**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

1. sudo systemctl restart vsftpd
2. Sudo ufw allow ftp
3. sudo useradd -m testuser
4. sudo passwd testuser (Abbas@110)
5. hostname
6. 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

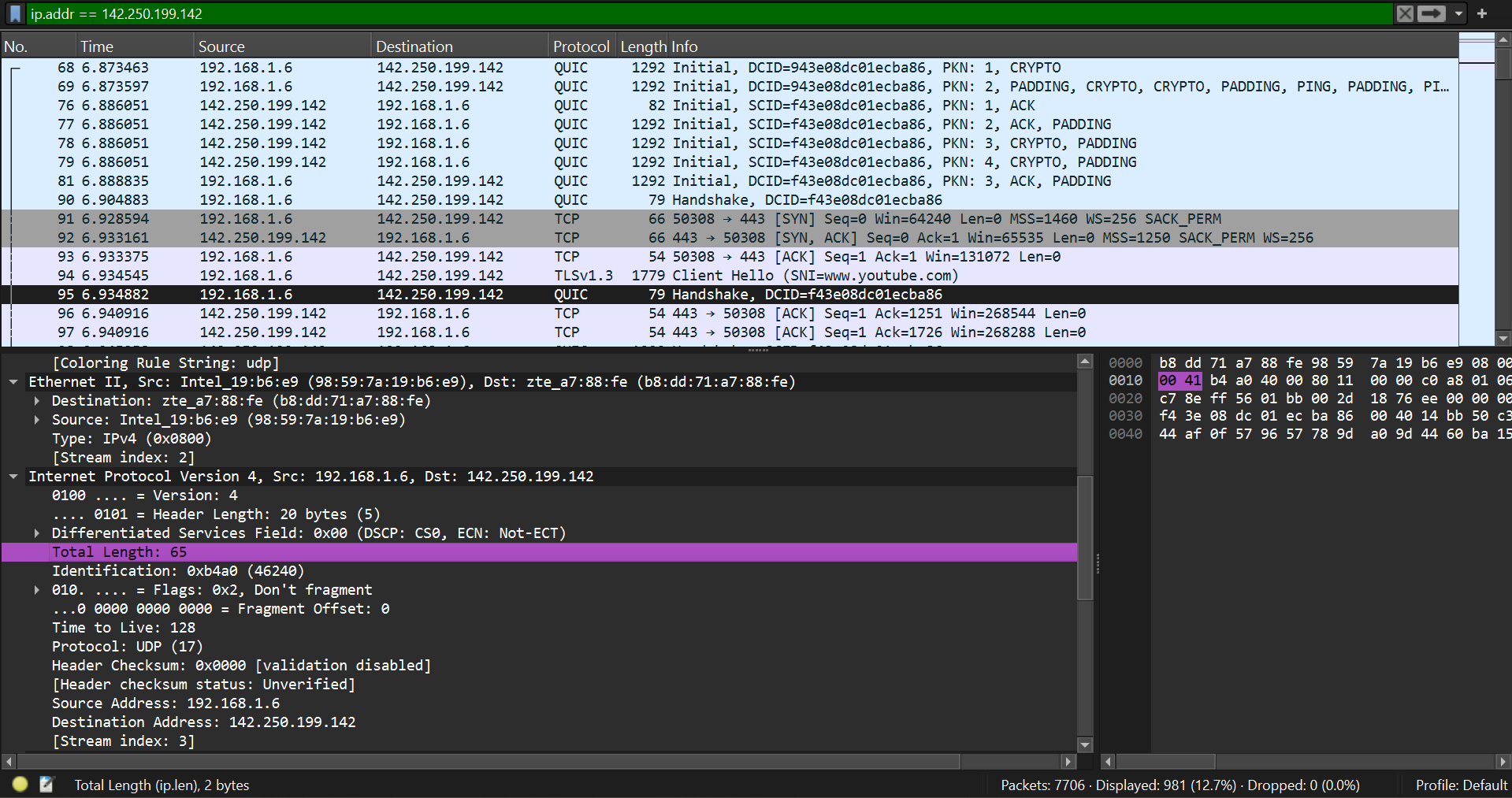
Mkdir -make directory

Rmdir -remove directory.

