

#### 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?

The image shows the Wireshark network protocol analyzer interface. The title bar indicates the file is 'network-traffic.cap (as superuser)'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane on the left shows a list of captured packets, with the first packet selected. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP). The packet bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
5702	74.989649	10.0.2.15	142.250.66.163	ICMP	98	Echo (ping) request id=0x373c, seq=1/256, ttl=64 (reply in 5707)
5707	75.027946	142.250.66.163	10.0.2.15	ICMP	98	Echo (ping) reply id=0x373c, seq=1/256, ttl=48 (request in 5702)
6008	75.991274	10.0.2.15	142.250.66.163	ICMP	98	Echo (ping) request id=0x373c, seq=2/512, ttl=64 (reply in 6012)
6012	76.025412	142.250.66.163	10.0.2.15	ICMP	98	Echo (ping) reply id=0x373c, seq=2/512, ttl=48 (request in 6008)
6132	76.992871	10.0.2.15	142.250.66.163	ICMP	98	Echo (ping) request id=0x373c, seq=3/768, ttl=64 (reply in 6135)
6135	77.024394	142.250.66.163	10.0.2.15	ICMP	98	Echo (ping) reply id=0x373c, seq=3/768, ttl=48 (request in 6132)
6387	77.995021	10.0.2.15	142.250.66.163	ICMP	98	Echo (ping) request id=0x373c, seq=4/1024, ttl=64 (reply in 6395)
6395	78.027373	142.250.66.163	10.0.2.15	ICMP	98	Echo (ping) reply id=0x373c, seq=4/1024, ttl=48 (request in 6387)
6457	78.997169	10.0.2.15	142.250.66.163	ICMP	98	Echo (ping) request id=0x373c, seq=5/1280, ttl=64 (reply in 6458)
6458	79.031458	142.250.66.163	10.0.2.15	ICMP	98	Echo (ping) reply id=0x373c, seq=5/1280, ttl=48 (request in 6457)
6621	79.998477	10.0.2.15	142.250.66.163	ICMP	98	Echo (ping) request id=0x373c, seq=6/1536, ttl=64 (reply in 6622)
6622	80.030327	142.250.66.163	10.0.2.15	ICMP	98	Echo (ping) reply id=0x373c, seq=6/1536, ttl=48 (request in 6621)

Frame 5702: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0  
Ethernet II, Src: PcsCompu\_85:d1:6a (08:00:27:85:d1:6a), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.66.163  
Internet Control Message Protocol

0000 52 54 00 12 35 02 08 00 27 85 d1 6a 08 00 45 00 RT..5...'.j..E.  
0010 00 54 30 9b 40 00 40 01 2c 62 0a 00 02 0f 8e fa .T@.@.,b.....  
0020 42 a3 08 00 47 a8 37 3c 00 01 8a 0d ca 5e 00 00 B...G.7<.....A..  
0030 00 00 65 db 00 00 00 00 00 00 10 11 12 13 14 15 ..e.....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .....!""\$%  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()\*+,-./012345  
0060 36 37 67

