

## USING WIRESHARK TO VIEW NETWORK TRAFFIC REPORT

Wireshark is a protocol analyzer application that works by capturing, filtering and analyzing packets over a network. In this exercise, we are going to use Wireshark to view the network traffic generated when we try to test and verify if devices on the same local area network as well as remotely are accessible using a network utility known as Ping which sends out and receives packets through a protocol known as Internet Control Message Protocol (ICMP) performed from the command prompt. Wireshark captured all the information that happened from the moment a ping command was issued from the host device through to the target IP address and allowed us to filter information off what we wanted displayed for this particular exercise, we were able to filter ICMP packets since that was the protocol we predominately interacted with.

It is by practically performing the steps provided from the exercise that I was able to answer the challenges given below backed by screenshots where necessary.

### PART 1: Capture and Analyze Local ICMP Data in Wireshark

#### Step 1: Retrieve your PC interface addresses

- a) In a command prompt window, enter `ipconfig /all`, to the IP address of your PC interface, its description, and its MAC (physical) address.

```
Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . . . : 
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-0D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::82a9:4f38:bddb:4b1c%13(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 503971879
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-1C-F6-76-68-F7-28-E5-A8-65
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

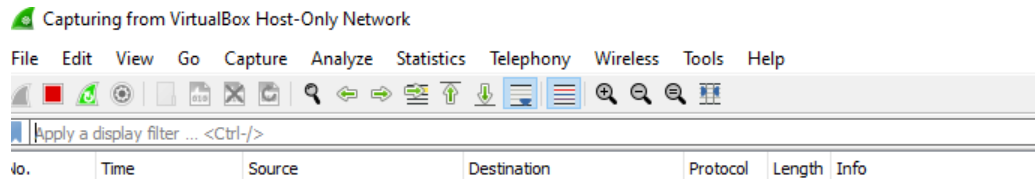
- b) Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not provide them with your MAC address at this time. For my team player member, I used Kali Linux on my VirtualBox whose IP address is 192.168.56.101

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
    inet 192.168.56.101 netmask 255.255.255.0
```

#### Step 2: Start Wireshark and begin capturing data.

- a) Navigate to Wireshark. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic. I chose VirtualBox host only network interface because I am using a Linux guest machine and I needed to be able to ping my guest machine from my Windows host machine.

## USING WIRESHARK TO VIEW NETWORK TRAFFIC REPORT



- b) Navigate to a command prompt window and ping the IP address that you received from your team member.

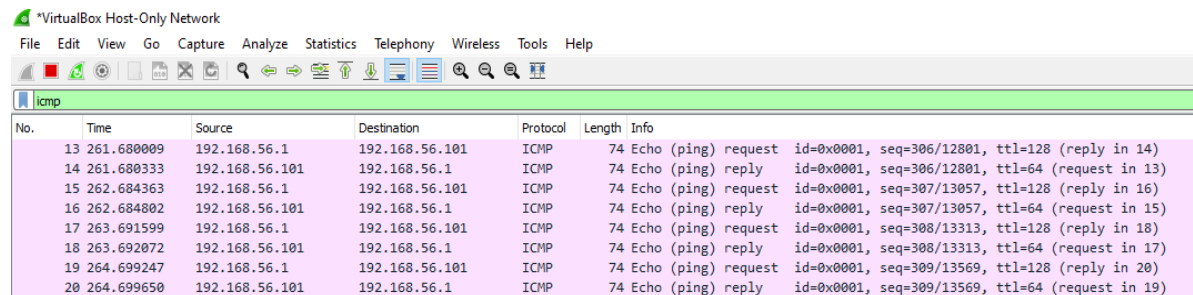
```
Command Prompt

C:\Users\Wariara>ping 192.168.56.101

Pinging 192.168.56.101 with 32 bytes of data:
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

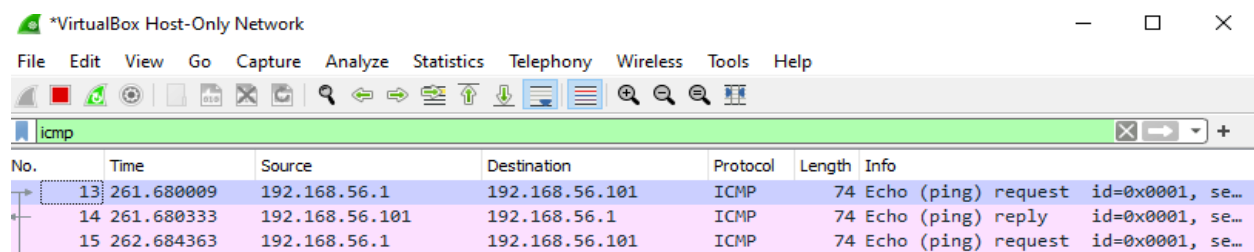
Upon running the command from my windows command prompt, Wireshark began to capture the packets as shown below



### Step 3: Examine the captured data

- a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC IP address, and the Destination column contains the IP address of the teammate PC that you pinged.

My host IP address is 192.168.56.1 and my teammate PC is 192.168.56.101 as verified earlier. The same source and destination IP is displayed on the ICMP PDU as highlighted in the screenshot below



## USING WIRESHARK TO VIEW NETWORK TRAFFIC REPORT

- b. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the destination and source MAC addresses.

1. Does the source MAC address match your PC interface? Yes

▼ Ethernet II, Src: 0a:00:27:00:00:0d (0a:00:27:00:00:0d), Dst: PcsCompu\_22:46:4f (08:00:27:22:46:4f)  
    > Destination: PcsCompu\_22:46:4f (08:00:27:22:46:4f)  
    > Source: 0a:00:27:00:00:0d (0a:00:27:00:00:0d)  
    Type: IPv4 (0x0800)

```
Connection-specific DNS Suffix . :  
Description . . . . . : VirtualBox Host-Only  
Physical Address. . . . . : 0A-00-27-00-00-0D
```

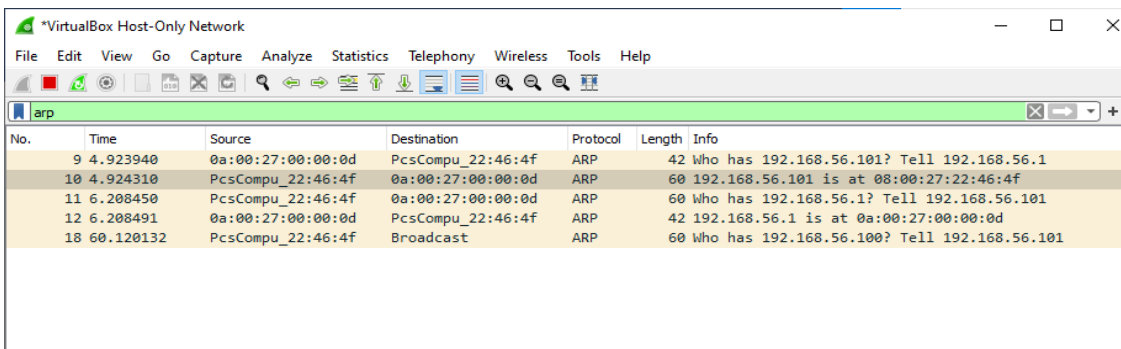
2. Does the destination MAC address in Wireshark match your team member MAC address?

Yes.

▼ Ethernet II, Src: 0a:00:27:00:00:0d (0a:00:27:00:00:0d), Dst: PcsCompu\_22:46:4f (08:00:27:22:46:4f)  
    > Destination: PcsCompu\_22:46:4f (08:00:27:22:46:4f)  
    > Source: 0a:00:27:00:00:0d (0a:00:27:00:00:0d)  
    Type: IPv4 (0x0800)

```
eth0: flags=4163<UP,BROADCAST,RUNNING>  
    inet 192.168.56.101 netmask 255.255.255.0  
    inet6 fe80::e41e:2c9e:c864:1111  
    ether 08:00:27:22:46:4f  
    RX packets 2 bytes 1770
```

3. How is the MAC address of the pinged PC obtained by your PC? Since my PC and that of my pinged machine are on the same local area network (LAN), a protocol called Address Resolution Protocol (ARP) comes into play where it is able to access the MAC address by sending a broadcast request to all devices on the LAN with an IP address and the machine with the attached address responds. For my case, my PC sends out ARP request as shown in the screenshot below and a reply is given by the pinged PC with the MAC address attached as shown below



No.	Time	Source	Destination	Protocol	Length	Info
9	4.923940	0a:00:27:00:00:0d	PcsCompu_22:46:4f	ARP	42	Who has 192.168.56.101? Tell 192.168.56.1
10	4.924310	PcsCompu_22:46:4f	0a:00:27:00:00:0d	ARP	60	192.168.56.101 is at 08:00:27:22:46:4f
11	6.208450	PcsCompu_22:46:4f	0a:00:27:00:00:0d	ARP	60	Who has 192.168.56.1? Tell 192.168.56.101
12	6.208491	0a:00:27:00:00:0d	PcsCompu_22:46:4f	ARP	42	192.168.56.1 is at 0a:00:27:00:00:0d
18	60.120132	PcsCompu_22:46:4f	Broadcast	ARP	60	Who has 192.168.56.100? Tell 192.168.56.101

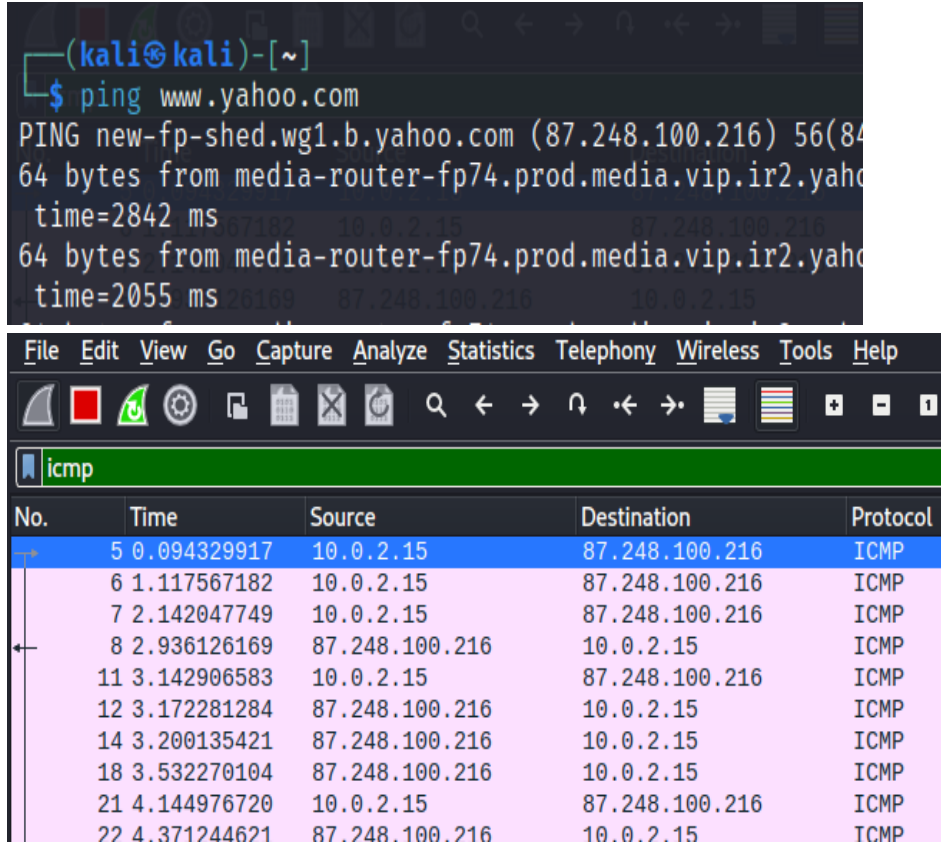
### Step 2: Examining and analyzing the data from the remote hosts.

- a. Review the captured data in Wireshark and examine the IP and MAC addresses of the three locations that you pinged. List the destination IP and MAC addresses for all three locations in the space provided.

## USING WIRESHARK TO VIEW NETWORK TRAFFIC REPORT

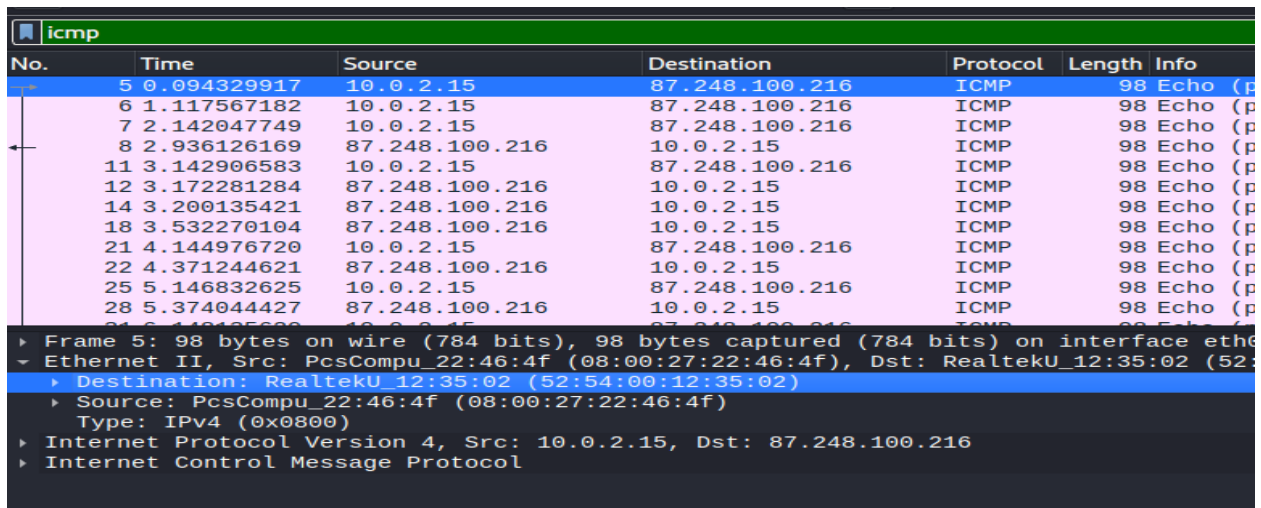
### 1. IP address for www.yahoo.com:

The Yahoo IP address is 87.248.100.216 which is resolved by the Domain Name System (DNS) on the command prompt and also indicated as the destination on the first packet on the Wireshark interface.



### 2. MAC address for www.yahoo.com:

52:54:00:12:35:02 which is derived from the ethernet II payload information as shown below



## USING WIRESHARK TO VIEW NETWORK TRAFFIC REPORT

### 3. IP address for [www.cisco.com](http://www.cisco.com):

95.100.76.145 is the IP address translated by DNS.

```
(kali㉿kali)-[~]
$ ping www.cisco.com
PING e2867.dsca.akamaiedge.net (95.100.76.145) 56(84) b
64 bytes from a95-100-76-145.deploy.static.akamaitechno
145): icmp_seq=1 ttl=54 time=265 ms
64 bytes from a95-100-76-145.deploy.static.akamaitechno
145): icmp_seq=2 ttl=54 time=240 ms
64 bytes from a95-100-76-145.deploy.static.akamaitechno
145): icmp_seq=3 ttl=54 time=260 ms
64 bytes from a95-100-76-145.deploy.static.akamaitechno
145): icmp_seq=4 ttl=54 time=193 ms
^X64 bytes from a95-100-76-145.deploy.static.akamaitechno
```

### 4. MAC address for [www.cisco.com](http://www.cisco.com): 52:54:00:12:35:02

icmp					
No.	Time	Source	Destination	Protocol	Length
7	0.134349353	10.0.2.15	95.100.76.145	ICMP	56
8	0.399587042	95.100.76.145	10.0.2.15	ICMP	56
11	1.136288825	10.0.2.15	95.100.76.145	ICMP	56
12	1.376266474	95.100.76.145	10.0.2.15	ICMP	56
15	2.137654514	10.0.2.15	95.100.76.145	ICMP	56
16	2.397871881	95.100.76.145	10.0.2.15	ICMP	56
19	3.138696836	10.0.2.15	95.100.76.145	ICMP	56
20	3.331451643	95.100.76.145	10.0.2.15	ICMP	56
23	4.140331171	10.0.2.15	95.100.76.145	ICMP	56
24	4.333483142	95.100.76.145	10.0.2.15	ICMP	56
27	5.141228474	10.0.2.15	95.100.76.145	ICMP	56
28	5.330967709	95.100.76.145	10.0.2.15	ICMP	56

▶ Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface  
▶ Ethernet II, Src: PcsCompu\_22:46:4f (08:00:27:22:46:4f), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
▶ Destination: RealtekU\_12:35:02 (52:54:00:12:35:02)  
▶ Source: PcsCompu\_22:46:4f (08:00:27:22:46:4f)  
Type: IPv4 (0x0800)  
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 95.100.76.145  
▶ Internet Control Message Protocol

### 5. IP address for [www.google.com](http://www.google.com):

172.217.170.164

