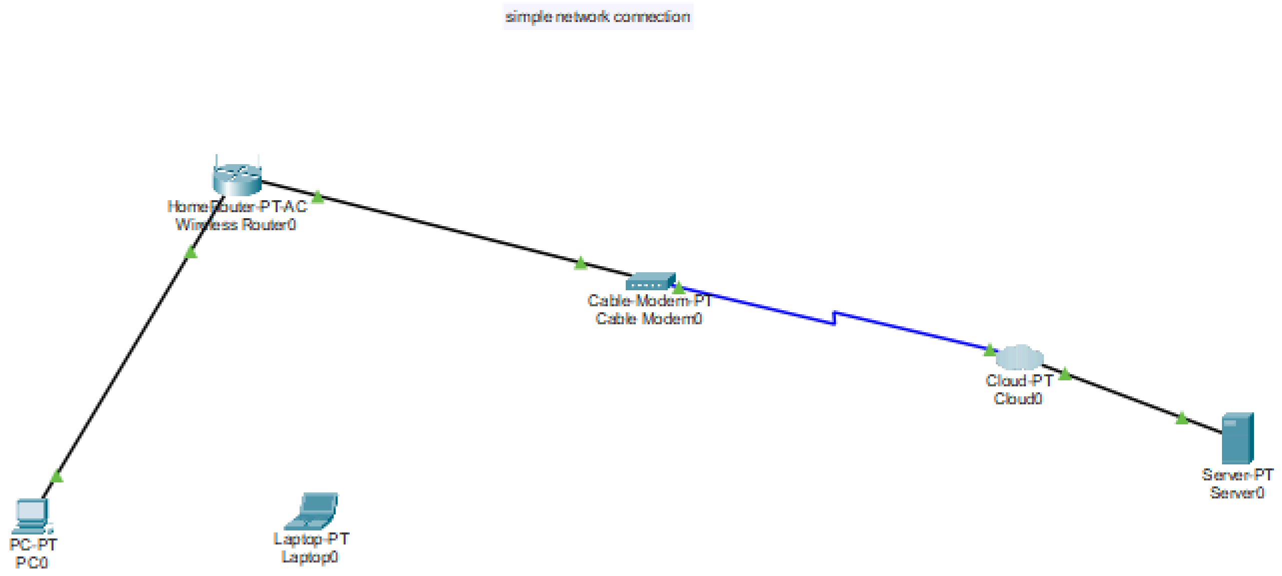
3) Sudo systemctl start inetd

4) Sudo ufw enable
5) Sudo ufw allow 23 (allowing port 23)
6) Sudo apt install net-tools
7) Telnet [ip address] [port number]

