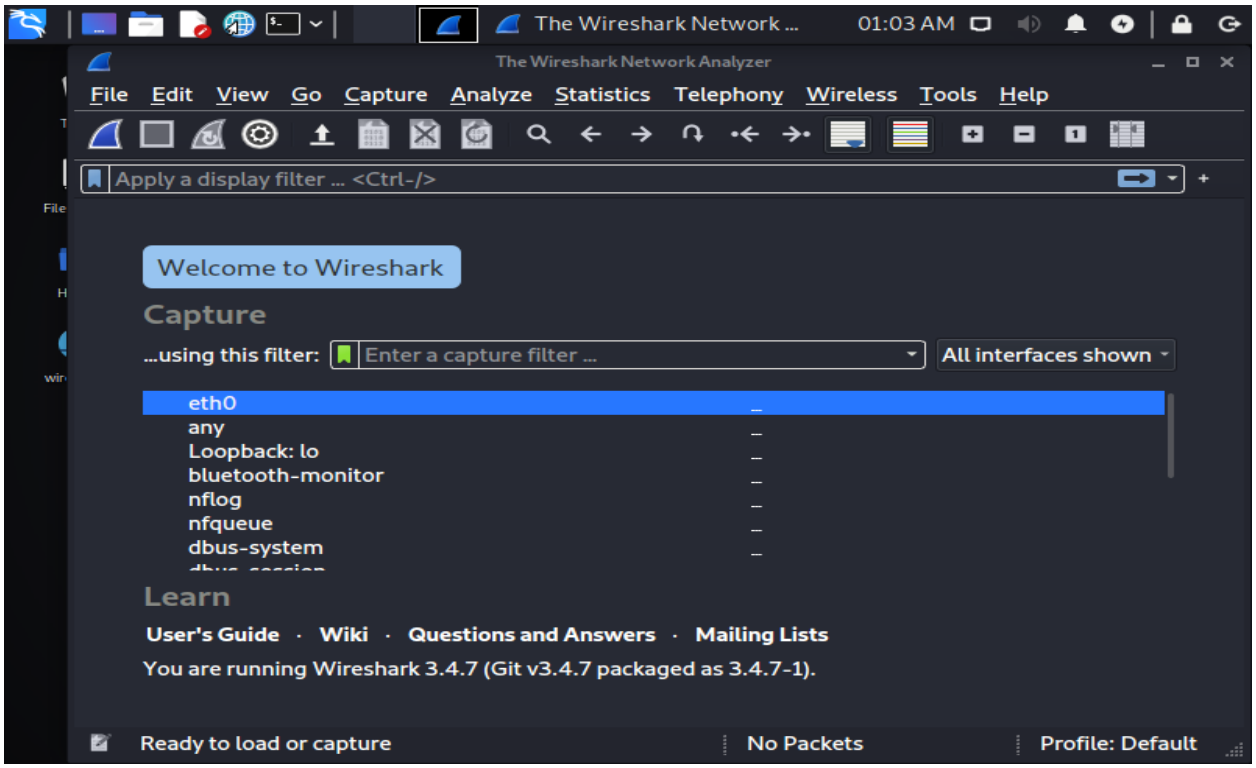
Everlyn Leon

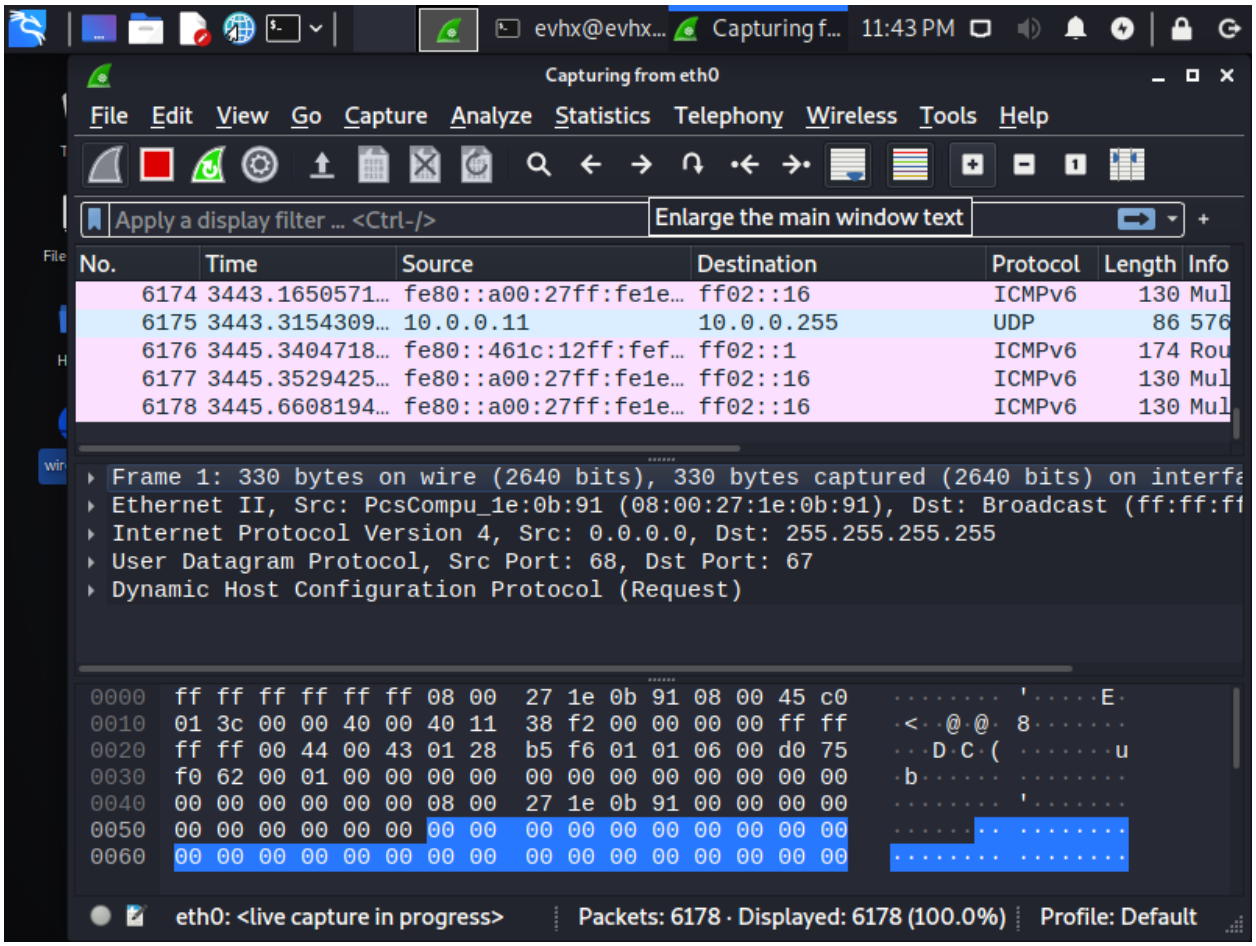
Abstract
Using Wireshark on a Kali Linux VM to intercept network traffic. Wireshark will capture network packets from the traffic being sent/received from the host computer and present the data captured in a readable format.

Introduction
Wireshark on a Kali Linux VM will be used to demonstrate how Wireshark captures and displays packets, along with useful tools Wireshark provides to make protocol analysis much easier. Communication between an Ubuntu VM and a Kali Linux VM using netcat will be demonstrated as an example to how Wireshark will analyze the network packets being sent from these two machines.

