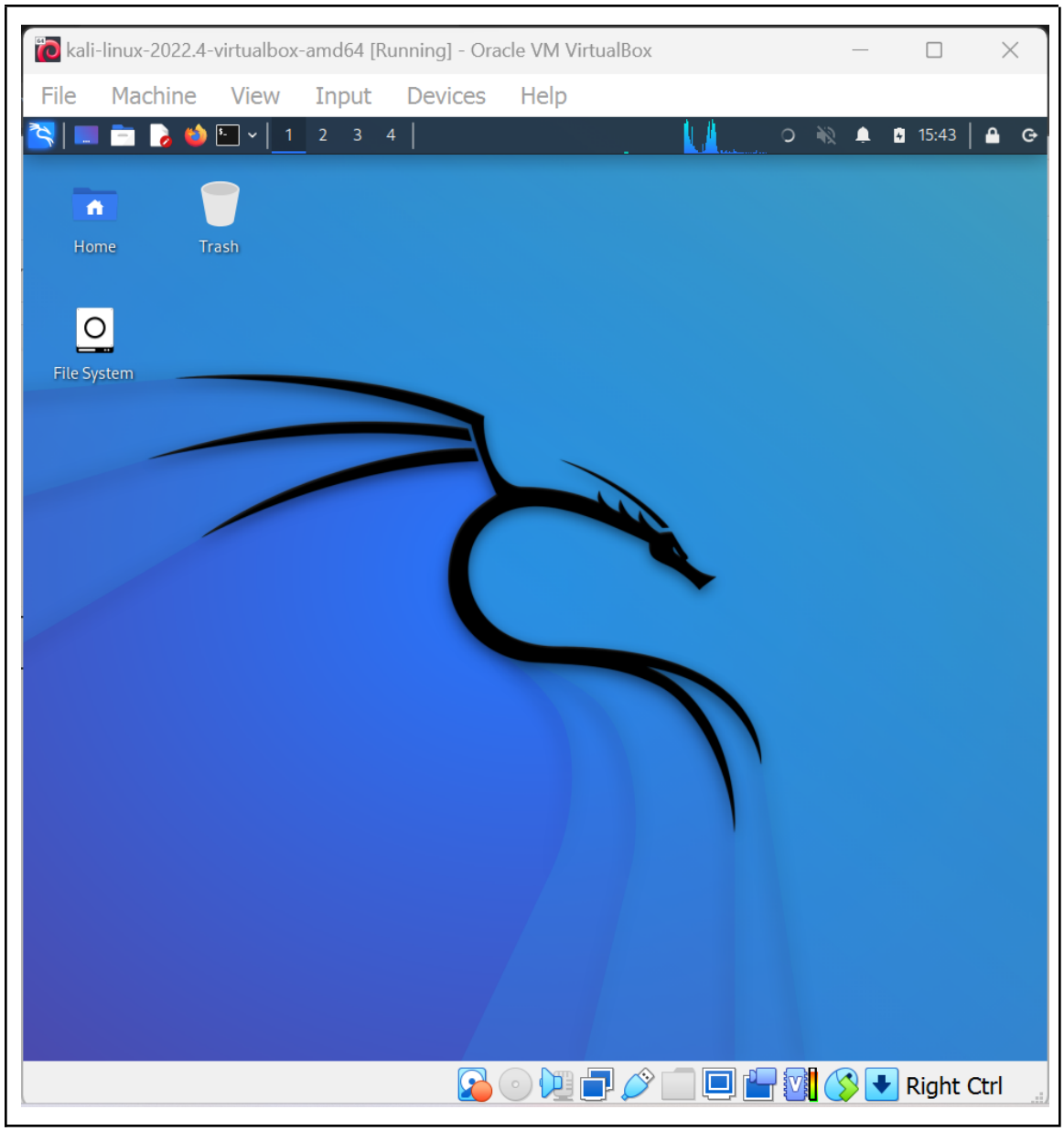
Table of Contents

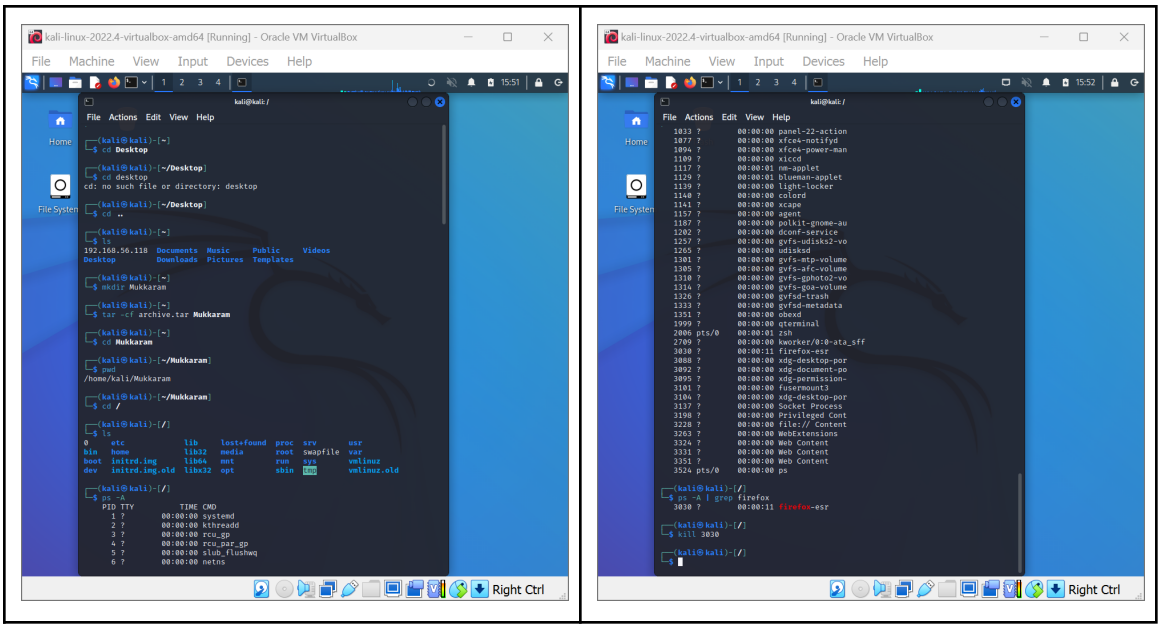
Lab 1

- Installed Kali Linux



