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.*

Ian Waweru

01151080

External Attacker Kali (192.168.217.3)

pFsense Firewall

WAN: LAN:
192.168.217.2 192.168.10.2 Ubuntu 64 bit VM

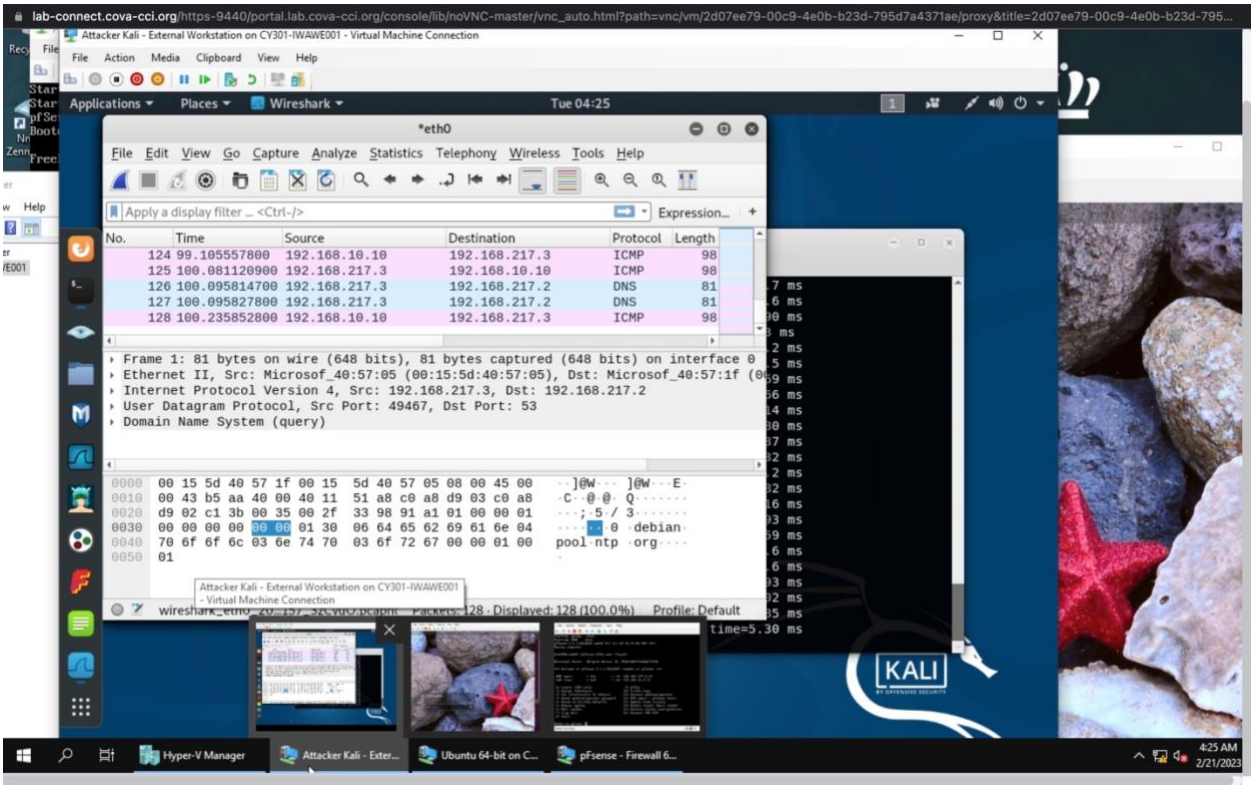
(192.168.10.10)

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 seocnds.
3. **Stop capturing (the red button on the tool bar).**

