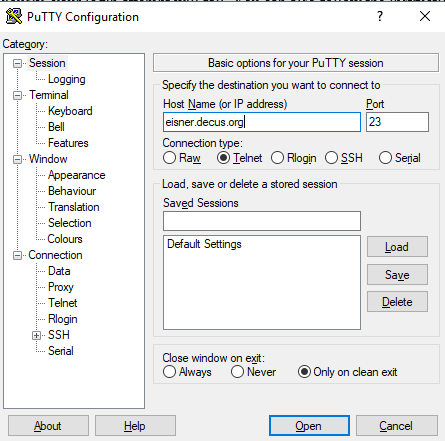
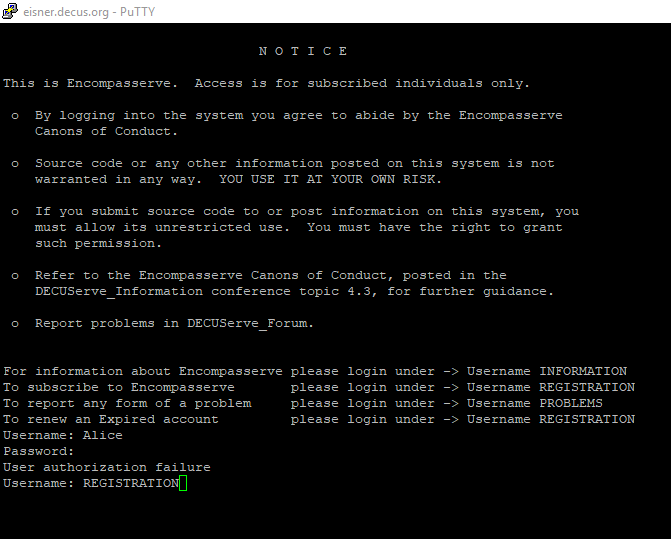
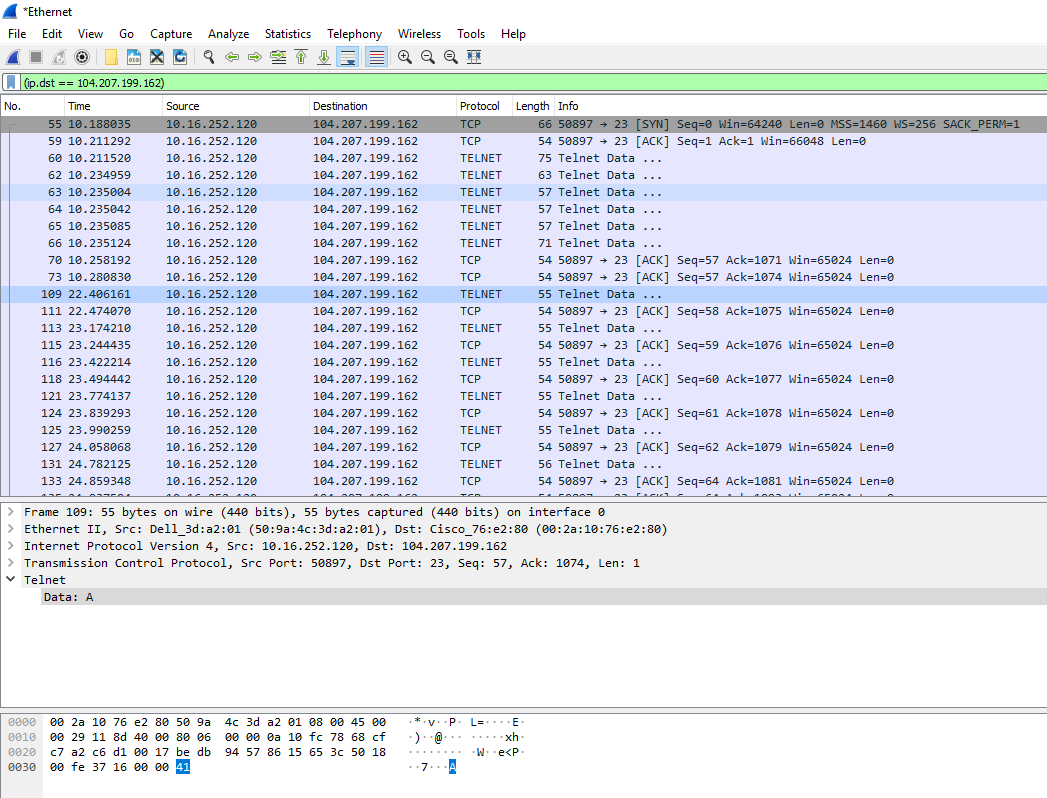
**PROJECT 1 : PACKET EAVESDROPPING AND ANALYSIS**

For this project I have used **PuTTY** for TELNET & SSH and **Wireshark** for capturing packets.