**Wire shark:**

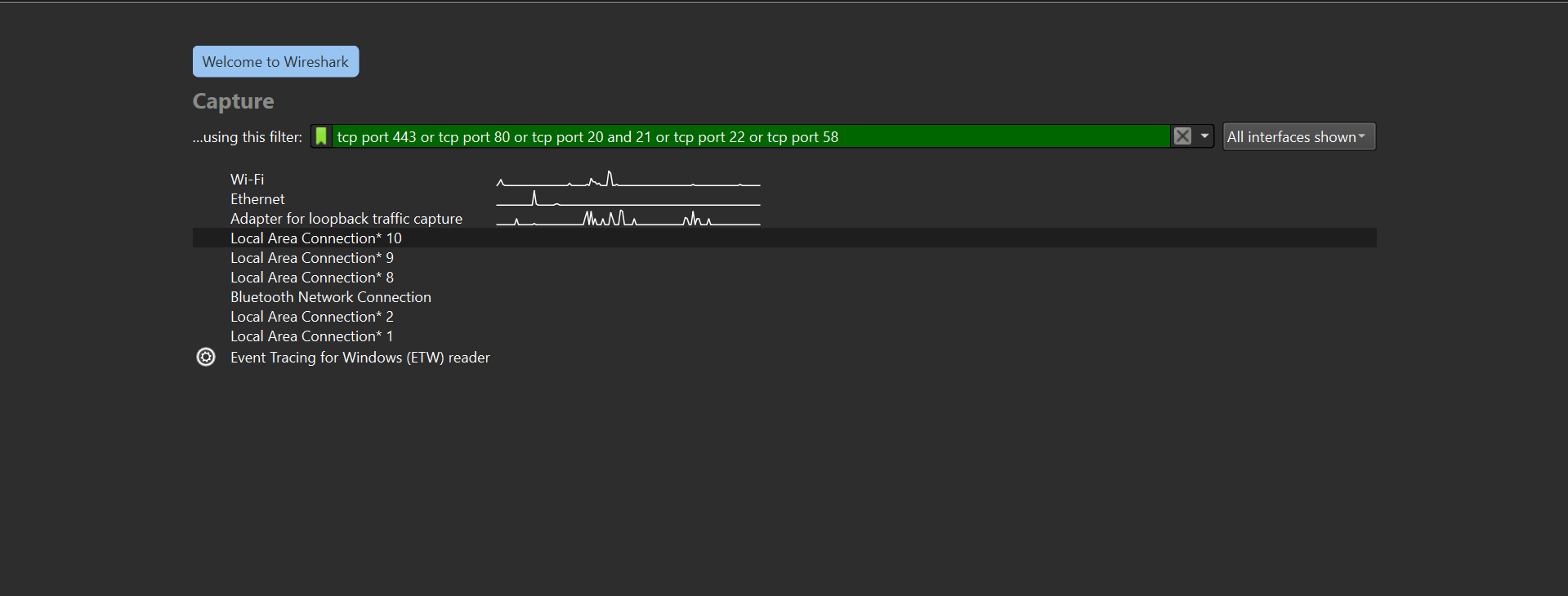
Filters:

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.



1. (Not secure website) tcp contains ‘username”
2. Capture filter (capture packets based only on certain filter).

