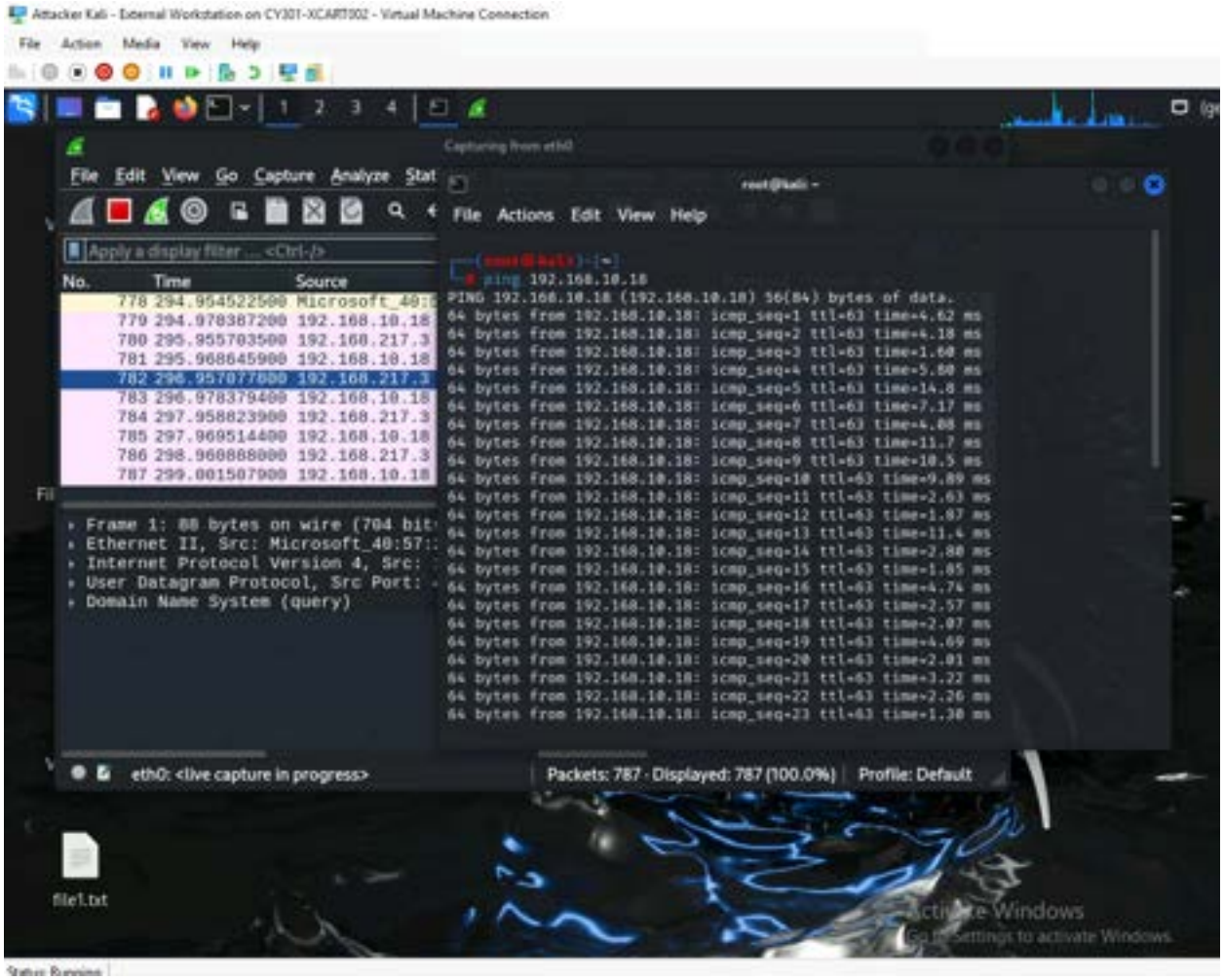