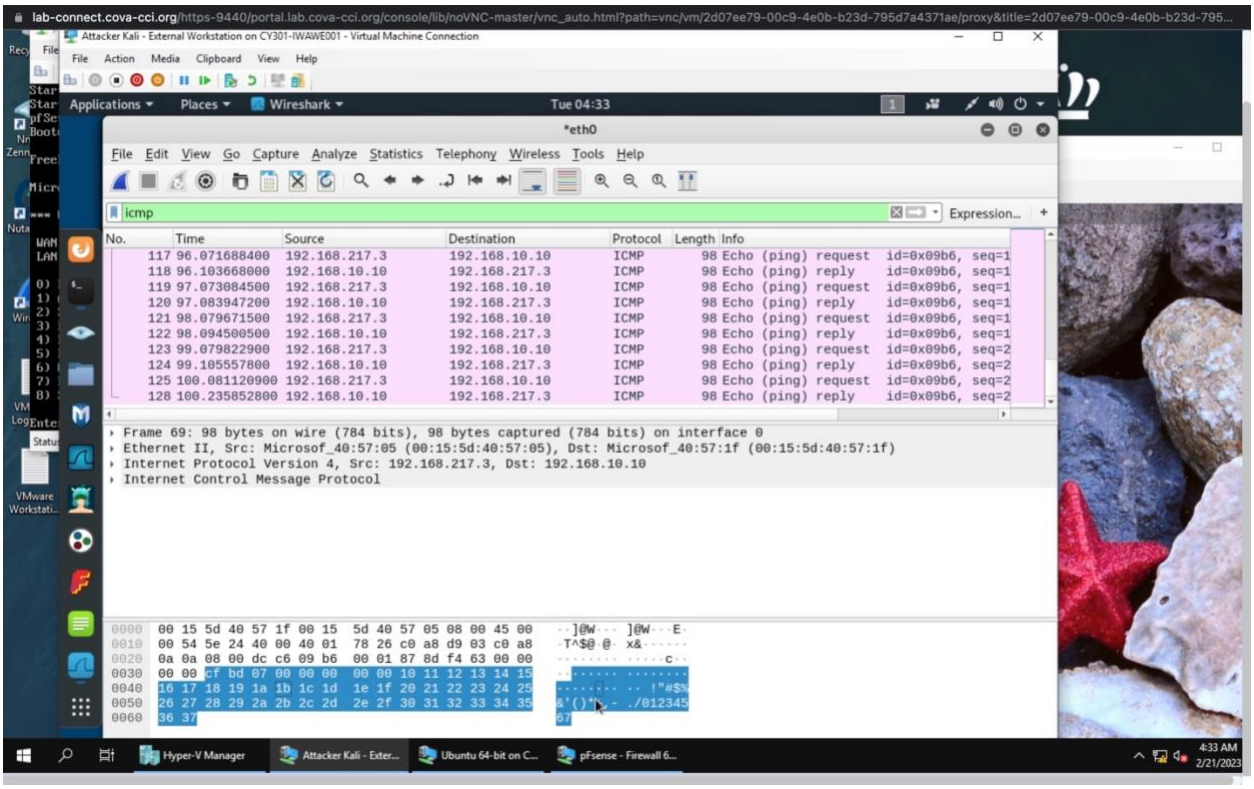
Now, answer the following questions. You need to provide a screenshot that contains the answers to each question.

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



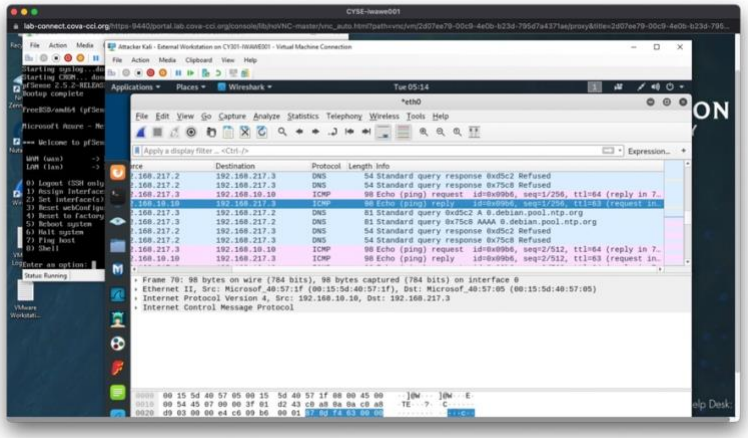
In total I had 128 packets displayed

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



It starts at 69 and ends at 129. The image shows ICMP packets and there is a total of 60 packets.

Q3. Select an Echo (replay) 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?