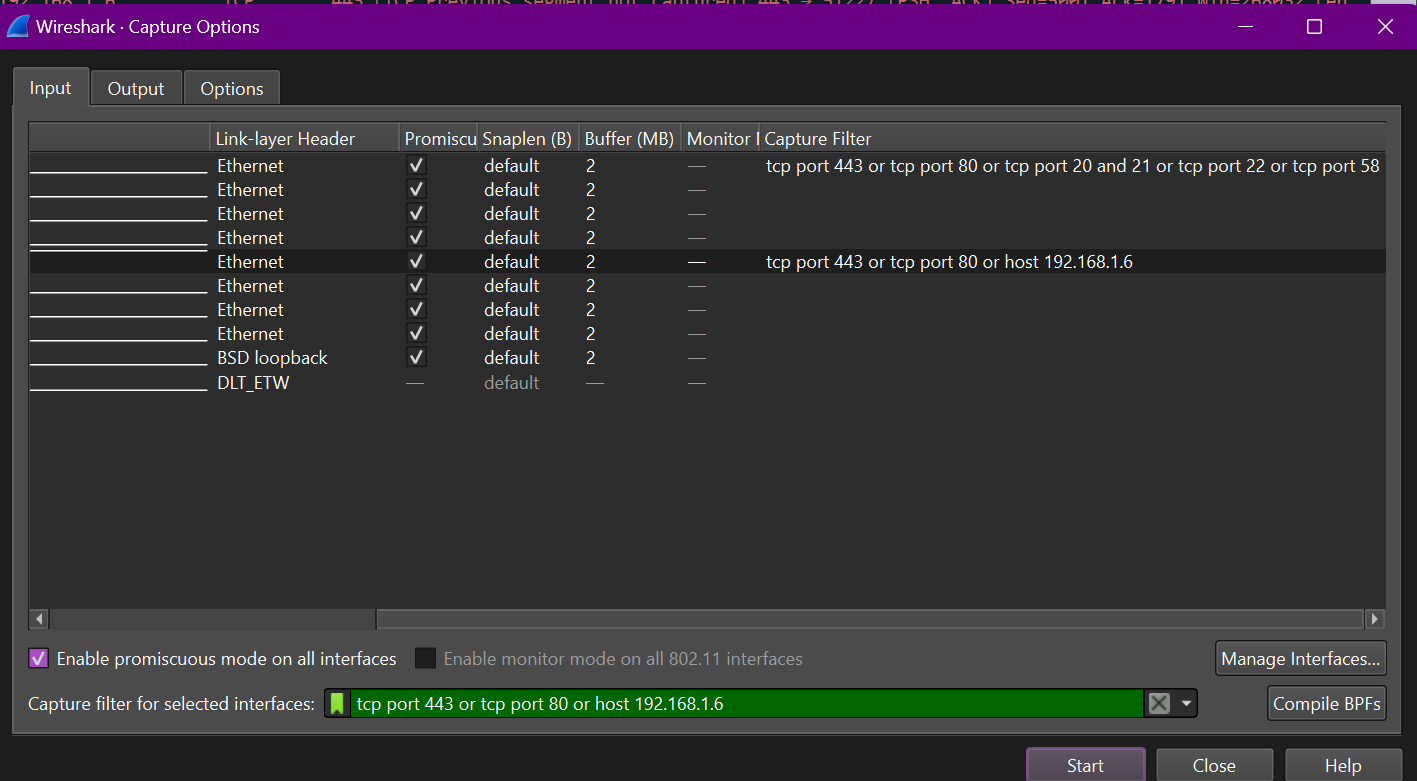
Tcp port 443 or tcp port 80



1. Capture

-> options

Can add more capture filters.

