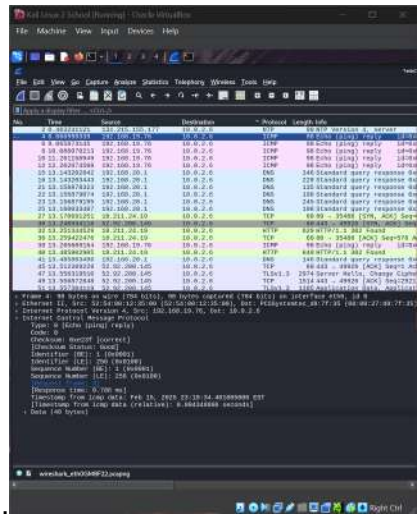
CYSE301: Cybersecurity Technique and Operations

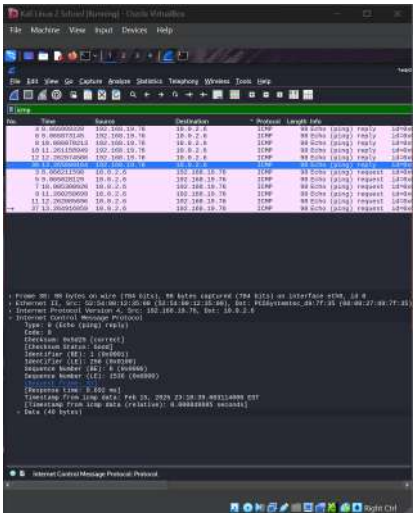
Assignment 2: Traffic Tracing and Sniffing

By George Trey Smith

Q1. 

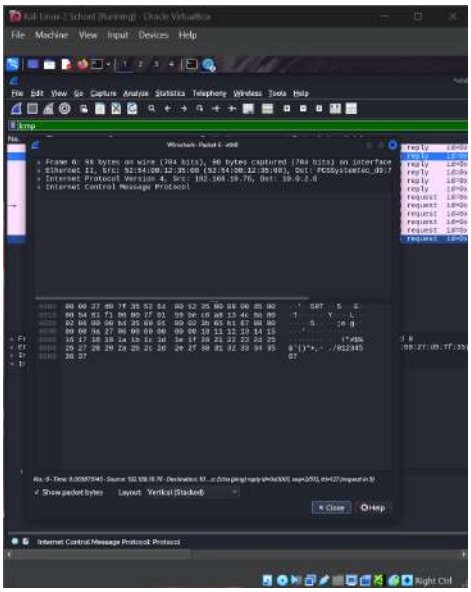
How many packets are captured in total? How many packets are displayed?

6 packets

Q2. 

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

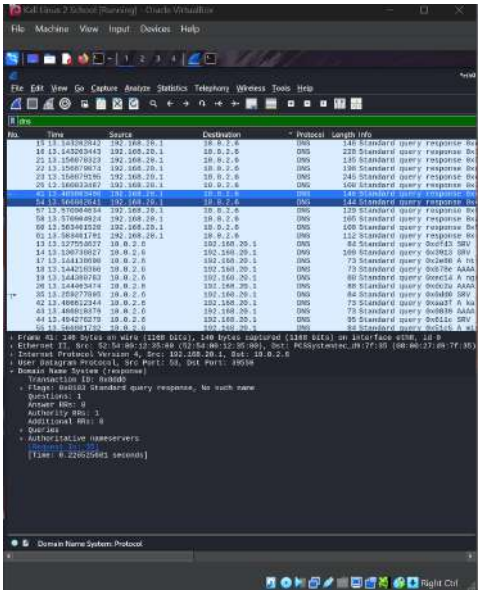
12 packets

Q3. 

Select an Echo (replay) message from the list. What are the source and destination IPs of this