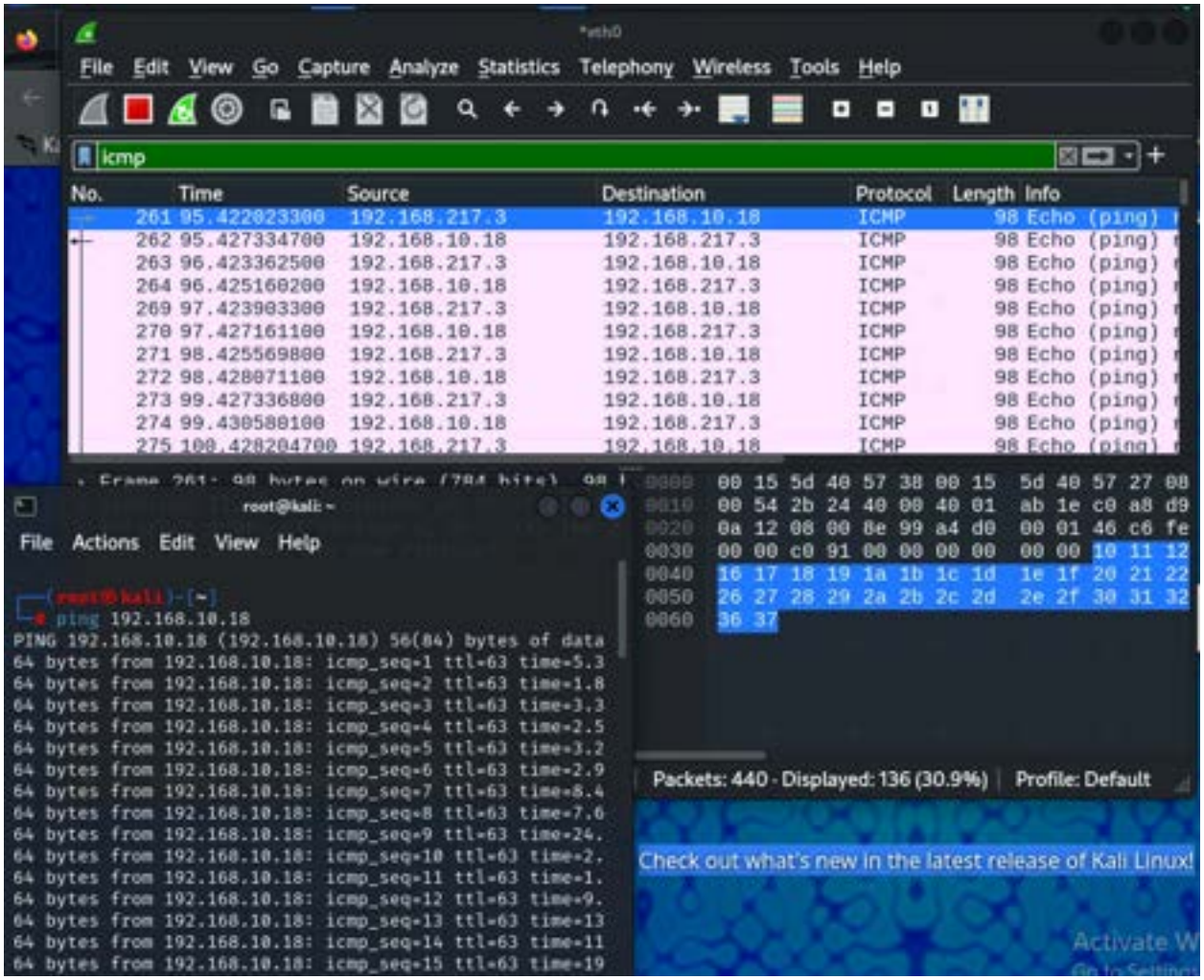
# Task A