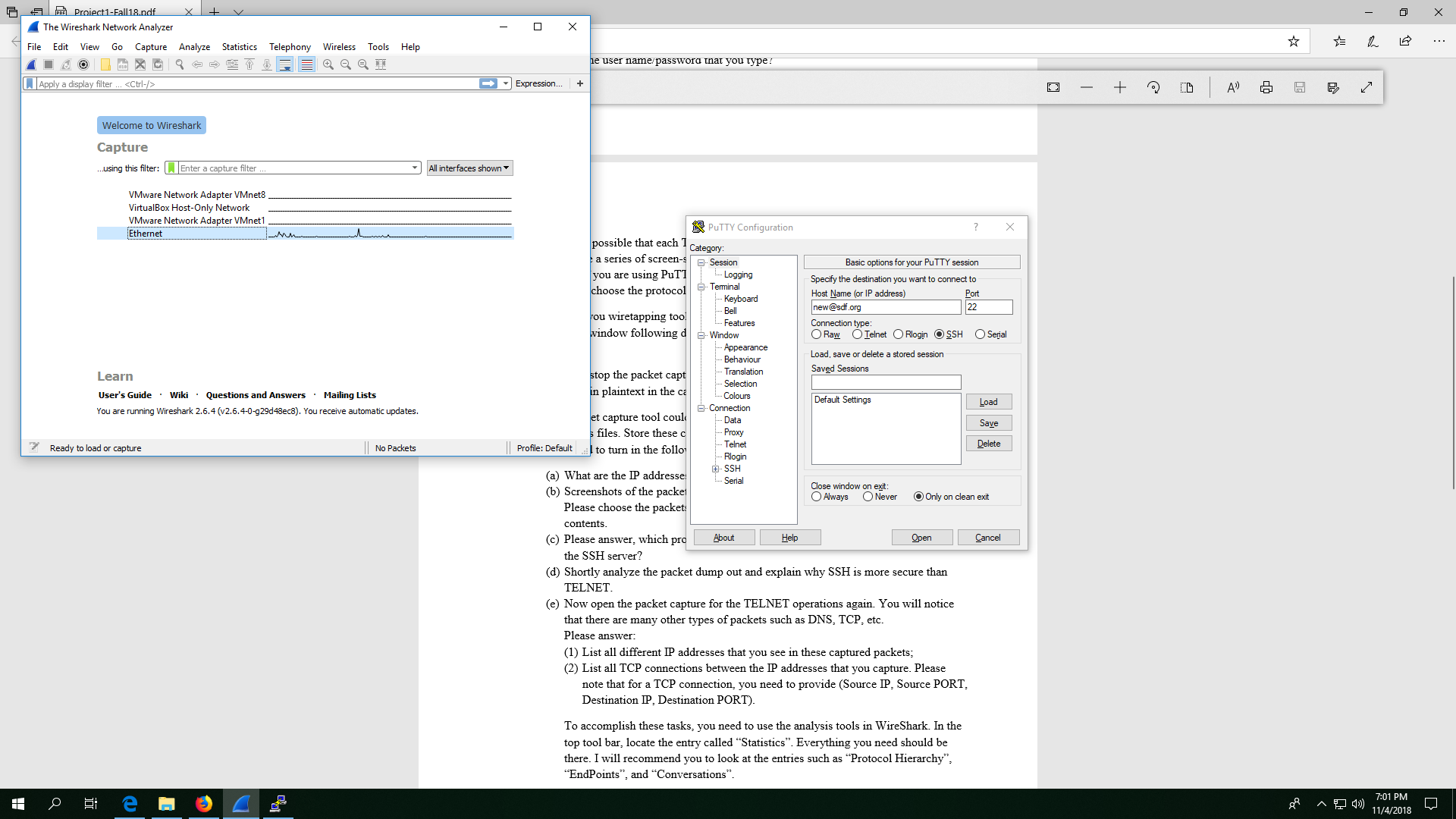
**TELNET:**

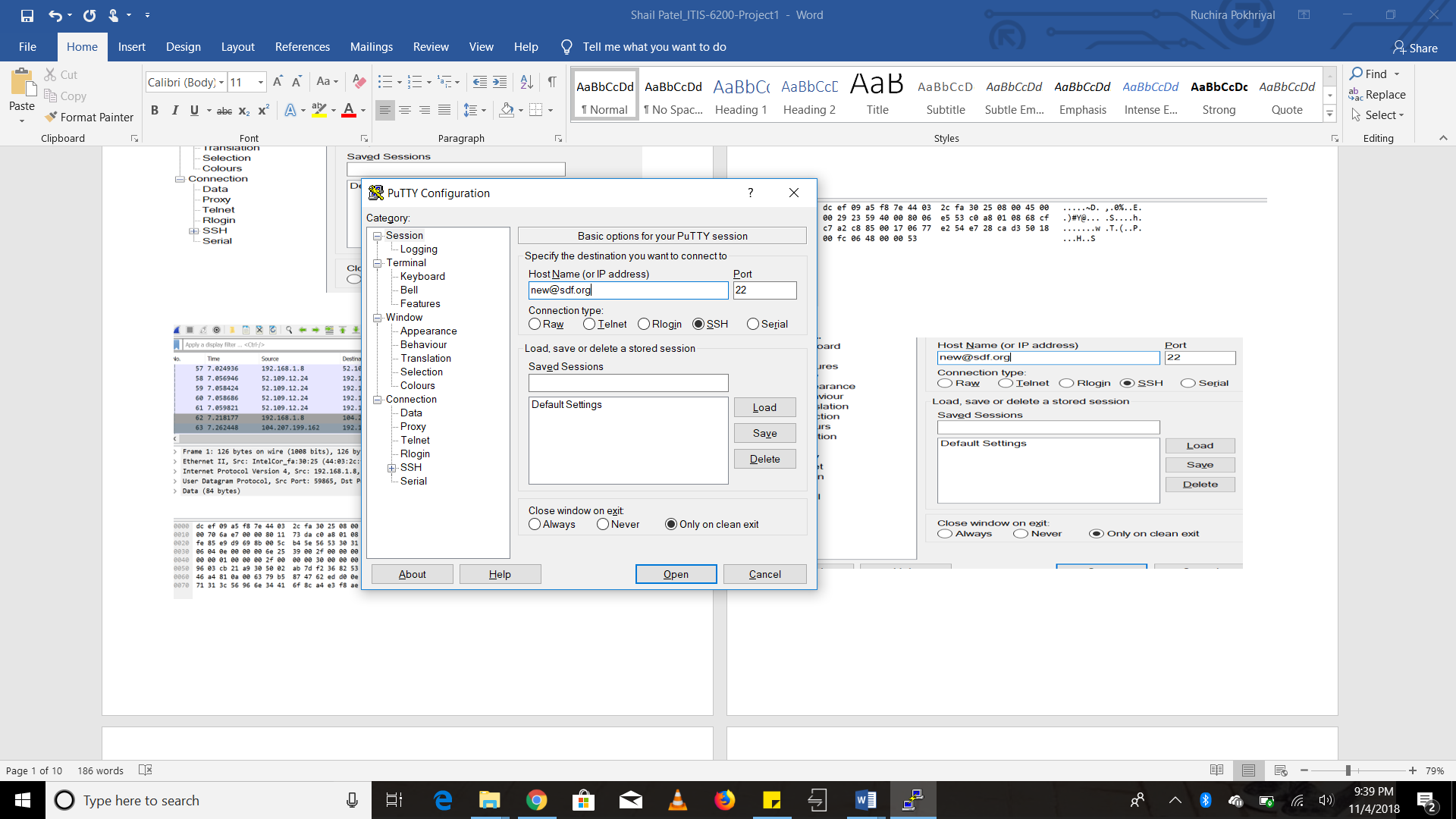


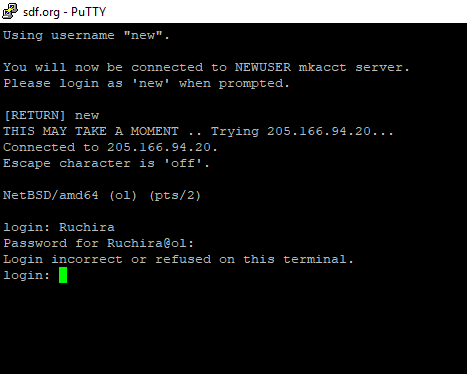


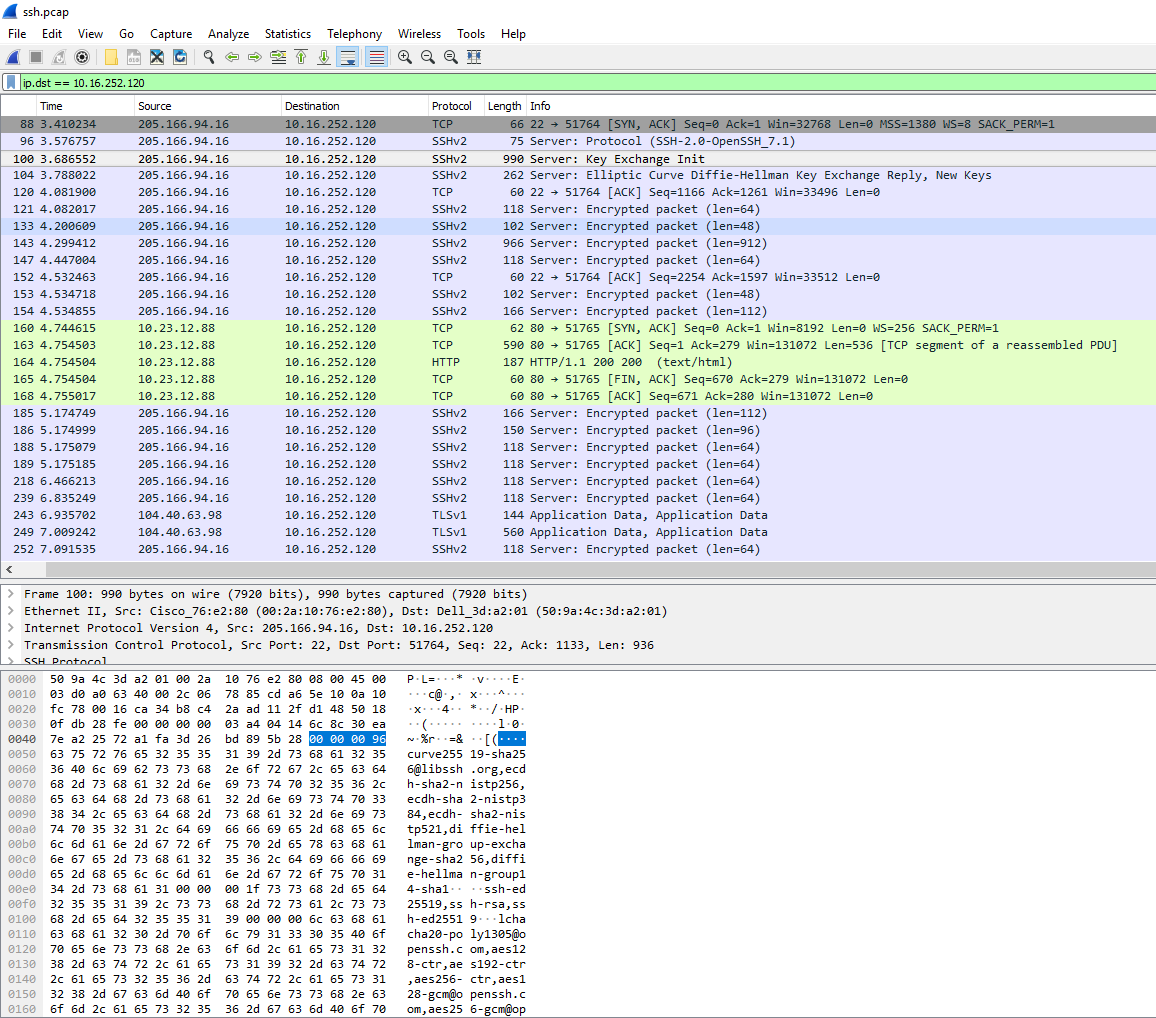


**SSH:**







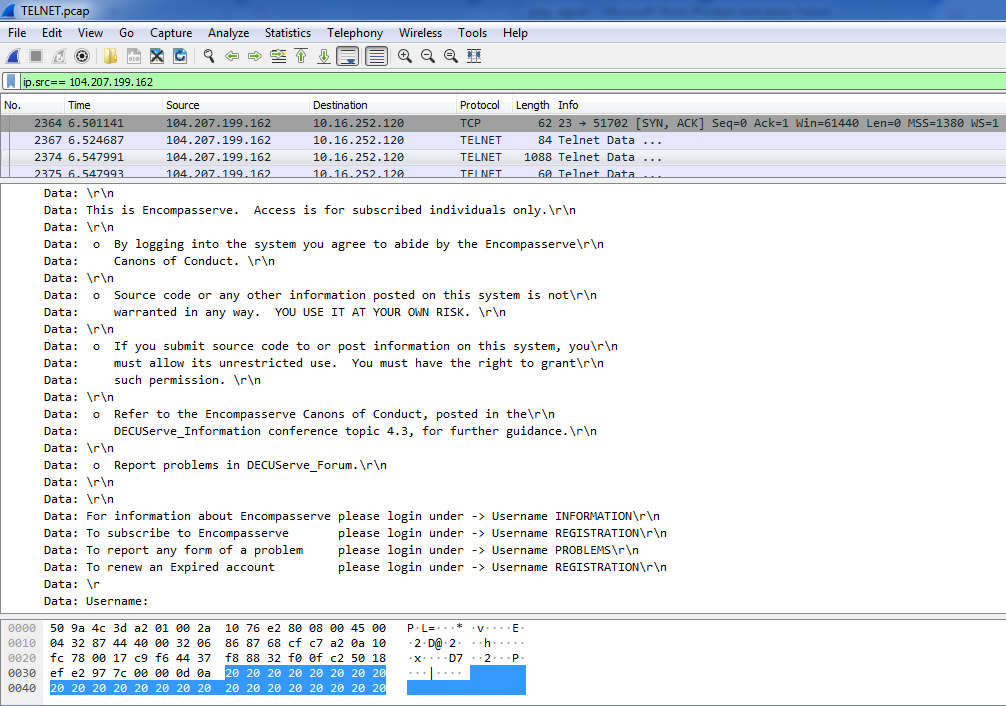


1. **What are the IP addresses of “eisner.decus.org” and “new@sdf.org”?**

