

CAPTURING NETWORKS USING WIRESHARK

1. Capturing packets from HTTP protocols.

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

The screenshot shows a Wireshark capture of network traffic on the interface eth0. The display filter is set to 'Apply a display filter ... <Ctrl-F>'. The packet list shows 41 packets. The selected packet (No. 1) is a DNS query from 10.0.2.15 to 188.184.21.108. The packet details pane shows the following information:

- Frame 1: 74 bytes on wire (592 bits): 74 bytes captured (592 bits) on interface eth0
- Ethernet II, Src: PcsCompu, 08:00:27:89:1a:cb, Dst: 08:00:27:89:1a:cb
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 188.184.21.108
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0x2a23 (10787)
- Flags: 0x2, Don't fragment
- Fragment Offset: 0
- Time to Live: 64

The packet bytes pane shows the raw data of the DNS query.

2. Capturing packets from HTTPS protocols.

Website: <https://www.amazon.com/>

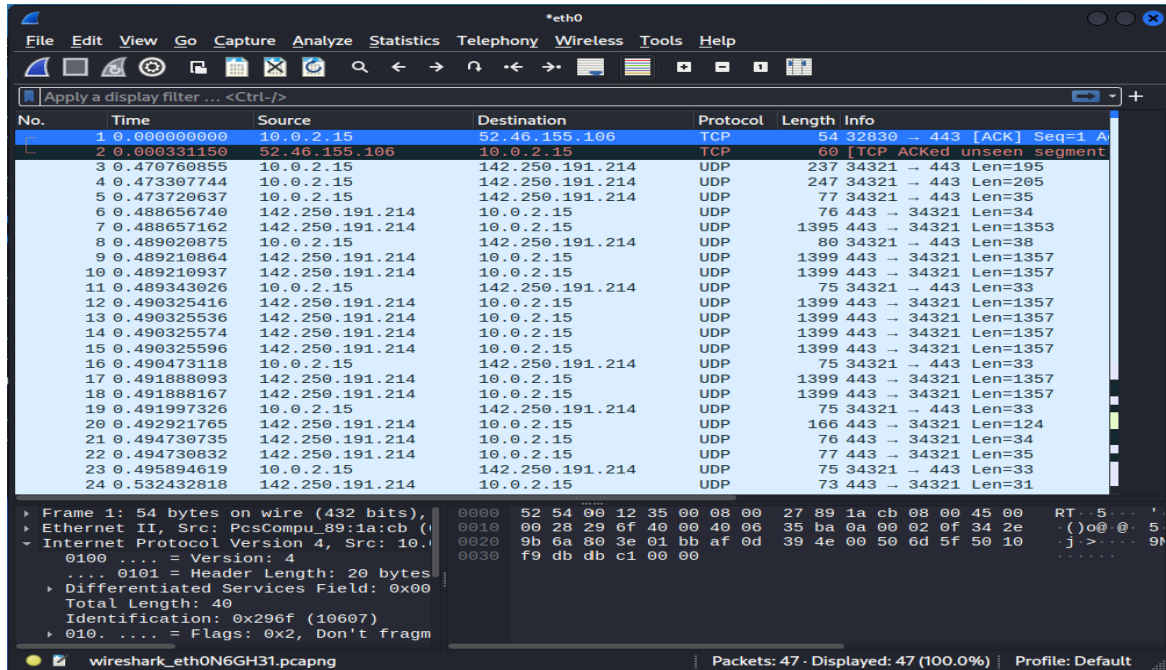
The screenshot shows a Wireshark capture of network traffic on the interface eth0. The display filter is set to 'Apply a display filter ... <Ctrl-F>'. The packet list shows 439 packets. The selected packet (No. 1) is a TCP segment from 10.0.2.15 to 142.250.190.3. The packet details pane shows the following information:

- Frame 1: 54 bytes on wire (432 bits): 54 bytes captured (432 bits) on interface eth0
- Ethernet II, Src: PcsCompu, 08:00:27:89:1a:cb, Dst: RealtekU, 08:00:27:89:1a:cb
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.190.3
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 40
- Identification: 0x6e9f (28319)
- Flags: 0x2, Don't fragment
- Fragment Offset: 0
- Time to Live: 64

The packet bytes pane shows the raw data of the TCP segment.

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.

Your Results:

www.youtube.com > 142.250.81.238

<https://www.youtube.com/watch?v=dQw4w9WgXcQ>

Convert

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 dhcpc
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-like
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/>

```
File Actions Edit View Help
└─$ sudo su
[sudo] password for andrews:
[root@Andydorsty]~# nmap -ss -sU 142.250.81.238 --top-ports 20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:32 CDT
Nmap scan report for lga25s74-in-f14.1e100.net (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
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 dhcp
68/udp    open|filtered dhcp
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 4.39 seconds
```