Q1. (5 pts) How many packets are captured in total? How many packets are displayed?



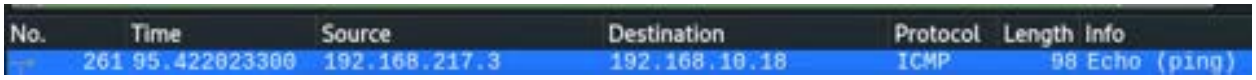

787 total and 787 displayed - Counting.

Q2. (5 pts) Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).



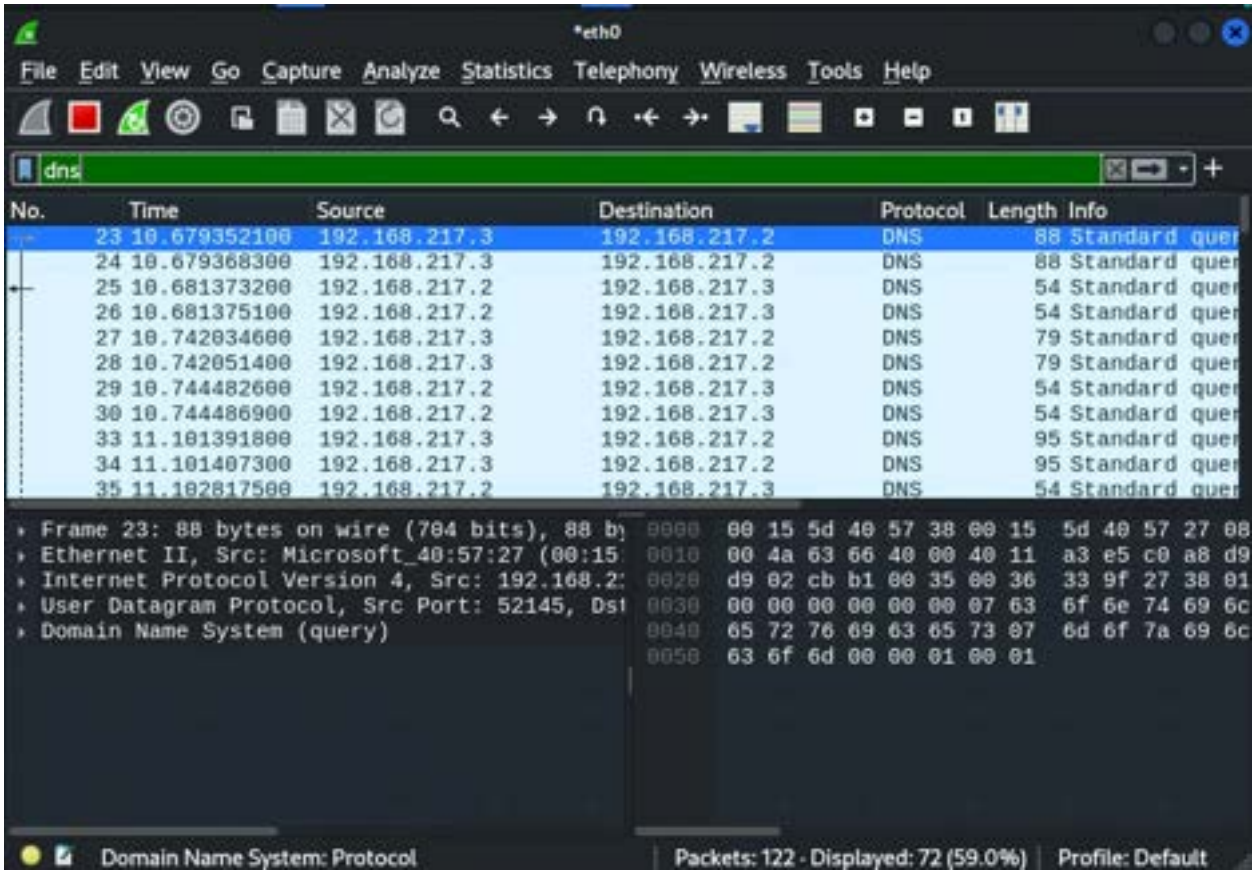

440 total, 136 displayed - Counting

Q3. (5 pts) 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?




Source and destination for “No.261” is: 192.168.217.3 and 192.168.10.18.
Response time is: 95.422
Size: 98

Q4. (5 pts) Apply “DNS” as a display filter in Wireshark. How many packets are displayed?



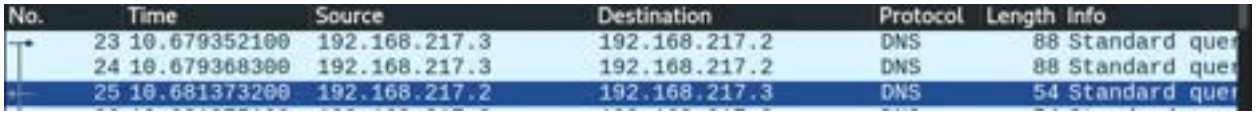

72 is displayed and counting.

Q5. (5 pts) 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?




The domain name it's trying to solve is 0x2738.
Source IP: 192.168.217.3 , No. 23
Destination: 192.168.217.2 , No. 23