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

The image shows the Wireshark network protocol analyzer interface. The title bar indicates the file is '\*Adapter for loopback traffic capture'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane on the left shows a list of captured packets, with the first packet selected. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP). The packet bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
293	16:15:15.874193	127.0.0.1	127.0.0.1	TCP	47	49754 → 49771 [PSH, ACK] Seq=67 Ack=208 Win=10201 Len=3
294	16:15:15.874225	127.0.0.1	127.0.0.1	TCP	44	49771 → 49754 [ACK] Seq=208 Ack=70 Win=10220 Len=0
295	16:15:23.653257	10.0.0.32	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
296	16:15:23.653480	127.0.0.1	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
297	16:15:26.653453	10.0.0.32	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
298	16:15:26.653571	127.0.0.1	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
299	16:15:29.653819	10.0.0.32	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
300	16:15:29.653931	127.0.0.1	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
301	16:15:31.112808	fe80::4cfb:b15f:24b9:3170	ff02::c	UDP	708	50688 → 3702 Len=656
302	16:15:31.112895	fe80::9975:5ab3:9fc:1e23	ff02::c	UDP	708	50688 → 3702 Len=656
303	16:15:31.112956	fe80::f8e8:93b9:240:5e51	ff02::c	UDP	708	50688 → 3702 Len=656
304	16:15:31.113077	::1	ff02::c	UDP	708	50688 → 3702 Len=656
305	16:15:31.113255	169.254.49.112	239.255.255.250	UDP	688	50687 → 3702 Len=656
306	16:15:31.113325	192.168.56.1	239.255.255.250	UDP	688	50687 → 3702 Len=656
307	16:15:31.113436	10.0.0.32	239.255.255.250	UDP	688	50687 → 3702 Len=656
308	16:15:31.113648	127.0.0.1	239.255.255.250	UDP	688	50687 → 3702 Len=656
309	16:15:31.281117	169.254.49.112	239.255.255.250	UDP	688	50687 → 3702 Len=656
310	16:15:31.281178	192.168.56.1	239.255.255.250	UDP	688	50687 → 3702 Len=656
311	16:15:31.281215	10.0.0.32	239.255.255.250	UDP	688	50687 → 3702 Len=656
312	16:15:31.281307	127.0.0.1	239.255.255.250	UDP	688	50687 → 3702 Len=656

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.

### Supported Platforms

See [CaptureSetup/NetworkMedia](#) for Wireshark capturing support on various platforms. Summary: you can capture on the loopback interface on Linux, on various BSDs including macOS, and on Digital/Tru64 UNIX, and you *might* be able to do it on Irix and AIX, but you definitely **cannot** do so on Solaris, HP-UX, or Windows.

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

## How to use Wireshark to capture between VirtualBox VM's

🕒 Created: Wednesday, 29 August 2018 10:34

👤 Hits: 7473

A great question and problem.

The fundamental answer is you can't. Why? Depends on who you believe. My conclusion is that Wireshark (really dumpcap) has to use either Winpcap in Windows or Libpcap in Linux to access the packet data within the stack. With Virtualbox, there is no path to the packet data that dumpcap can reach, even though the VirtualBox networks/virtual interfaces appear. See the vboxnet interfaces I have below:

<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](http://www.flinders.edu.au):**

**\$ tracepath [www.flinders.edu.au](http://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:

No.	Time	Source	Destination	Protocol	Length	Info
11	17:03:47.209696	172.22.55.180	13.224.179.8	ICMP	98	Echo (ping) request id=0x1844, seq=2/512, ttl=64 (reply in 12)
12	17:03:47.243219	13.224.179.8	172.22.55.180	ICMP	98	Echo (ping) reply id=0x1844, seq=2/512, ttl=244 (request in 11)
13	17:03:48.211803	172.22.55.180	13.224.179.8	ICMP	98	Echo (ping) request id=0x1844, seq=3/768, ttl=64 (reply in 14)
14	17:03:48.245823	13.224.179.8	172.22.55.180	ICMP	98	Echo (ping) reply id=0x1844, seq=3/768, ttl=244 (request in 13)
15	17:03:49.213385	172.22.55.180	13.224.179.8	ICMP	98	Echo (ping) request id=0x1844, seq=4/1024, ttl=64 (reply in 16)
16	17:03:49.247100	13.224.179.8	172.22.55.180	ICMP	98	Echo (ping) reply id=0x1844, seq=4/1024, ttl=244 (request in 15)
17	17:03:50.739417	Microsoft_b7:df:b6	Microsoft_ef:40:f3	ARP	42	Who has 172.22.55.180? Tell 172.22.48.1
18	17:03:50.739689	Microsoft_ef:40:f3	Microsoft_b7:df:b6	ARP	42	172.22.55.180 is at 00:15:5d:ef:40:f3
19	17:03:51.143845	Microsoft_ef:40:f3	Microsoft_b7:df:b6	ARP	42	Who has 172.22.48.1? Tell 172.22.55.180
20	17:03:51.143856	Microsoft_b7:df:b6	Microsoft_ef:40:f3	ARP	42	172.22.48.1 is at 00:15:5d:b7:df:b6