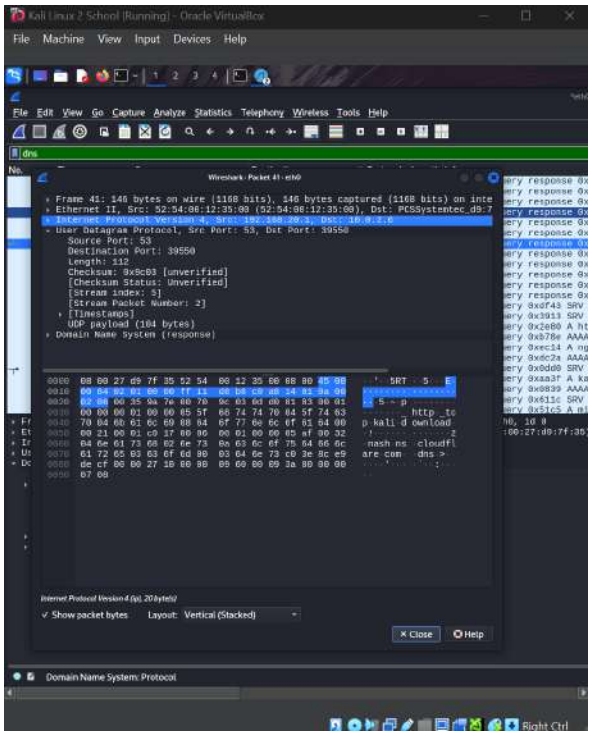
Packet? What are the sequence number and the size of the data? What is the response time?

Src: 192.168.19.76 | Dest: 10.0.2.6 | Sequence number: 1 (0x0001) 256 (0x0100) | RT: 0.788 ms

Q4. 

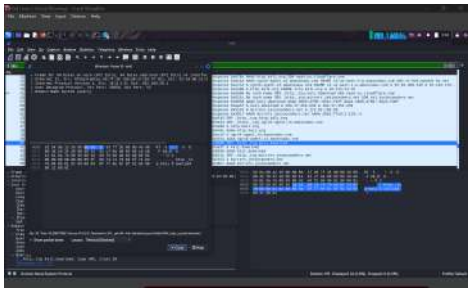
Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

The total number of DNS packets displayed within the capture.

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.

Http.tcp.kali.download | Src: 192.168.20.1 : PortNum: 53 | Dest: 10.0.2.6 : PortNum: 39550 |

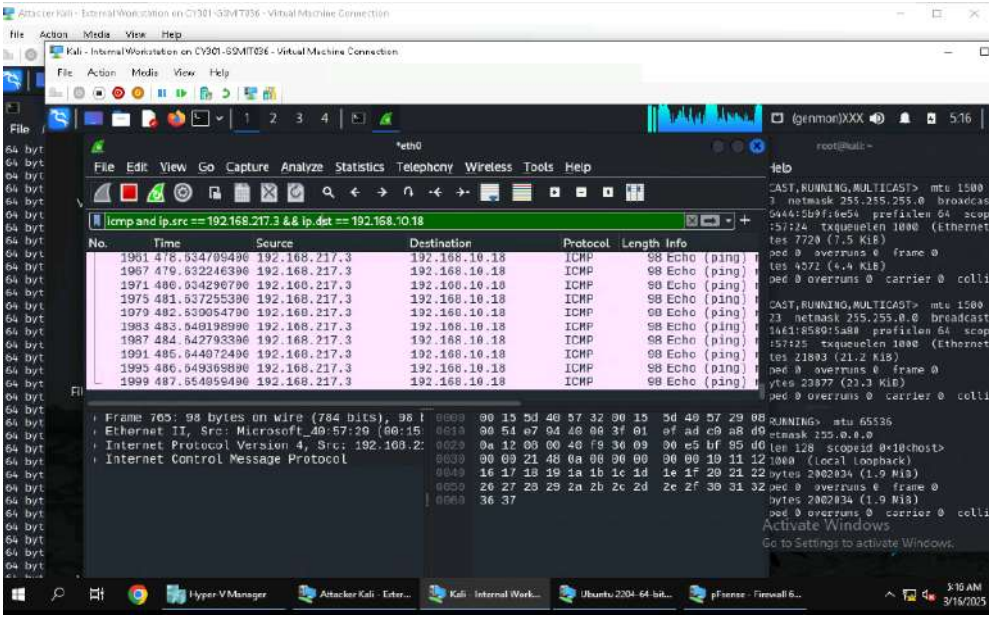
Q6. 