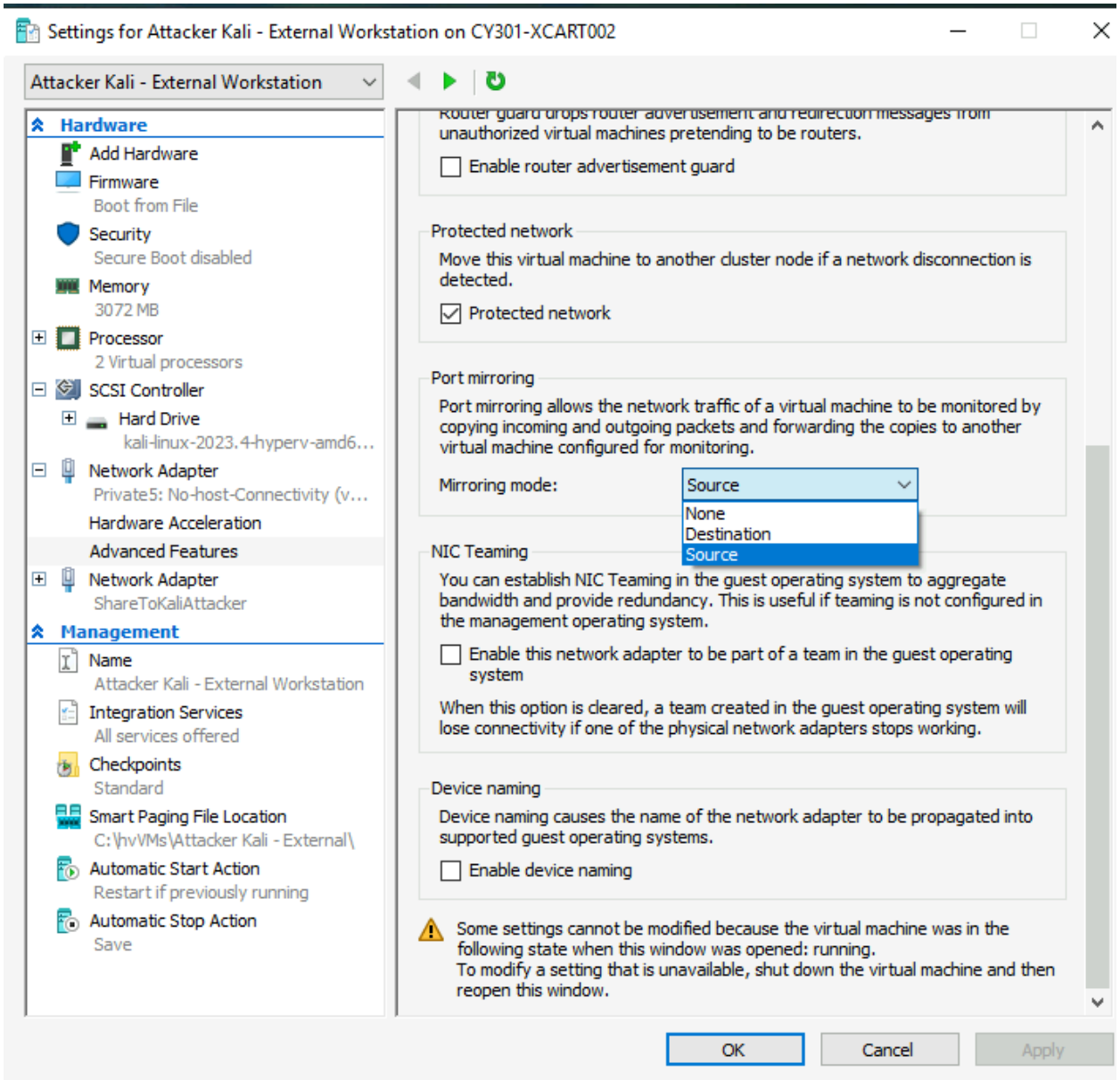
Q6. (5 pts) Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