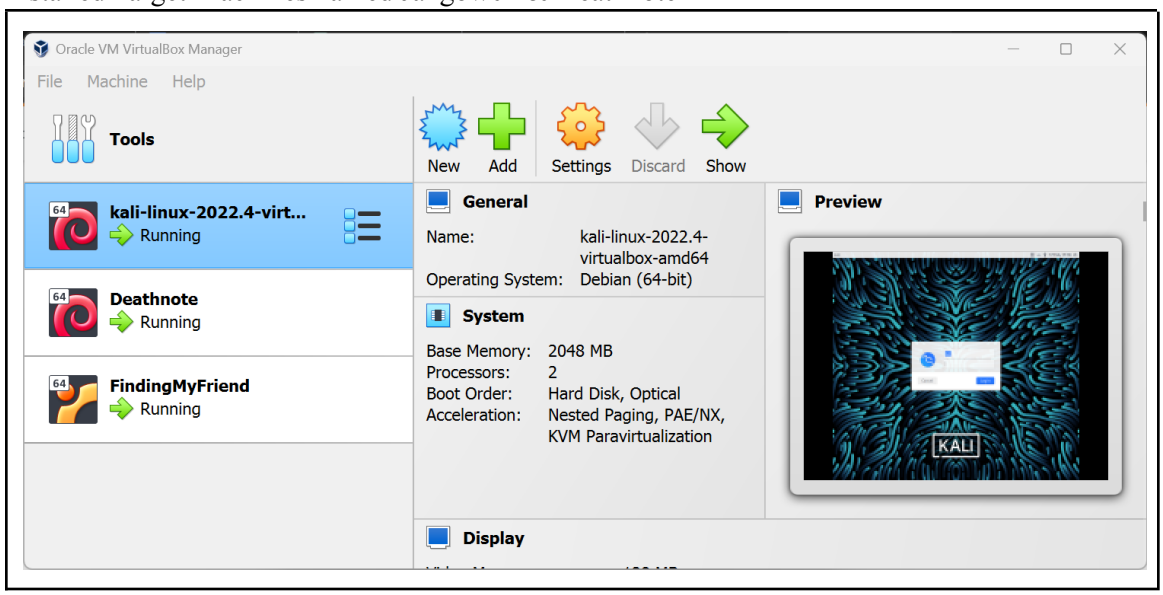
- Getting familiar with basic commands

Mirza Mukkaram BaigBSCE19029

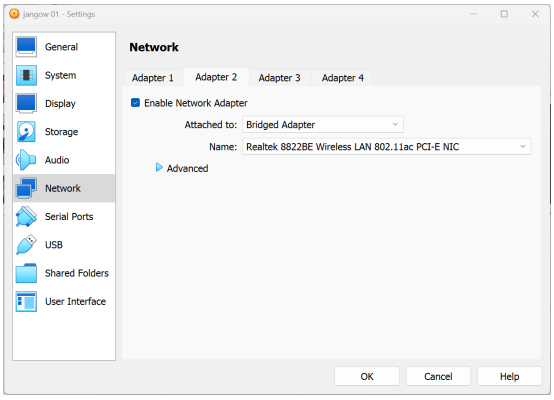