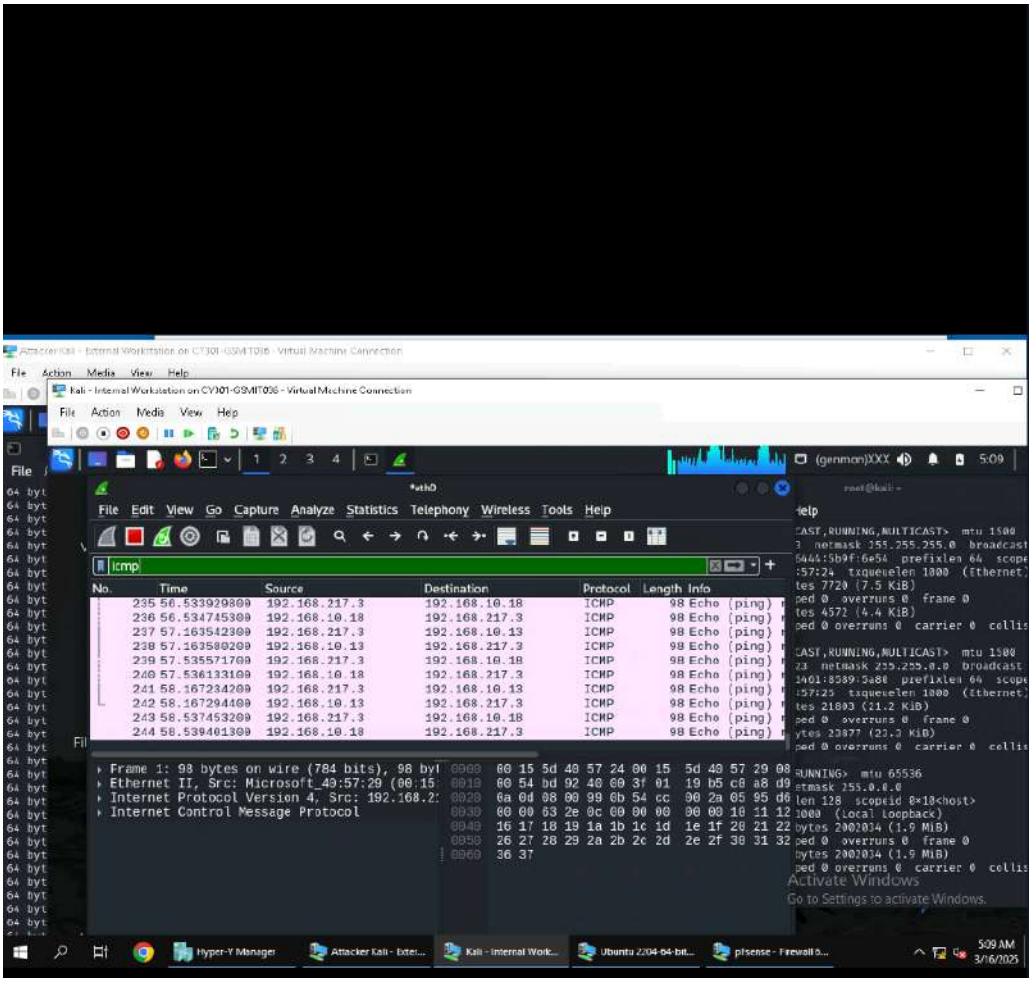
Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

Src: 10.0.2.6 : PortNum: 39550 | Dest: 192.168.20.1 : PortNum: 53 | Answer RRs: 0

Task B. Sniffing

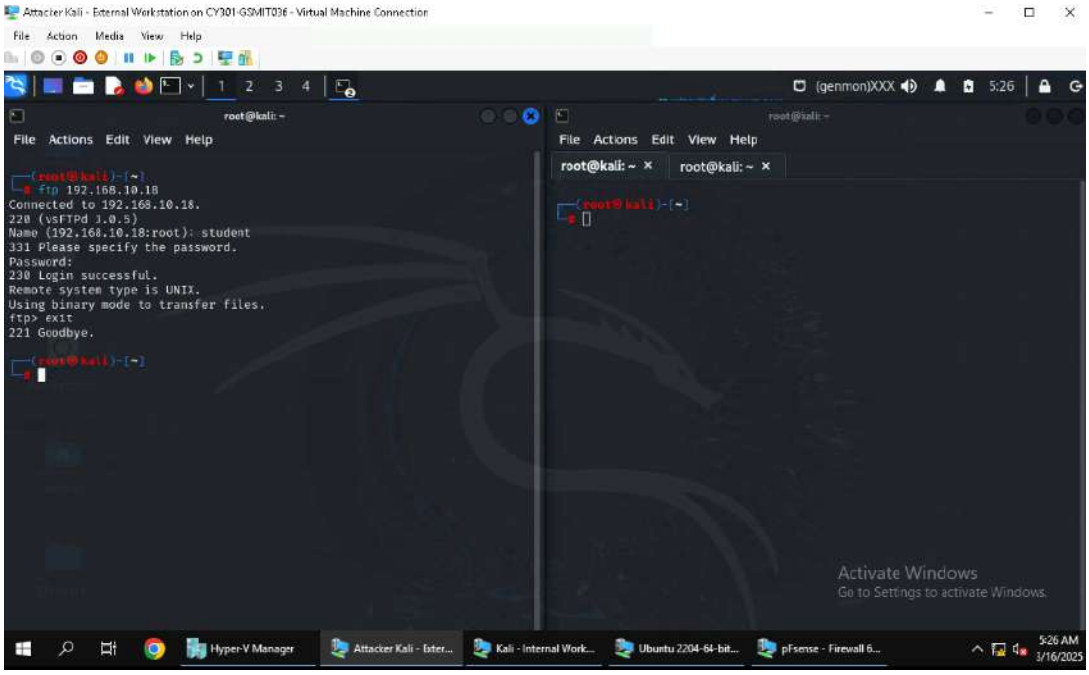
Q1.



