Lab 2

COMP6035: Computer Security Principles



**Your Name**

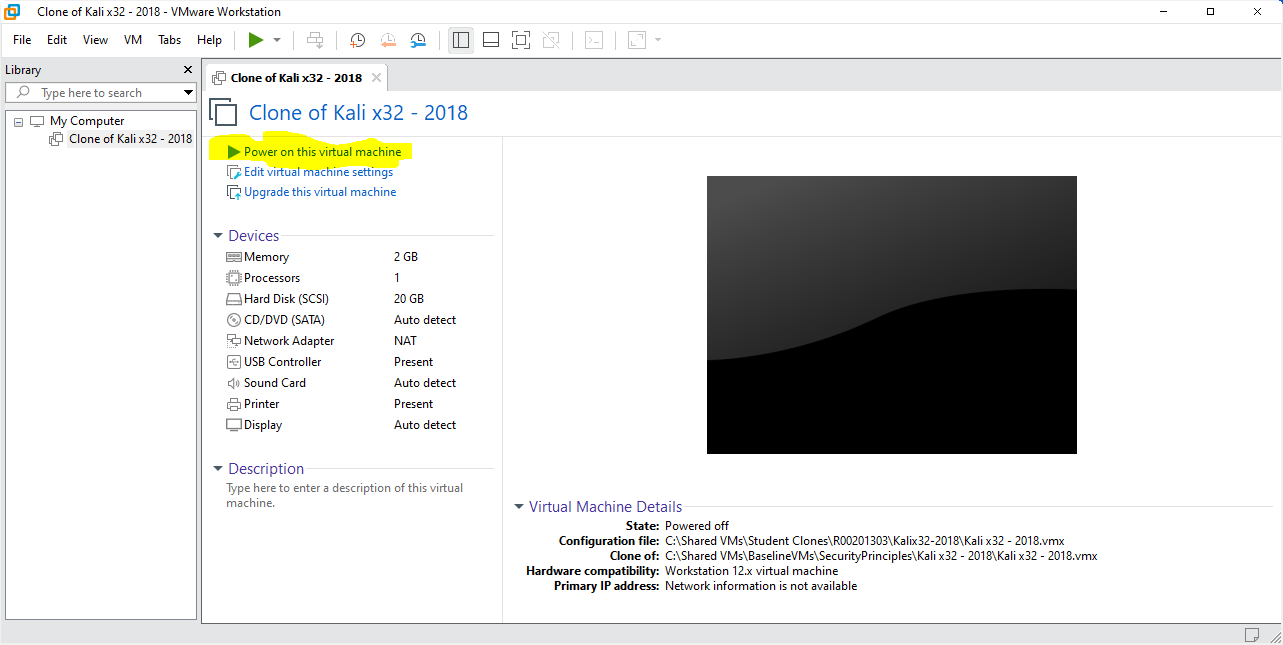
Student #: R00201303

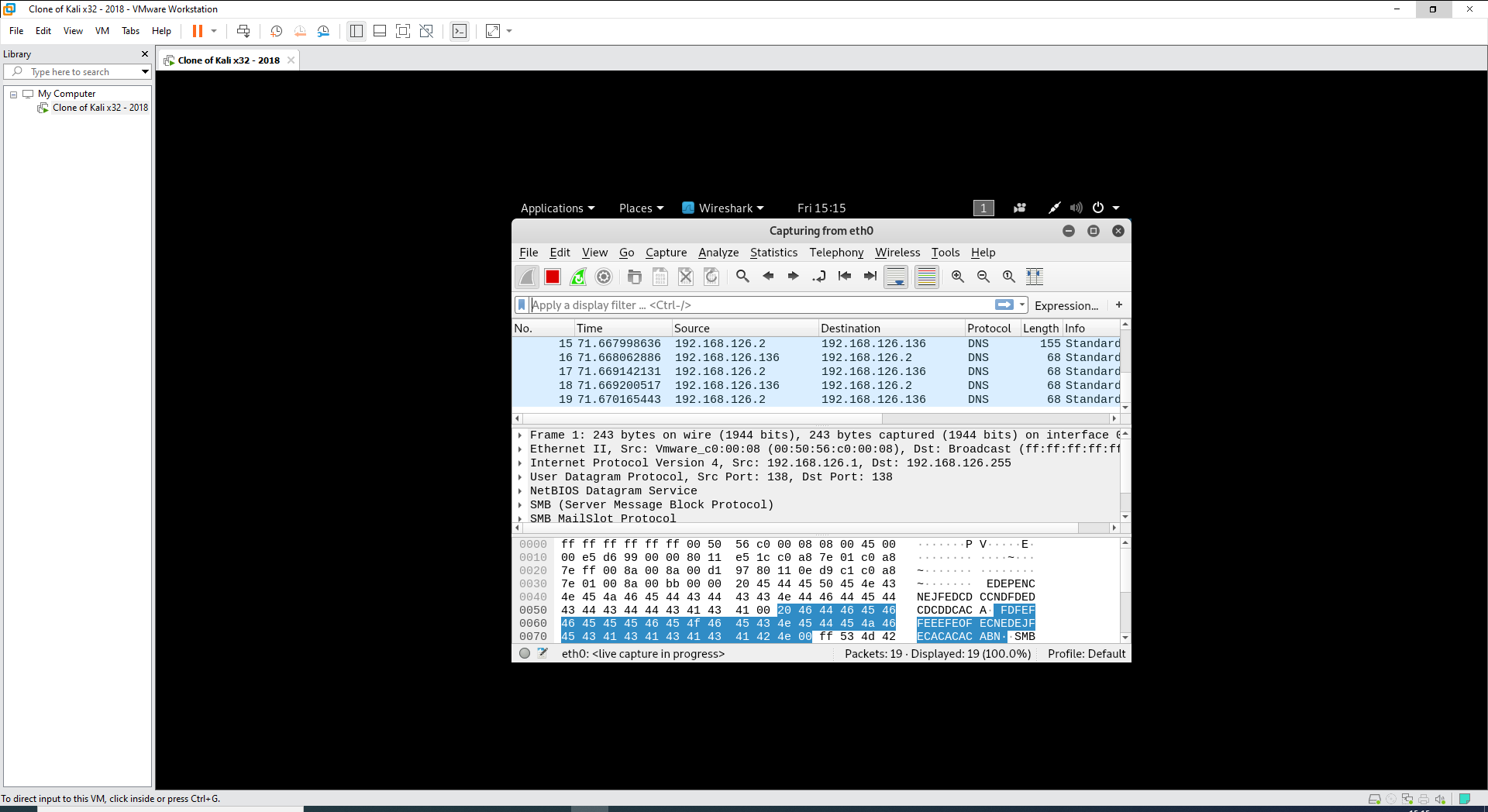