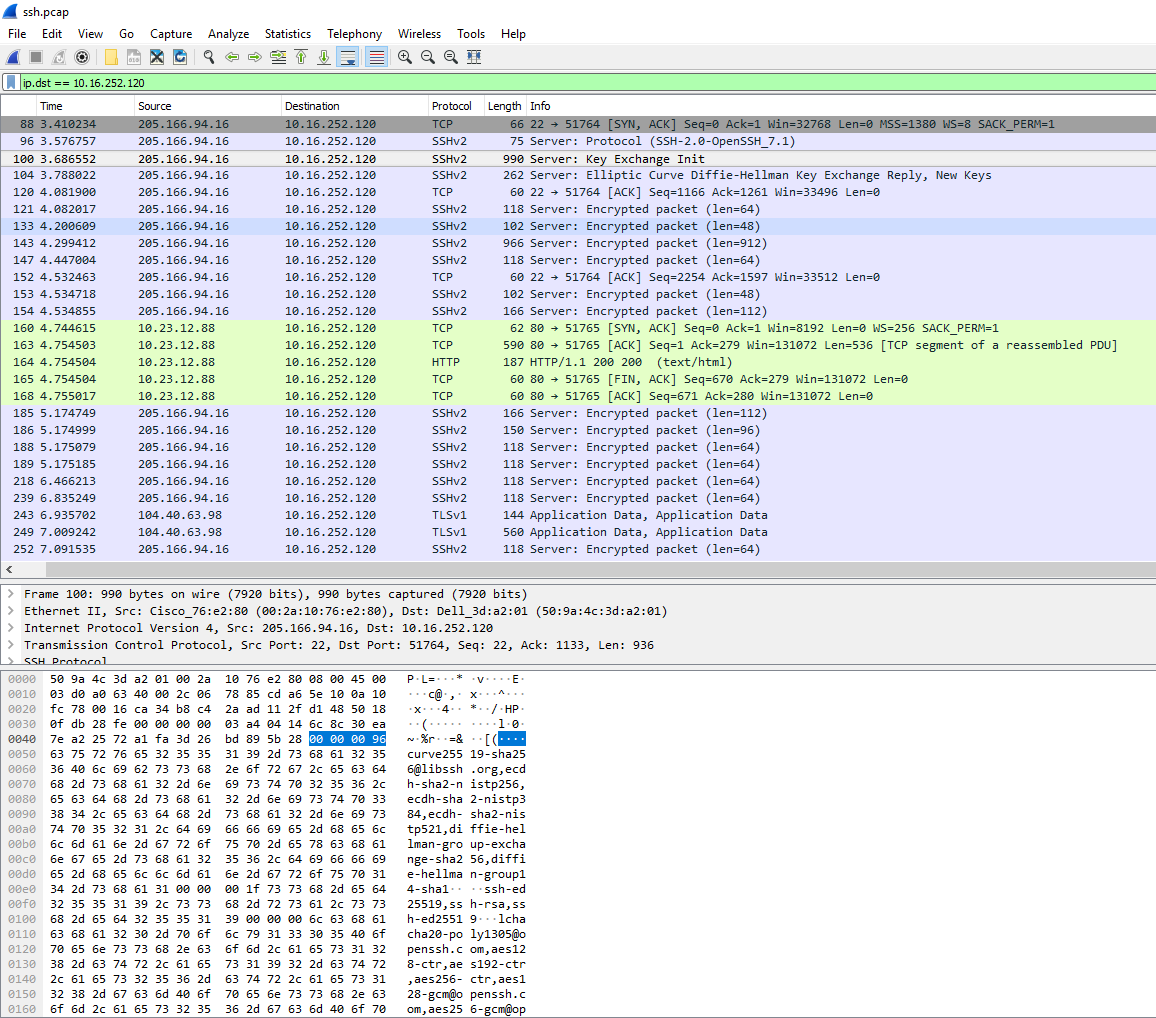
* The IP address of “***eisner.decus.or*g”** is: **104.207.199.162**
* The IP address of “[**new@sdf.org**](mailto:new@sdf.org)**”** is: **205.166.94.16**

**(b) Screenshots of the packet dump for the TELNET operation and the SSH operation.**

**Screenshots of packet dump for TELNET:**



**Screenshot of packet dump for SSH:**



**(c) Please answer, which protocol does PuTTY use to establish encryption key with the SSH server?**

* As seen in the above screenshot, PuTTY uses **Diffie-Hellman** protocol to establish encryption key with the SSH server.