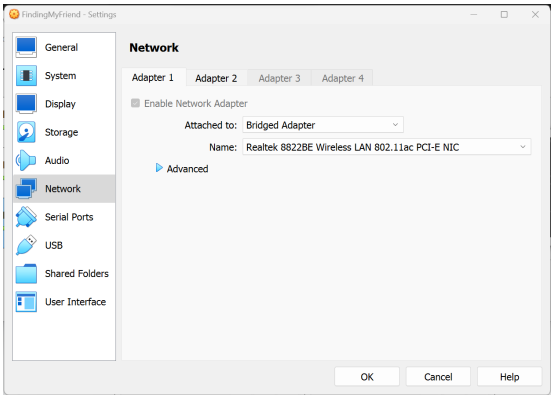


Lab 2

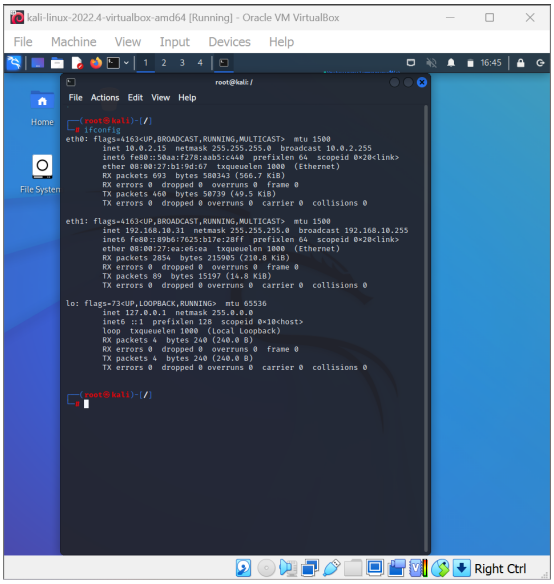
- Installed Target Machines named Jangow01 & Deathnote



