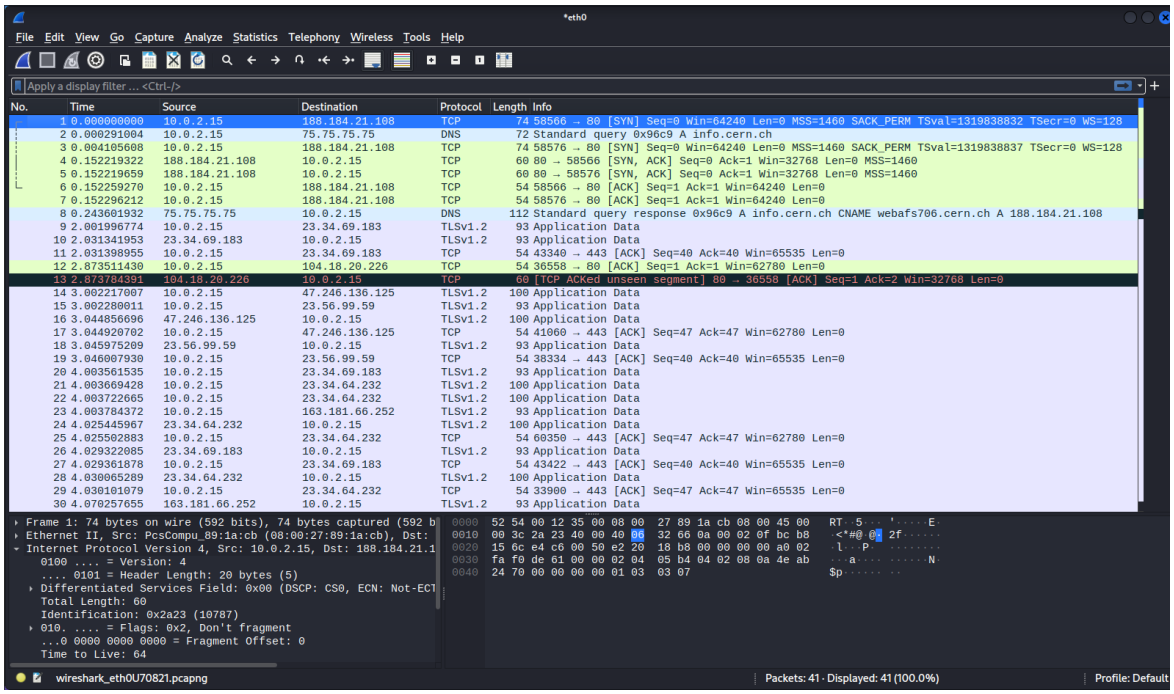
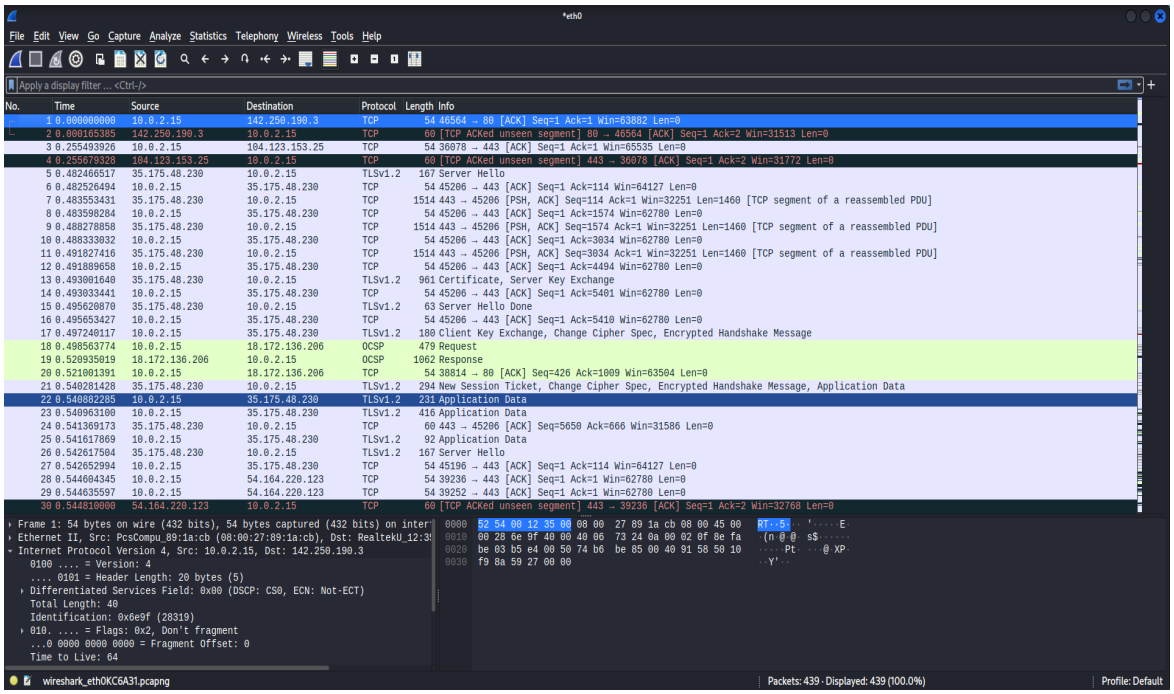
CAPTURING NETWORKS USING WIRESHARK

