**CHECKPOINT 4**

\*\*\*\*\*\*\* CLI Output \*\*\*\*\*\*\*

root@student64:~# tcpdump -i eth0 -w network-traffic.cap

tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

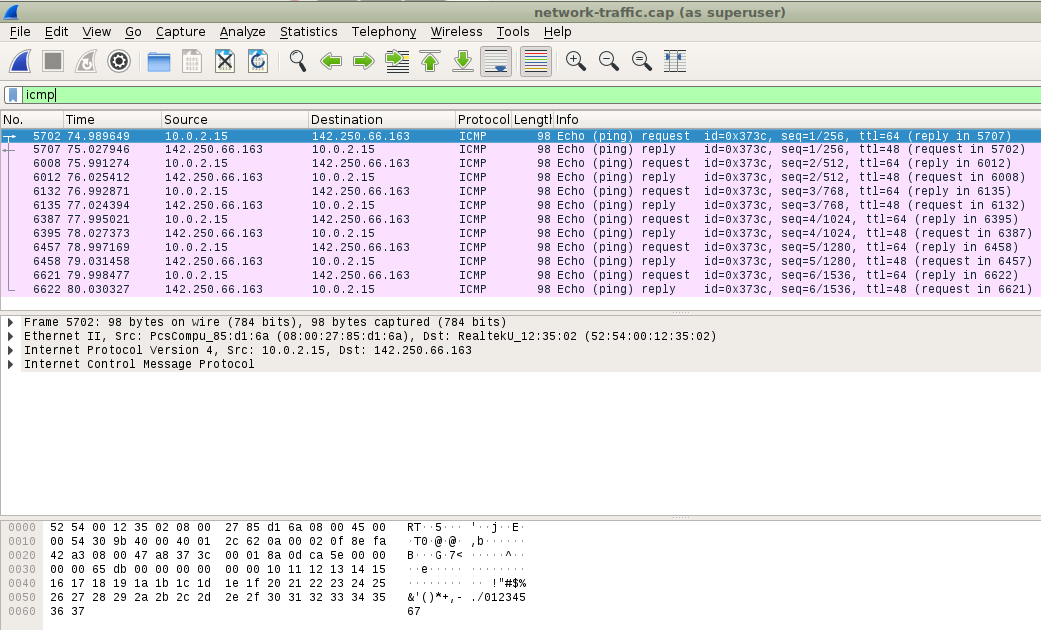
^C

6836 packets captured

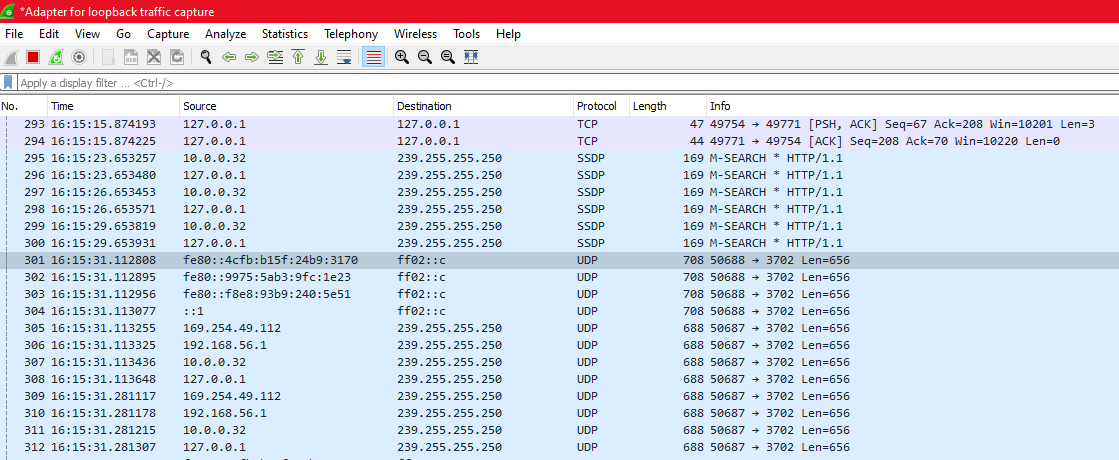
6838 packets received by filter

0 packets dropped by kernel

root@student64:~# wireshark -r network-traffic.cap

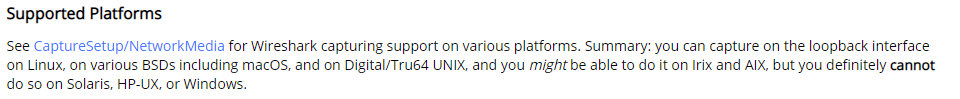
**Q) Can you identify ICMP traffic on the network interface?**