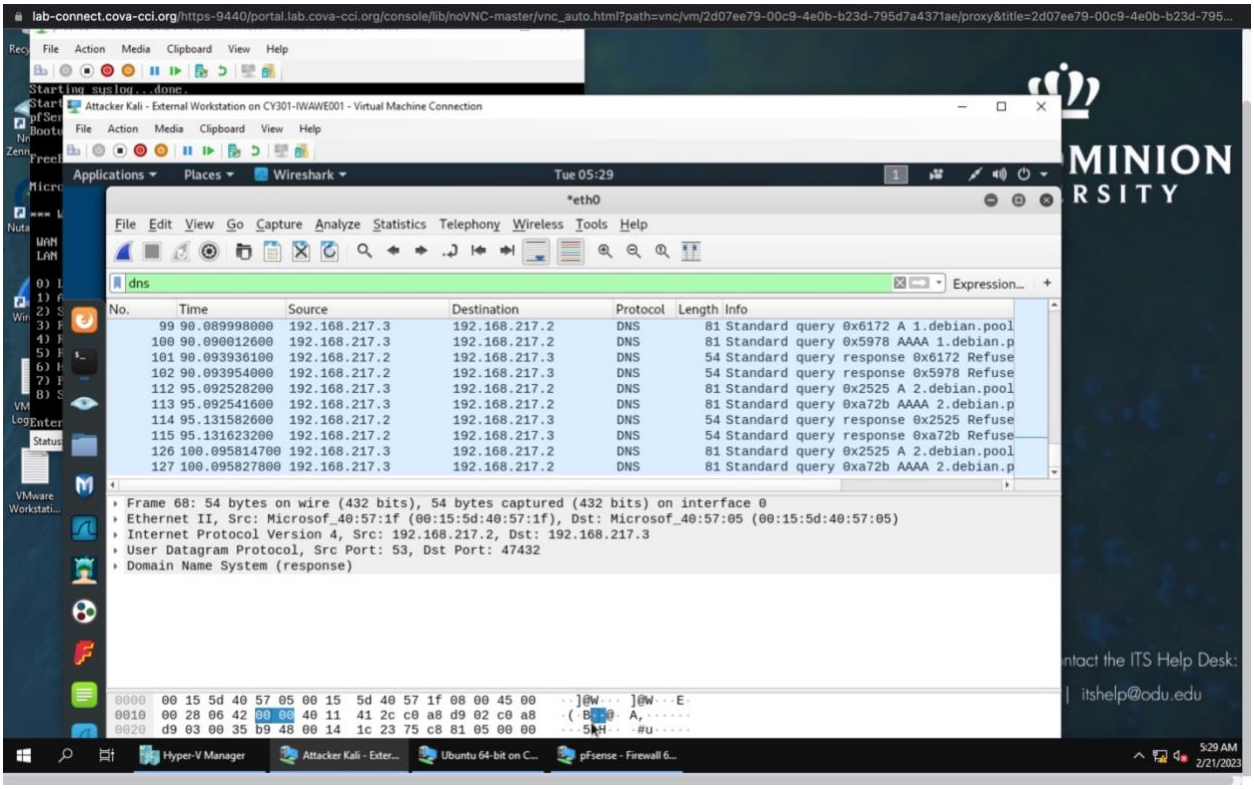
1) Source IP: 192.168.10.10 Destinations IP: 192.168.217.3