1. **Shortly analyze the packet dump out and explain why SSH is more secure than TELNET.**

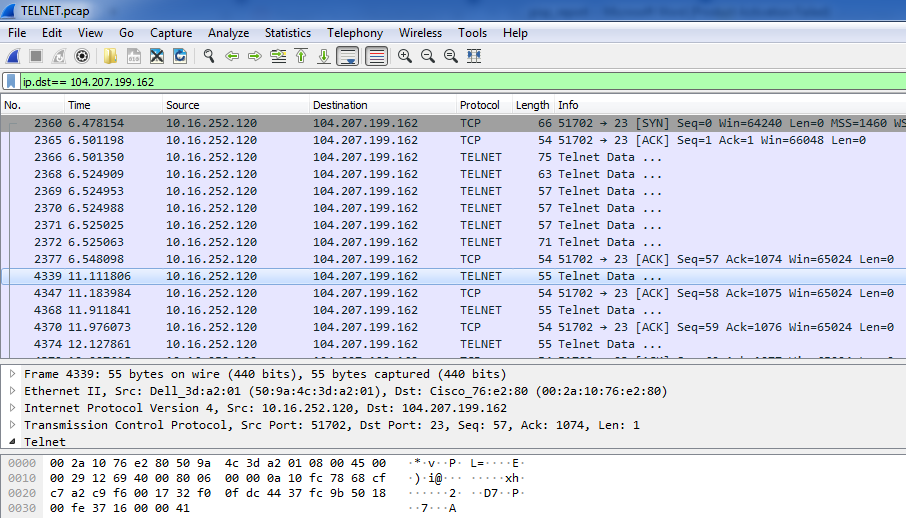
* It is evident from the screenshots below, that in Telnet communication the data (usernames and passwords) is sent over the communication channel in plaintext format. On the other hand, the data (usernames and passwords) is sent in encrypted format in an SSH connection, making it more secure.

