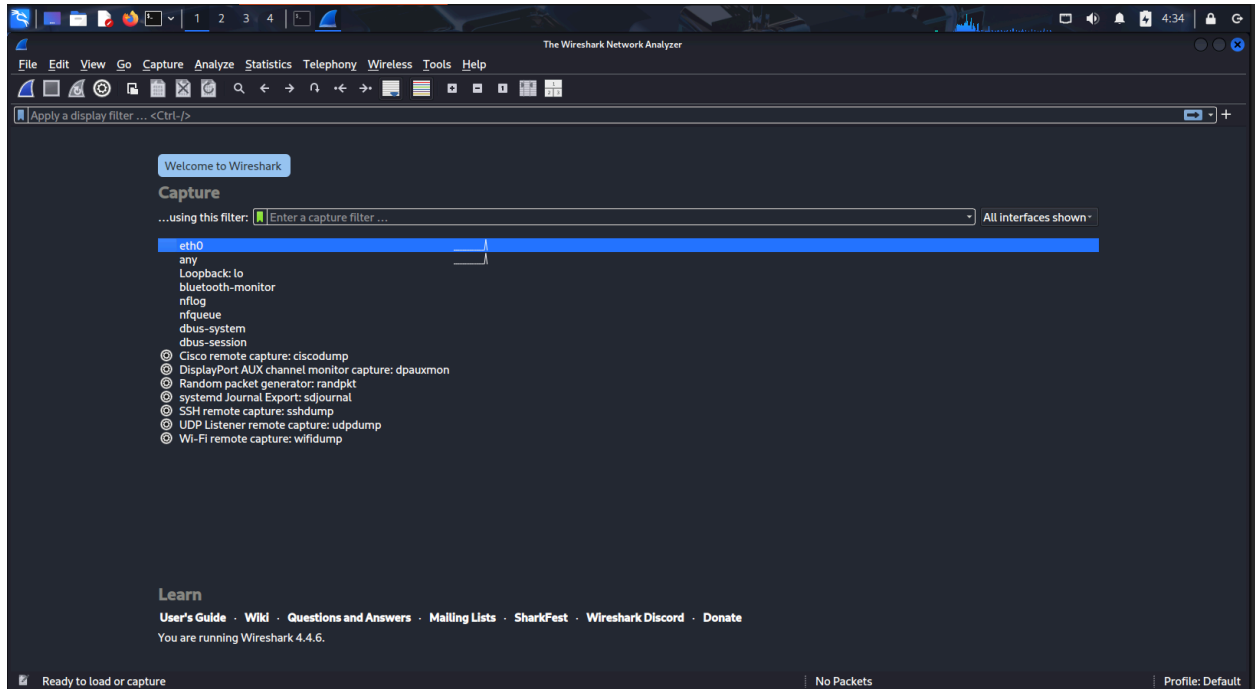


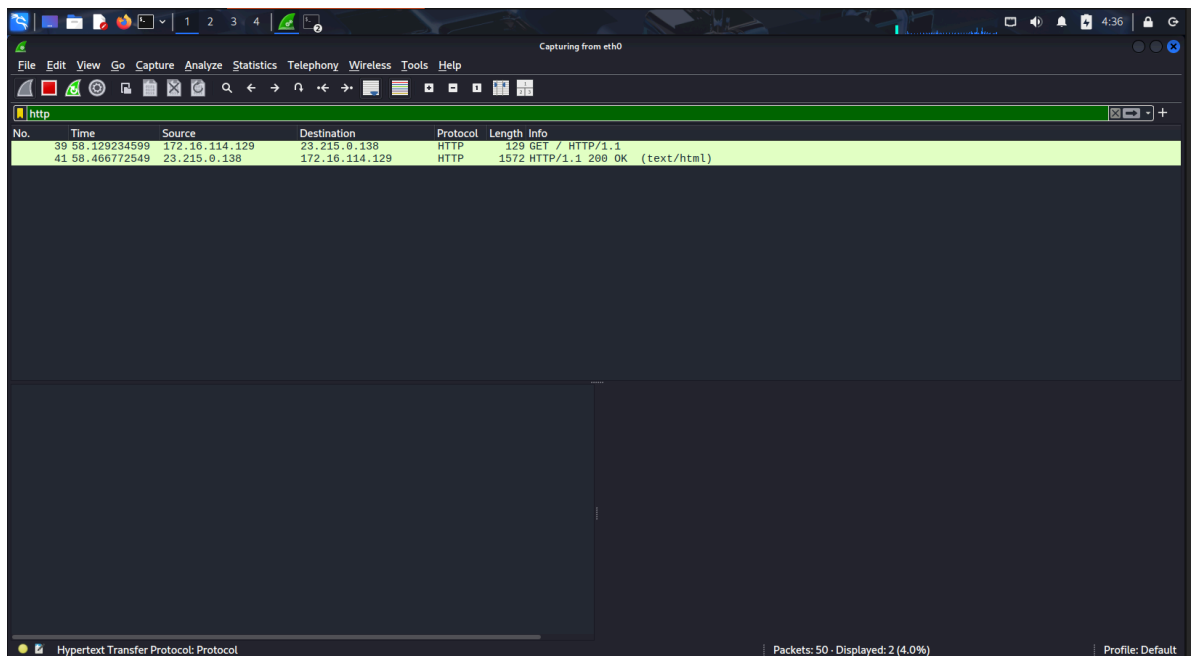
# OSI Layer Packet Simulation using Wireshark