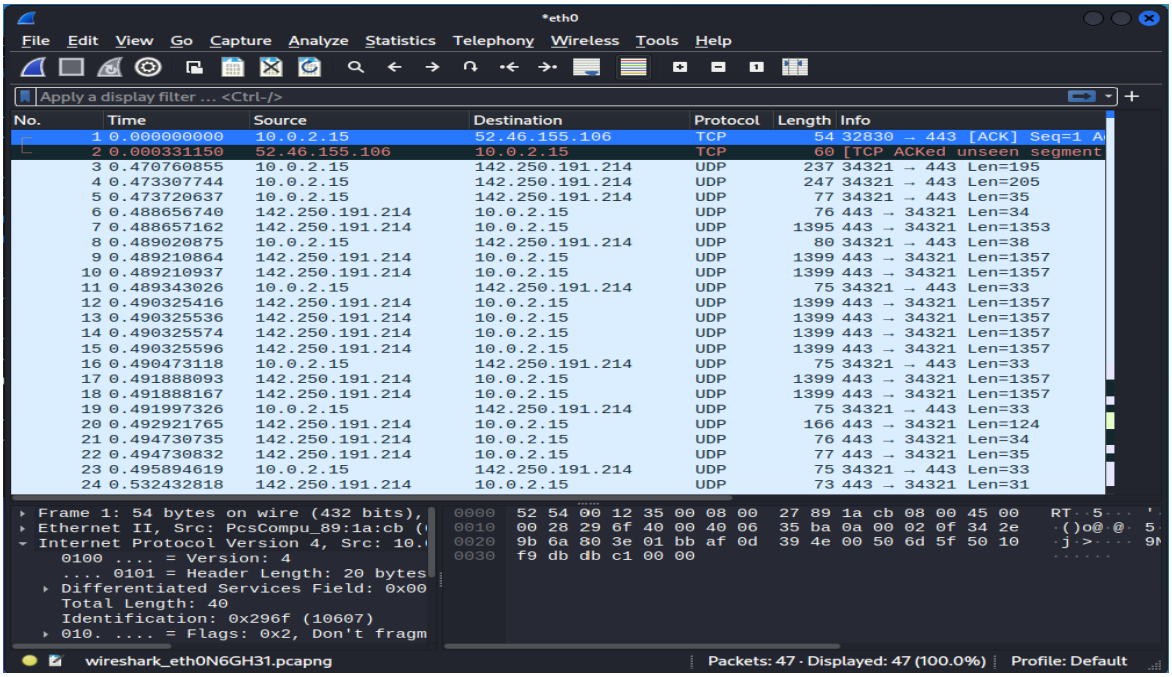
1. Capturing packets from HTTP protocols.
   Website: **http://info.cern.ch/**



2. Capturing packets from HTTPS protocols.
   Website: https://www.amazon.com/



3. **Capturing packets from youtube video.**
   Website: https://youtu.be/dQw4w9WgXcQ



CAPTURING PACKETS USING NMAP

1. **Scanning youtube video with Nmap**

- **First convert the youtube domain name address into an IP address using the provided resource.**

2. **Scanning the IP address using Nmap**

```
┌──(andrews㉿Andydorsty)-[~/Downloads]
└─$ sudo su
[sudo] password for andrews:
┌──(root㉿Andydorsty)-[/home/andrews/Downloads]
└─# nmap -sS -n 142.250.81.238 --top-ports 10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:12 CDT
Nmap scan report for 142.250.81.238
Host is up (0.012s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
```

3. **Performing TCP and UDP scan on IP address**

```
File  Actions  Edit  View  Help
└─# nmap -sS -sU 142.250.81.238 --top-ports 20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:20 CDT
Nmap scan report for lga25s74-in-f14.1e100.net (142.250.81.238)
Host is up (0.013s latency).

PORT      STATE         SERVICE
21/tcp    filtered      ftp
22/tcp    filtered      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   open          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
53/udp    open|filtered domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
123/udp   open|filtered ntp
135/udp   open|filtered msrpc
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   open|filtered snmp
162/udp   open|filtered snmptrap
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
514/udp   open|filtered syslog
520/udp   open|filtered route
631/udp   open|filtered ipp
1434/udp  open|filtered ms-sql-m
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
49152/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds

┌──(root㉿Andydorsty)-[/home/andrews/Downloads]
└─#
```

4. **Scanning HTTP website with Nmap**

Website: http://info.cern.ch/