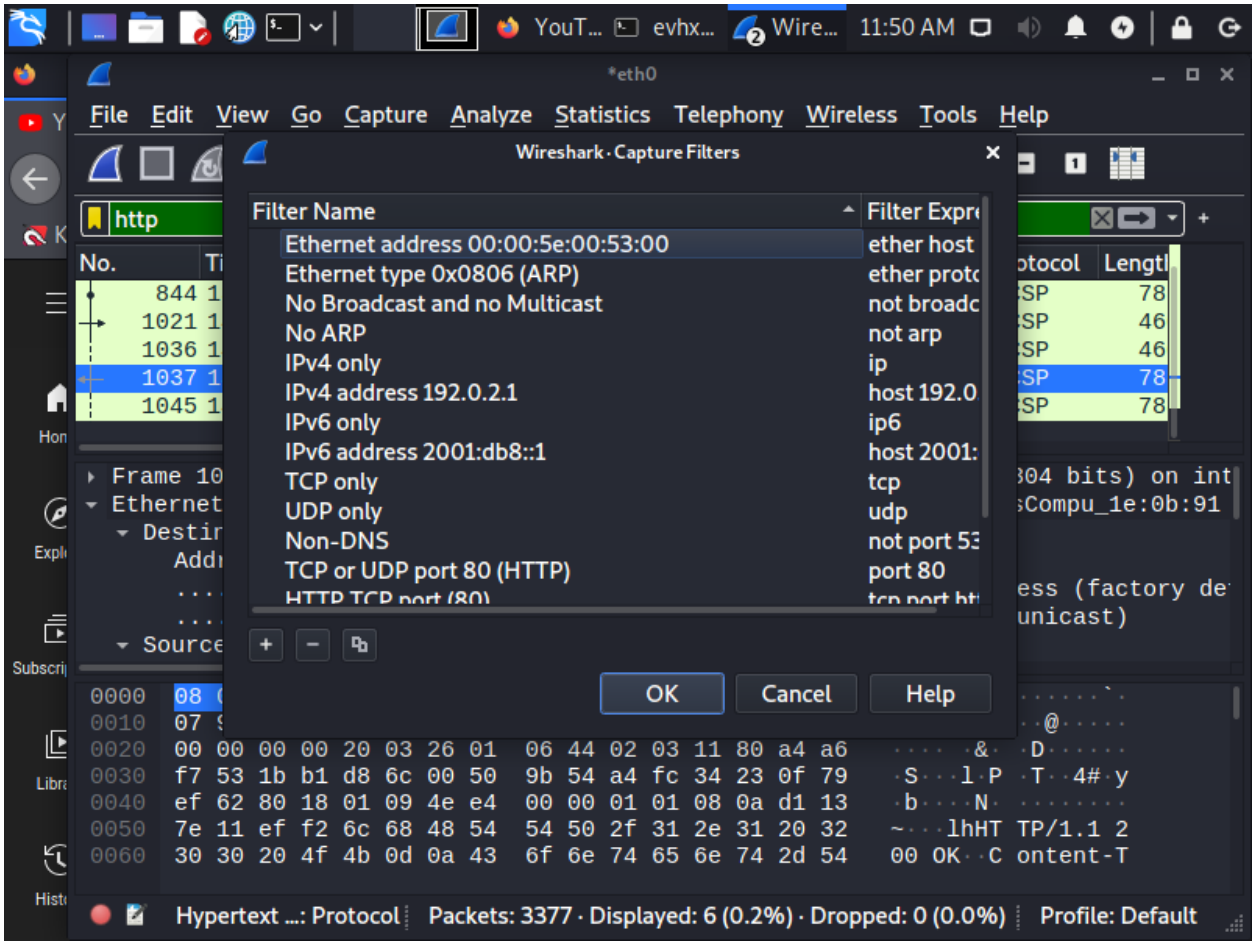
Summary of Results
In Kali Linux, Wireshark will be used to observe the network packet exchanges. Here selecting 'any' will allow Wireshark to listen on all available interfaces.



Wireshark provides a variety of tools to make network packets easy to analyze, such as a display filter, the list of captured packets, the details to any selected packet, and the ASCII and hexadecimal contained within the packets. The display filter helps with having to narrow down specific types of packets, for example typing ‘HTTP’ for finding packets received from websites, or looking up a specific ip with a ‘ip.addr == [ipaddress]’ command.