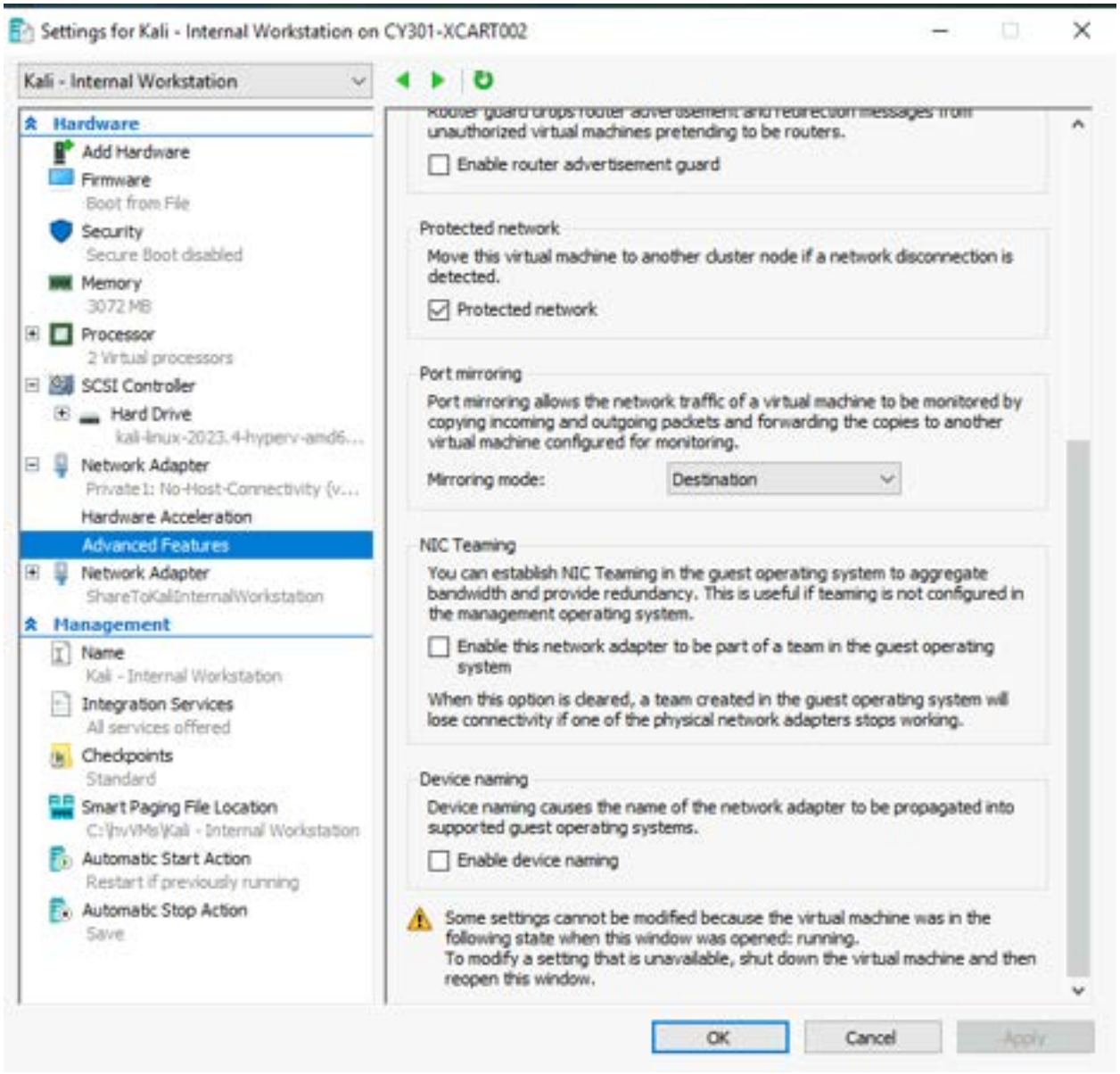


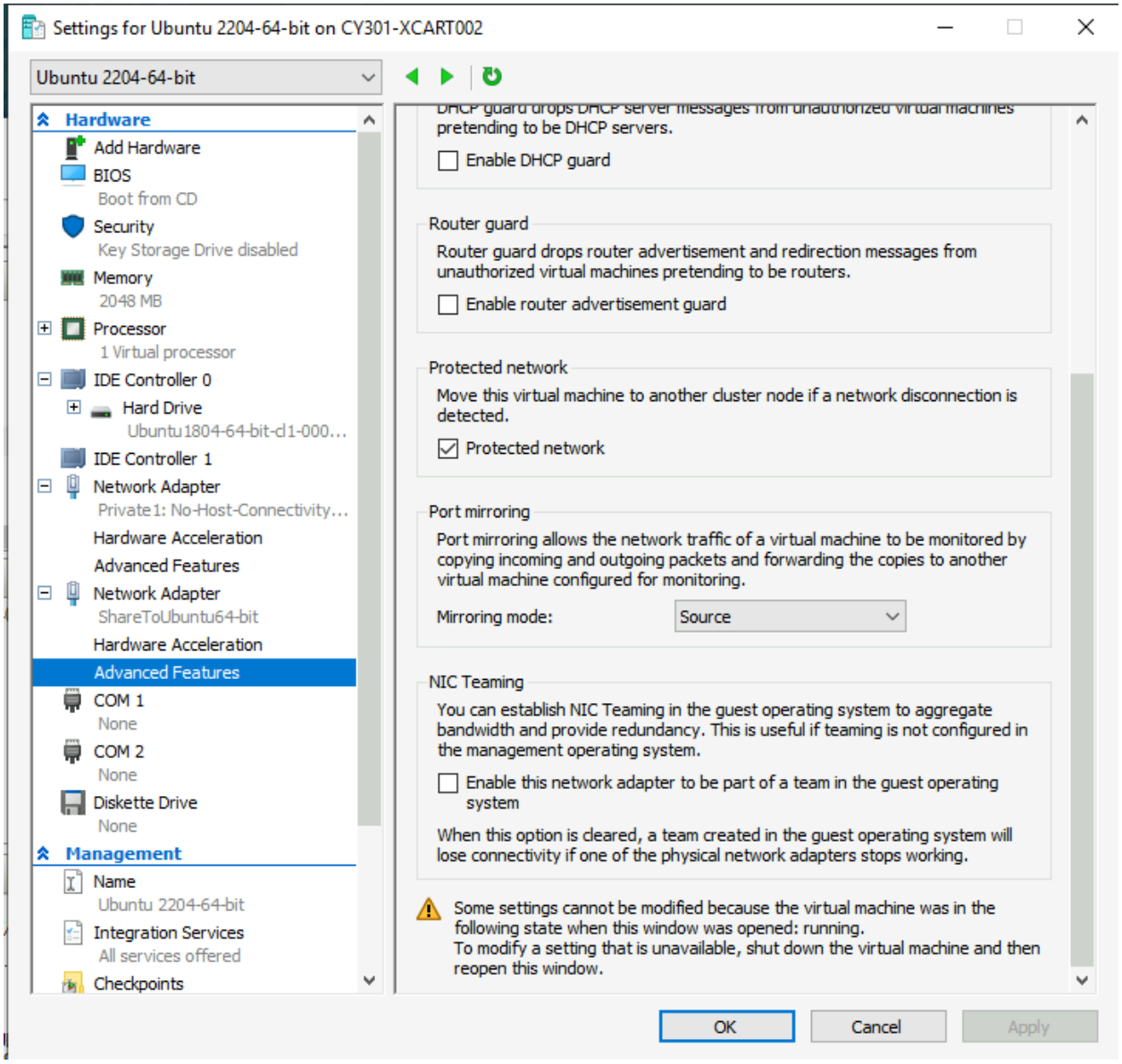
```
▸ Queries
  [Response In: 25]
```

Source IP and PN:  192.168.217.2, No.25
Destination and PN: 192.168.217.3, No.25

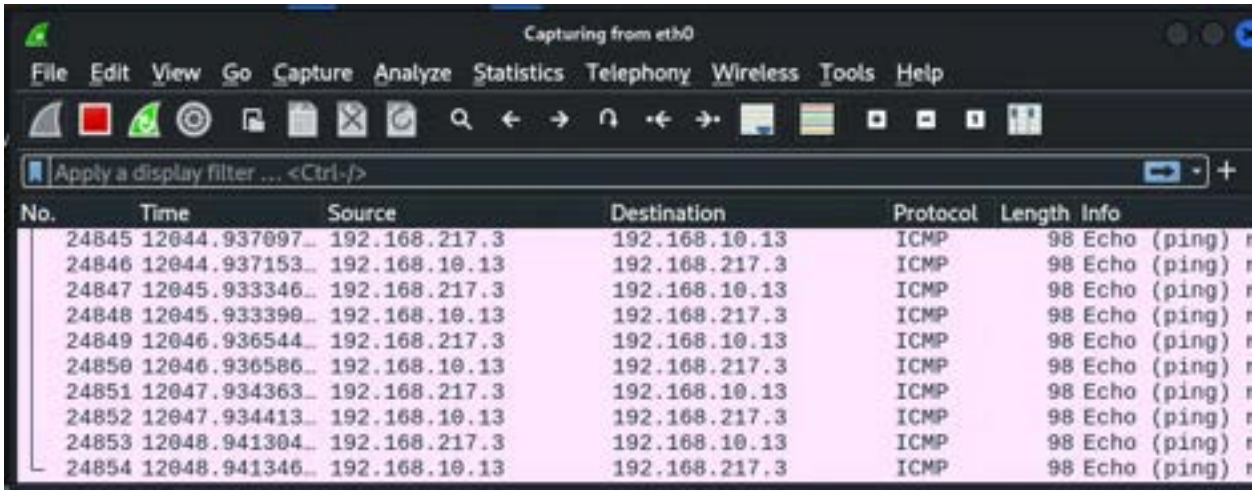
# Task B

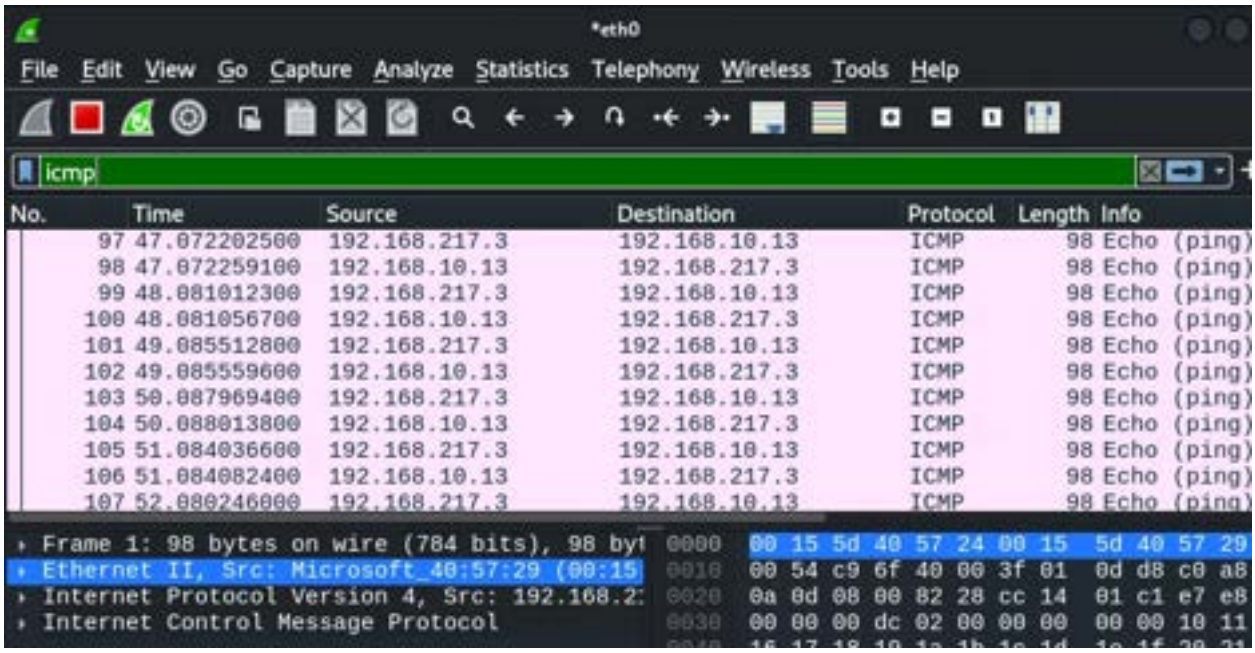



Settings for Kali - Internal Workstation on CY301-XCART002
Kali - Internal Workstation
Hardware
Add Hardware
Firmware
Boot from File
Security
Secure Boot disabled
Memory
3072 MB
Processor
2 Virtual processors
SCSI Controller
Hard Drive
kali-linux-2023.4-hyperv-amd6...
Network Adapter
Private1: No-Host-Connectivity (v...
Hardware Acceleration
Advanced Features
Network Adapter
ShareToKaliInternalWorkstation
Management
Name
Kali - Internal Workstation
Integration Services
All services offered
Checkpoints
Standard
Smart Paging File Location
C:\hvVMs\Kali - Internal Workstation
Automatic Start Action
Restart if previously running
Automatic Stop Action
Save
unauthorized virtual machines pretending to be routers.
Enable router advertisement guard
Protected network
Move this virtual machine to another cluster node if a network disconnection is detected.
Protected network
Port mirroring
Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.
Mirroring mode:
Destination
NIC Teaming
You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.
Enable this network adapter to be part of a team in the guest operating system
When this option is cleared, a team created in the guest operating system will lose connectivity if one of the physical network adapters stops working.
Device naming
Device naming causes the name of the network adapter to be propagated into supported guest operating systems.
Enable device naming
Some settings cannot be modified because the virtual machine was in the following state when this window was opened: running.
To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.
OK
Cancel
Apply

