

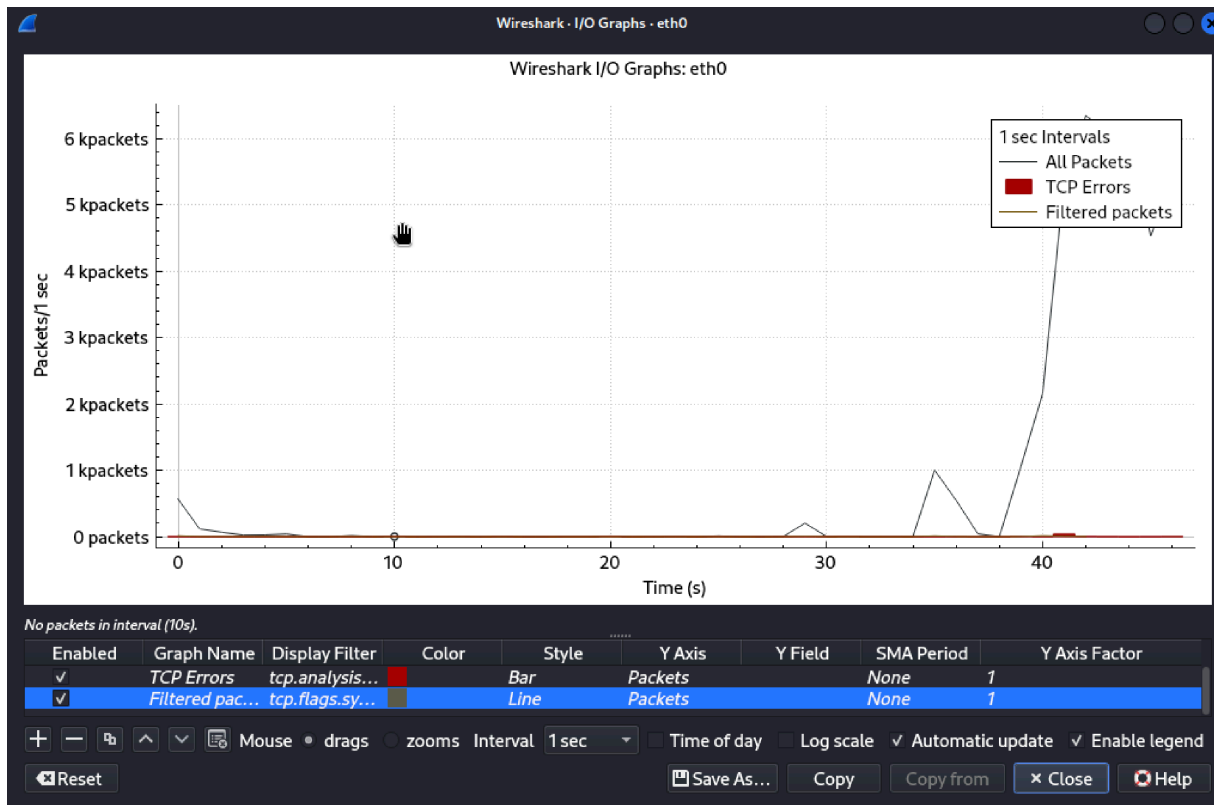
Wireshark packet capture window showing ICMP traffic. The packet list displays several ICMP Destination unreachable (Port unreachable) messages from 192.168.64.2 to 104.18.80.204. The packet details pane shows the structure of the selected packet (Frame 19279).

No.	Time	Source	Destination	Protocol	Length	Info
19279	43.277137528	192.168.64.2	104.18.80.204	ICMP	561	Destination unreachable (Port unreachable)
19280	43.277161189	192.168.64.2	104.18.80.204	ICMP	105	Destination unreachable (Port unreachable)
22103	43.736598821	192.168.64.2	104.18.80.204	ICMP	561	Destination unreachable (Port unreachable)
22104	43.736603696	192.168.64.2	104.18.80.204	ICMP	105	Destination unreachable (Port unreachable)
27801	44.662037684	192.168.64.2	104.18.80.204	ICMP	561	Destination unreachable (Port unreachable)
27802	44.662044142	192.168.64.2	104.18.80.204	ICMP	105	Destination unreachable (Port unreachable)
37796	46.516463889	192.168.64.2	104.18.80.204	ICMP	561	Destination unreachable (Port unreachable)
37798	46.516470972	192.168.64.2	104.18.80.204	ICMP	105	Destination unreachable (Port unreachable)

Frame 19279: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bytes) on interface eth0  
Ethernet II, Src: ce:06:10:c5:6e:b0 (ce:06:10:c5:6e:b0), Dst: 12:bd:00:00:00:00  
Internet Protocol Version 4, Src: 192.168.64.2, Dst: 104.18.80.204  
Internet Control Message Protocol

Internet Control Message Protocol: Protocol

Packets: 39914 · Displayed: 8 (0.0%) · Dropped: 0 (0.0%) · Profile: Default



Wireshark capture of TCP traffic on interface \*eth0. The display filter is `tcp.flags.syn==1 and tcp.flags.ack==0`. The packet list shows several SYN packets from 192.168.64.2 to 142.250.206.3. The packet details pane shows the selected packet (No. 34) with its Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (SYN) layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Wireshark capture of HTTP traffic on interface \*eth0. The display filter is `http`. The packet list shows several HTTP requests and responses. The packet details pane shows the selected packet (No. 38) with its Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol (GET /success.txt?ip=192.168.64.2) layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Wireshark capture of DNS traffic on interface \*eth0. The display filter is `Apply a display filter ... <Ctrl-/>`. The packet list shows several DNS queries and responses. The packet details pane shows the selected packet (No. 1) with its Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (DNS query) layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.