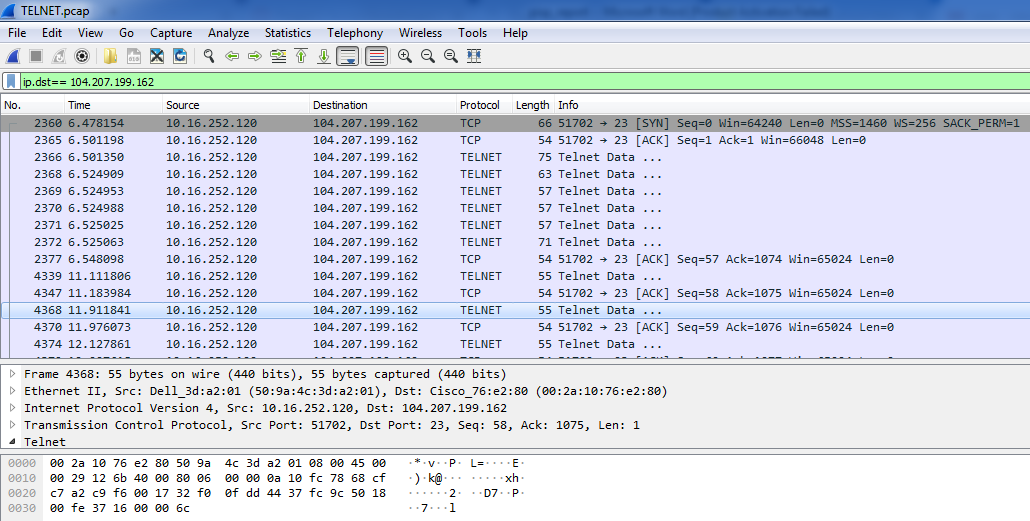
**Telnet Packets:**

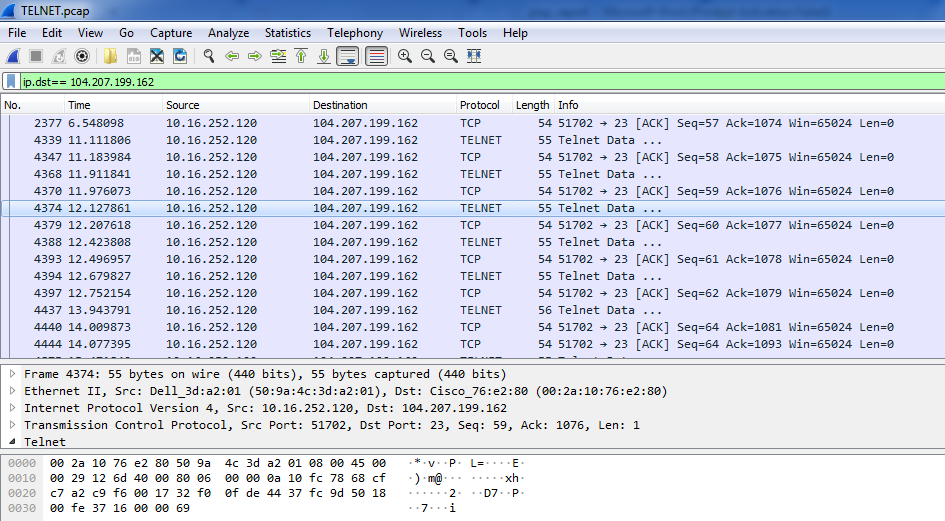
Username: Alice

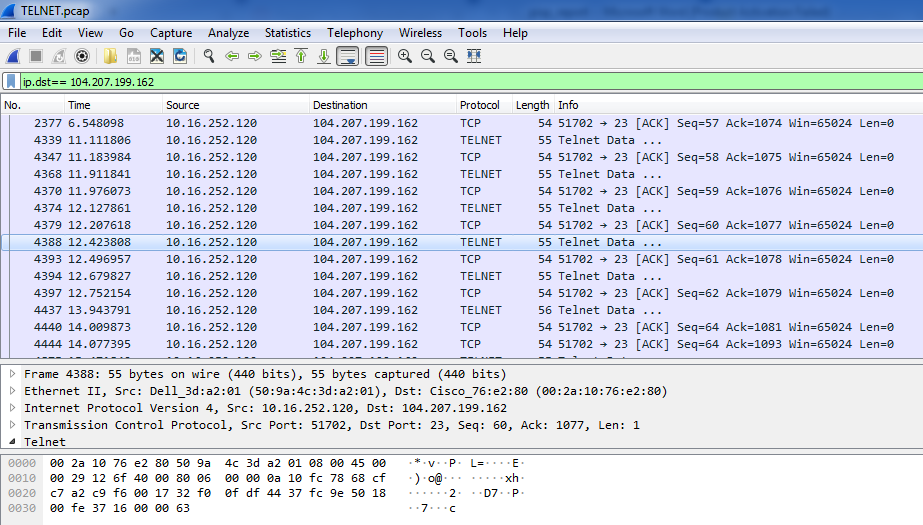
Password: 1234567

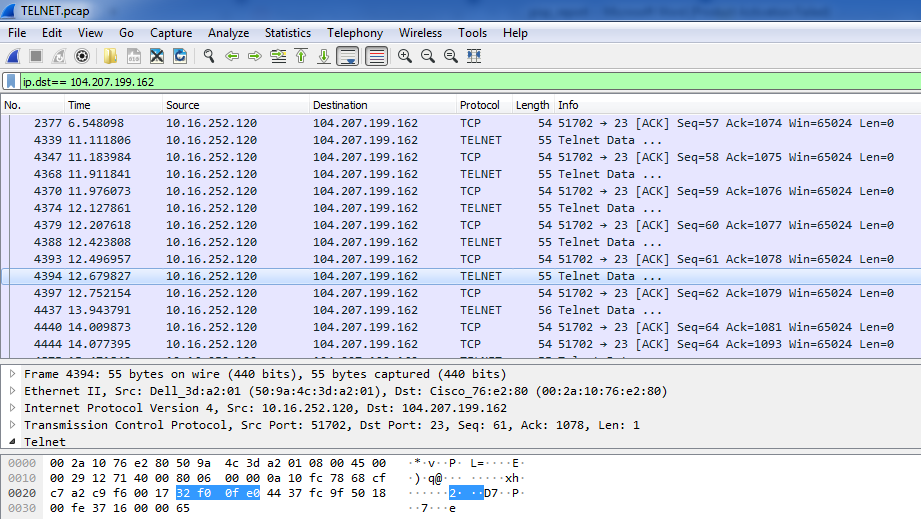
**Username can be seen in clear-text:**



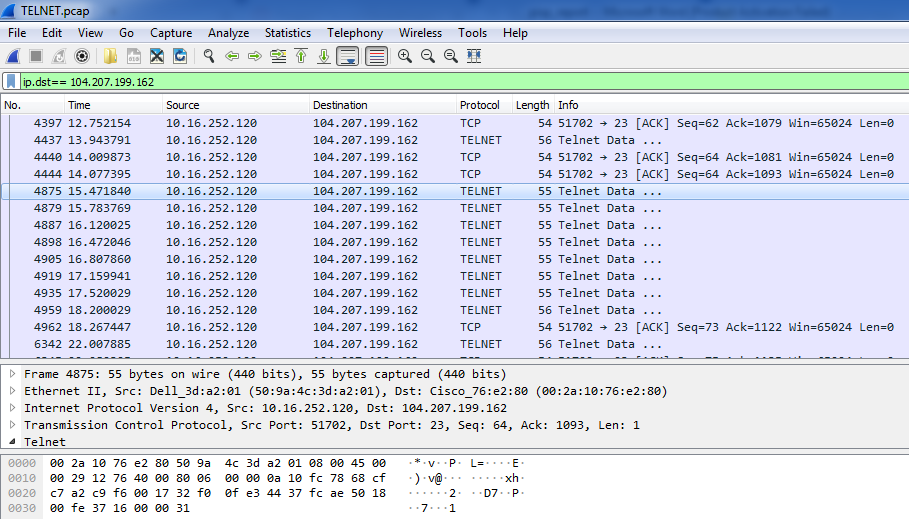