Tracepath generates DNS, ICMP and UDP traffic:

No.	Time	Source	Destination	Protocol	Length	Info
21	17:03:57.845335	172.22.55.180	172.22.48.1	DNS	75	Standard query 0x2062 A flinders.edu.au
22	17:03:57.845336	172.22.55.180	172.22.48.1	DNS	75	Standard query 0xaa69 AAAA flinders.edu.au
23	17:03:57.886693	172.22.48.1	172.22.55.180	DNS	106	Standard query response 0x2062 A flinders.edu.au A 129.96.88.39
24	17:03:57.908924	172.22.48.1	172.22.55.180	DNS	75	Standard query response 0xaa69 AAAA flinders.edu.au
25	17:03:57.909418	172.22.55.180	129.96.88.39	UDP	1514	40517 → 44444 Len=1472
26	17:03:57.909467	172.22.48.1	172.22.55.180	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
27	17:03:57.909913	172.22.55.180	172.22.48.1	DNS	84	Standard query 0xa26f PTR 1.48.22.172.in-addr.arpa
28	17:03:57.910401	172.22.48.1	172.22.55.180	DNS	138	Standard query response 0xa26f PTR 1.48.22.172.in-addr.arpa PTR JOELZ.mshome.net
29	17:03:57.910740	172.22.55.180	129.96.88.39	UDP	1514	40517 → 44445 Len=1472
30	17:03:57.910768	172.22.48.1	172.22.55.180	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
31	17:03:57.911089	172.22.55.180	172.22.48.1	DNS	84	Standard query 0x6030 PTR 1.48.22.172.in-addr.arpa
32	17:03:57.911468	172.22.48.1	172.22.55.180	DNS	138	Standard query response 0x6030 PTR 1.48.22.172.in-addr.arpa PTR JOELZ.mshome.net
33	17:03:57.911802	172.22.55.180	129.96.88.39	UDP	1514	40517 → 44446 Len=1472
34	17:03:57.916538	10.0.0.1	172.22.55.180	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)

Traceroute also generates DNS, ICMP and UDP traffic:

No.	Time	Source	Destination	Protocol	Length	Info
1	17:07:43.306341	172.22.55.180	172.22.48.1	DNS	75	Standard query 0xe0b4 A flinders.edu.au
2	17:07:43.311375	172.22.48.1	172.22.55.180	DNS	106	Standard query response 0xe0b4 A flinders.edu.au A 129.96.88.39
3	17:07:43.311983	172.22.55.180	129.96.88.39	UDP	51	49272 → 33434 Len=9
4	17:07:43.312035	172.22.48.1	172.22.55.180	ICMP	79	Time-to-live exceeded (Time to live exceeded in transit)
5	17:07:43.312503	172.22.55.180	129.96.88.39	UDP	51	49272 → 33434 Len=9
6	17:07:43.312544	172.22.48.1	172.22.55.180	ICMP	79	Time-to-live exceeded (Time to live exceeded in transit)
7	17:07:43.312837	172.22.55.180	129.96.88.39	UDP	51	49272 → 33434 Len=9
8	17:07:43.312854	172.22.48.1	172.22.55.180	ICMP	79	Time-to-live exceeded (Time to live exceeded in transit)
9	17:07:43.313760	172.22.55.180	129.96.88.39	UDP	51	49272 → 33435 Len=9
10	17:07:43.318378	10.0.0.1	172.22.55.180	ICMP	79	Time-to-live exceeded (Time to live exceeded in transit)
11	17:07:43.318691	172.22.55.180	129.96.88.39	UDP	51	49272 → 33435 Len=9
12	17:07:43.322243	10.0.0.1	172.22.55.180	ICMP	79	Time-to-live exceeded (Time to live exceeded in transit)