Date: 26.11.2021

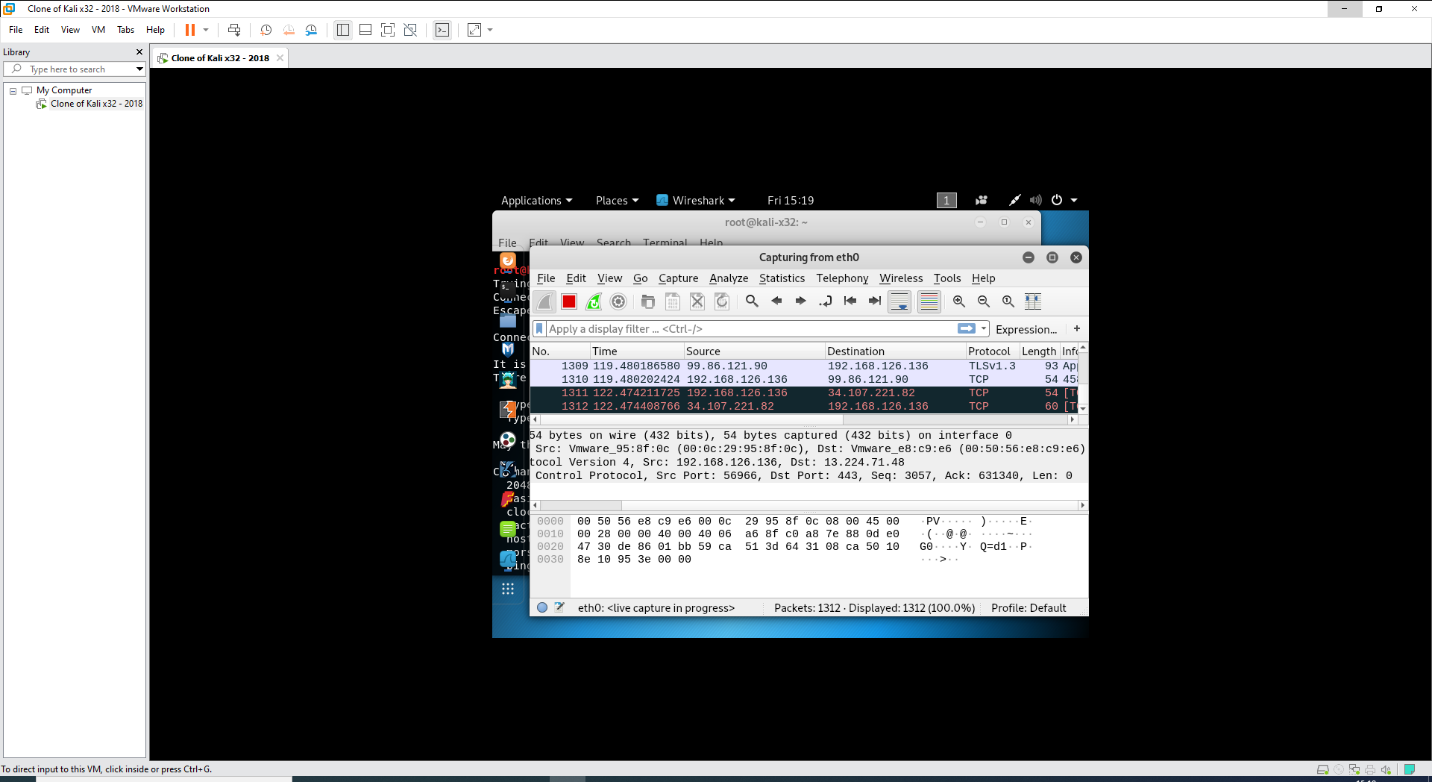
Group: COMP1D-Y

# PART 1

# TASK 1:



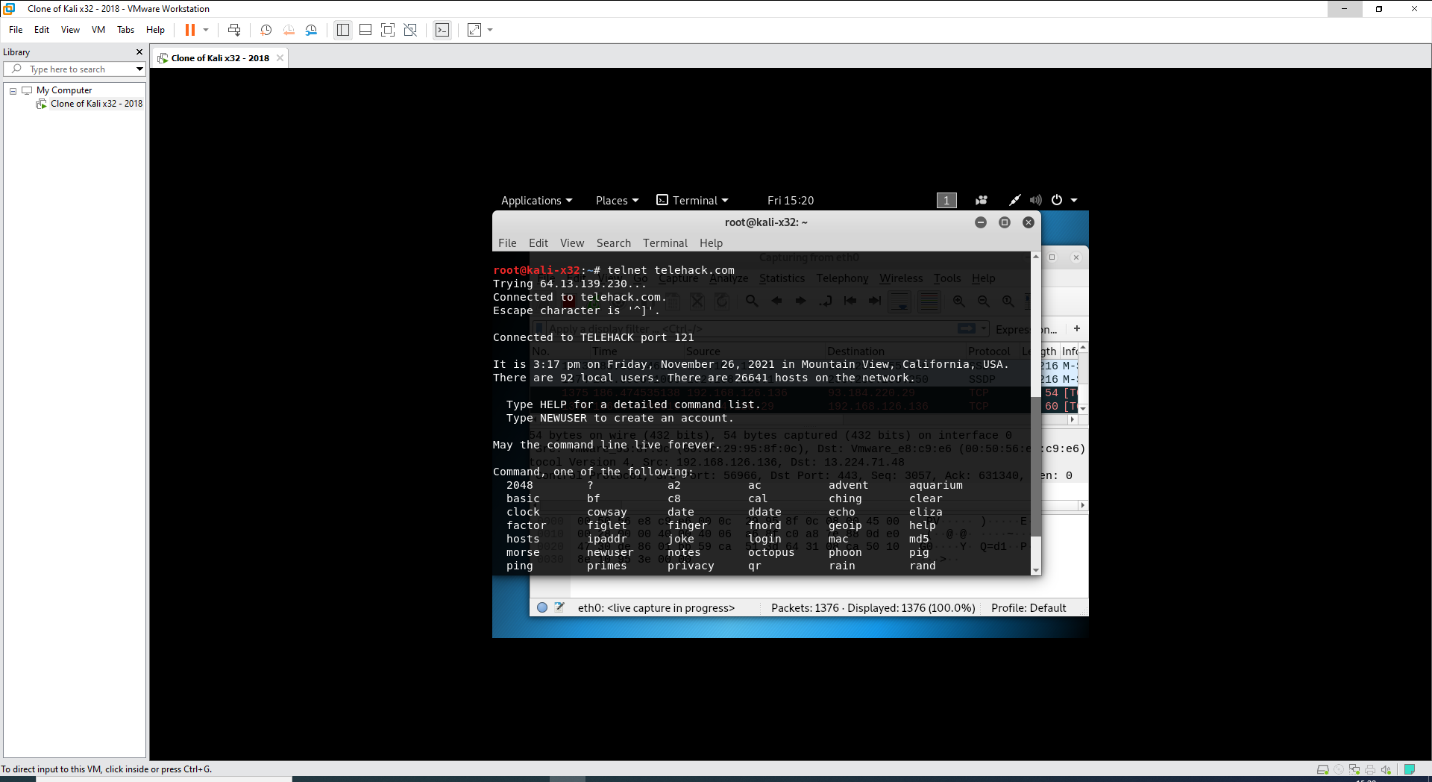