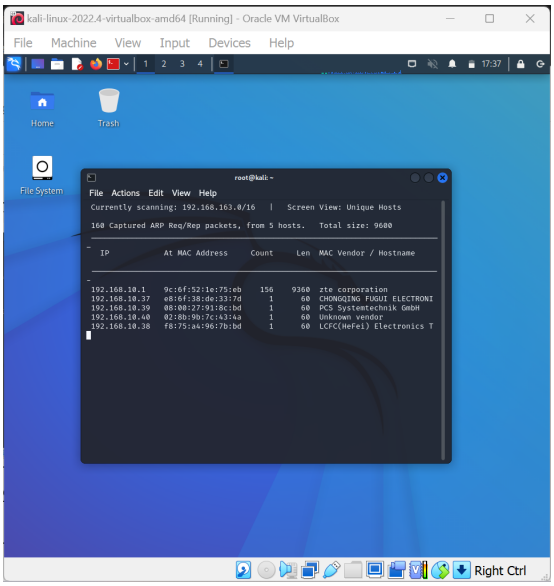
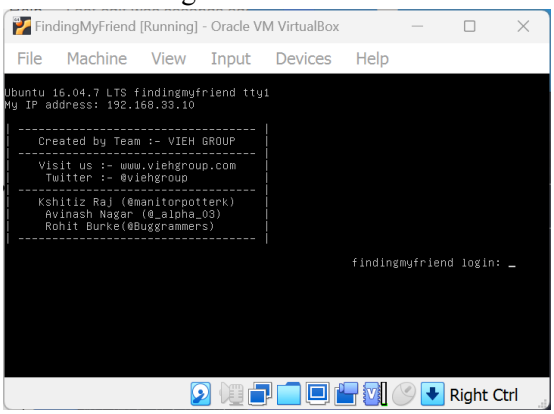
- Bridged Network

Jangow01	Finding My Friend
	

- Finding Ip Address of my kali

	Command: ifconfig Ip address: 192.168.10.31

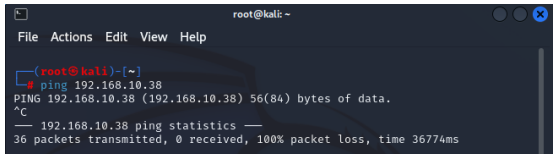
- Discovering Ip Address of target machines

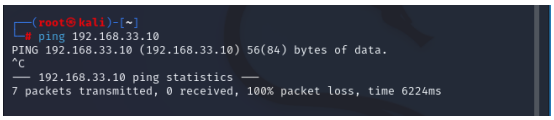
Jangow01	Finding My Friend
IP Address: 192.168.10.38 Command: netdiscover -i eth1 	IP Address: 192.168.33.10 Given in the target machine 