**Q) Or if running a VM, can you install and run Wireshark on the host machine running the VM to capture the VMs traffic?**

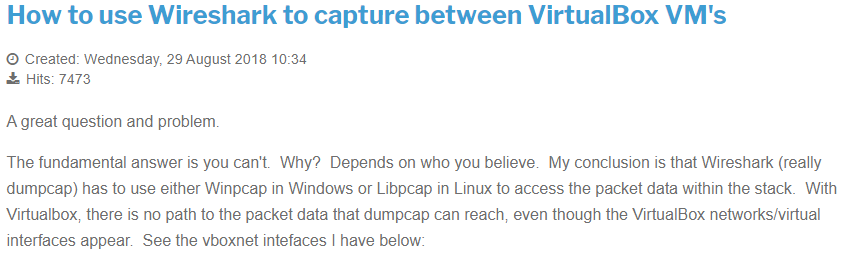


These packets are largely just for identifying all the interfaces and services on my host (the VirtualBox VM network address is 169.254.49.112). There are no packets corresponding to pings or website requests that I run in the VM.

A couple of websites suggest capturing this traffic is not possible on Windows.



<https://wiki.wireshark.org/CaptureSetup/Loopback>



<https://www.cellstream.com/reference-reading/tipsandtricks/396-wiresharinvboxvm>

**CHECKPOINT 5**

\*\*\*\*\*\*\* CLI Output \*\*\*\*\*\*\*

The traceroute and tracepath commands just show all stars on the VirtualBox VM. So I ran these in WSL2 on my Windows host instead.

**Q) Can you run the following commands and compare the resulting times to the host www.flinders.edu.au:**

**$ tracepath www.flinders.edu.au**

pill0032@JOELZ:~$ tracepath flinders.edu.au

1?: [LOCALHOST] pmtu 1500

1: JOELZ.mshome.net 0.311ms

1: JOELZ.mshome.net 0.250ms

2: 10.0.0.1 4.452ms

3: ??? 14.714ms

4: ??? 12.697ms

5: be10-3999.core1.yourdc-haw.adl.aussiebb.net 14.081ms

6: be1.core2.yourdc-haw.adl.aussiebb.net 14.668ms

7: as7575.adl.edgeix.net.au 23.849ms asymm 8

8: xe-0-0-2.pe1.adel.sa.aarnet.net.au 21.904ms

9: gw1.vlan253.xe-5-2-0.pe1.adel.sa.aarnet.net.au 25.357ms asymm 8

10: no reply

11: no reply

12: no reply

13: no reply

14: no reply

15: no reply

16: no reply

17: no reply

18: no reply

19: no reply

20: no reply

21: no reply

22: no reply

23: no reply

24: no reply

25: no reply

26: no reply

27: no reply

28: no reply

29: no reply

30: no reply

Too many hops: pmtu 1500

Resume: pmtu 1500

**$ traceroute www.flinders.edu.au**

pill0032@JOELZ:~$ traceroute flinders.edu.au --resolve-hostnames

traceroute to flinders.edu.au (129.96.88.39), 64 hops max

1 172.22.48.1 (JOELZ.mshome.net) 0.228ms 0.166ms 0.162ms

2 10.0.0.1 (10.0.0.1) 3.216ms 1.606ms 2.082ms

3 100.80.0.1 (100.80.0.1) 12.619ms 12.267ms 10.519ms

4 180.150.2.73 (180.150.2.73) 14.707ms 14.817ms 9.918ms

5 202.142.143.194 (be10-3999.core1.yourdc-haw.adl.aussiebb.net) 18.123ms 13.852ms 12.659ms

6 180.150.2.39 (be1.core2.yourdc-haw.adl.aussiebb.net) 13.138ms 12.807ms 17.840ms

7 103.136.101.18 (as7575.adl.edgeix.net.au) 20.226ms 21.889ms 20.657ms

8 113.197.15.130 (xe-0-0-2.pe1.adel.sa.aarnet.net.au) 22.506ms 19.396ms 19.910ms

9 138.44.192.99 (gw1.vlan253.xe-5-2-0.pe1.adel.sa.aarnet.net.au) 22.723ms 23.986ms 20.479ms

10 \* \* \*

11 \* \* \*

12 \* \* \*

13 \* \* \*

14 \* \* \*

15 \* \* \*

16 \* \* \*

17 \* \* \*

18 \* \* \*

19 \* \* \*

20 \* \* \*

21 \* \* \*

22 \* \* \*

23 \* \* \*

24 \* \* \*

25 \* \* \*

26 \* \* \*

27 \* \* \*

28 \* \* \*

29 \* \* \*

30 \* \* \*

**$ ping -c 10 www.flinders.edu.au**

pill0032@JOELZ:~$ ping -c 10 www.flinders.edu.au

PING cdn.prod.flinders.adobecqms.net (13.35.149.54) 56(84) bytes of data.

