



PRATICAL FILE

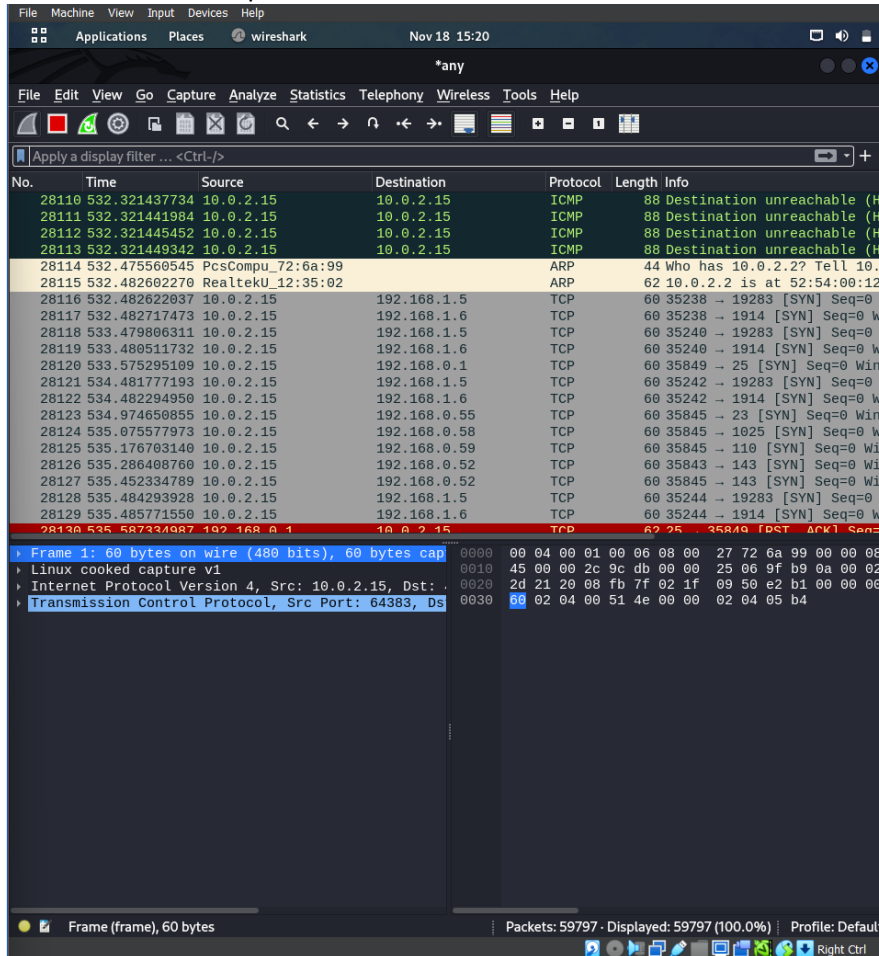
Dr. Gopal Singh Rawat
Course- Physical IT & Sec