## 1. wireshark &



## 2. curl <http://example.com>

Wireshark filter: http



3. Terminal 1: nc -lvp 5555  
Terminal 2: nc 127.0.0.1 5555  
Wireshark filter: tcp.port == 5555

The image shows a Wireshark network traffic capture. The top bar indicates 'Capturing from eth0'. The main display area shows a list of captured packets, with the 'tcp' filter applied. The packet list shows a series of TCP segments, including a SYN packet (No. 28) and several retransmissions. A red packet (No. 35) is highlighted, showing a RST, ACK segment. Below the packet list, the packet details pane shows the selected packet (No. 74) as a TCP segment. The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
28	49.765551156	172.16.114.129	96.7.128.198	TCP	74	47676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1921692234 TSecr=0 WS=128
29	50.769212309	172.16.114.129	96.7.128.198	TCP	74	[TCP Retransmission] 47676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1921693238 TSecr=0 WS=128
30	51.793229984	172.16.114.129	96.7.128.198	TCP	74	[TCP Retransmission] 47676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1921694262 TSecr=0 WS=128
31	52.817202763	172.16.114.129	96.7.128.198	TCP	74	[TCP Retransmission] 47676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1921695286 TSecr=0 WS=128
32	53.841350122	172.16.114.129	96.7.128.198	TCP	74	[TCP Retransmission] 47676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1921696310 TSecr=0 WS=128
33	54.865355157	172.16.114.129	96.7.128.198	TCP	74	[TCP Retransmission] 47676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1921697334 TSecr=0 WS=128
34	56.881259469	172.16.114.129	96.7.128.198	TCP	74	[TCP Retransmission] 47676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1921699350 TSecr=0 WS=128
35	57.793766172	96.7.128.198	172.16.114.129	TCP	60	80 → 47676 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
36	57.794351353	172.16.114.129	23.215.0.138	TCP	74	33954 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3442208422 TSecr=0 WS=128
37	58.128719650	23.215.0.138	172.16.114.129	TCP	60	80 → 33954 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
38	58.128813229	172.16.114.129	23.215.0.138	TCP	54	33954 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
39	58.129234599	172.16.114.129	23.215.0.138	HTTP	129	GET / HTTP/1.1
40	58.129616599	23.215.0.138	172.16.114.129	TCP	60	80 → 33954 [ACK] Seq=1 Ack=76 Win=64240 Len=0
41	58.466772549	23.215.0.138	172.16.114.129	HTTP	1572	HTTP/1.1 200 OK (text/html)
42	58.466907801	172.16.114.129	23.215.0.138	TCP	54	33954 → 80 [ACK] Seq=76 Ack=1519 Win=62722 Len=0
43	58.467704377	172.16.114.129	23.215.0.138	TCP	54	33954 → 80 [FIN, ACK] Seq=76 Ack=1519 Win=62722 Len=0
44	58.468103115	23.215.0.138	172.16.114.129	TCP	60	80 → 33954 [ACK] Seq=1519 Ack=77 Win=64239 Len=0
45	58.792754574	23.215.0.138	172.16.114.129	TCP	60	80 → 33954 [FIN, PSH, ACK] Seq=1519 Ack=77 Win=64239 Len=0
46	58.792794122	172.16.114.129	23.215.0.138	TCP	54	33954 → 80 [ACK] Seq=77 Ack=1520 Win=62722 Len=0