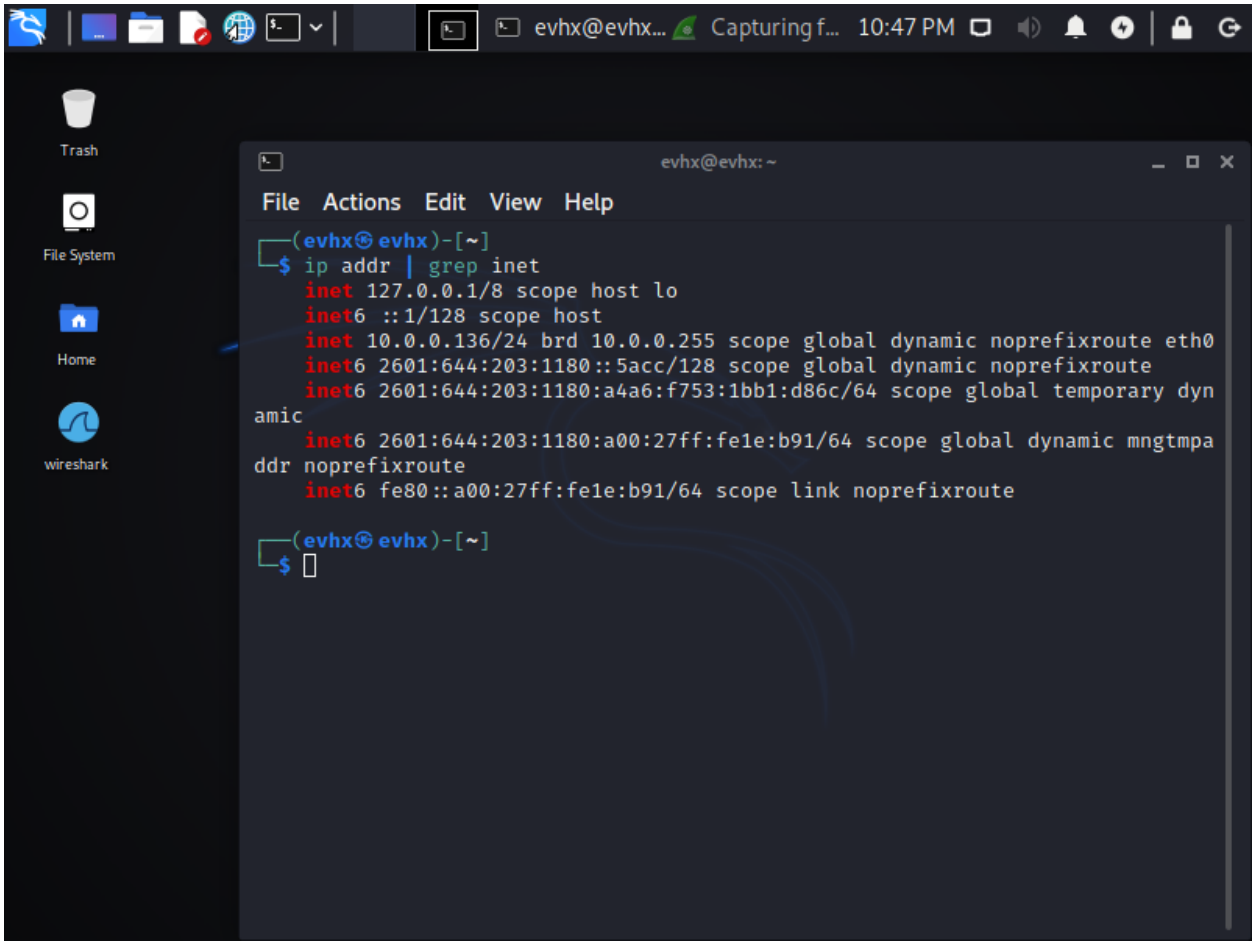


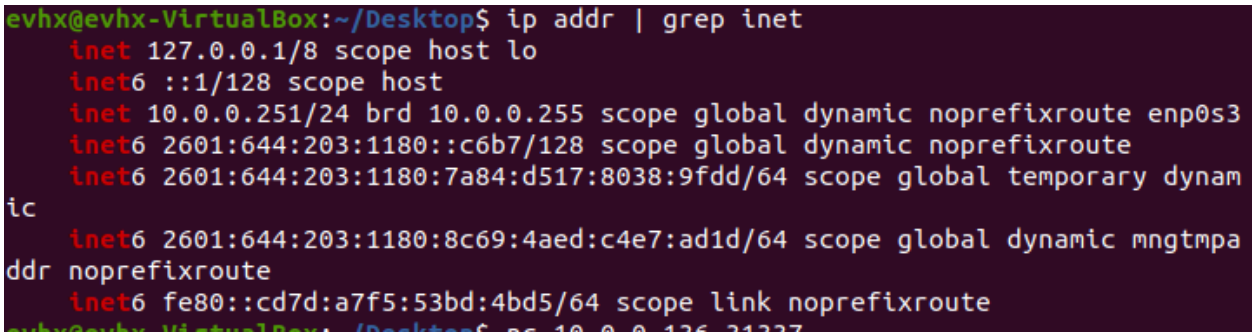
Network packets can also be filtered by going into the ‘Capture Filters’ command in the menu.



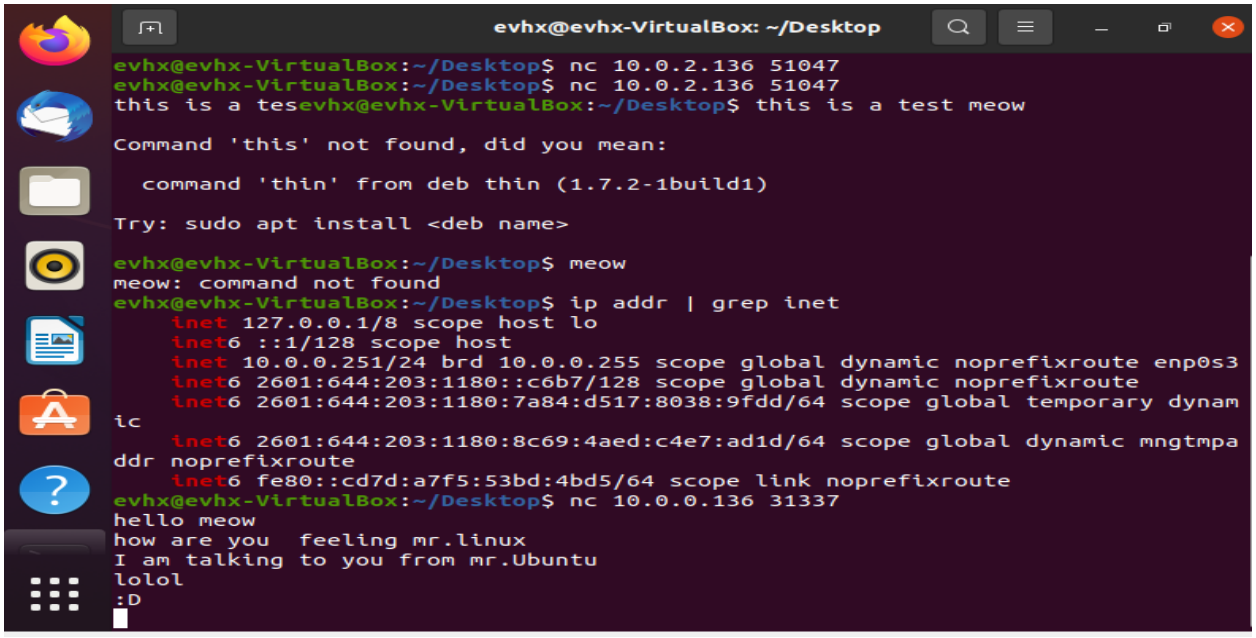
Capturing Packets from Communication Between a Ubuntu VM and a Kali Linux VM

In both Kali Linux and Ubuntu, open the terminal and type in '`ip addr | grep inet`' to retrieve the IP address of the machines.
Kali Linux IP: 10.0.0.136
Ubuntu IP: 10.0.0.251