2) SEQ: 1/256

3) Size 98 in length

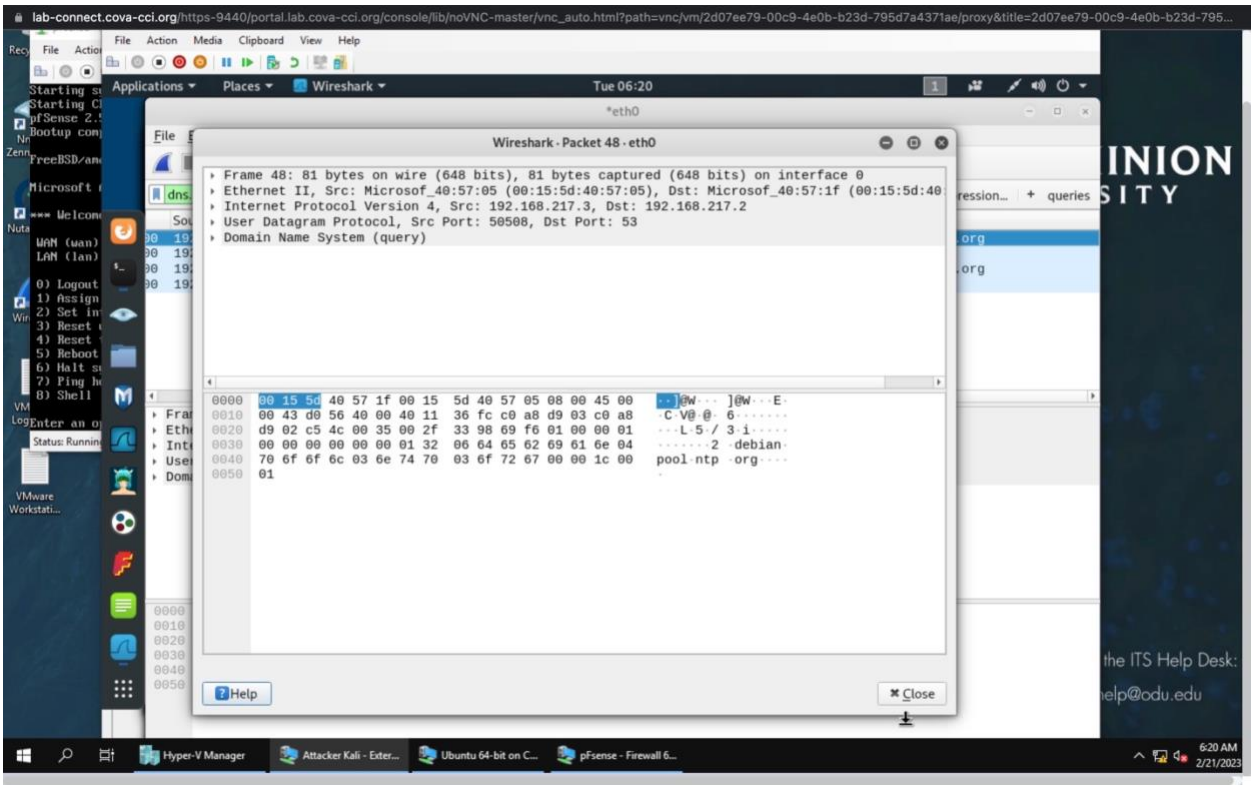
4) Time: 80.047664100

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



There are a total of 127 DNS 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.**



1) Domain name (query)

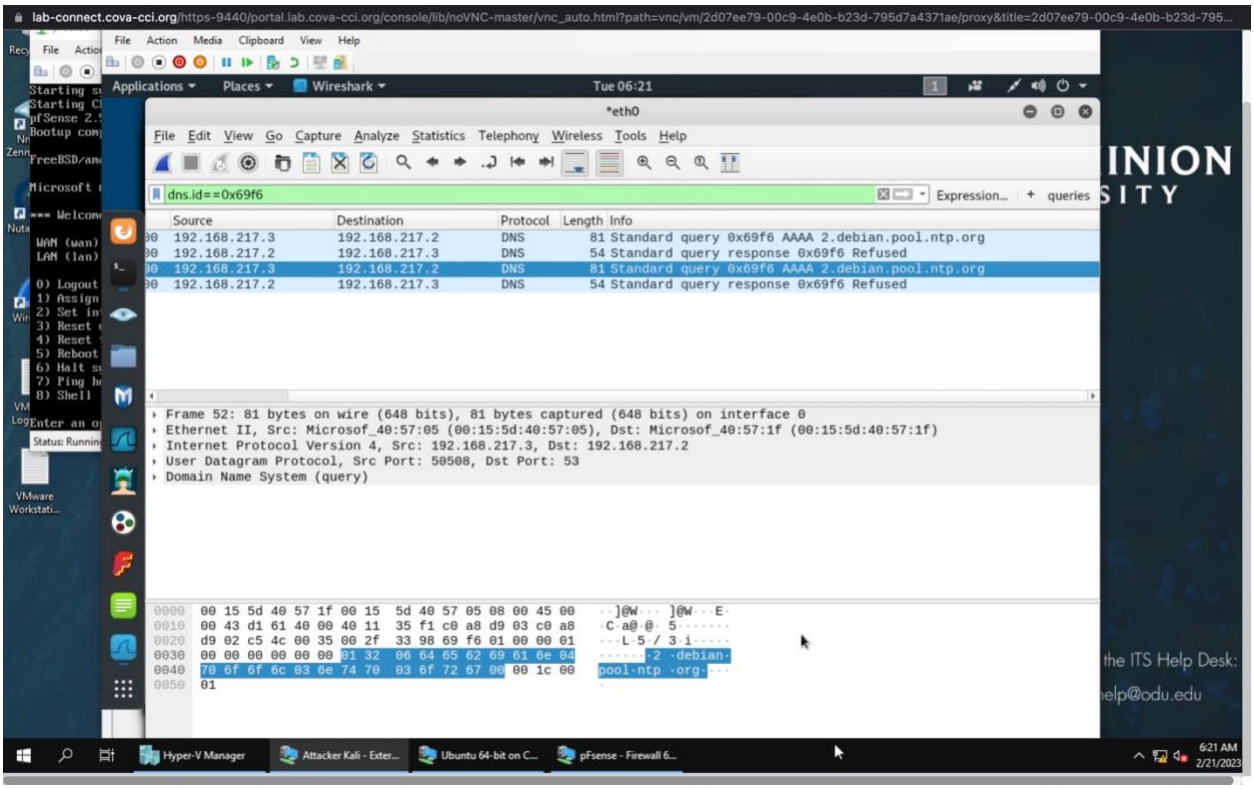
2)Source IP: 192.168.217.3

3) Source port: 50508

4) Destination IP: 192.168.217.2

5) Destination 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?



1)Source IP: 192.168.217.3

2)Source port: 50508

3)Destination IP: 192.168.217.2

4)Destination Port:53

5)Message replied from the DNS server contains the Ip address of Debian.pool.ntp.org