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=1 ttl=244 time=35.6 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=2 ttl=244 time=31.5 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=3 ttl=244 time=33.4 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=4 ttl=244 time=31.1 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=5 ttl=244 time=46.6 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=6 ttl=244 time=33.2 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=7 ttl=244 time=35.1 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=8 ttl=244 time=33.6 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=9 ttl=244 time=32.3 ms

64 bytes from server-13-35-149-54.syd1.r.cloudfront.net (13.35.149.54): icmp\_seq=10 ttl=244 time=32.0 ms

--- cdn.prod.flinders.adobecqms.net ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9015ms

rtt min/avg/max/mdev = 31.144/34.491/46.696/4.298 ms

**Q) Identify which hosts/routers create the largest latency**

The two hosts/routers creating the largest latency are:

1. the first host/router outside my home network, which is 100.80.0.1 in traceroute
2. the host/router 103.136.101.18 (as7575.adl.edgeix.net.au) in step 6/7.

Both increase the RTT by around 8-10ms. They are highlighted in red above.

**Q) Do you see asymmetric routes, if so why might that be?**

Asymmetric routes occur when an outgoing packet takes a different path than a return packet and consequently has a large difference in time taken for outgoing vs return paths.

Tracepath identified two asymmetric routes in steps 7 and 9.

It also appears that one of the pings (ping 5, in blue) has a much higher RTT than the others, perhaps indicating an asymmetric route taken.

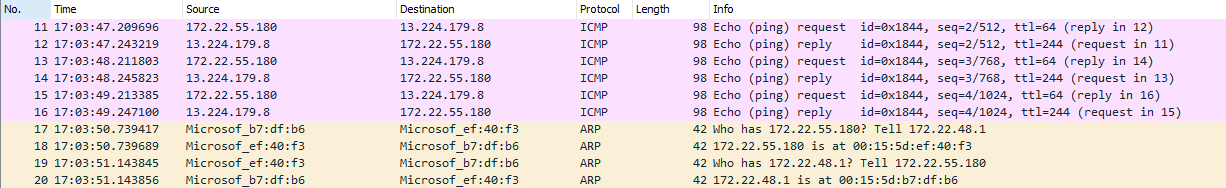
Traceroute works by sending out UDP packets with an incrementing Time To Live (TTL). When it makes the TTL number of hops (so TTL = 0), the node where it stopped will send back a ICMP message, that will count return hops. If return hops is not equal to TTL, then the route was asymmetric.

Ref 1: <https://community.cisco.com/t5/data-center-documents/identifying-and-troubleshooting-asymmetric-routing-in-waas/ta-p/3123733>

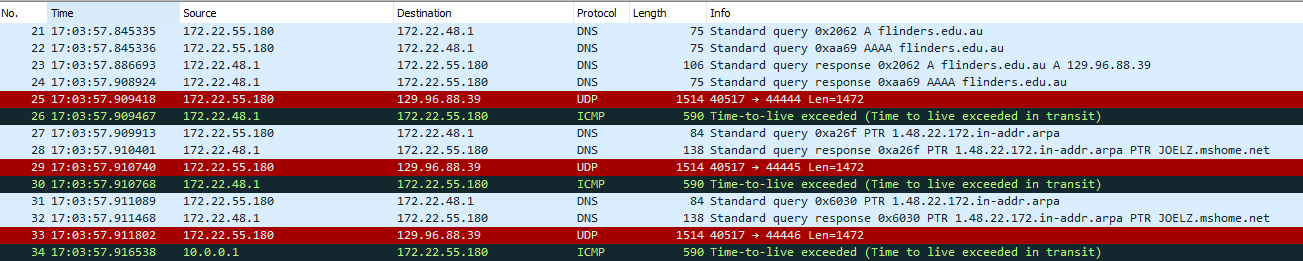
Ref 2: <https://www.fir3net.com/Networking/Terms-and-Concepts/how-does-traceroute-calculate-asymmetric-routing.html>

**Q) Using tcpdump or wireshark, what type of traffic do these programs generate?**

Pings generate ICMP and ARP traffic:



Tracepath generates DNS, ICMP and UDP traffic:



Traceroute also generates DNS, ICMP and UDP traffic:

