

# CYSE 301: Cybersecurity Technique and Operations

## Assignment 2: Traffic Tracing and Sniffing

### • Task A – Get started with Wireshark

This document covers the first half of the assignment #2. The second half will be released after the

complete discussion of Computer Network. Student needs to submit a report that covers both halves.

Each student needs to login into the CCIA virtual environment to complete this assignment.

### Task A: Get started with Wireshark (5 point each x 6 questions = 30 points)

In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and

Ubuntu VM are talking to each other.

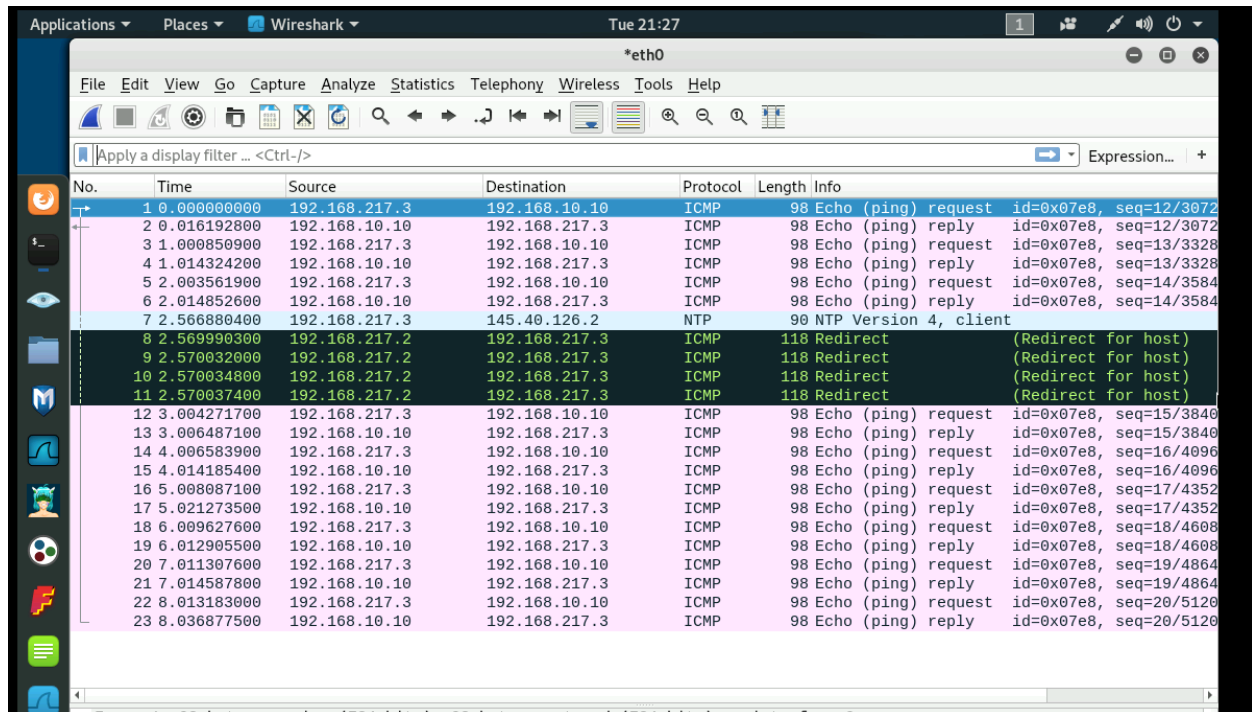
Tip: Please power on the pfsense VM and DO NOT revert to a previous checkpoint.

You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface “eth0”.
2. Open a new terminal then ping Ubuntu VM for 5 – 10 secocnds.
3. Stop capturing ( the red button on the tool bar).

Q1. How many packets are captured in total? How many packets are displayed?

**23 packets**



**Q2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).**

**22 packets were icmp**

| No. | Time        | Source        | Destination   | Protocol | Length | Info                                       |
|-----|-------------|---------------|---------------|----------|--------|--|
| 1   | 0.000000000 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=12/3072 |
| 2   | 0.016192800 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=12/3072   |
| 3   | 1.000850900 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=13/3328 |
| 4   | 1.014324200 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=13/3328   |
| 5   | 2.003561900 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=14/3584 |
| 6   | 2.014852600 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=14/3584   |
| 8   | 2.569990300 | 192.168.217.2 | 192.168.217.3 | ICMP     | 118    | Redirect (Redirect for host)               |
| 9   | 2.570032000 | 192.168.217.2 | 192.168.217.3 | ICMP     | 118    | Redirect (Redirect for host)               |
| 10  | 2.570034800 | 192.168.217.2 | 192.168.217.3 | ICMP     | 118    | Redirect (Redirect for host)               |
| 11  | 2.570037400 | 192.168.217.2 | 192.168.217.3 | ICMP     | 118    | Redirect (Redirect for host)               |
| 12  | 3.004271700 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=15/3840 |
| 13  | 3.006487100 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=15/3840   |
| 14  | 4.006583900 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=16/4096 |
| 15  | 4.014185400 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=16/4096   |
| 16  | 5.008087100 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=17/4352 |
| 17  | 5.021273500 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=17/4352   |
| 18  | 6.009627600 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=18/4608 |
| 19  | 6.012905500 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=18/4608   |
| 20  | 7.011307600 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=19/4864 |
| 21  | 7.014587800 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=19/4864   |
| 22  | 8.013183000 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x07e8, seq=20/5120 |
| 23  | 8.036877500 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x07e8, seq=20/5120   |