Sudo apt-get install xinetd telentd

Cisco packet tracker

1) Set all components

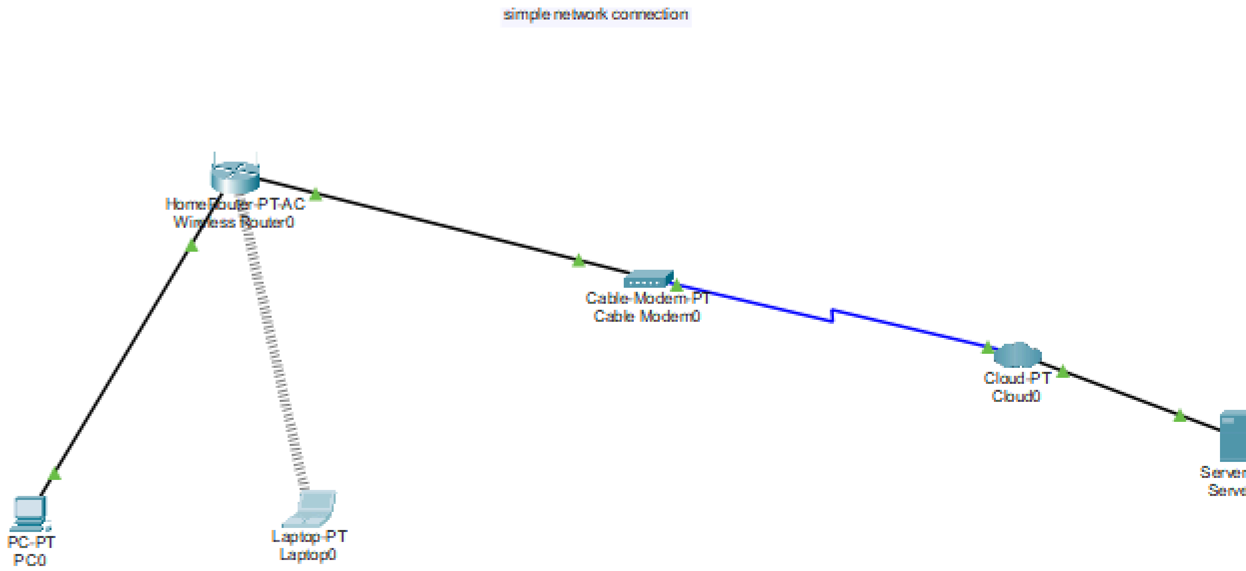


To wireless router

2) Network name ssid ->abbas -> save
3) Setup -> static dns 1-> 208.67.220.220 -> save

To laptop Add wpc300n module to laptop

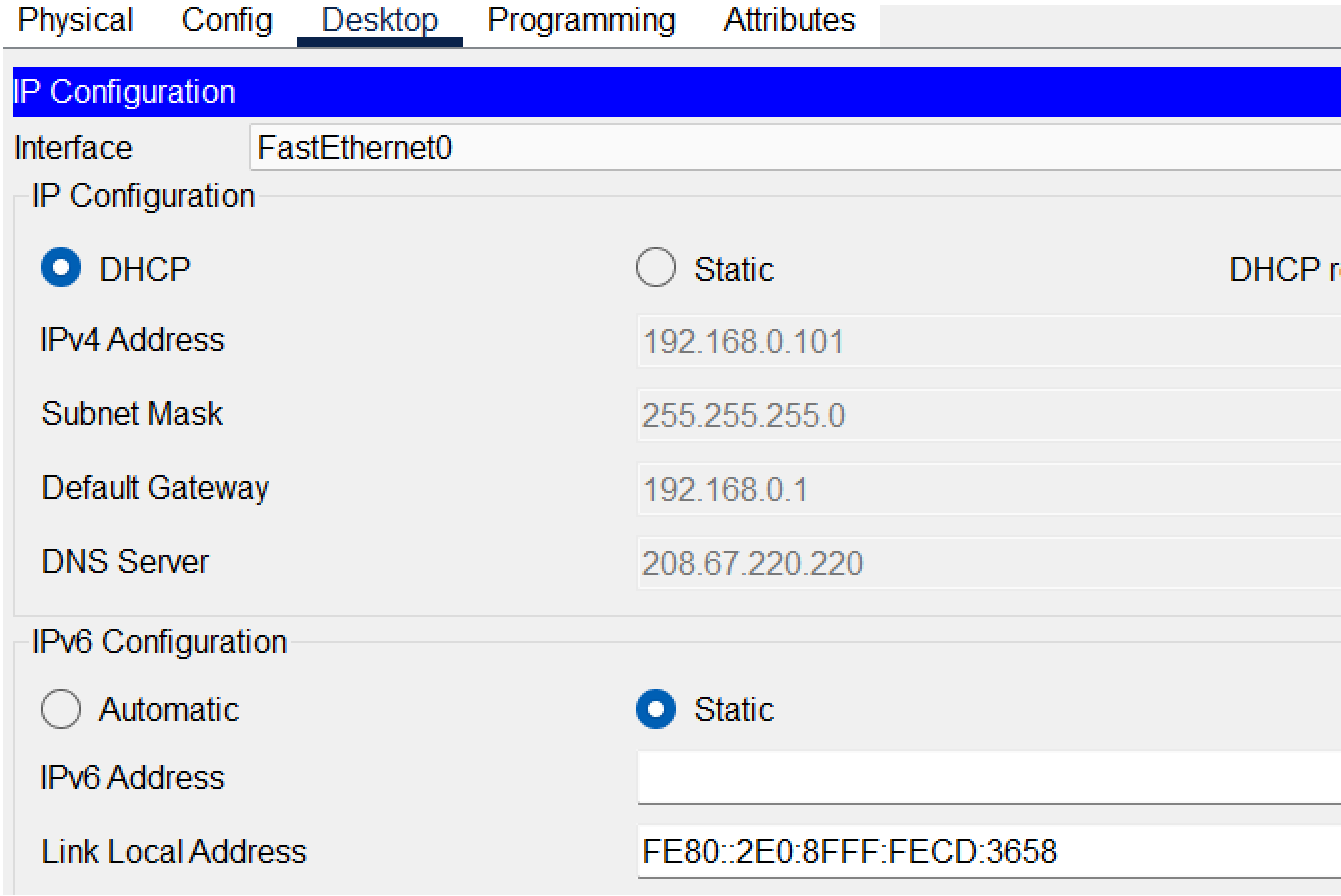
4) Power off
5) Remove the empty module from side of the laptop (in right to the power button)\
6) Add the wpc module over there
7) Turn on power



