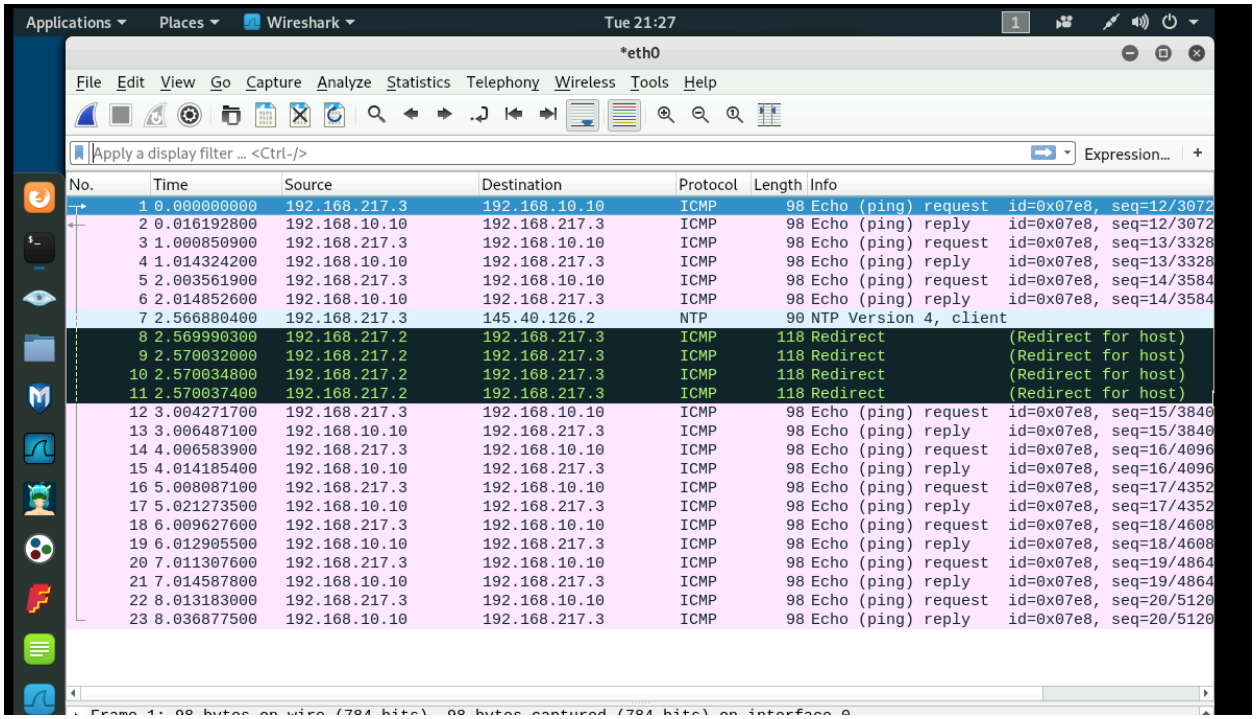
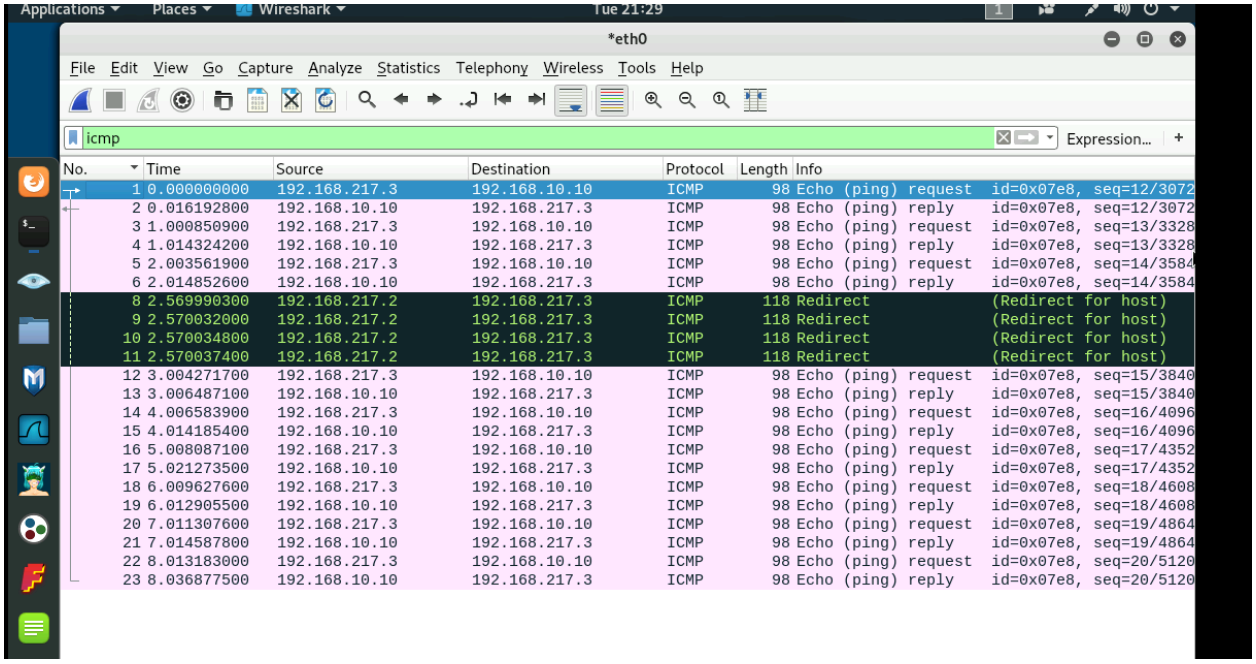
CYSE 301: Cybersecurity Technique and Operations
Assignment 2: Traffic Tracing and Sniffing
• Task A – Get started with Wireshark
This document covers the first half of the assignment #2. The second half will be released after the
complete discussion of Computer Network. Student needs to submit a report 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 seocnds.
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