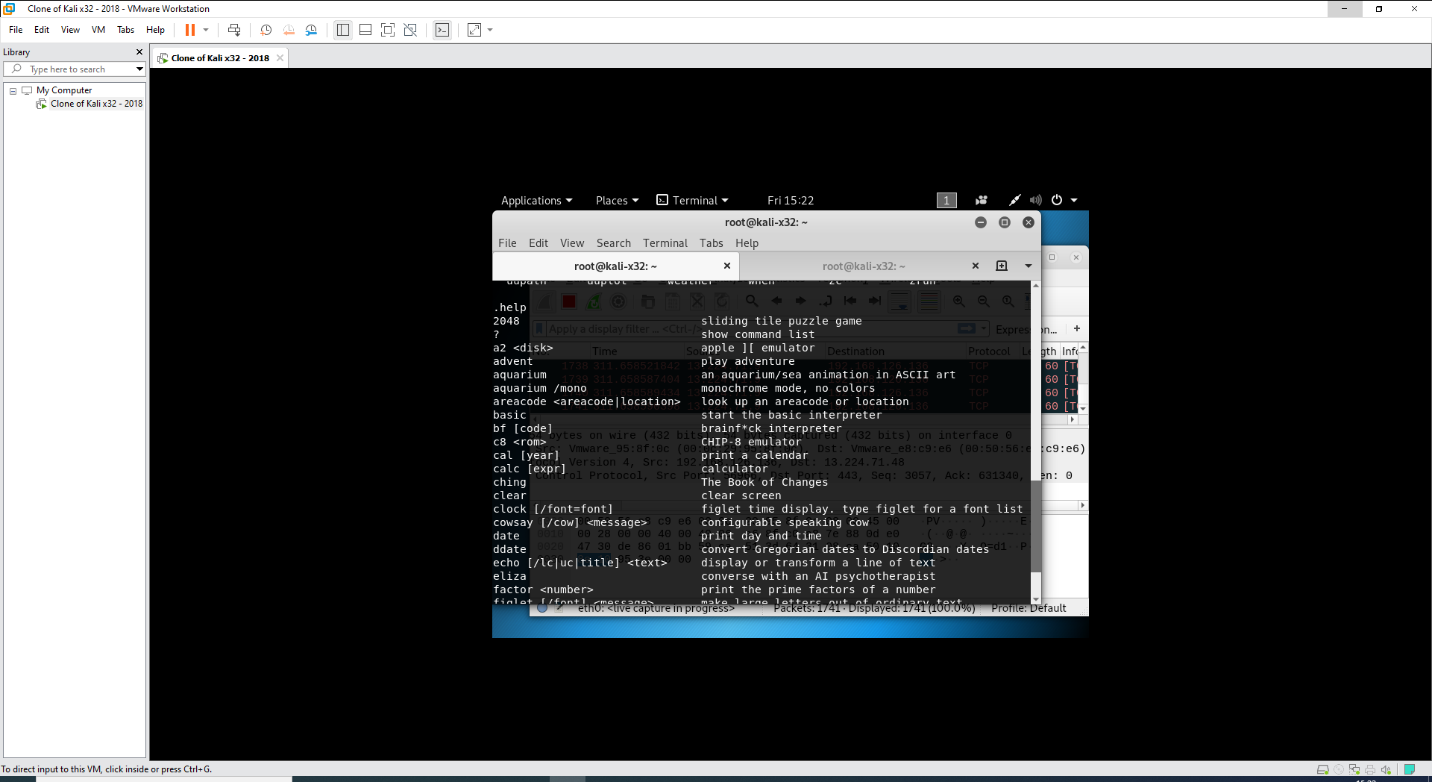


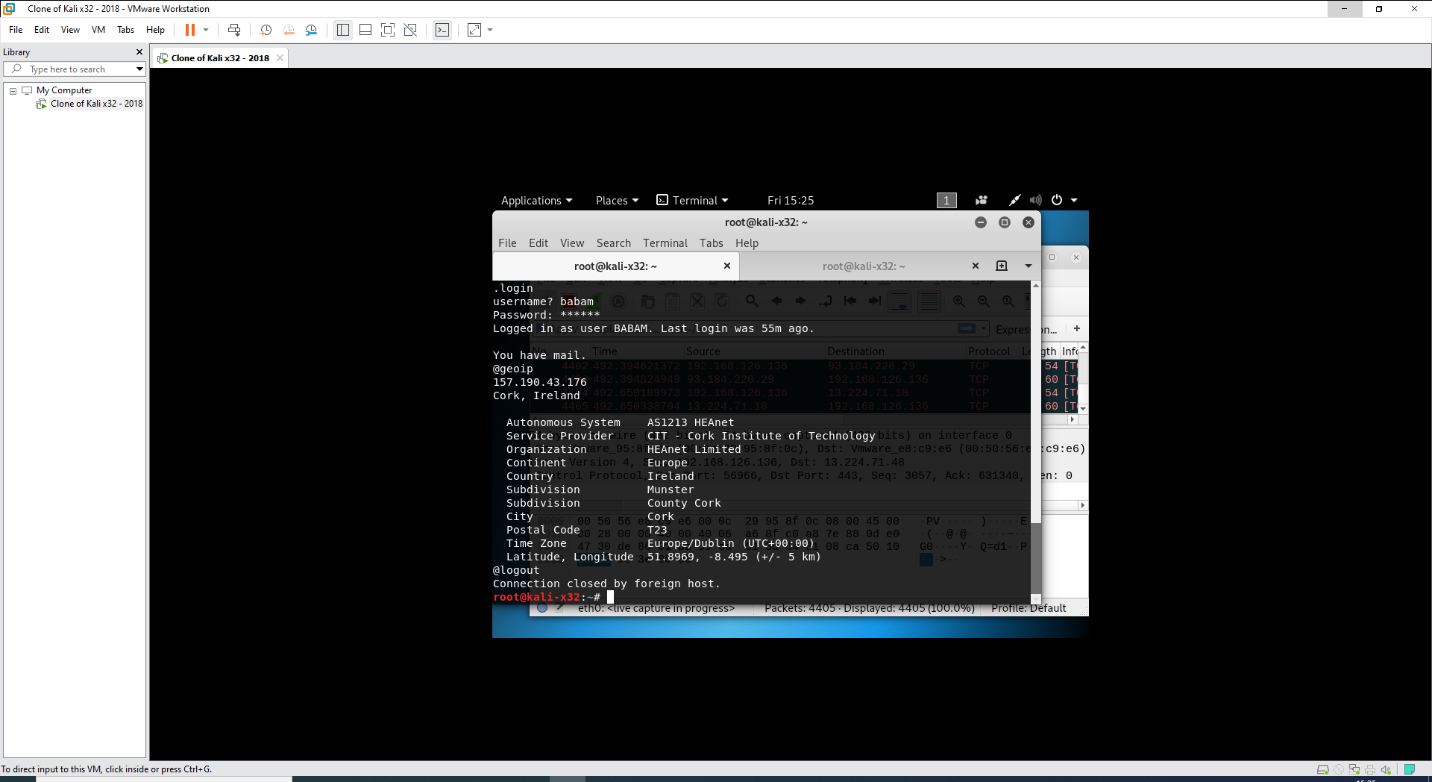
Capturing traffic screenshot(s) & observations:

Working on kali linux traffic caputre can be done

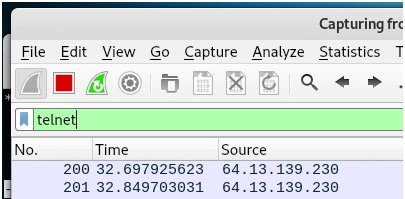
# TASK 2:

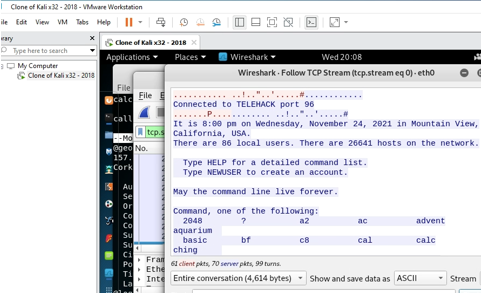






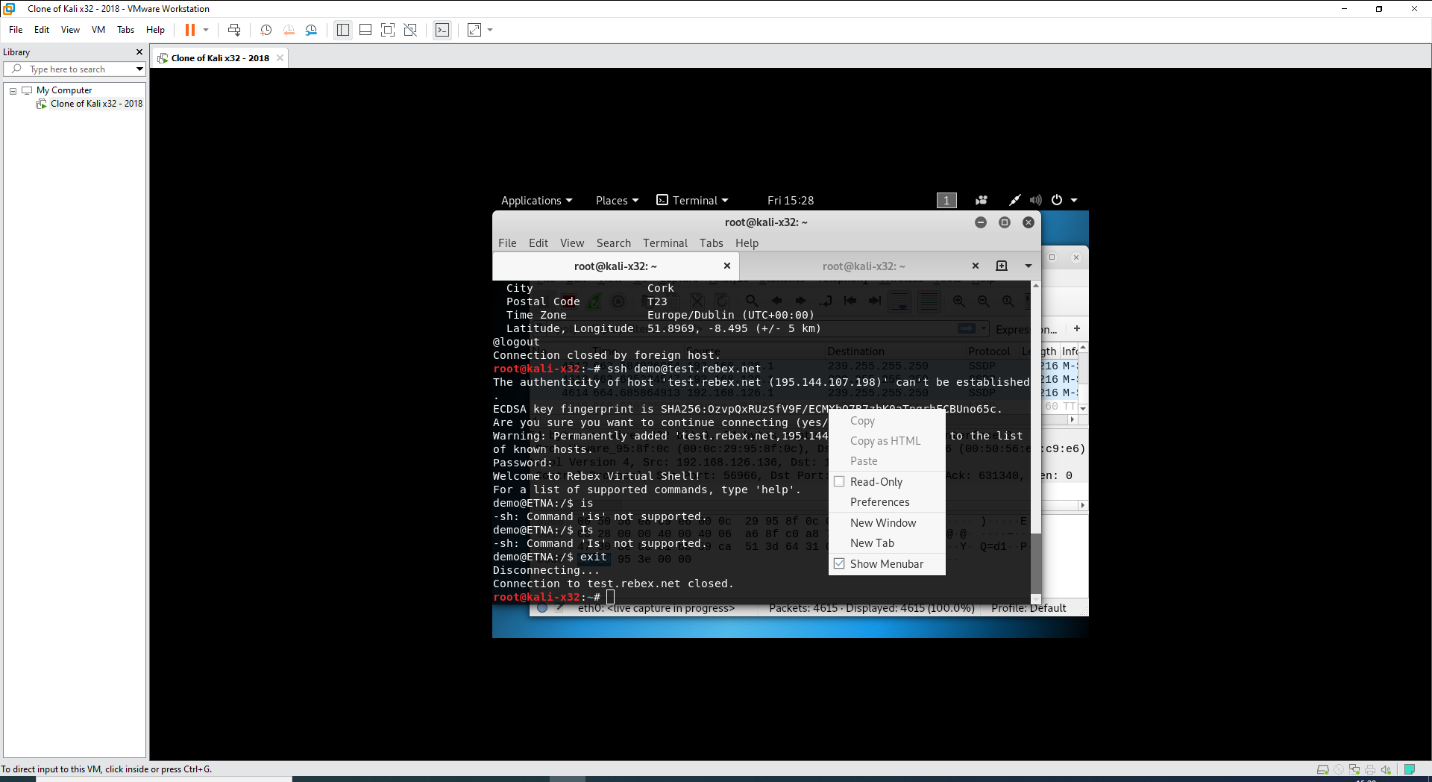
Filtering & viewing **telnet** data screenshot(s) & observations:

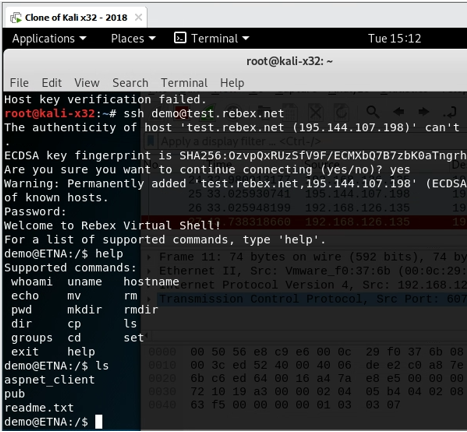


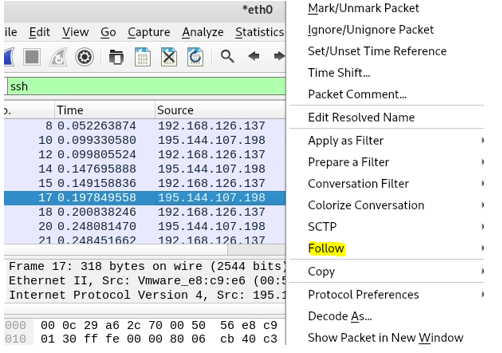


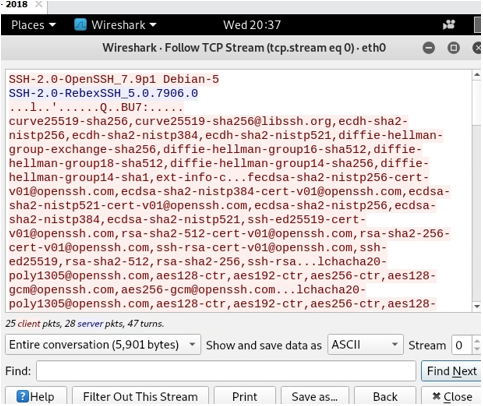
Telnet is a bidirectional interactive text-oriented communication system that uses an 8-byte virtual terminal connection. Over the transmission control protocol, user data is intermingled in-band with telnet control information (TCP).