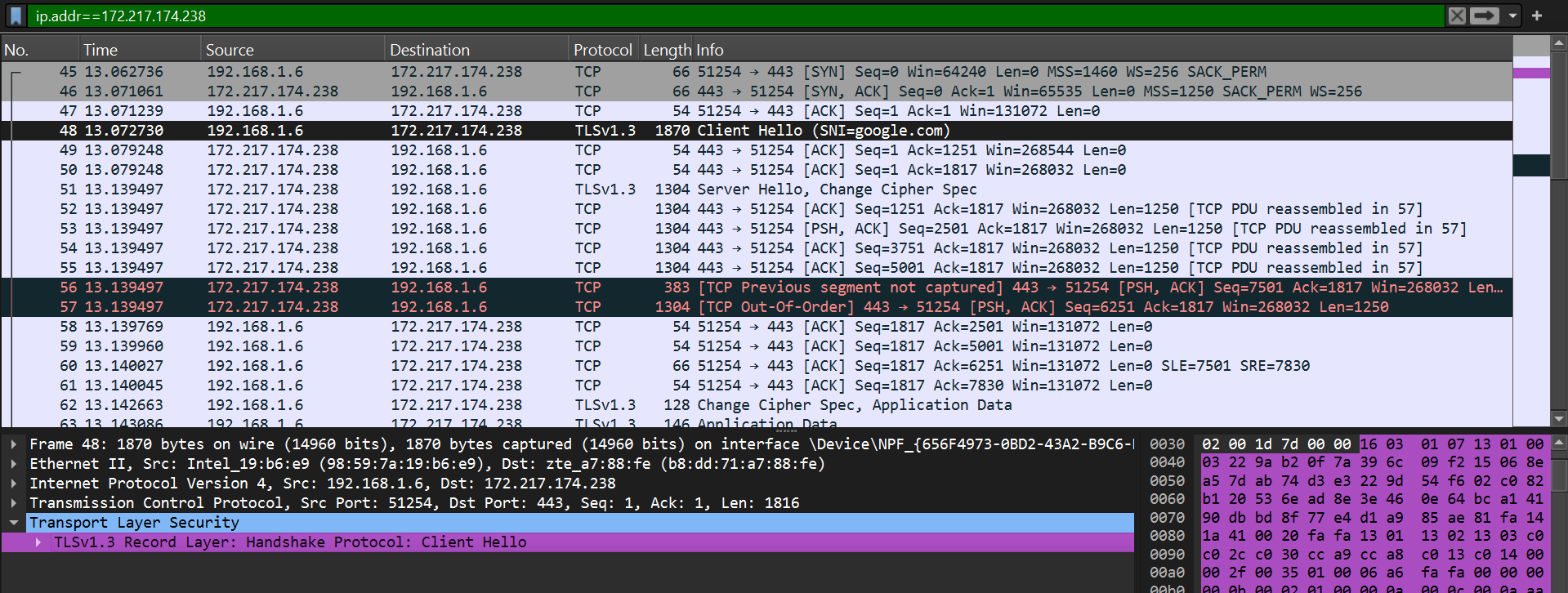