Dhairya Jain
500105432 | R2142220251
B.Tech_CSE_CSF_B-1_Sem-III

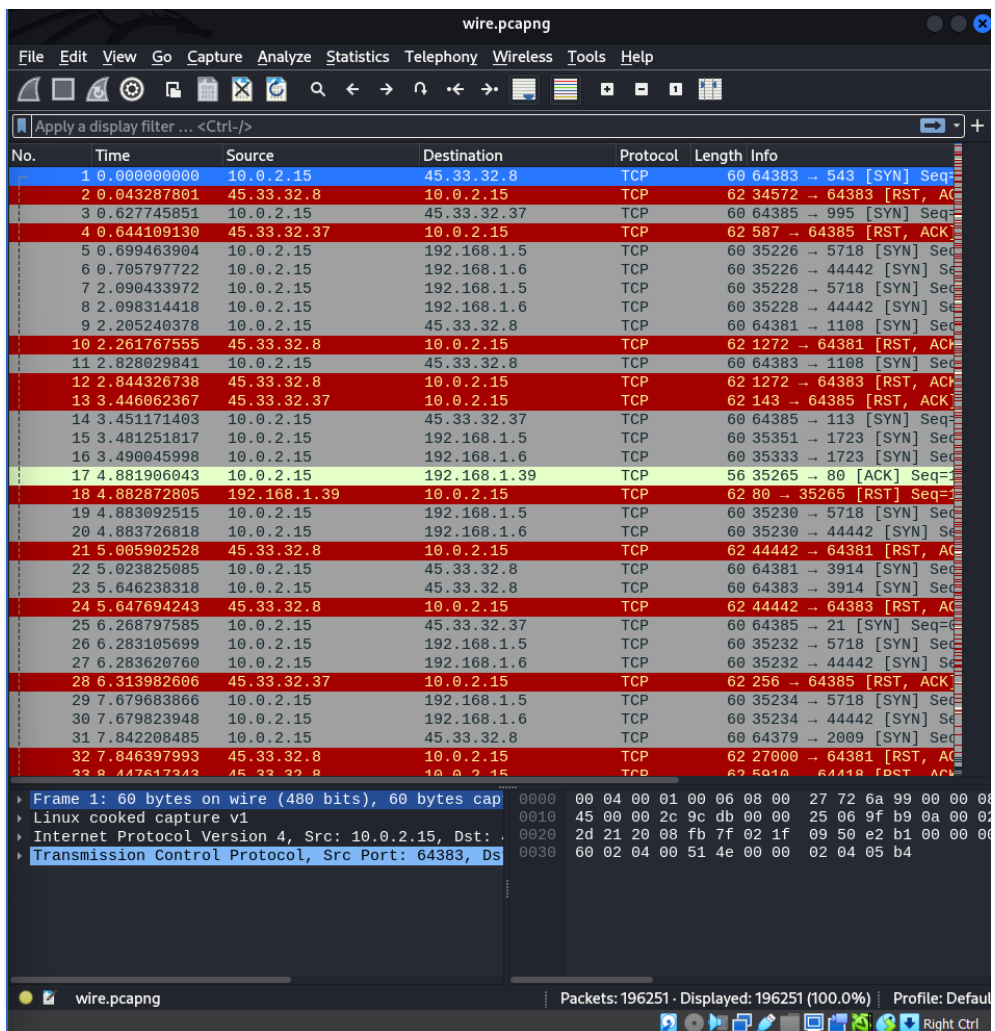
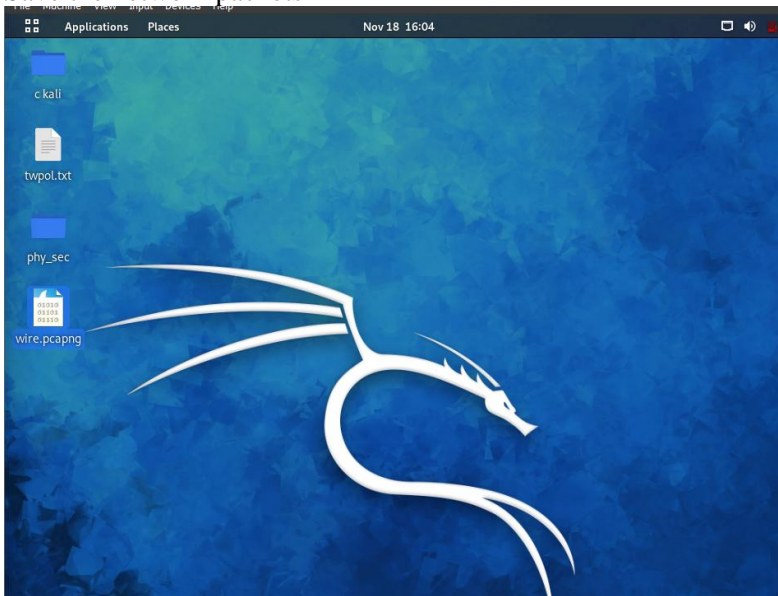
Aim- Network Scanning