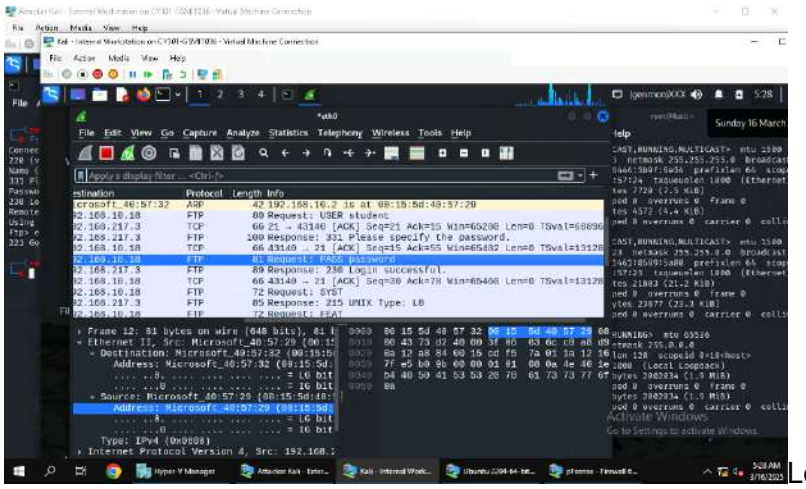


a. Apply the proper display or capture filter in Wireshark on the internal Kali VM to show active ICMP traffic.

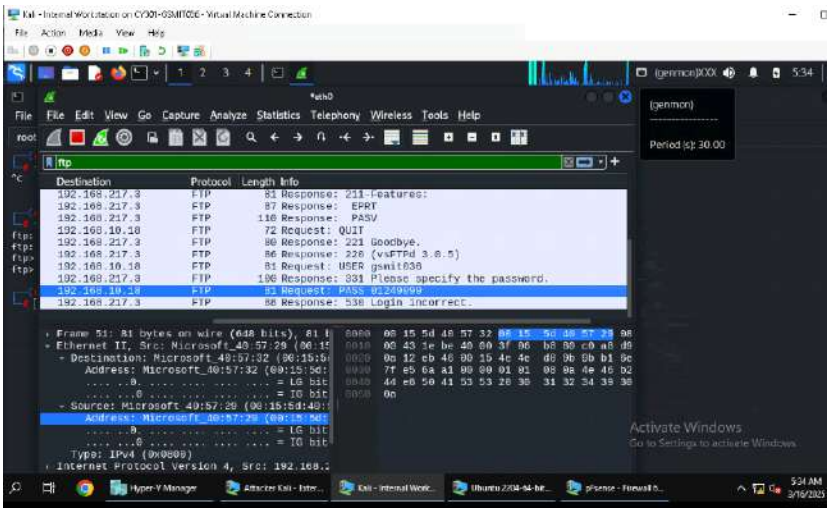
b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM

Q2. 

a. ^^

b.  Looked at the password field in the packet request through wireshark

C.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
Destination Protocol Length Info
192.168.217.3 FTP 81 Response: 211-Features:
192.168.217.3 FTP 87 Response: EPRT
192.168.217.3 FTP 116 Response: PASV
192.168.10.18 FTP 72 Request: QUIT
192.168.217.3 FTP 80 Response: 221 Goodbye.
192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.5)
192.168.10.18 FTP 81 Request: USER gsmit030
192.168.217.3 FTP 106 Response: 331 Please specify the password.
192.168.10.18 FTP 81 Request: PASS 01249999
192.168.217.3 FTP 88 Response: 530 Login incorrect.
(genmon)
Period [s]: 30.00
Activate Windows