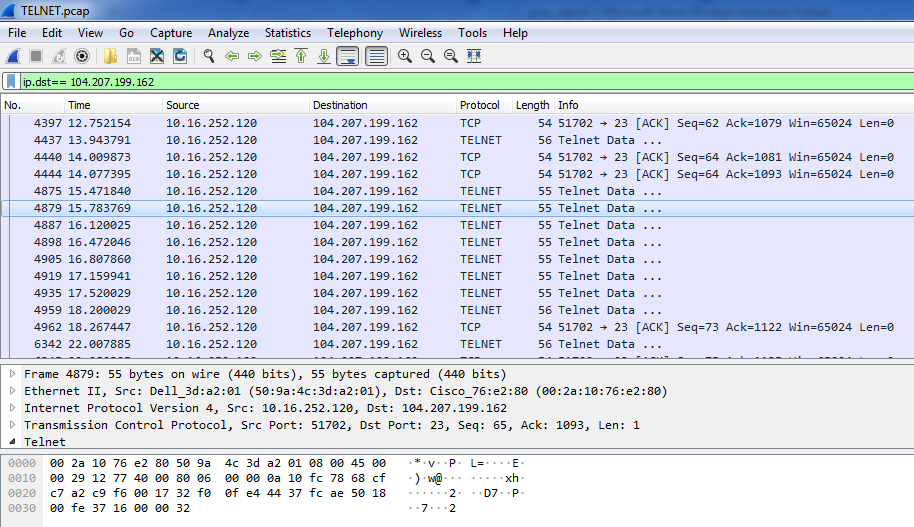


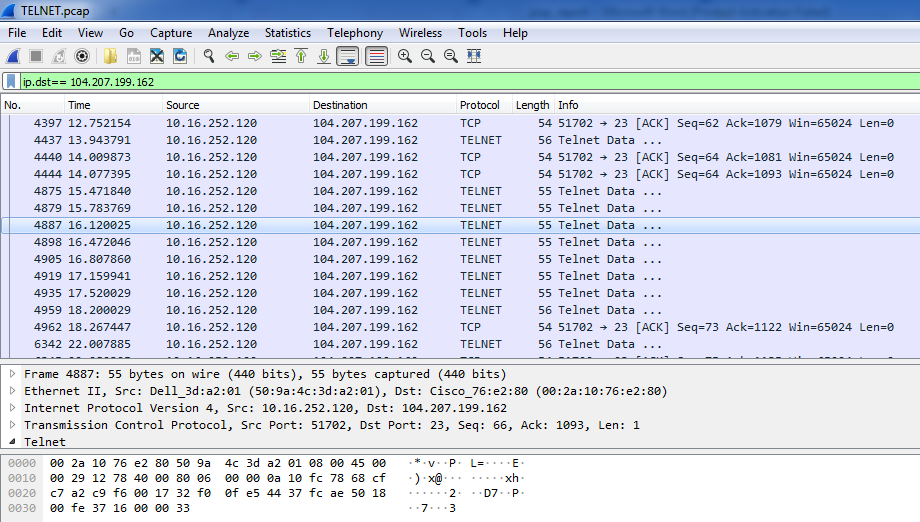


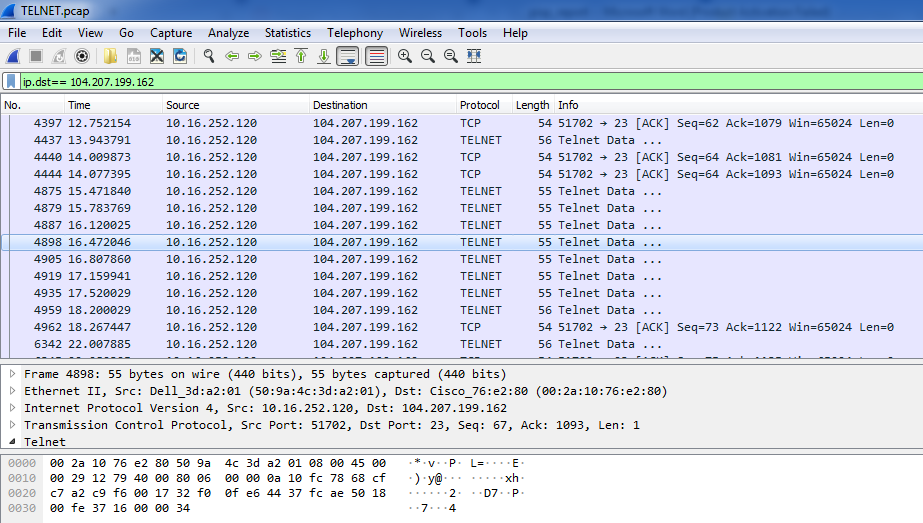


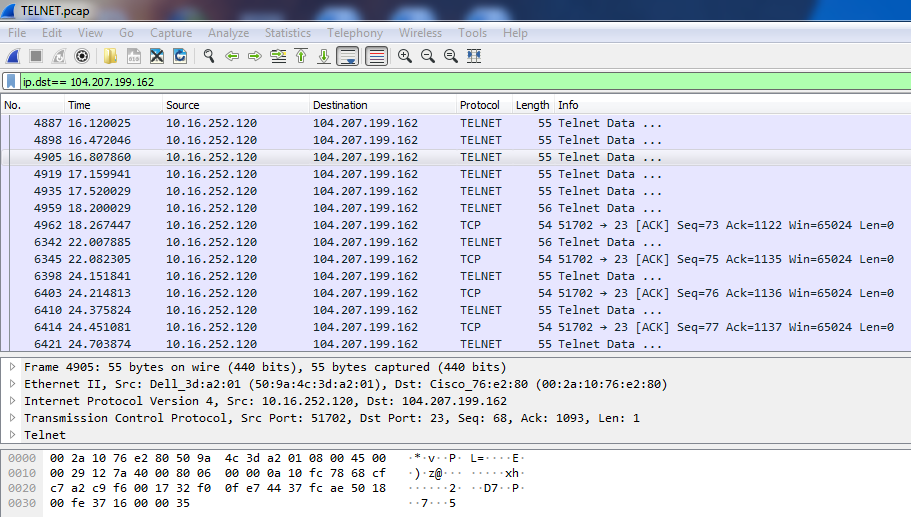
**Password can be seen in clear-text:**

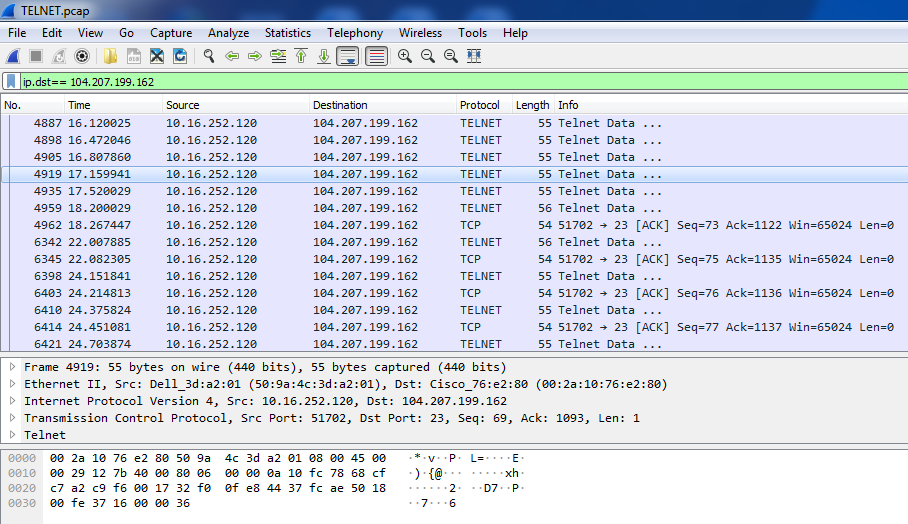