Used tool- wire shark

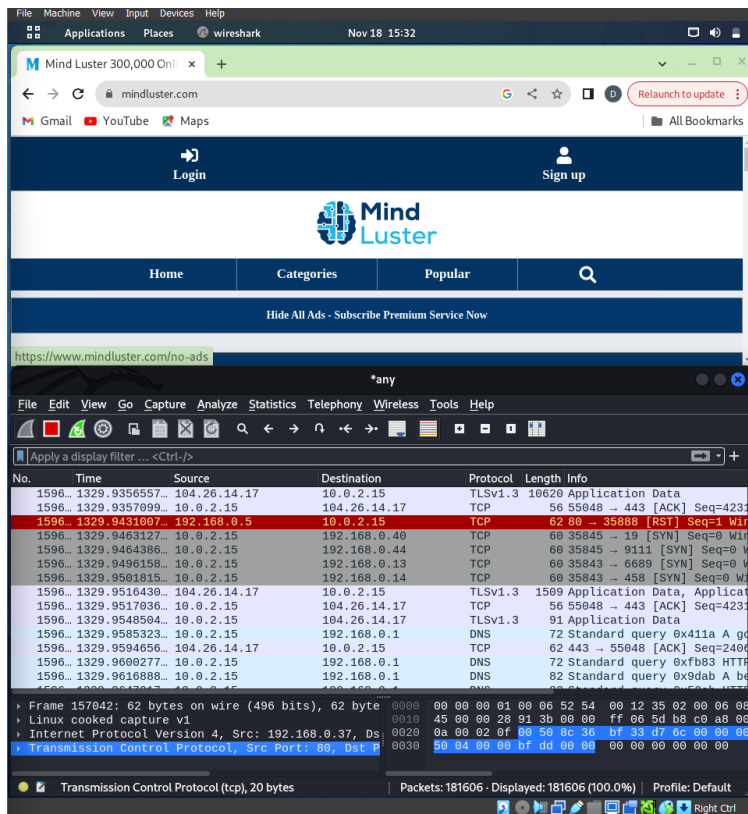
- Perform this experiment to capture Network Traffic for at least 15 minutes from your VM.
- PING other systems on the same network as your VM.
- Run Wireshark to capture network traffic



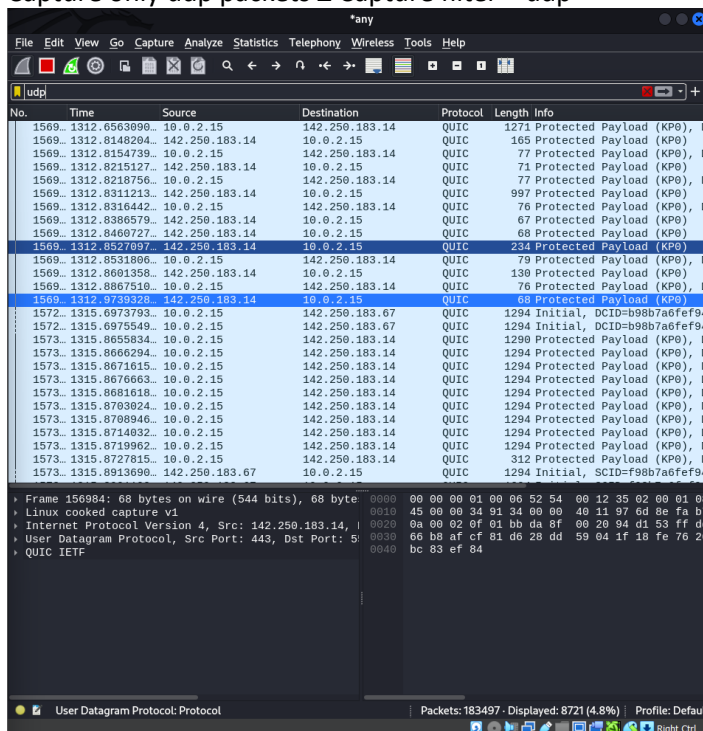
- Save the network packets



- Open browser and go to any website



- Perform this experiment to capture ONLY UDP and TCP packets
- A. Capture only udp packets ☒ Capture filter = udp



B. Capture only tcp packets ☐ Capture filter = “tcp

The screenshot shows the Wireshark interface with the capture filter "tcp" applied. The packet list displays a series of TCP packets between source IP 10.0.2.15 and destination IP 192.168.0.34. The selected packet (No. 1312) is expanded, showing the following details:

- Frame 156983: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface v1
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.34
- Transmission Control Protocol, Src Port: 35843, Dst Port: 5801

The packet bytes pane shows the raw data in hexadecimal and ASCII.

C. Capture only DNS Requests ☐ “udpdst port 53”

The screenshot shows the Wireshark interface with the capture filter "udpdst port 53" applied. The packet list displays a series of DNS Standard query packets from source IP 10.0.2.15 to destination IP 192.168.0.1. The selected packet (No. 1312) is expanded, showing the following details:

- Frame 156864: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface v1
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.1
- User Datagram Protocol, Src Port: 48377, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII.

D. Capture only UDP packets with source port 53 (DNS replies) “udpsrc port 53”

Wireshark capture showing DNS replies filtered by "udp.srcport==53". The packet list shows various DNS responses from 192.168.0.1 to 10.0.2.15. The packet details pane shows the structure of a DNS response, including the header, question, answer, and authority sections.