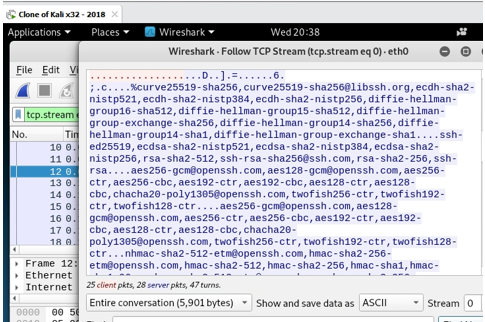
# TASK 3:









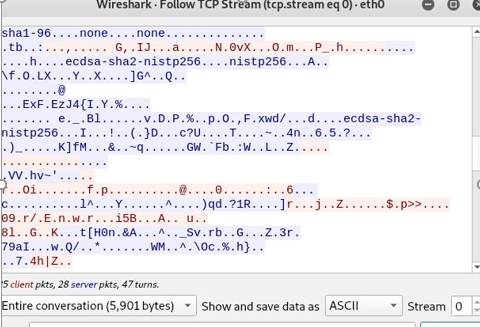


Filtering & viewing **ssh** data screenshot(s) & observations:

Implementing live monitoring and session recording makes it easier to spot unwanted behavior and ensures that distant users are only accessing systems that they can access. You may take proactive measures to defend your servers using SSH log information (such as invalid access type, faulty private keys, and remote IP addresses).

# TASK 4:

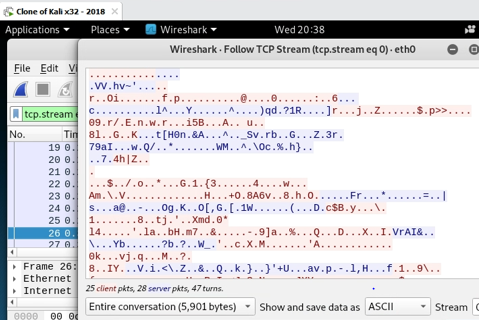
Directory content data screenshot(s) & observations:



In a distributed database system, the goal of a data directory is to identify the master source of certain data as well as replicas of that data.

# TASK 5:

Telnet security issue screenshot(s) & observations:



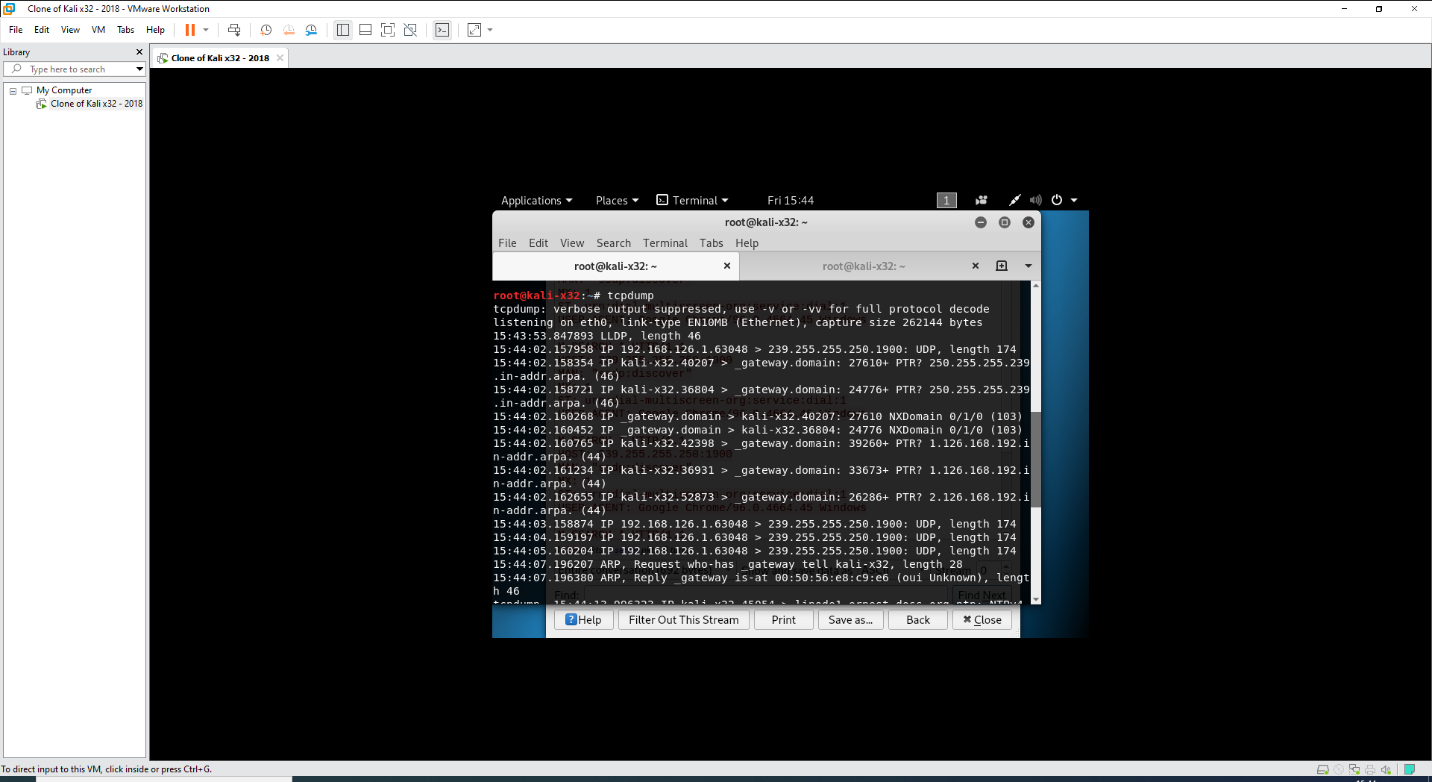
The user ID and password are not encrypted and are sent unencrypted. This puts the Telnet protocol at danger since eavesdropping and spying are easier for intruders or hackers to deploy.