- Executing Ping Command

Jangow01	Finding My Friend

Mirza Mukkaram BaigBSCE19029

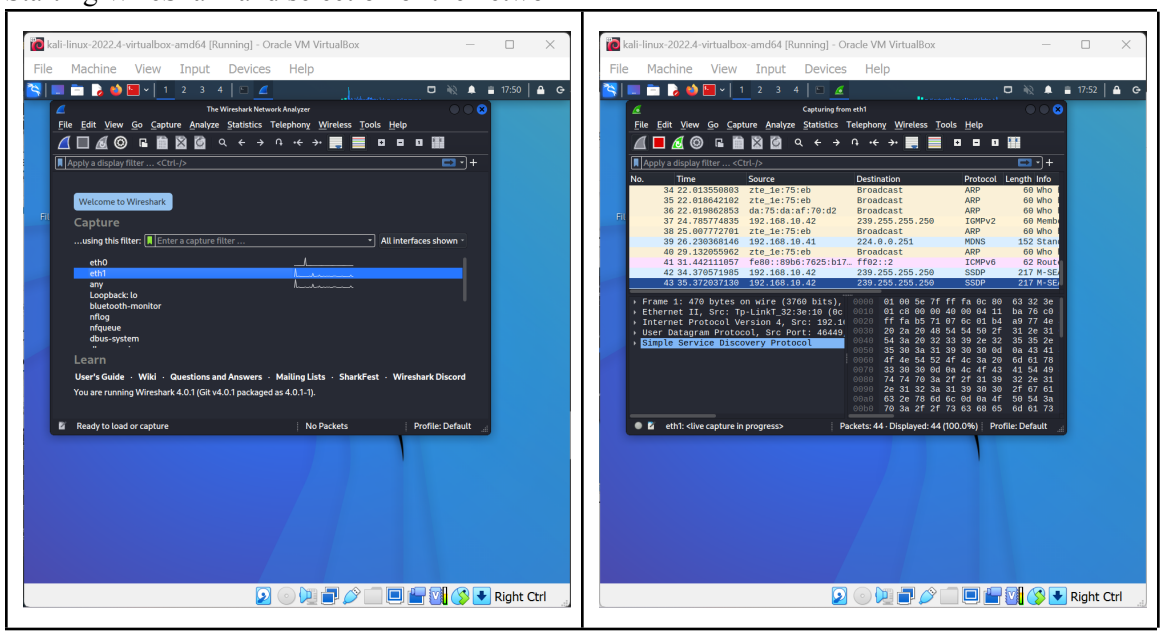




Comments: Both machine are working properly as no packet is lost while executing the ping command.

Lab 3

- Starting WireShark and selection of the network



- Statistics

File	Packets Captured	No. ICMP packets	No. of HTTP packets
ping.pcapng	188	40	0
web.pcapng	1202	0	28

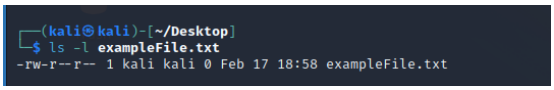
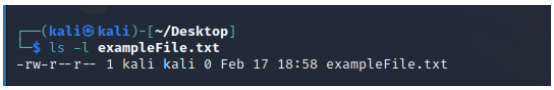
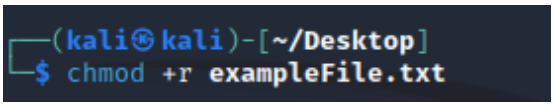
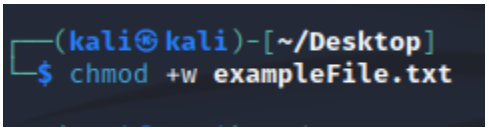
- For the last task creating my own file of youtube using firefox as done in the previous task

How many packets are there in total?	4377
How many different protocols are there, and what are they?	Internet Control Message Protocol v6 1 QUIC IFTF 2925 Domain Name System 62 Transport Layer Security 240 Online Certificate Status Protocol 8 Address Resolution Protocol 4
Easy Way	Go to Statistics -> Protocol Hierarchy Statistics
Packet 1 Src IP Address	192.168.10.31
Packet 1 Dest IP Address	192.168.10.1
Which Layer hold ip address info	Network Layer
Packet 1 Src port	44468

Packet 1 Dest port	53
Information from above points	The source port 44468 and destination port 53 suggest that a network communication session is likely taking place between a client and a DNS server. Port 53 is the well-known port used by the DNS protocol for name resolution and the fact that the destination port is set to 53 indicates that the traffic is targeting the DNS server. Meanwhile, the source port 44468 is likely a dynamically assigned port number used by the client to send the DNS request. When a client initiates a communication session, it typically selects a random source port to use, in this case, 44468
Which layer holds port info	Transport Layer
TCP flag in packet 1	DNS service thus no TCP Flags
TCP flag in packet 2	DNS service thus no TCP Flags
TCP flag in packet 3	DNS service thus no TCP Flags
Info about Packt 1, 2, 3	The source port 44468 and destination port 53 suggest that a network communication session is likely taking place between a client and a DNS server. Port 53 is the well-known port used by the DNS protocol for name resolution and the fact that the destination port is set to 53 indicates that the traffic is targeting the DNS server. Meanwhile, the source port 44468 is likely a dynamically assigned port number used by the client to send the DNS request. When a client initiates a communication session, it typically selects a random source port to use, in this case, 44468
Protocol in Packet 4	DNS
IP address and other info of Packet 4	192.168.10.31 & 192.168.10.1 Standard Query for 0x6fff and 0x4cfa
Packet 13 info	13 6.454391993 142.250.185.46 192.168.10.31 TCP 74 443 → 35836 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=2664872550 TSecr=2121977103 WS=256

TCP Flags	SYN and ACK

- Commands to check permission

ls -l <file_name>	
chmod +x <file_name> *** grants execution perimision	
chmod +r <file_name> *** grants read perimision	
chmod +w <file_name> *** grants writing perimision	
chmod +xwr <file_name> *** grants execution, write and read perimision