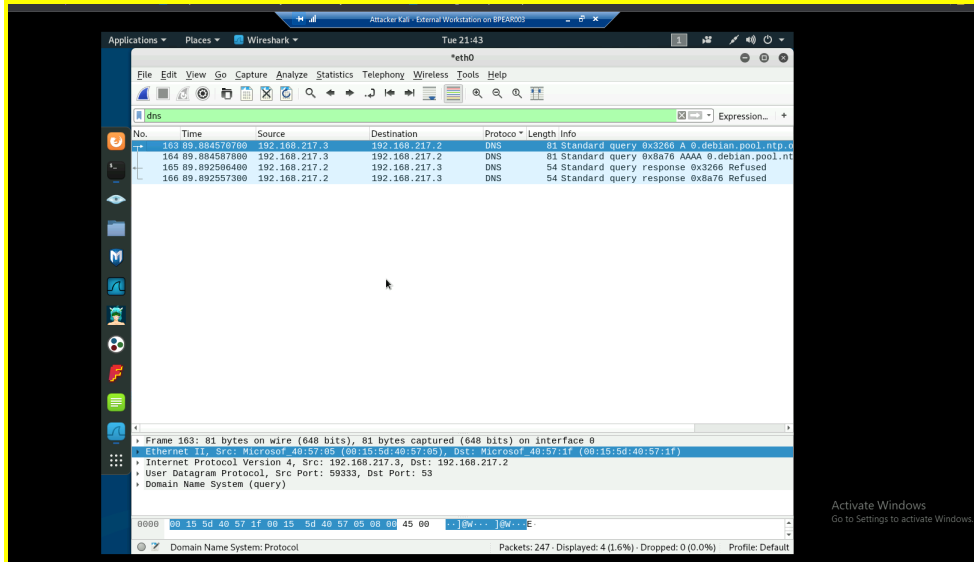
**Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?**

| No. | Time         | Source        | Destination   | Protocol | Length | Info                                 |
|-----|--------------|---------------|---------------|----------|--------|--------------------------------------|
| 13  | 15.926326800 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=1 |
| 14  | 15.940550100 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=1   |
| 15  | 16.928349700 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=2 |
| 16  | 16.933537200 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=2   |
| 17  | 17.930172100 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=3 |
| 18  | 17.939535300 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=3   |
| 19  | 18.931992600 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=4 |
| 20  | 18.935669000 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=4   |
| 21  | 19.934458100 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=5 |
| 22  | 19.942816000 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=5   |
| 23  | 20.930631500 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=6 |
| 24  | 20.941201500 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=6   |
| 25  | 21.937736300 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=7 |
| 26  | 21.948377000 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=7   |
| 27  | 22.939888200 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=8 |
| 28  | 22.948001600 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=8   |
| 29  | 23.943641100 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=9 |
| 30  | 23.948262900 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=9   |
| 31  | 24.944944900 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=1 |
| 32  | 24.950322900 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=1   |
| 33  | 25.946862800 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=1 |
| 34  | 25.950098900 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=1   |
| 35  | 26.948086500 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=1 |
| 36  | 26.949915800 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=1   |
| 37  | 27.949548800 | 192.168.217.3 | 192.168.10.10 | ICMP     | 98     | Echo (ping) request id=0x0893, seq=1 |
| 38  | 27.953808400 | 192.168.10.10 | 192.168.217.3 | ICMP     | 98     | Echo (ping) reply id=0x0893, seq=1   |

Frame 18: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 Ethernet II, Src: Microsof\_40:57:1f (00:15:5d:40:57:1f), Dst: Microsof\_40:57:05 (00:15:5d:40:57:05)  
 Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3  
 Internet Control Message Protocol