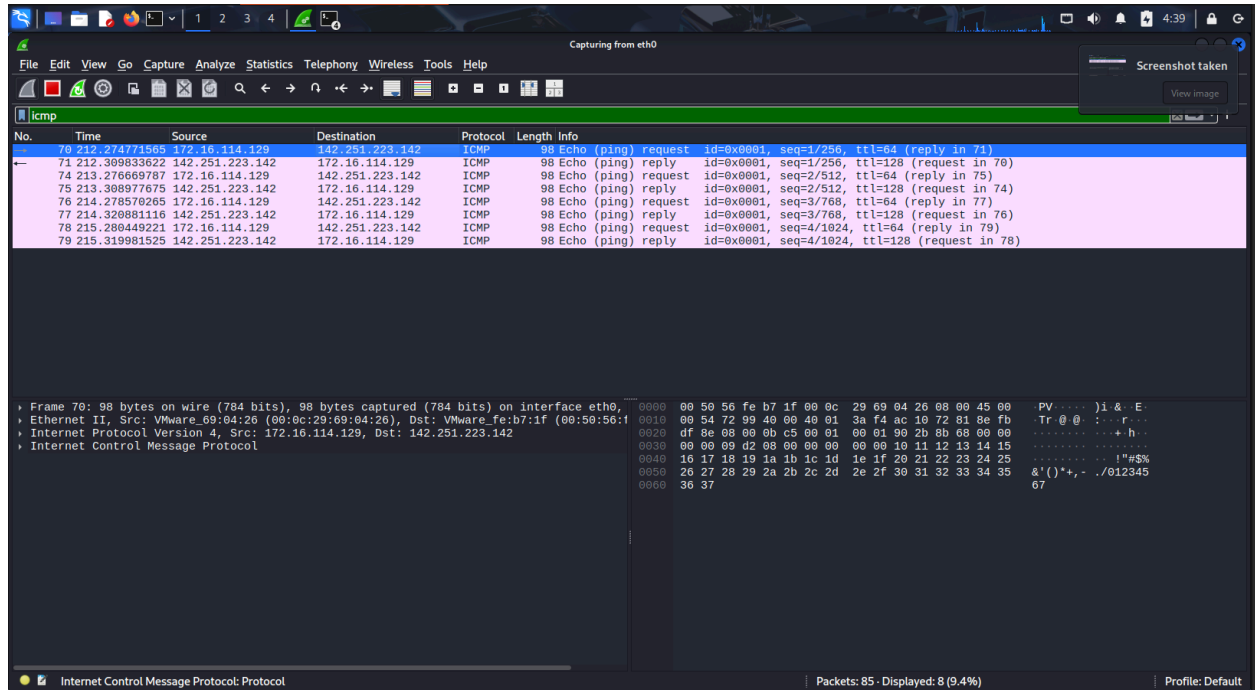
Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, Jumbo Frames  
Ethernet II, Src: VMware\_69:04:26 (00:0c:29:69:04:26), Dst: VMware\_fe:b7:1f (00:50:56:00:00:00)  
Internet Protocol Version 4, Src: 172.16.114.129, Dst: 96.7.128.175  
Transmission Control Protocol, Src Port: 60678, Dst Port: 80, Seq: 0, Len: 0

Transmission Control Protocol: Protocol

Packets: 59 · Displayed: 34 (57.6%)