No.	Time	Source	Destination	Protocol	Length	Info
1396	1204.5020518	192.168.0.1	10.0.2.15	DNS	165	Standard query response 0x
1396	1204.5020518	192.168.0.1	10.0.2.15	DNS	182	Standard query response 0x
1396	1204.5020519	192.168.0.1	10.0.2.15	DNS	208	Standard query response 0x
1396	1204.5020519	192.168.0.1	10.0.2.15	DNS	167	Standard query response 0x
1396	1204.9817522	192.168.0.1	10.0.2.15	DNS	126	Standard query response 0x
1398	1204.9817527	192.168.0.1	10.0.2.15	DNS	367	Standard query response 0x
1400	1205.9514267	192.168.0.1	10.0.2.15	DNS	155	Standard query response 0x
1400	1206.4101513	192.168.0.1	10.0.2.15	DNS	195	Standard query response 0x
1401	1206.6207810	192.168.0.1	10.0.2.15	DNS	94	Standard query response 0x
1402	1206.7186866	192.168.0.1	10.0.2.15	DNS	146	Standard query response 0x
1402	1206.7187393	10.0.2.15	192.168.0.1	ICMP	174	Destination unreachable (P
1403	1206.9915296	192.168.0.1	10.0.2.15	DNS	136	Standard query response 0x
1403	1206.9915299	192.168.0.1	10.0.2.15	DNS	95	Standard query response 0x
1406	1207.2769556	192.168.0.1	10.0.2.15	DNS	133	Standard query response 0x
1406	1207.2769560	192.168.0.1	10.0.2.15	DNS	98	Standard query response 0x
1410	1207.9527873	192.168.0.1	10.0.2.15	DNS	109	Standard query response 0x
1412	1208.1681304	192.168.0.1	10.0.2.15	DNS	150	Standard query response 0x
1412	1208.1681725	10.0.2.15	192.168.0.1	ICMP	178	Destination unreachable (P
1412	1208.1681310	192.168.0.1	10.0.2.15	DNS	114	Standard query response 0x
1412	1208.1681311	192.168.0.1	10.0.2.15	DNS	105	Standard query response 0x
1454	1232.4470059	192.168.0.1	10.0.2.15	DNS	107	Standard query response 0x
1455	1232.4745527	192.168.0.1	10.0.2.15	DNS	148	Standard query response 0x
1455	1232.4747468	10.0.2.15	192.168.0.1	ICMP	176	Destination unreachable (P
1532	1266.9544648	192.168.0.1	10.0.2.15	DNS	94	Standard query response 0x
1539	1276.4502431	192.168.0.1	10.0.2.15	DNS	92	Standard query response 0x
1539	1276.5175736	192.168.0.1	10.0.2.15	DNS	101	Standard query response 0x
1539	1276.5176133	10.0.2.15	192.168.0.1	ICMP	129	Destination unreachable (P

Source Port: Unsigned Integer (2 bytes) | Packets: 184731 · Displayed: 600 (0.3%) | Profile: Default

- Filter to find out

A. Find out PING traffic “icmp”

Wireshark capture showing ICMP traffic filtered by "icmp". The packet list shows various ICMP destination unreachable messages from 192.168.0.1 to 10.0.2.15. The packet details pane shows the structure of an ICMP message, including the header and data sections.

No.	Time	Source	Destination	Protocol	Length	Info
1563	1249.9858852	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9858853	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9858854	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9858854	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859280	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859281	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859282	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859283	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859283	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859284	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859285	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9859286	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861163	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861165	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861166	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861166	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861167	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861168	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861168	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9861169	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9862532	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9862536	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9862536	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9862537	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1563	1249.9862538	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
1567	1250.8662284	10.0.2.15	142.250.183.14	ICMP	97	Destination unreachable (P
1539	1276.5176133	10.0.2.15	192.168.0.1	ICMP	129	Destination unreachable (P

Internet Control Message Protocol: Protocol | Packets: 185148 · Displayed: 11495 (6.2%) | Profile: Default