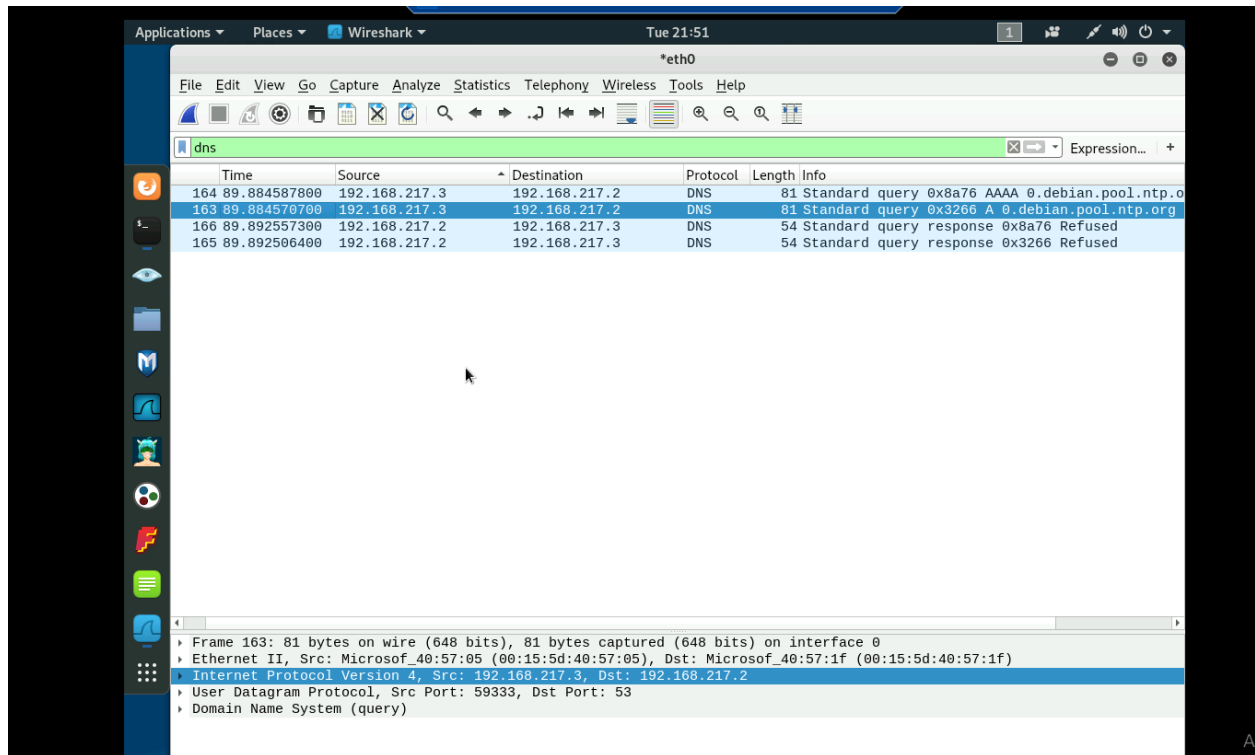
Source 192.168.10.10 destination 192.168.217.3 seq= 3/768 98 bytes

Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?



4 packets

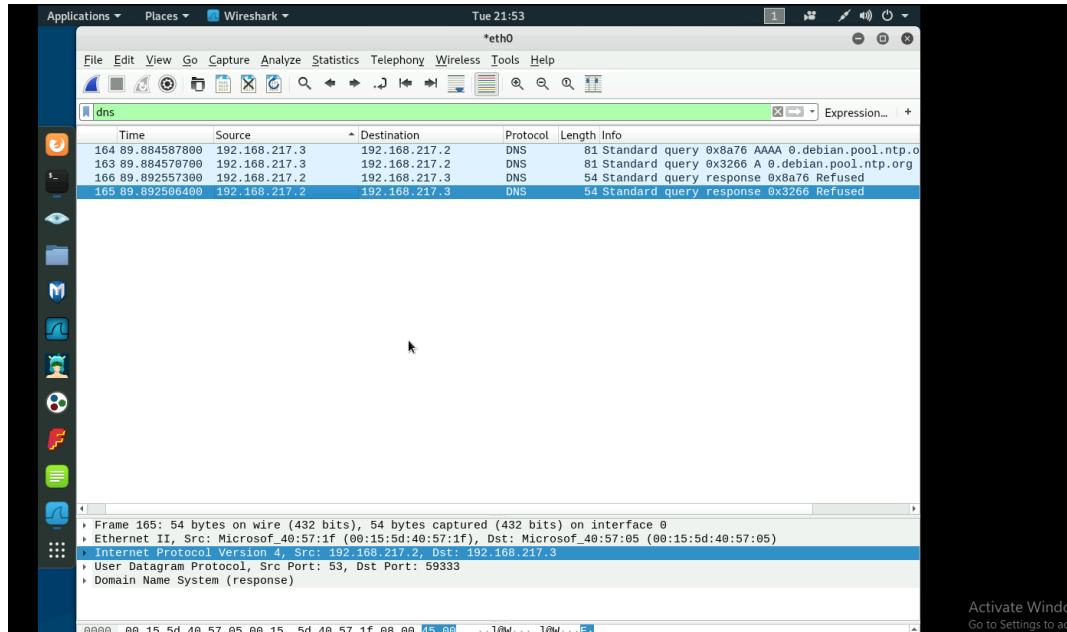
**Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.**



**0.debian.pool.ntp.org**

**Source ip =192.168.217.3 port 59333, destination IP 192.168.217.2 port 53**

**Q6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP, and port number? What is the message replied from the DNS server?**



**Source ip= 192.168.217.2 port 53**

**Desitainton ip = 192.168.217.3 port 59333**

**Message replied = REFUSED**