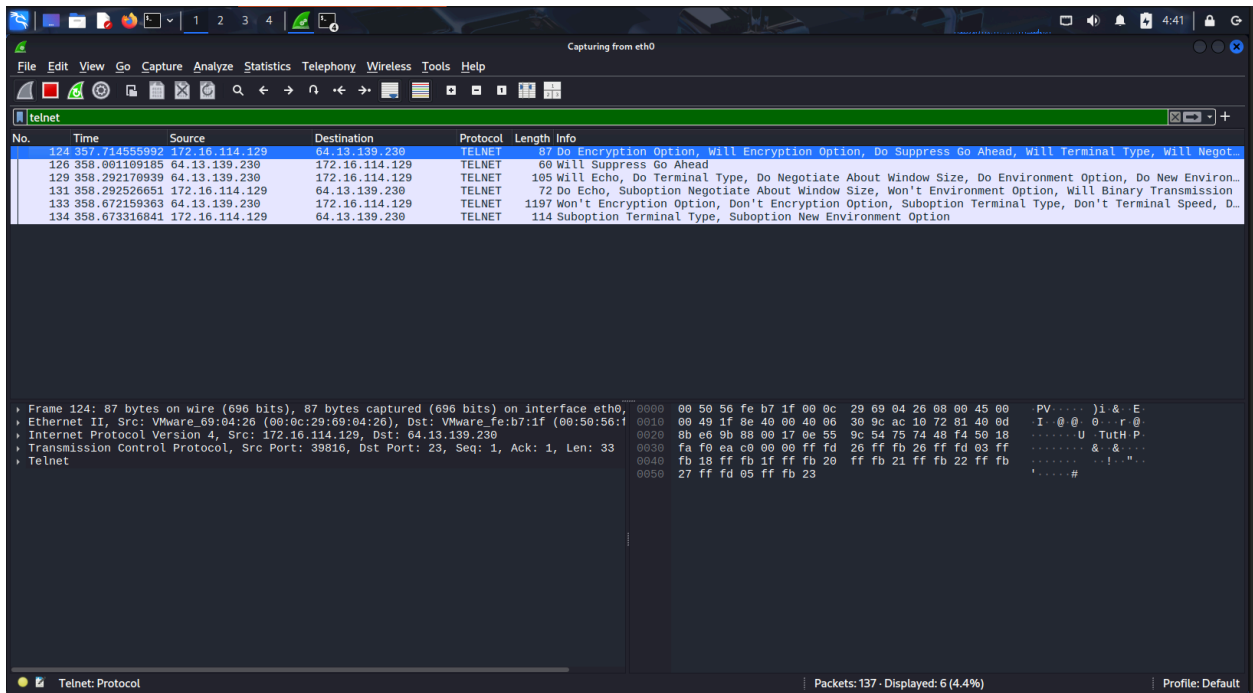
Profile: Default

4. ping -c 4 google.com  
Wireshark filter: icmp

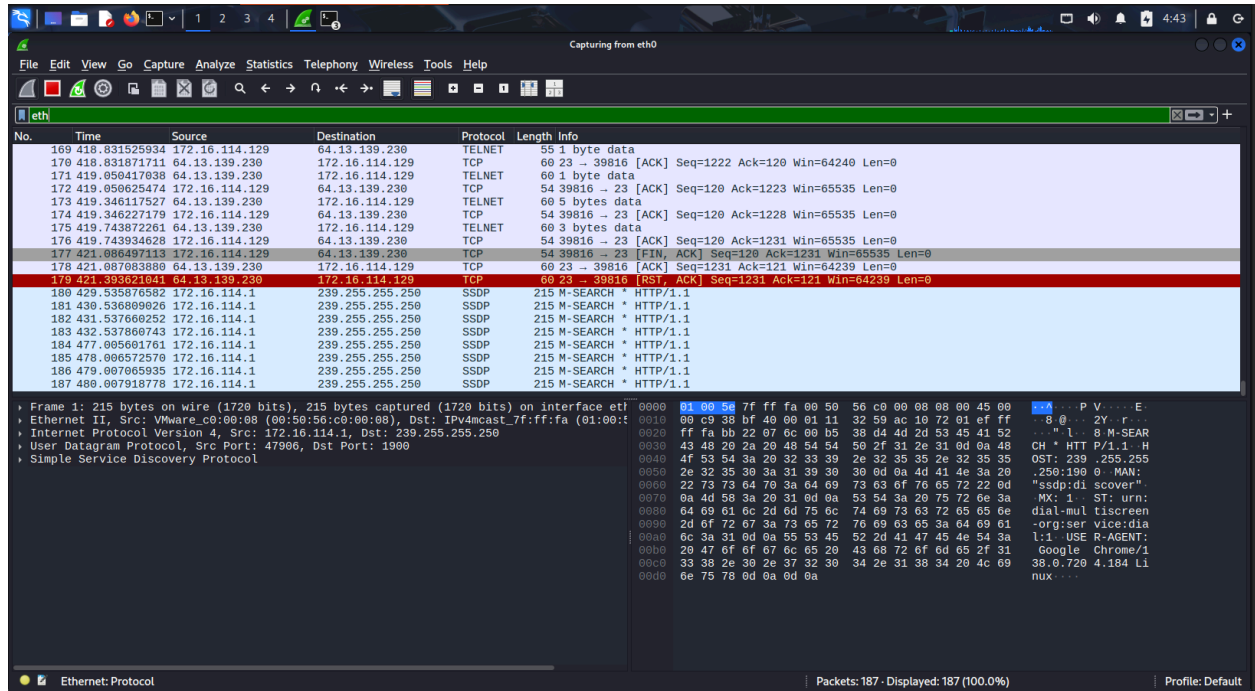


## 5. telnet towel.blinkenlights.nl

Wireshark filter: telnet



```
wireshark filter: eth.addr == aa:bb:cc:dd:ee:ff
```



7. curl https://testphp.vulnweb.com  
Wireshark filter: tls