```
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.170.164
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x9d2b (40235)
▶ Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x39f1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 172.217.170.164
```



## USING WIRESHARK TO VIEW NETWORK TRAFFIC REPORT

6. MAC address for [www.google.com](http://www.google.com): 52:54:00:12:35:02

```
▶ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on i
▼ Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: RealtekU
  ▶ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▶ Source: PcsCompu_22:46:4f (08:00:27:22:46:4f)
    Type: IPv4 (0x0800)
  ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.170.164
    Internet Control Message Protocol
```

- b. What is significant about this information?

The MAC addresses of the three locations are the same which is the physical default gateway address LAN of the router but the IP addresses are different.

- c. How does this information differ from the local ping information you received in Part 1?

In part one, a ping request on a local host returns the network interface card (NIC) MAC address while a ping to a local host returns the default gateway's LAN interface MAC address.

### Reflection Question

1. **Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?** This is because for local hosts are in the same local area network and Wireshark uses ARP to resolve and get the MAC addresses while when it comes to remote hosts, the only accessible MAC address is that of default gateway interface which is attached information about the remote host.

Conclusively, this exercise has enabled me to see Wireshark capture packet traffic on the network, to be able to reduce noise on the data presented by filtering where I mostly worked on the ICMP protocol as required. I was also able to work with the ping network utility and see how the packets go through the network until they get to the target host. Wireshark displayed the logical working of the ping command where I saw the various request and reply PDU in Wireshark. I was also able to investigate the packets payload and from them I was able to acquire information to answer the questions in the exercise. I further was able to filter the request to display ARP packets and from them I was able to have an in-depth understanding of how it resolves for MAC addresses in a LAN. From pinging domain names, I was able to identify how the traffic differed as compared to just pinging IP addresses as well as noticing how DNS translates domain names to IP addresses. The activity enabled me to gain knowledge on creating ICMP inbound rules in firewall to allow my device to be pinged. Overall, this activity has equipped me with foundational knowledge when it comes to navigating, capturing, investigating and analyzing network traffic using Wireshark.