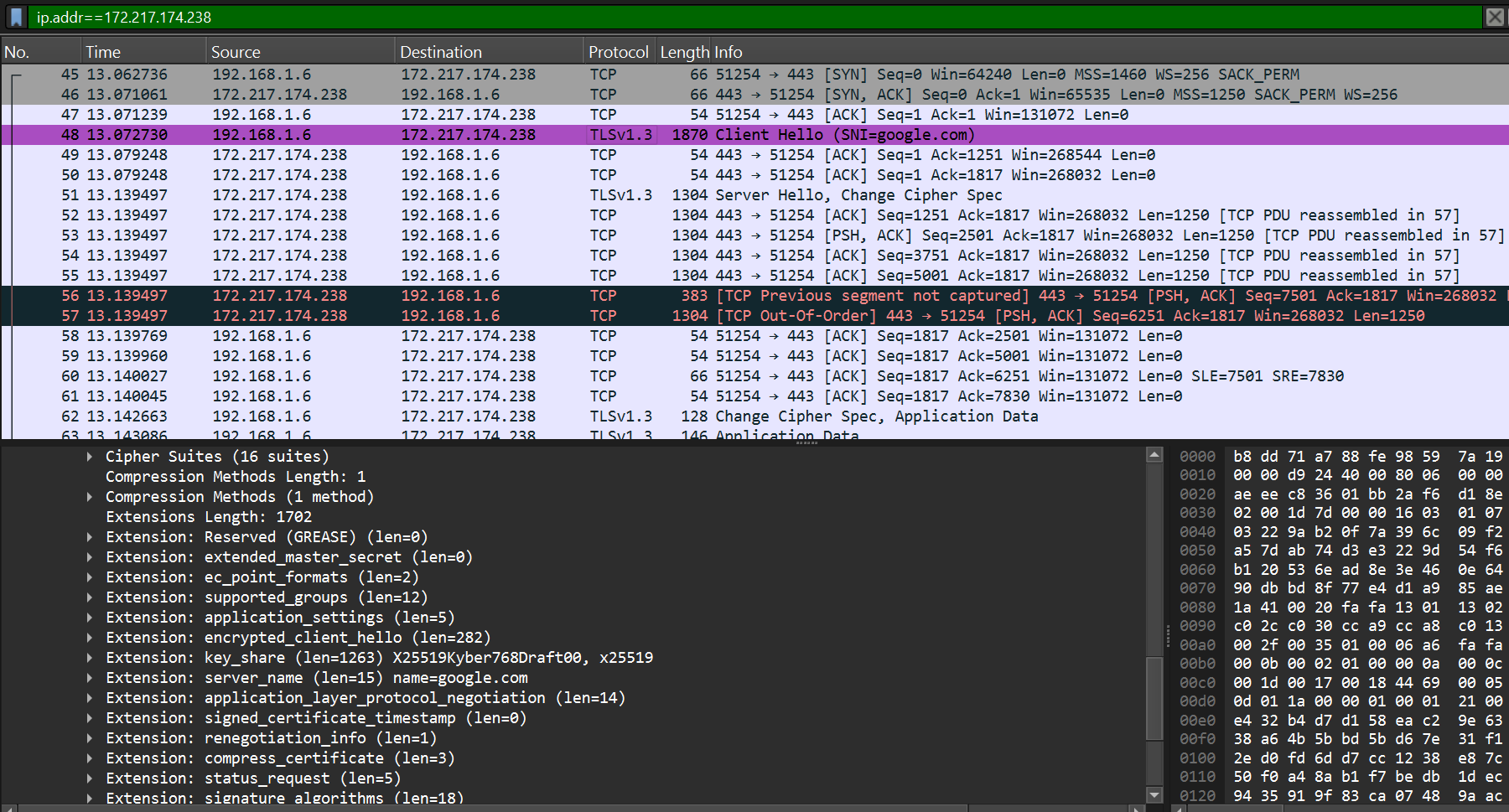