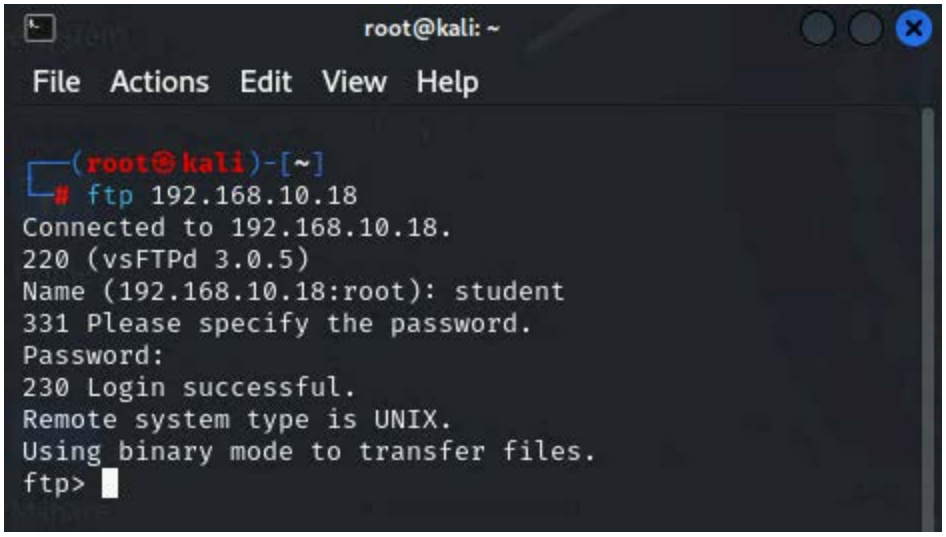



1. Sniff ICMP traffic (5 + 5 + 5 + 15 = 30 points)



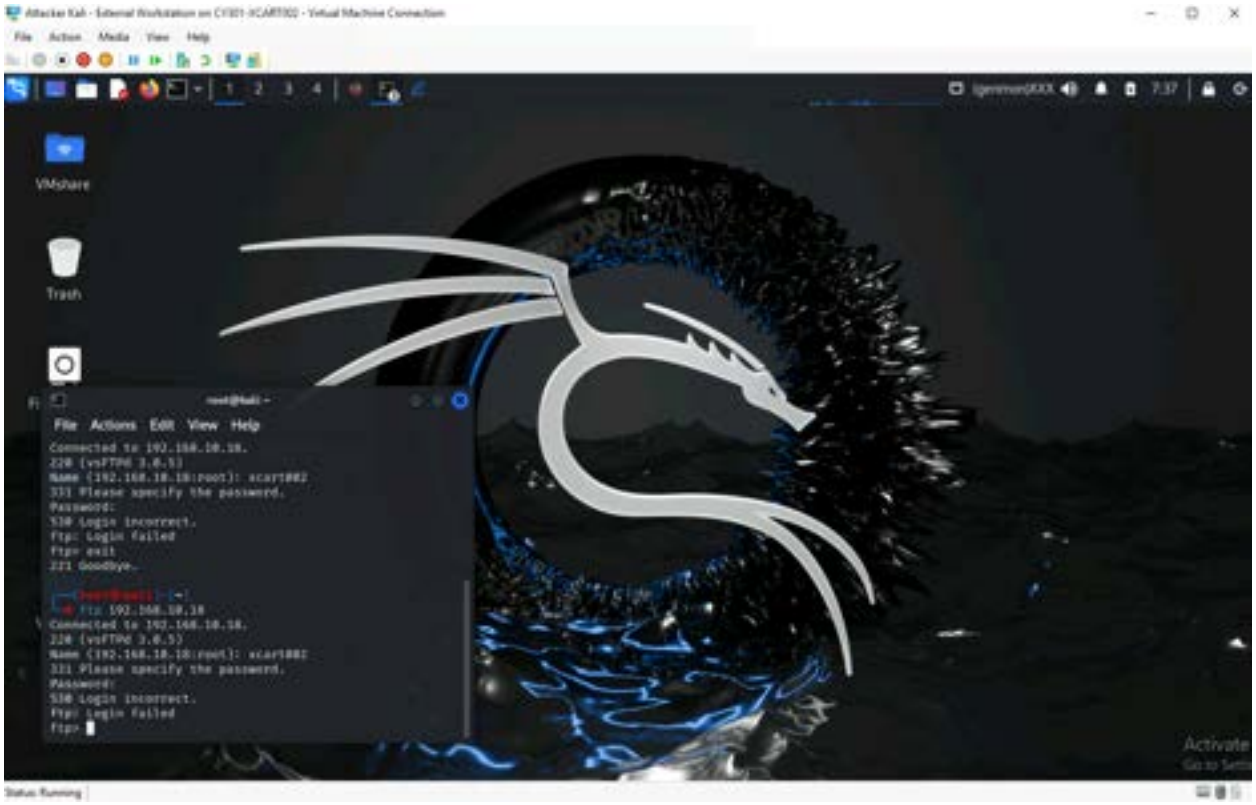

2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)
   a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu VM]. The username for the FTP server is student, and the password is password. You can follow the steps below to access the FTP server.




Unfortunately, Internal Kali, the attacker, is also sniffing into the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to take a screenshot and explain how you found the Password.

N/A

After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to re-access the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is Internal Kali.


File Action Media View Help
VMshare
Trash
File Actions Edit View Help
Connected to 192.168.10.10.
220 (vsFTPd 3.0.5)
Name (192.168.10.10:root): scart002
331 Please specify the password.
Password:
530 Login incorrect.
Ftp: Login failed
ftp> exit
221 Goodbye.
ftp 192.168.10.10
Connected to 192.168.10.10.
220 (vsFTPd 3.0.5)
Name (192.168.10.10:root): scart002
331 Please specify the password.
Password:
530 Login incorrect.
Ftp: Login failed
ftp>
Activate
Status: Running