8) Desktop -> pc wireless -> connect-> wireless name - Abbas -> click - > connect

To pc

9) Desktop -> ip config -> select from static to DHCP



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static DHCP r

IPv4 Address 192.168.0.101

Subnet Mask 255.255.255.0

Default Gateway 192.168.0.1

DNS Server 208.67.220.220

IPv6 Configuration

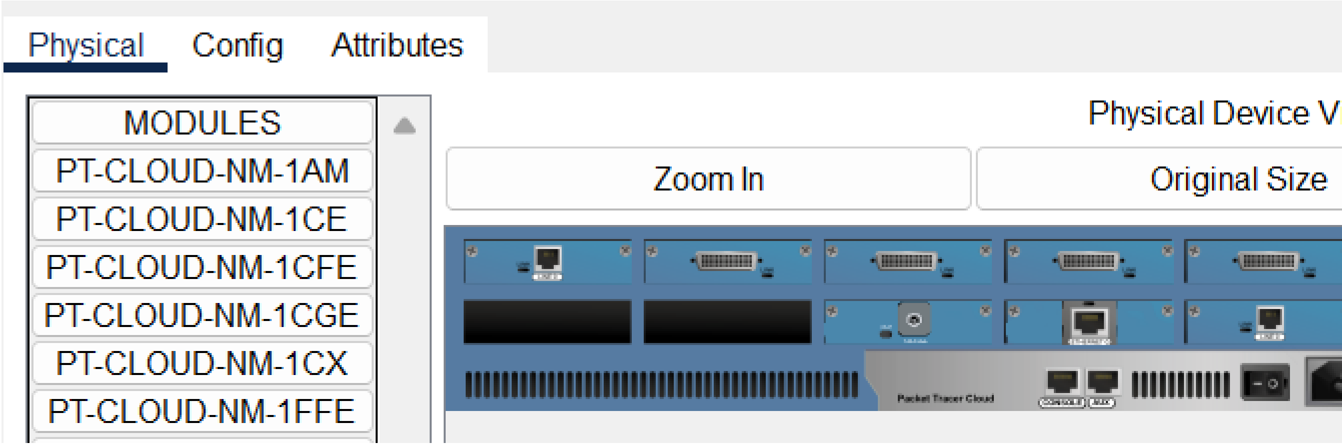
○ Automatic ● Static

IPv6 Address

Link Local Address FE80::2E0:8FFF:FECD:3658

To internet cloud

1) Power off
2) Make all port empty



3) And put pt-cloud - 1cx and pt cloud 1CFE
4) Power on
5) Config -> fast ethernet enable cable from DSl . then cable ->click ADD
6) Again make connection coaxial from clod to cable modem and copper straight from cloud to server

To server

1) Service -> DHCP -> Services -> On
2) Pool name DHCPPool
3) Default gateway and DNS Server add -208.67.220.220
4) Start ip add - 208.67.220.1
5) Subnet mask 255.255.255.0
6) Maximum users 50
7) Click add

8) Service -> DNS
9) DNS service -> ON
10) Name - Cisco.com, Address- 208.67.220.220 ->click add.