***Handshake***

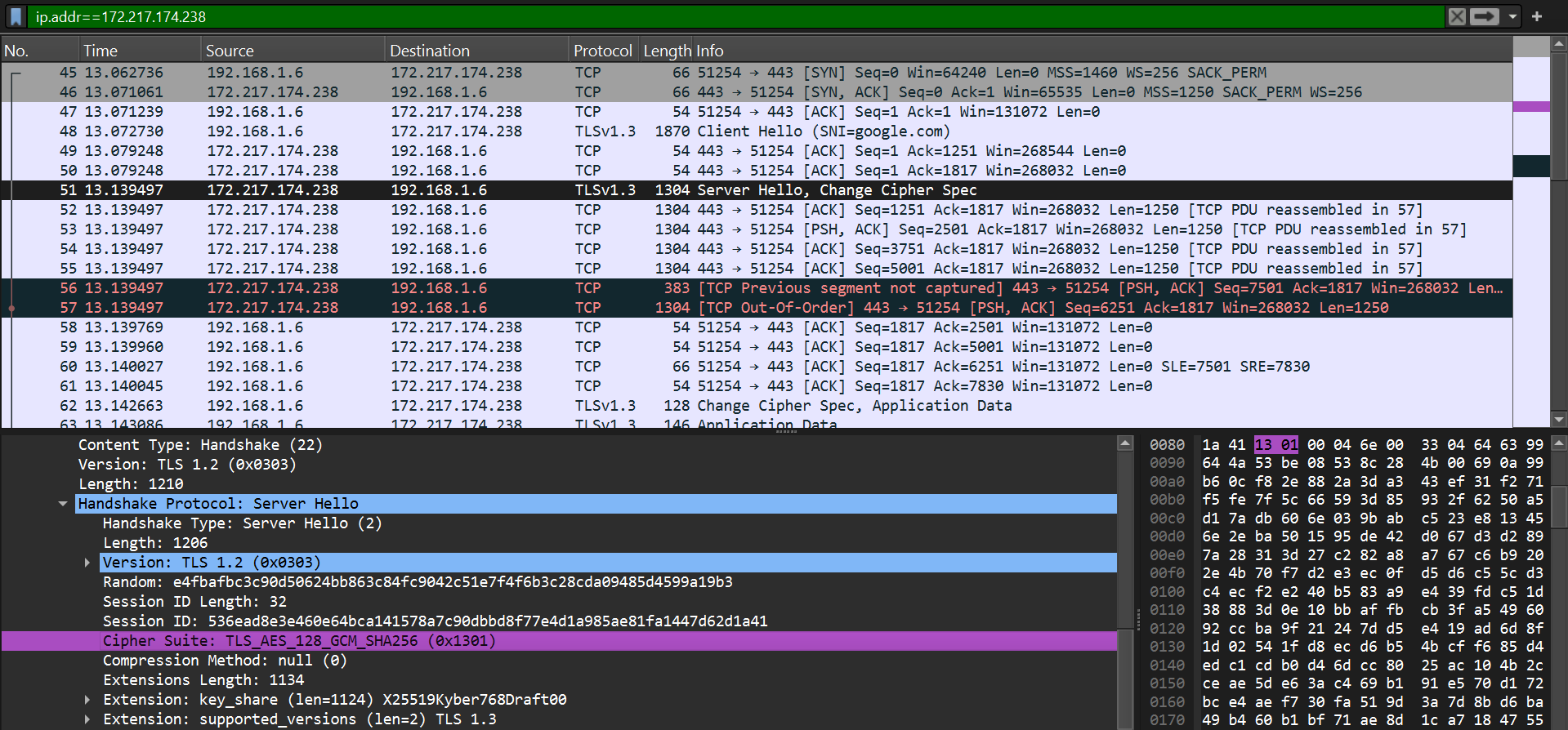
Start capture

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****

Which suit server used



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

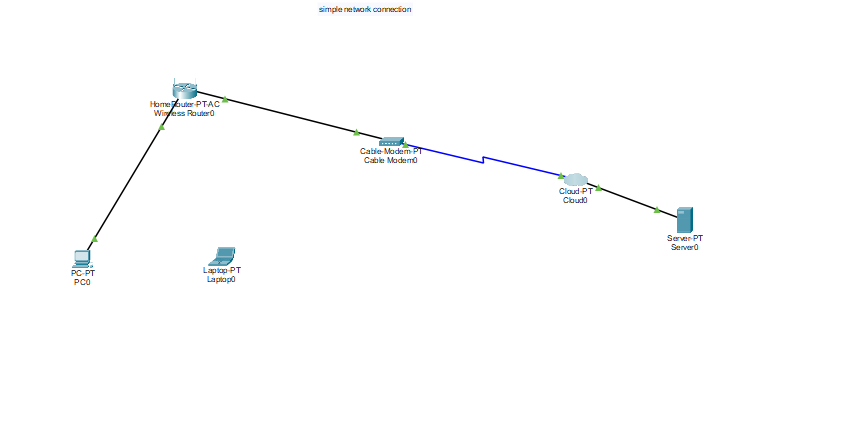
sudo systemctl status inetd

1. Sudo systemctl start inetd
2. Sudo ufw enable
3. Sudo ufw allow 23 (allowing port 23)
4. Sudo apt install net-tools
5. Telnet [ip address] [port number]

