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

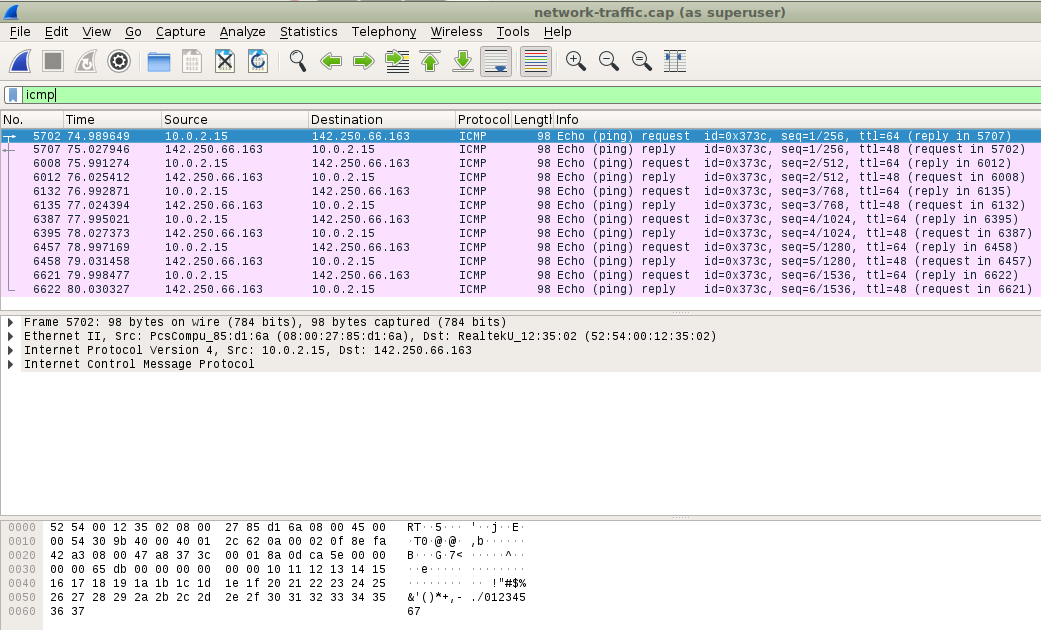
^C

6836 packets captured

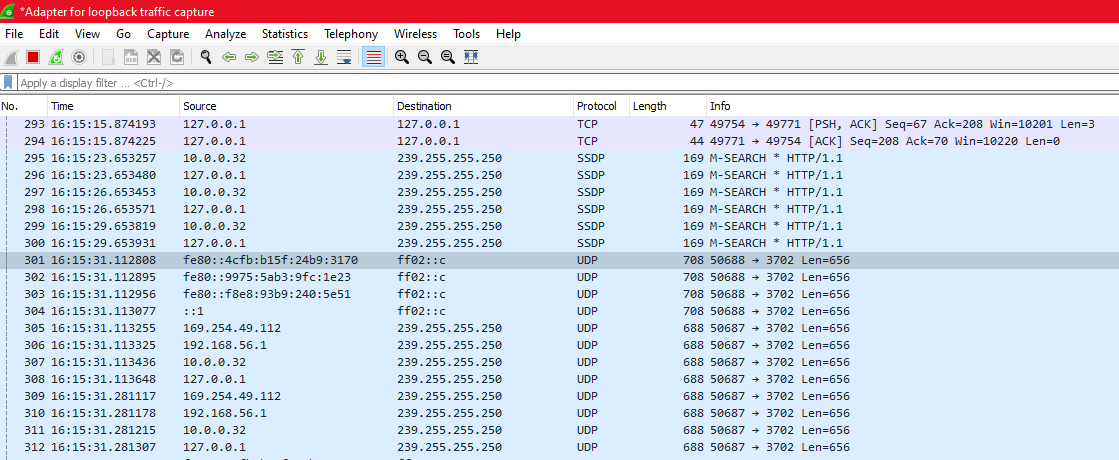
6838 packets received by filter

0 packets dropped by kernel

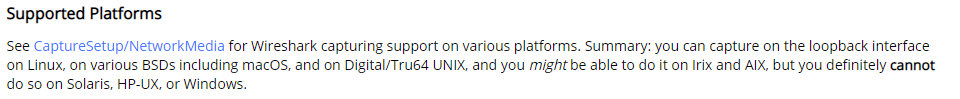
root@student64:~# wireshark -r network-traffic.cap

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

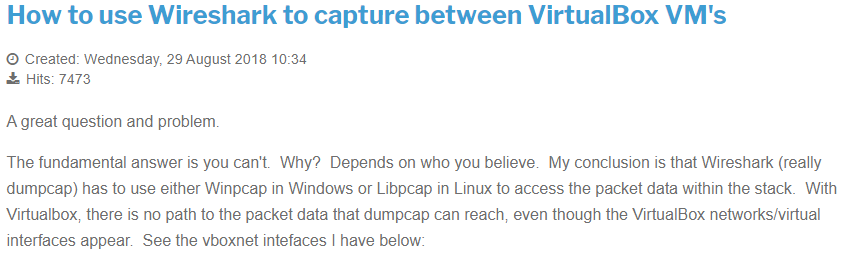
**Q) Or if running a VM, can you install and run Wireshark on the host machine running the VM to capture the VMs traffic?**



These packets are largely identifying all the interfaces and services onn my host (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>