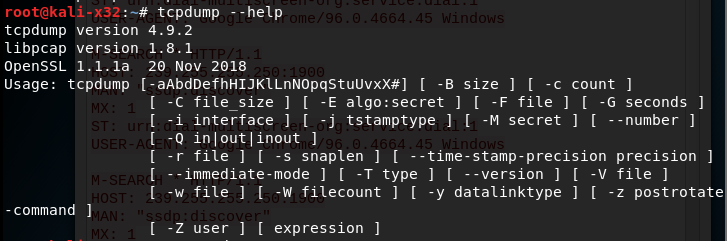
# 

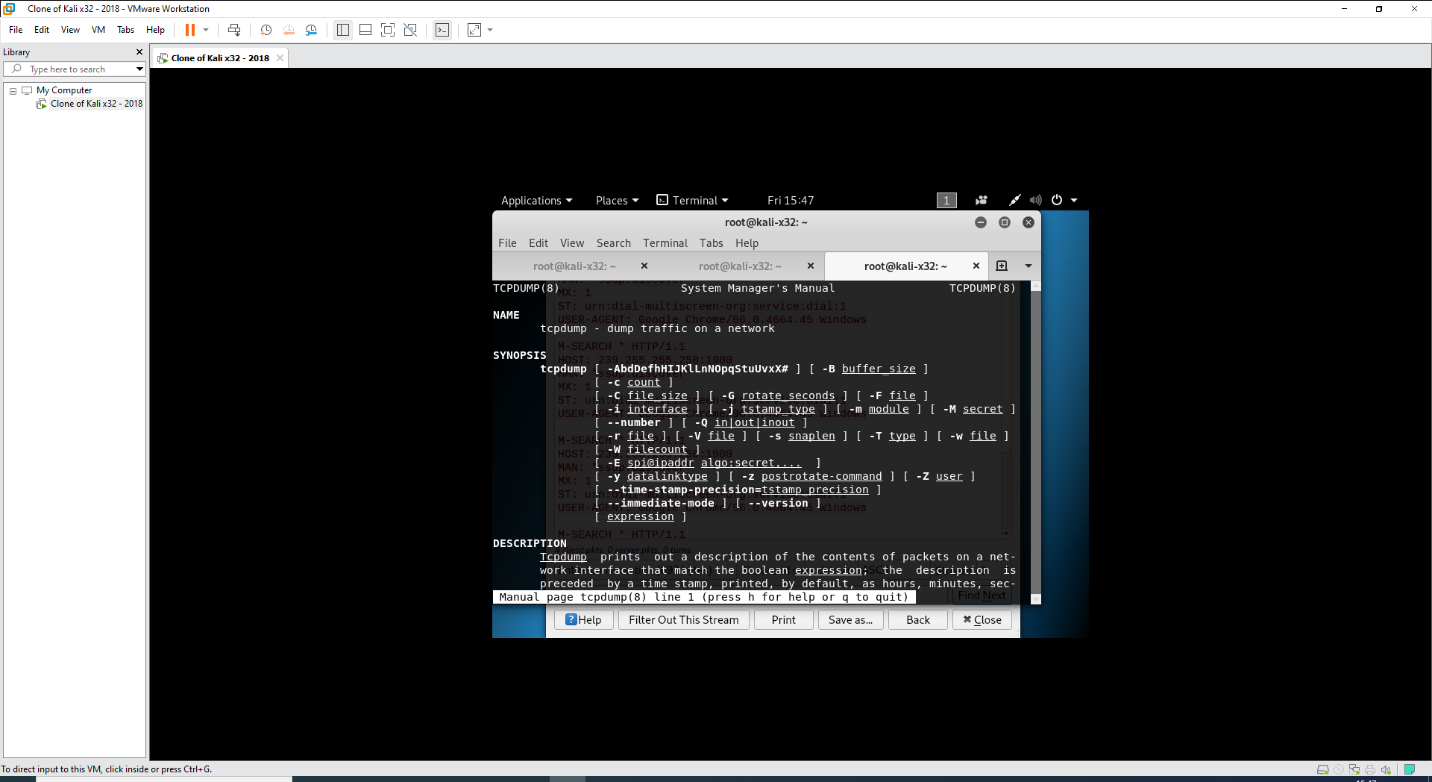
# 

# PART 2

# TASK 1:







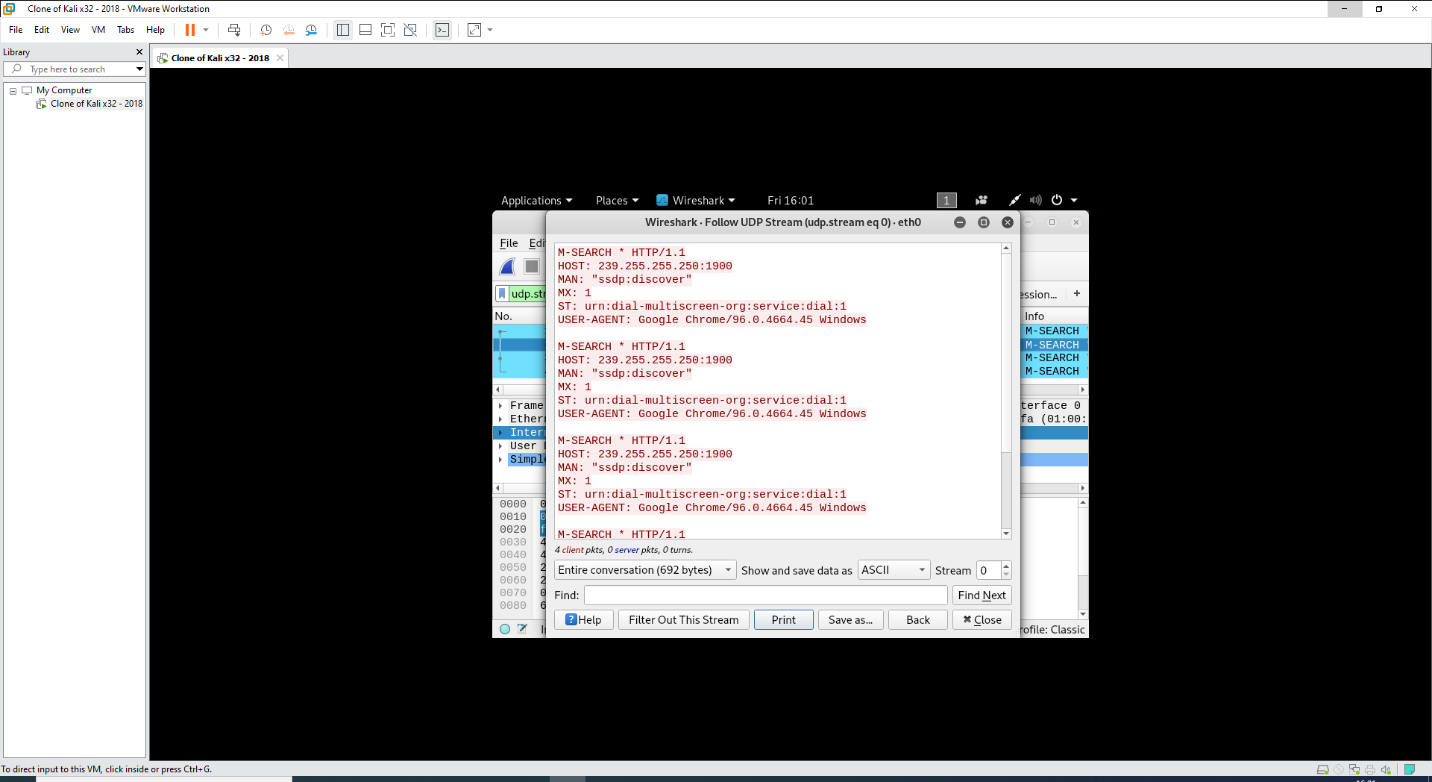
Tcpdump screenshot(s) & observations:

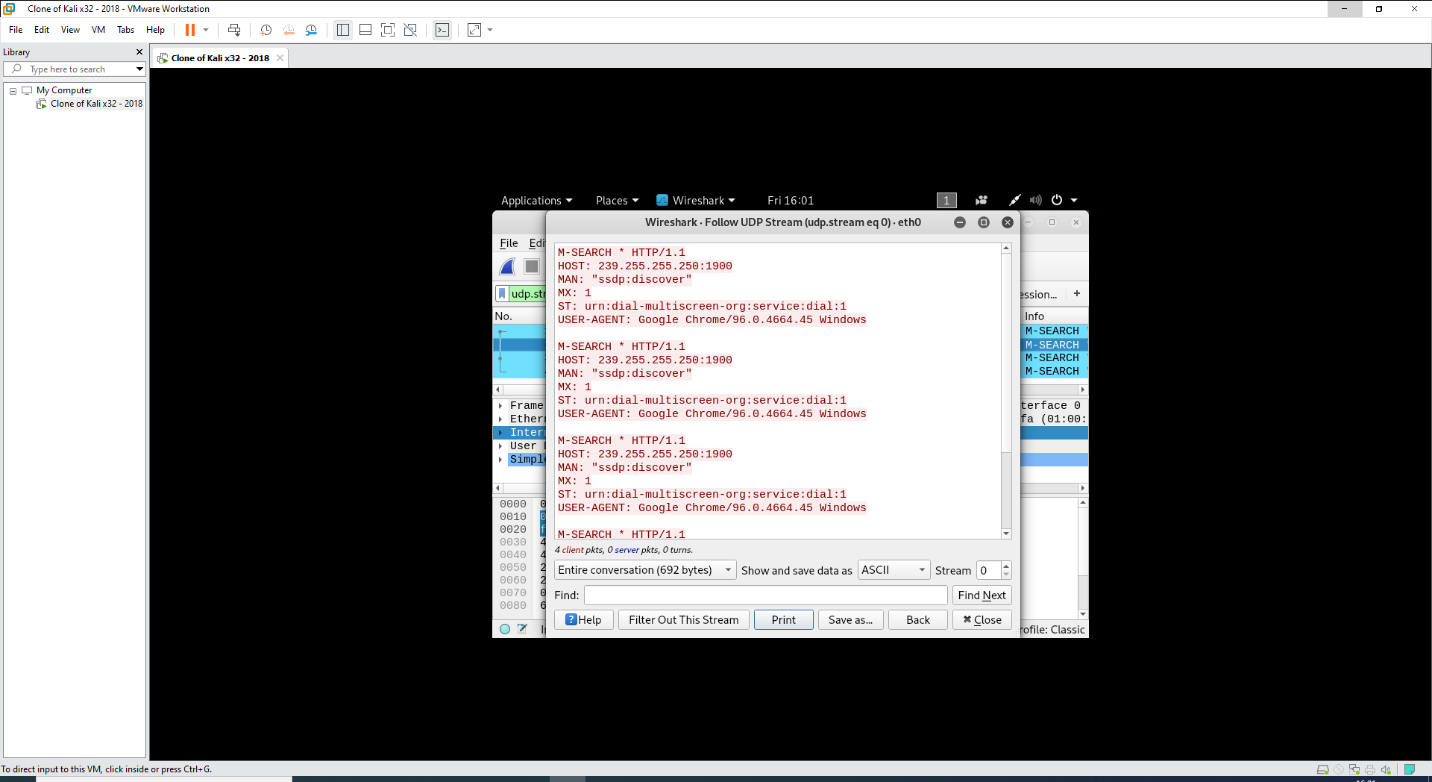
It may be used to investigate network traffic by intercepting and showing packets produced or received by the machine on which it is installed.

# TASK 2:

Ascii packet representation screenshot(s) & observations:

The tcpdump command, when run without any options, captures all packets passing over all interfaces. With the tcpdump command's -i option, you may filter on a specific ethernet interface.

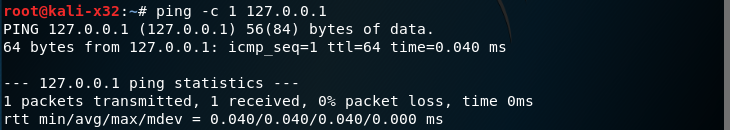




# TASK 3:

Ping payload screenshot(s) & observations:

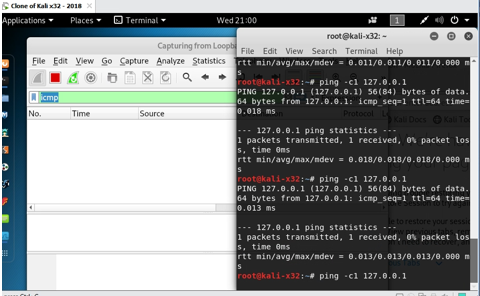
The payload of the packet is generally filled with [ASCII](https://en.wikipedia.org/wiki/ASCII) characters, as the output of the [tcpdump](https://en.wikipedia.org/wiki/Tcpdump) utility shows in the last 32 bytes of the following example (after the eight-byte ICMP header starting with 0x0800)