Sudo apt-get install xinetd telentd

**Cisco packet tracker**

1. Set all components

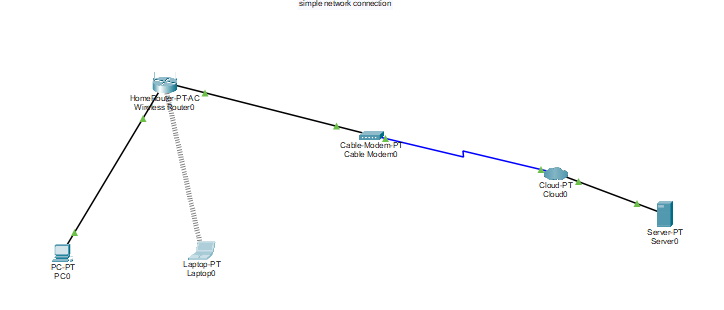


To wireless router

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

To laptop Add wpc300n module to laptop

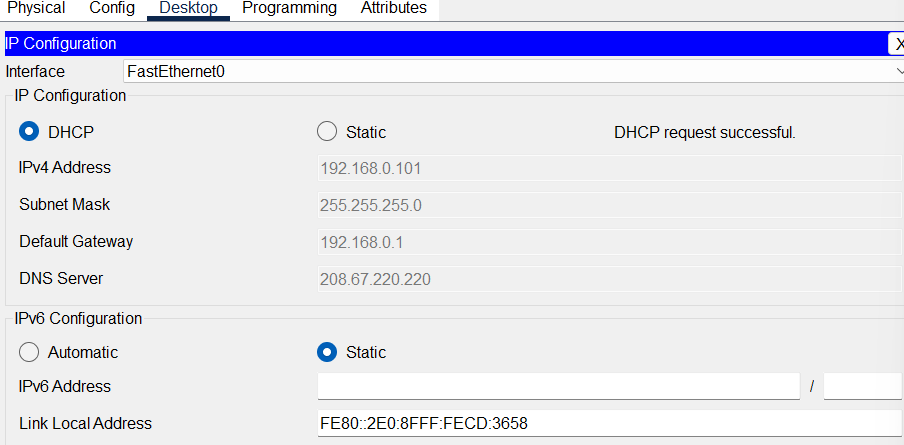
1. Power off
2. Remove the empty module from side of the laptop (in right to the power button)\
3. Add the wpc module over there
4. Turn on power



1. Desktop -> pc wireless -> connect-> wireless name - Abbas -> click - > connect

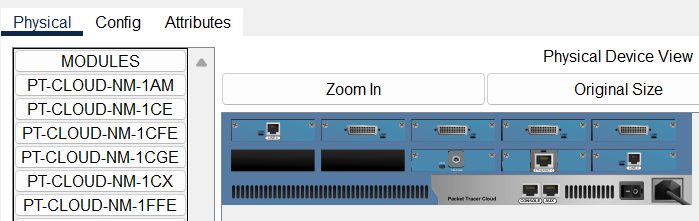
To pc

1. Desktop -> ip config -> select from static to DHCP



To internet cloud

1. Power off
2. Make all port empty



1. And put pt-cloud - 1cx and pt cloud 1CFE
2. Power on
3. Config -> fast ethernet enable cable from DSl . then cable ->click ADD
4. 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](http://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.

1. 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.

1. Nmap -h for getting all commands in nmap.
2. Nmap -sS [www.google.com](http://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.

1. Nmap -sU [www.google.com](http://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.
2. 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.

1. 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>

1. nmap -p 1-80 <Domain Name> - to get from a range of ports
2. 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>

1. 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.

1. 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 (“ “ “ “ “ )

1. 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.
2. 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.
3. 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.

1. 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.)
2. 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:)