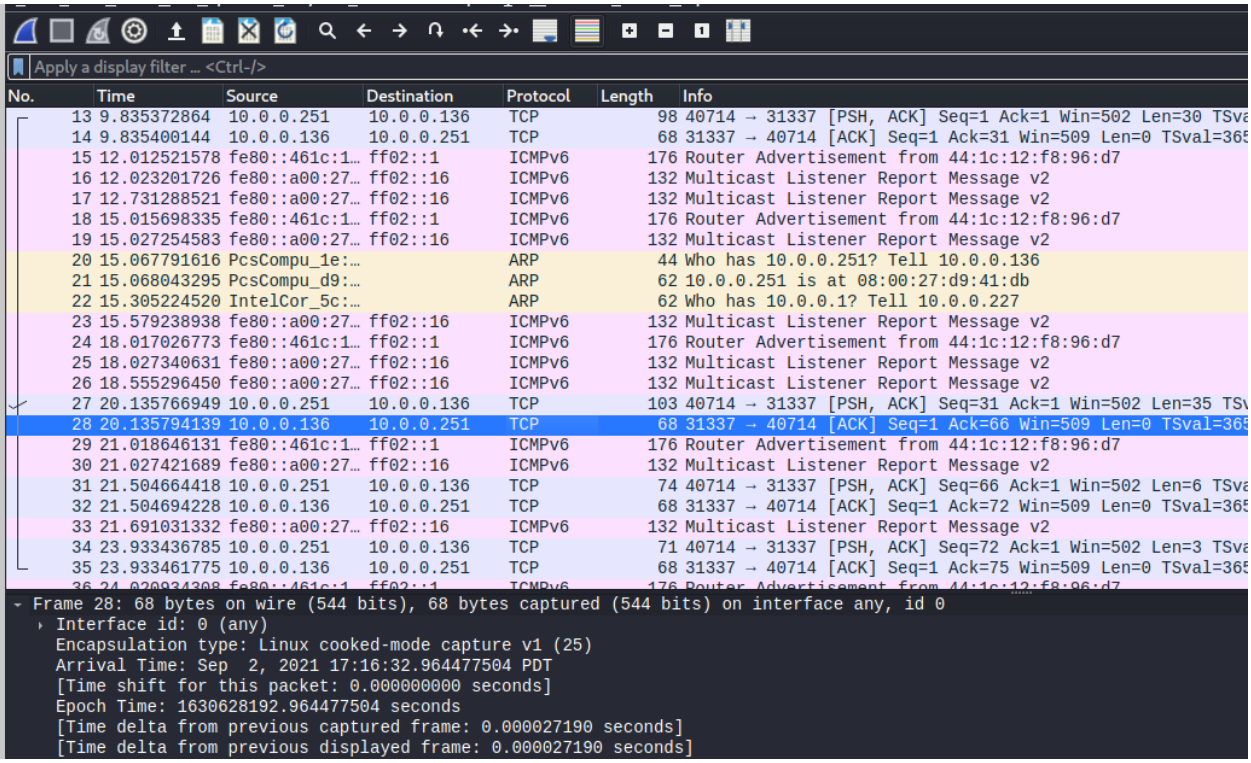




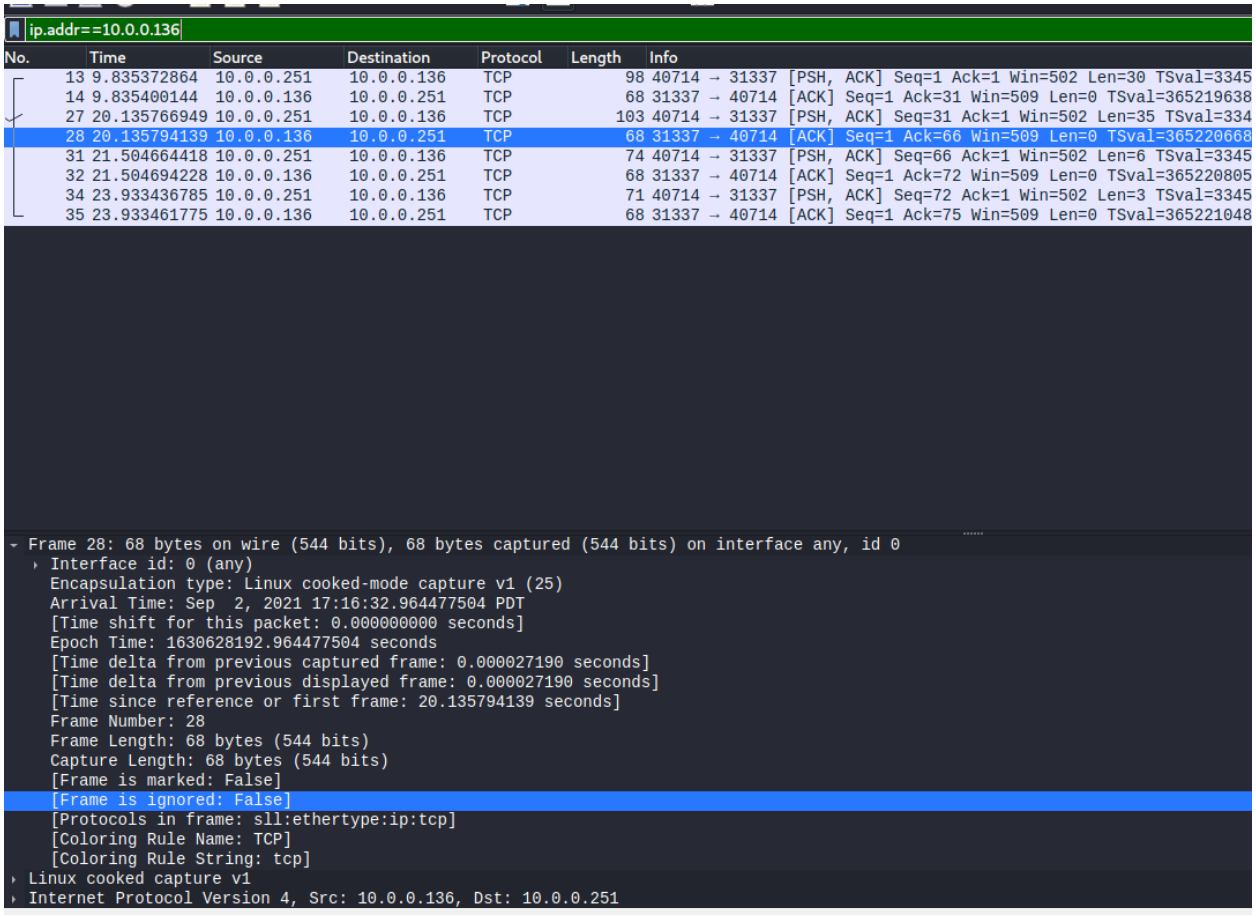
Here the command ‘nc’ will be used, which stands for netcat--a utility that can be used to read and write network connections in relation to TCP, UDP and UNIX sockets. Here a socket will be created in Kali Linux using the command ‘`nc -l -p [socket number]`’, and then in Ubuntu we will use the command ‘`nc [IP address of machine being contacted with] [socket number]`’ to connect to the Kali Linux machine, and communicate the displayed message.