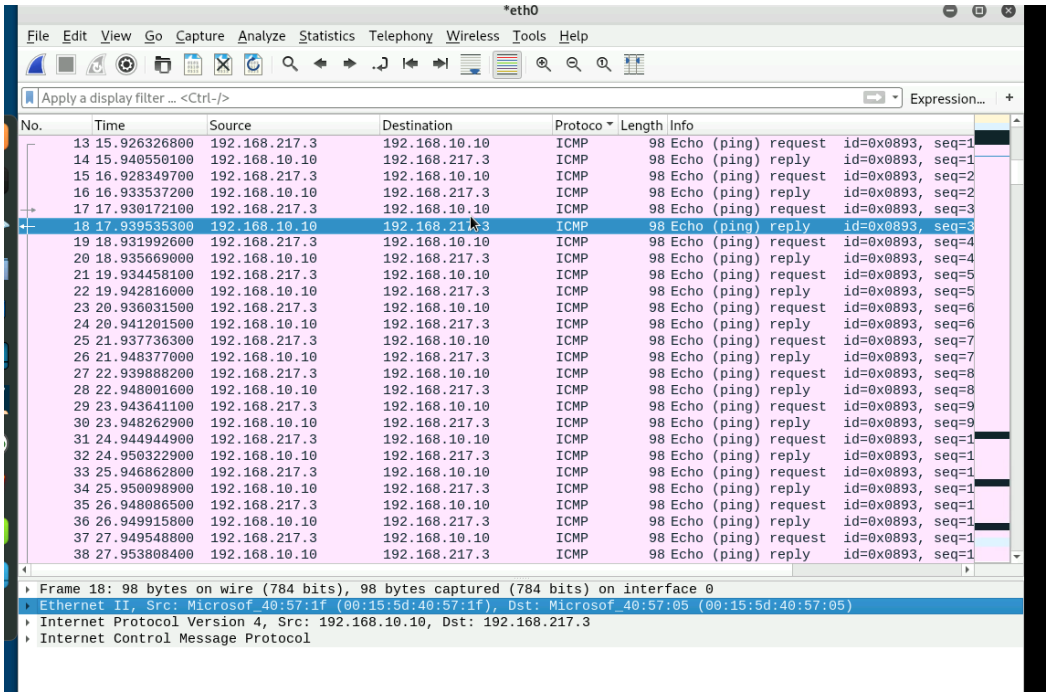


Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).