B. Packets coming to your system “dst host”

File Machine View Input Devices Help
Applications Places Wireshark Nov 18 15:46

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
1539	1276.2292724	10.0.2.15	192.168.0.43	TCP	60	35843 → 9111 [SYN] Seq=0 W
1539	1276.2421883	10.0.2.15	192.168.0.21	TCP	60	35845 → 7435 [SYN] Seq=0 W
1539	1276.2478160	10.0.2.15	192.168.0.14	TCP	60	35845 → 144 [SYN] Seq=0 W
1539	1276.2508016	10.0.2.15	192.168.0.24	TCP	60	35845 → 458 [SYN] Seq=0 W
1539	1276.2536463	10.0.2.15	192.168.0.63	TCP	60	35845 → 49153 [SYN] Seq=0
1539	1276.2577810	10.0.2.15	192.168.0.29	TCP	60	35845 → 1067 [SYN] Seq=0 W
1539	1276.2614601	10.0.2.15	192.168.0.56	TCP	60	35843 → 61900 [SYN] Seq=0
1539	1276.2750937	10.0.2.15	192.168.1.6	TCP	60	35228 → 4 [SYN] Seq=0 Win=
1539	1276.3241766	10.0.2.15	192.168.0.56	TCP	56	[TCP Dup ACK 37254#1] 3587
1539	1276.3286475	192.168.0.56	10.0.2.15	TCP	62	80 → 35874 [RST] Seq=1 Win
1539	1276.3314557	10.0.2.15	192.168.0.32	TCP	60	35845 → 32779 [SYN] Seq=0
1539	1276.3316295	10.0.2.15	192.168.0.61	TCP	60	35843 → 1067 [SYN] Seq=0 W
1539	1276.3317208	10.0.2.15	192.168.0.62	TCP	60	35843 → 10003 [SYN] Seq=0
1539	1276.3400467	10.0.2.15	192.168.0.4	TCP	60	35843 → 7019 [SYN] Seq=0 W
1539	1276.3505903	10.0.2.15	192.168.0.7	TCP	60	35843 → 1201 [SYN] Seq=0 W
1539	1276.4256223	10.0.2.15	192.168.0.10	TCP	60	35843 → 49 [SYN] Seq=0 Win
1539	1276.4380964	10.0.2.15	192.168.0.13	TCP	60	35843 → 6112 [SYN] Seq=0 W
1539	1276.4392588	10.0.2.15	192.168.0.1	DNS	76	Standard query 0x2b9b A ww
1539	1276.4399470	10.0.2.15	192.168.0.1	DNS	76	Standard query 0xa303 HTTP
1539	1276.4502431	192.168.0.1	10.0.2.15	DNS	92	Standard query response 0x
1539	1276.4554162	10.0.2.15	192.168.0.48	TCP	60	35845 → 50001 [SYN] Seq=0
1539	1276.4864364	10.0.2.15	192.168.0.45	TCP	60	35845 → 8180 [SYN] Seq=0 W
1539	1276.4865972	10.0.2.15	192.168.0.18	TCP	60	35843 → 1433 [SYN] Seq=0 W
1539	1276.5135398	10.0.2.15	142.250.183.170	TCP	56	[TCP Keep-Alive] 59010 → 4
1539	1276.5142751	10.0.2.15	142.251.42.22	TCP	56	[TCP Keep-Alive] 52624 → 4
1539	1276.5175736	192.168.0.1	10.0.2.15	DNS	181	Standard query response 0x
1539	1276.5170133	10.0.2.15	192.168.0.1	ICMP	129	Destination unreachable (P

Frame 153999: 129 bytes on wire (1032 bits), 129 b
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.15, Dst:
Internet Control Message Protocol
Domain Name System (response)

wireshark_any3AYRE2.pcapng | Packets: 186304 - Displayed: 186086 (99.9%) | Profile: Default

C. Packets from other system “src host”

File Machine View Input Devices Help
Applications Places Wireshark Nov 18 15:47

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.2.2&&icmp

No.	Time	Source	Destination	Protocol	Length	Info
592	142.668103625	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
594	142.681827324	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
596	142.693763568	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
601	142.698618533	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
602	142.698619194	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
603	142.698619264	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
604	142.698619324	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
606	142.706526492	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
608	142.709920364	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
612	142.716010931	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
613	142.716011462	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
614	142.716011542	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
617	142.720941730	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
618	142.720942221	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
621	142.724566303	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
623	142.726617023	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
624	142.726617503	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
627	142.729612438	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
628	142.729613119	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
631	142.733379833	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
632	142.733380484	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
636	142.738185240	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
637	142.738185871	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
639	142.738185941	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
646	142.744446181	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
647	142.744446651	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H
648	142.744446722	10.0.2.2	10.0.2.15	ICMP	72	Destination unreachable (H

Frame 592: 72 bytes on wire (576 bits), 72 bytes c
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.2, Dst: 1
Internet Control Message Protocol

wireshark_any3AYRE2.pcapng | Packets: 186666 - Displayed: 10471 (5.6%) | Profile: Default