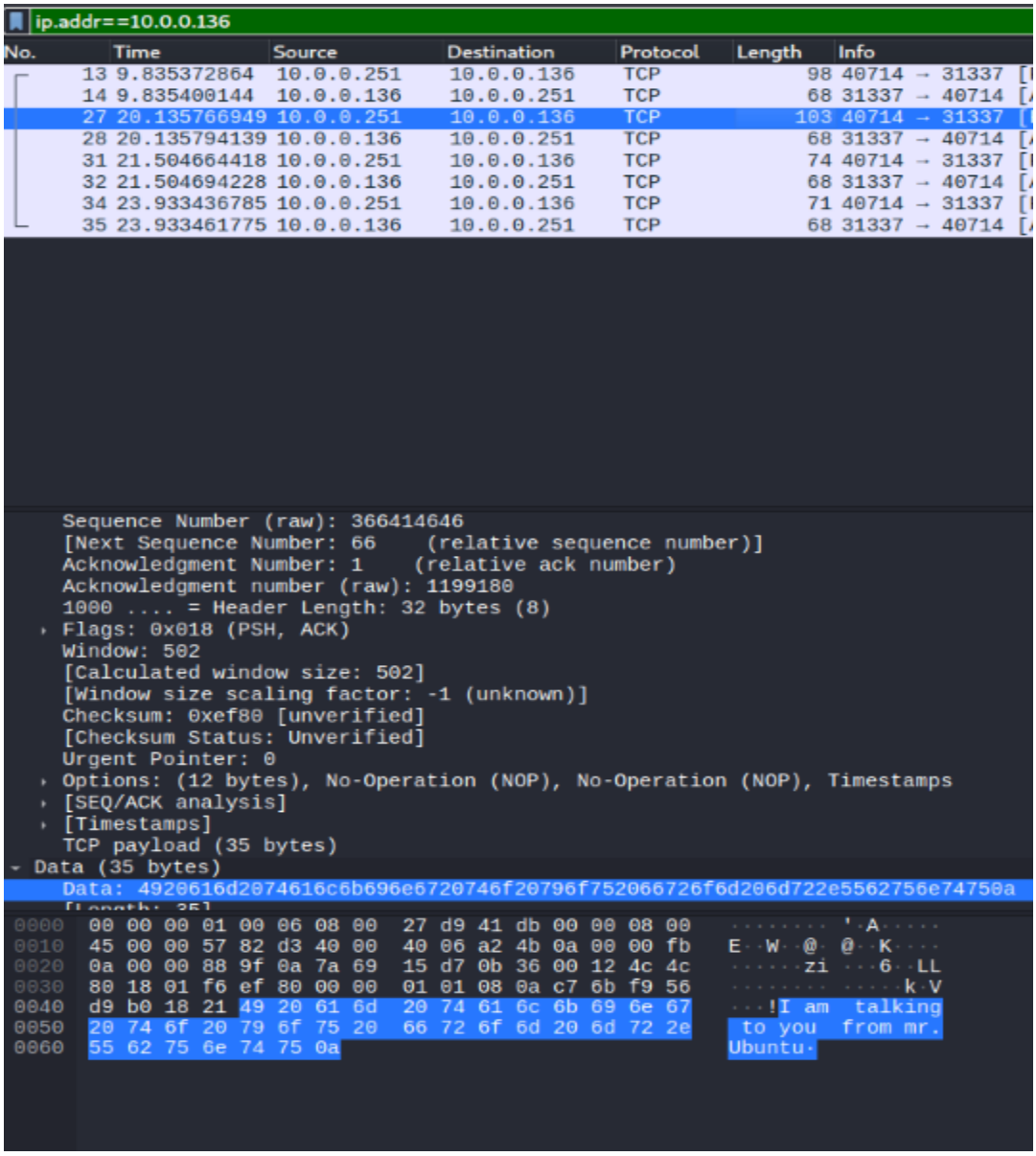
In Kali Linux, using Wireshark we can see the IP address from the Ubuntu machine as a TCP protocol.



To view all of the packets being sent/received from the Ubuntu VM, type in ‘ip.addr==10.0.0.136’ or ‘ip.addr==10.0.0.251’ into the filter to view the packets being communicated between the two machines.



Wireshark is able to thoroughly inspect packet data and display it in an easy-to-read format. Data such as:
No. : Order of the packet when captured.
Time: How long it took for the packet to be captured.
Source: Address of the system sent from the packet.
Destination: Address of the system receiving the packet.
Protocol: Type of packet.
Length: Length of the packet in bytes.
Info: More information about the packet.
Packet Bytes: Data displayed in hexadecimal or ASCII (message communicated between the Linux and Ubuntu machine is located here)



Conclusion

Wireshark is able to capture network packets and displays the content of the packets in an easy-to-read format, which is especially useful when troubleshooting issues like malicious activity, dropped packets, and in general allowing you to thoroughly analyze every packet in detail. Wireshark is best used when the user has knowledge of how a network operates, in order to understand the details provided by Wireshark.