22 packets were icmp

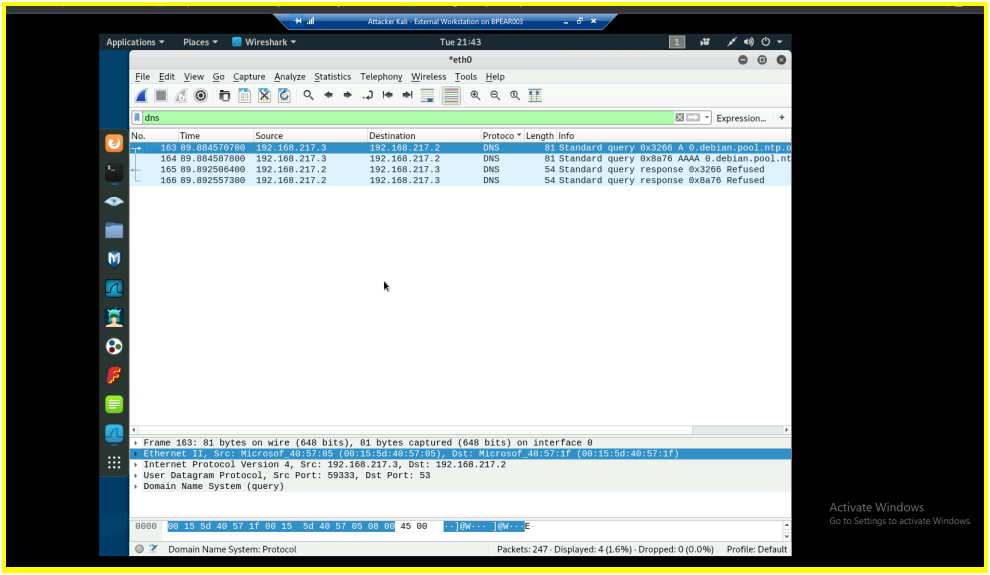


Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?