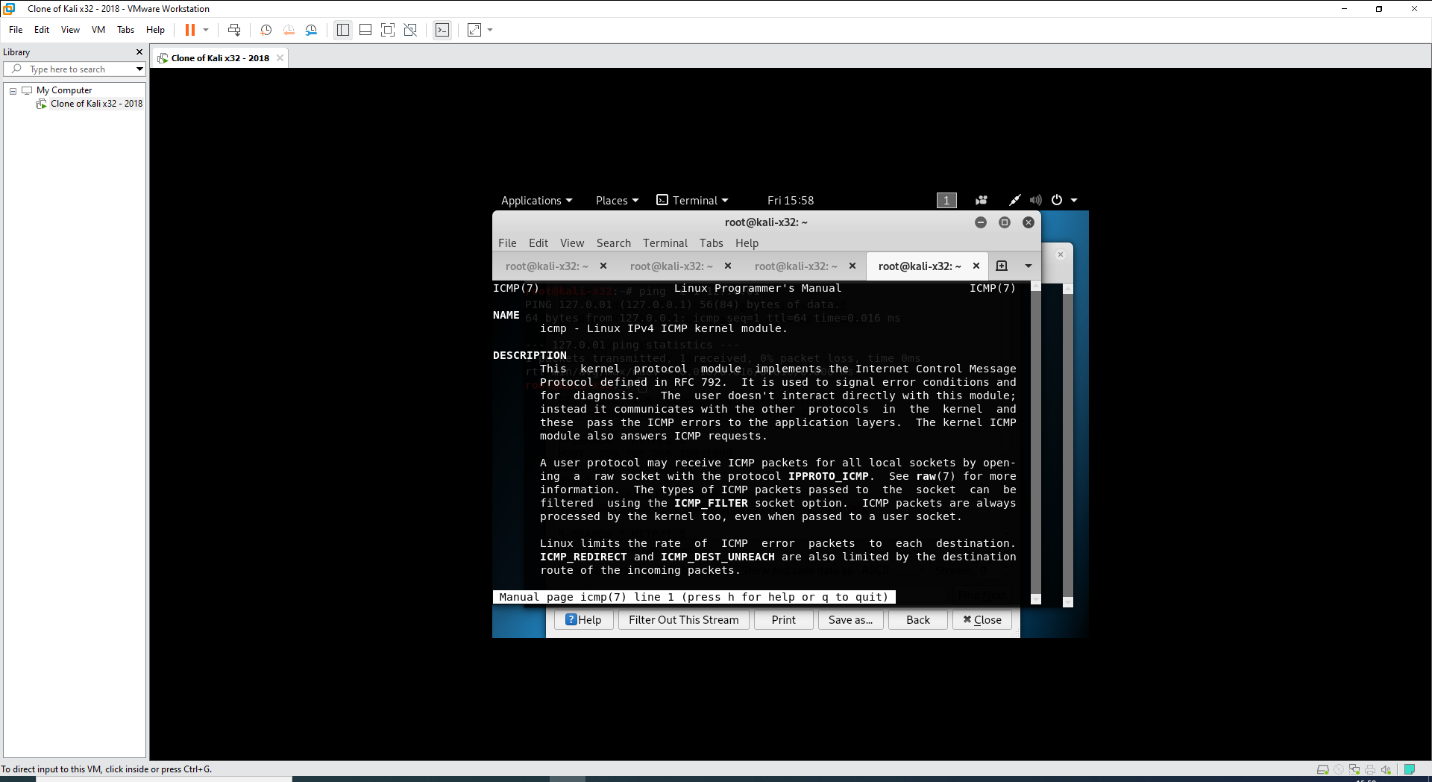


# TASK 4:

ICMP payload screenshot(s) & observations:

As previously stated, the default size of an ICMP payload packet is 32 bytes, with a maximum size of 1472 bytes. If the payload packet is larger than 1472 bytes, it will be fragmented into little packets.





# 

# 

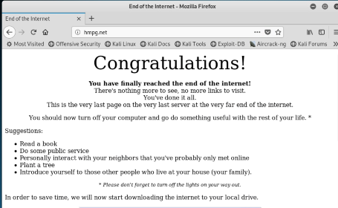
# 

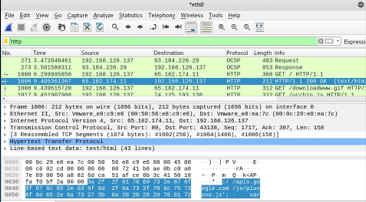
# 

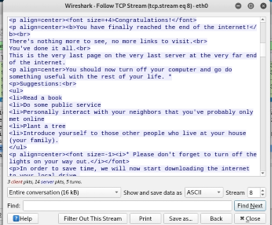
# PART 3

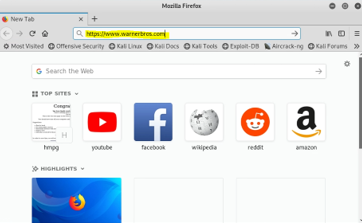
# TASK 1:

Website traffic capture screenshot(s) & observations:





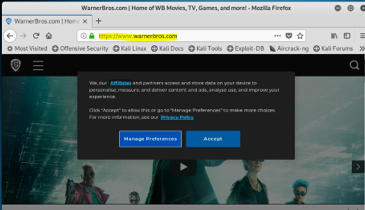




# TASK 2:

What filters could be used to distinguish between the connections to the two websites? Include screenshot(s) & observations:

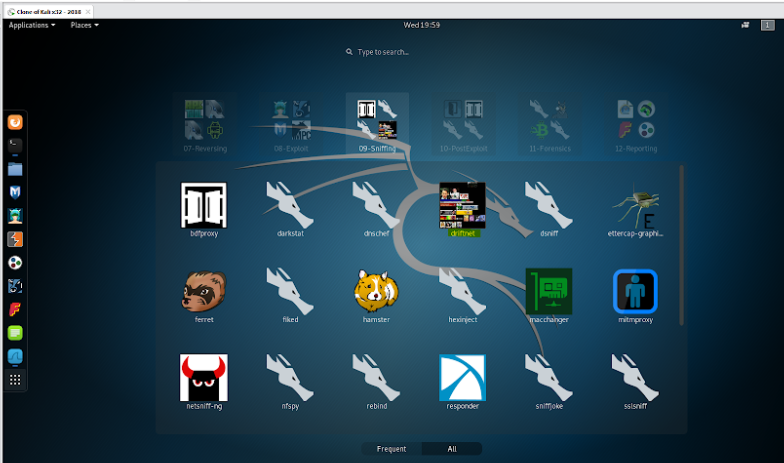
To filter for HTTPs traffic, I will filter for ‘ssl’

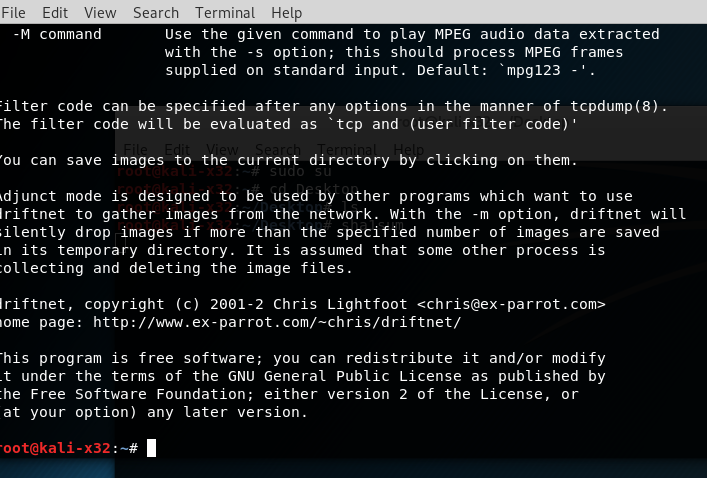


# TASK 3:

What difference can you observe between the two connections? Can you view the data from the web pages in Wireshark? Include screenshot(s) & observations:

# TASK 4:

Driftnet screenshot(s) & observations: 



collect and show pictures from network traffic in an X window; optionally, catch and play audio streams.

# Conclusion

Summarise what you have learned in the lab. This is an important and significant part of completing lab work.

in Part 1 Using Wireshark to capture and analyze traffic, as well as Telnet and SSH in the Linux terminal.

in part 2 Tcpdump, Linux tool options, and man pages.

 in part 3 Driftnet, more Wireshark filters, and secure online browsing.