11) Config - > global settings - > default gateway -208.67.220.1
12) DNS server -208.67.220.220
13) Fast ethernet 0 port status -> ON
14) Ipv4 add -> 208.67.220.220
15) Subnet mask -> 255.255.255.0

To pc

Cmd -> ipconfig /release

Ipconfig /renew

Ping Cisco.com

Send packet from pc to laptop in simulation mode.
Then from pc to cisco server

NMAP

1) Sudo apt-get install nmap
2) Nmap www.geeksforgeeks.com
3) nmap -v geeksforgeeks.org
4) nmap 103.76.228.* for entire subnet
5) sudo nmap -sA 103.76.228.244
   Detecting firewall settings can be useful during penetration testing and vulnerability scans. To detect it we use “-sA” option. This will provide you with information about the firewall being active on the host. It uses an ACK scan to receive the information.

6) sudo nmap -sL 172.217.174.238
   We use “sL” option to find hostnames for the given host by completing a DNS query for each one.

7) Nmap -h for getting all commands in nmap.

8) Nmap -sS www.google.com - can be accessed by root privileges.
   Here -sS flag is used for TCP SYN Scan, Which is a stealthy and efficient method of scanning for open ports on a target system.

9) Nmap -sU www.google.com - **.** The “-sU” flag is used with nmap to perform a UDP scan, which allows the user to discover open UDP ports and services on a target system.

10) nmap -sn www.geeksforgeeks.com
    The “-sn” flag is used with nmap to perform a ping scan, which sends ICMP requests to a target host or network to determine hosts is up or not.

11) The “-p” flag is used with nmap to perform scan on a specific port or range of ports. (In our case it will scan port 80,443 and 21)
    nmap -p 80 443 21 <Domain Name>

12) nmap -p 1-80 <Domain Name> - to get from a range of ports

13) Here -A indicates aggressive, it will give us extra information, like OS detection (-O), version detection, script scanning (-sC), and traceroute (–traceroute). It even provides a lot of valuable information about the host.

nmap -A <Domain Name>

14)Nmap --trace out google.com-root access

Exp 2

1) ping google.com (Used to test the reachability of a host and measure the round-trip time for messages sent from the originating host to a destination computer.)
2) traceroute google.com (Traces the route that packets take to a network host.)
3) nslookup google.com (Queries Internet domain name servers to find IP addresses associated with a domain name.)
    - The **nbstat** command is specific to the Windows operating system and is used for troubleshooting NetBIOS name resolution.
    - In Linux, the equivalent command for troubleshooting network issues and name resolution is **nslookup**, which stands for **Name Server Lookup**. It serves as a network administration tool used to query the **Domain Name System (DNS)** for obtaining domain name-to-IP address mappings or other specific DNS records, making it valuable for troubleshooting DNS-related issues.
    -
4) netstat -tuln (Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.)
    - To list all tcp ports netstat -at
    - Udp - netstat -au
    - Listening ports -l (tcp -lt, udp - lu)
    - Static prots -s (“ “ “ “ “)
5) Ipconfig - is used for displaying details of our network configuration and refreshing the DNS and DHCP settings. The ipconfig command by default shows our IP address, default gateway, and subnet mask but we can get several details using this command with correct parameters.
6) Hostname - A hostname is a name given to a computer and attached to the network. Its main purpose is to uniquely identify over a network.

7) arp -a (Displays and modifies the IP-to-Physical address translation tables used by the Address Resolution Protocol (ARP))

```
 arp -a
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s3
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s3
```

The `arp -a` command shows the ARP (Address Resolution Protocol) cache on your system, listing IP addresses and their corresponding MAC addresses, which are associated with the network interface.

Here's what each part means:

- `?` - Placeholder for the hostname (if not resolved).
- `(10.0.2.3)` and `(10.0.2.2)` - IP addresses on your local network.
- `52:55:0a:00:02:03` and `52:55:0a:00:02:02` - MAC addresses associated with those IP addresses.
- `[ether]` - Type of physical layer, here indicating Ethernet.

8) rarp -a (Reverse Address Resolution Protocol, used to request an IP address from a gateway server based on the MAC address. Often replaced by DHCP.)

9) `Pingpath google.com`

`pingpath` combines functionality similar to both `ping` and `traceroute`. It attempts to ping a remote host while also identifying the path (network route) the packets take to reach the target. Essentially, it provides both reachability and routing information,

ip add show (To show IP addresses:)
ip route show (To display routing table:)
ifconfig (Configures network interfaces.)
ifconfig eth0 up
dig google.com (DNS lookup utility, provides more detailed information than `nslookup`.)
route -n (To display the routing table:)