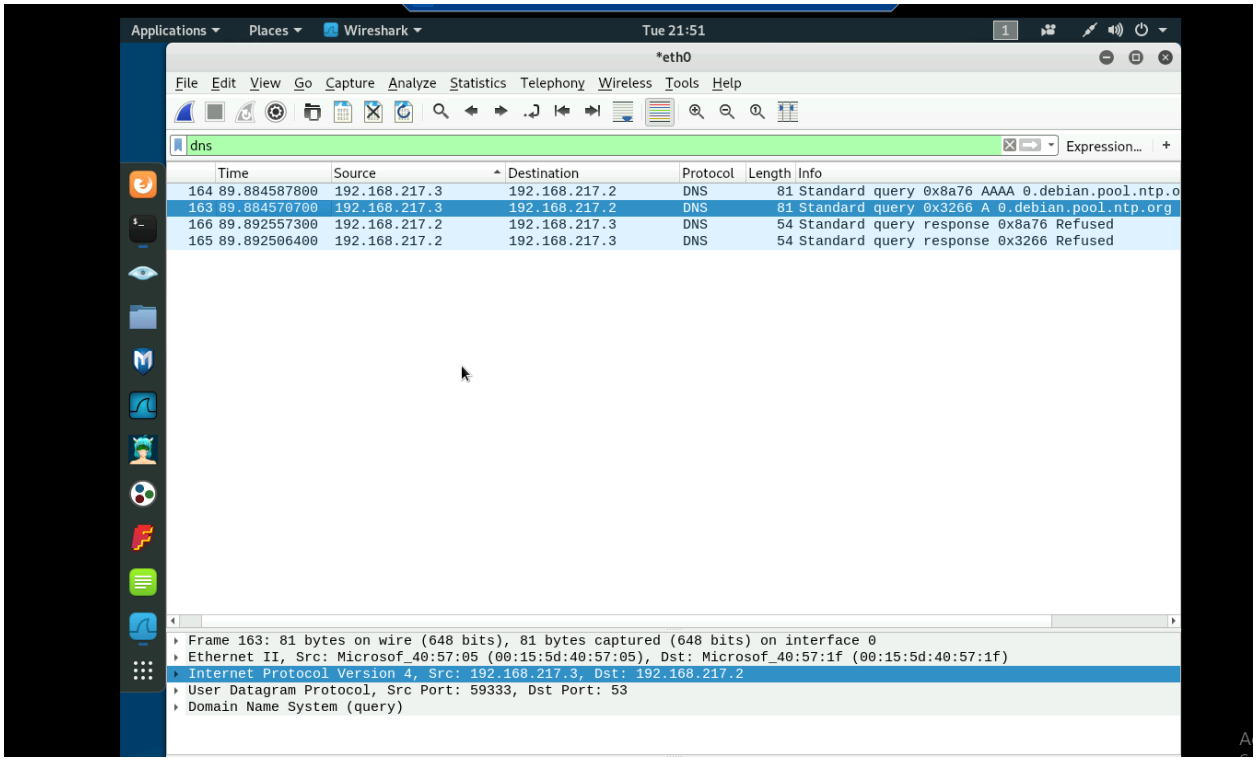
Source 192.168.10.10 desnitaion 192.168.217.3 seq= 3/768 98 bytes

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



4 packets

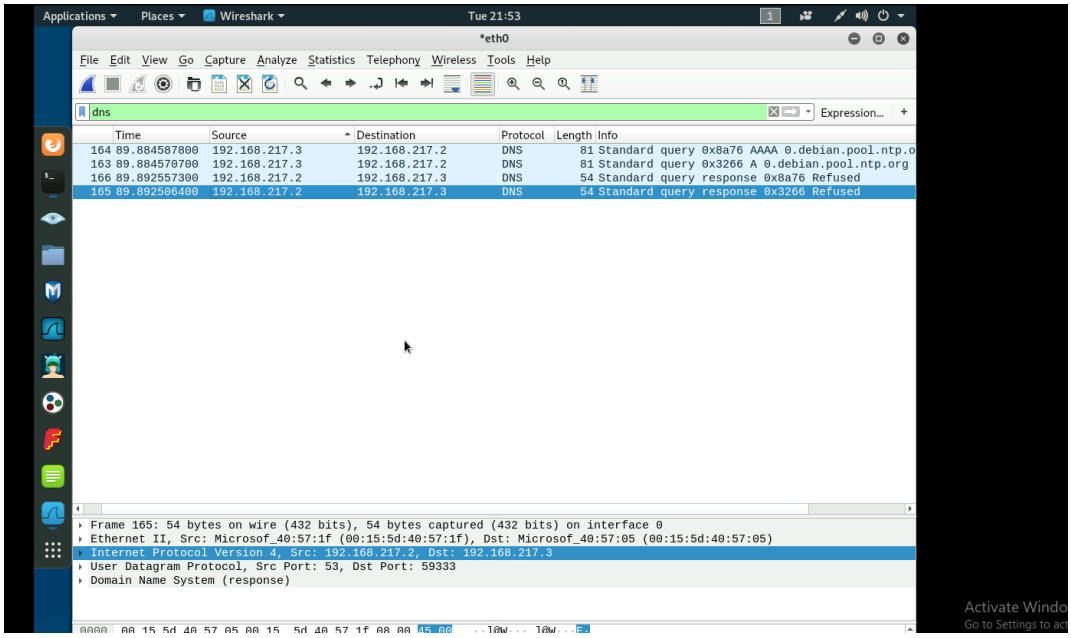
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.



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