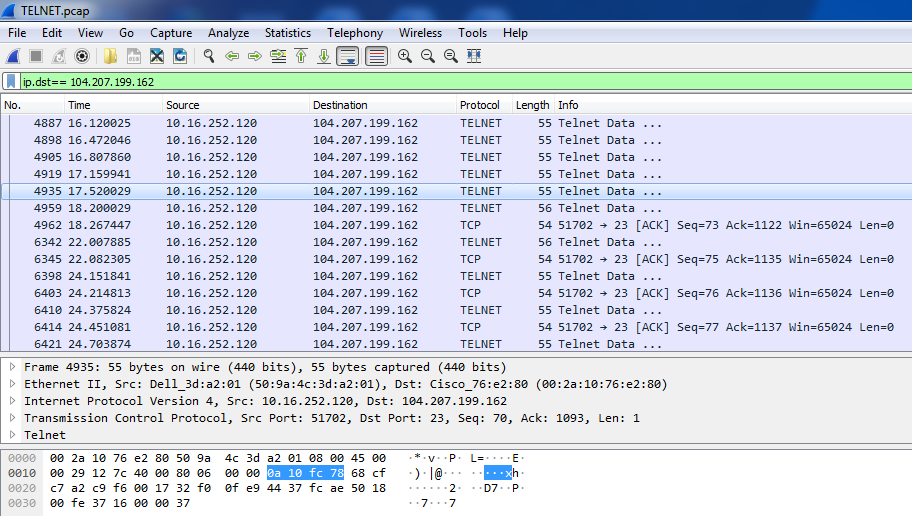










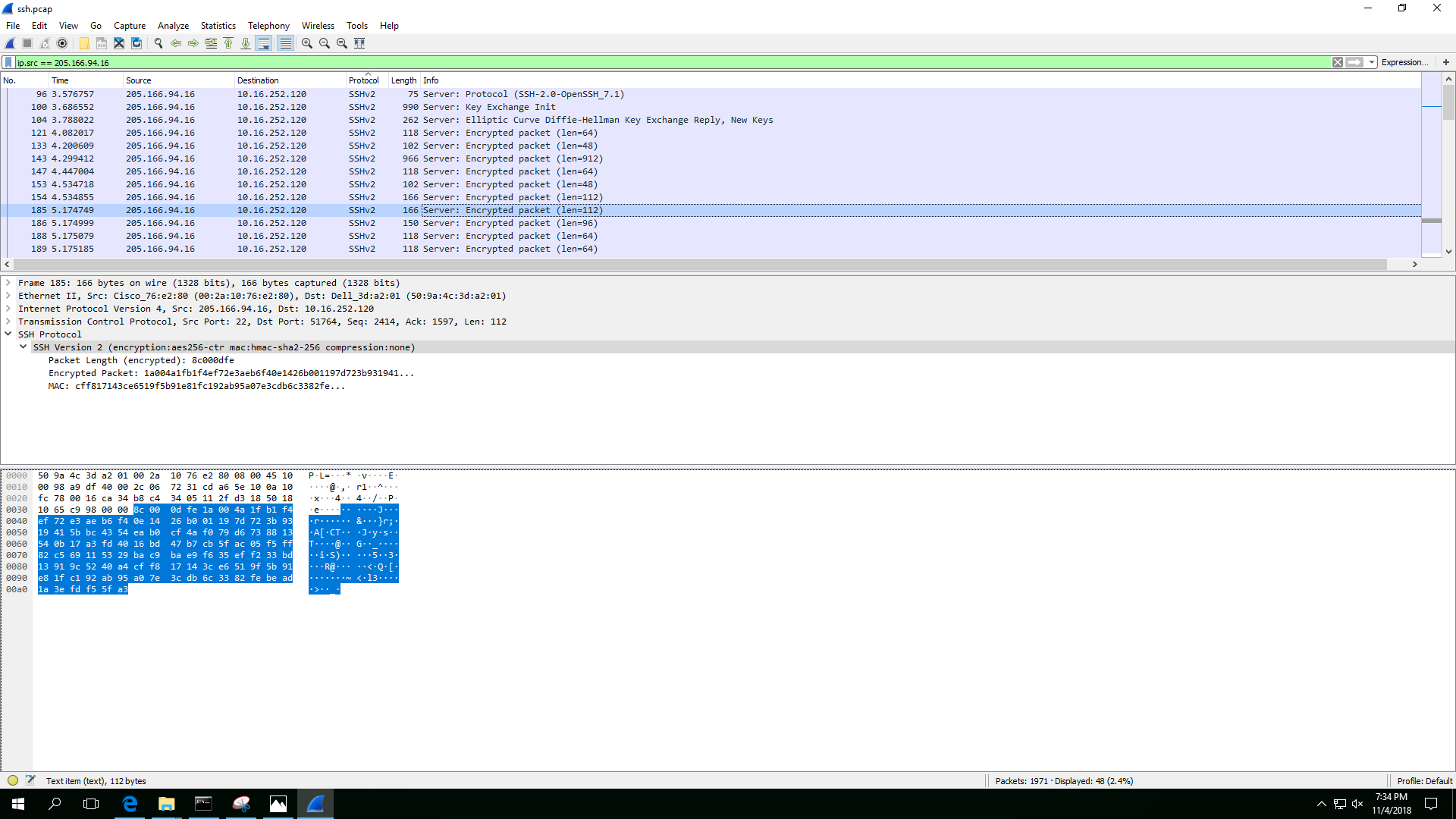


**SSH Packets:**

Username: Ruchira

Password: 1245

**Username and Password are encrypted in SSH and hence can not be seen in the screenshot below:**

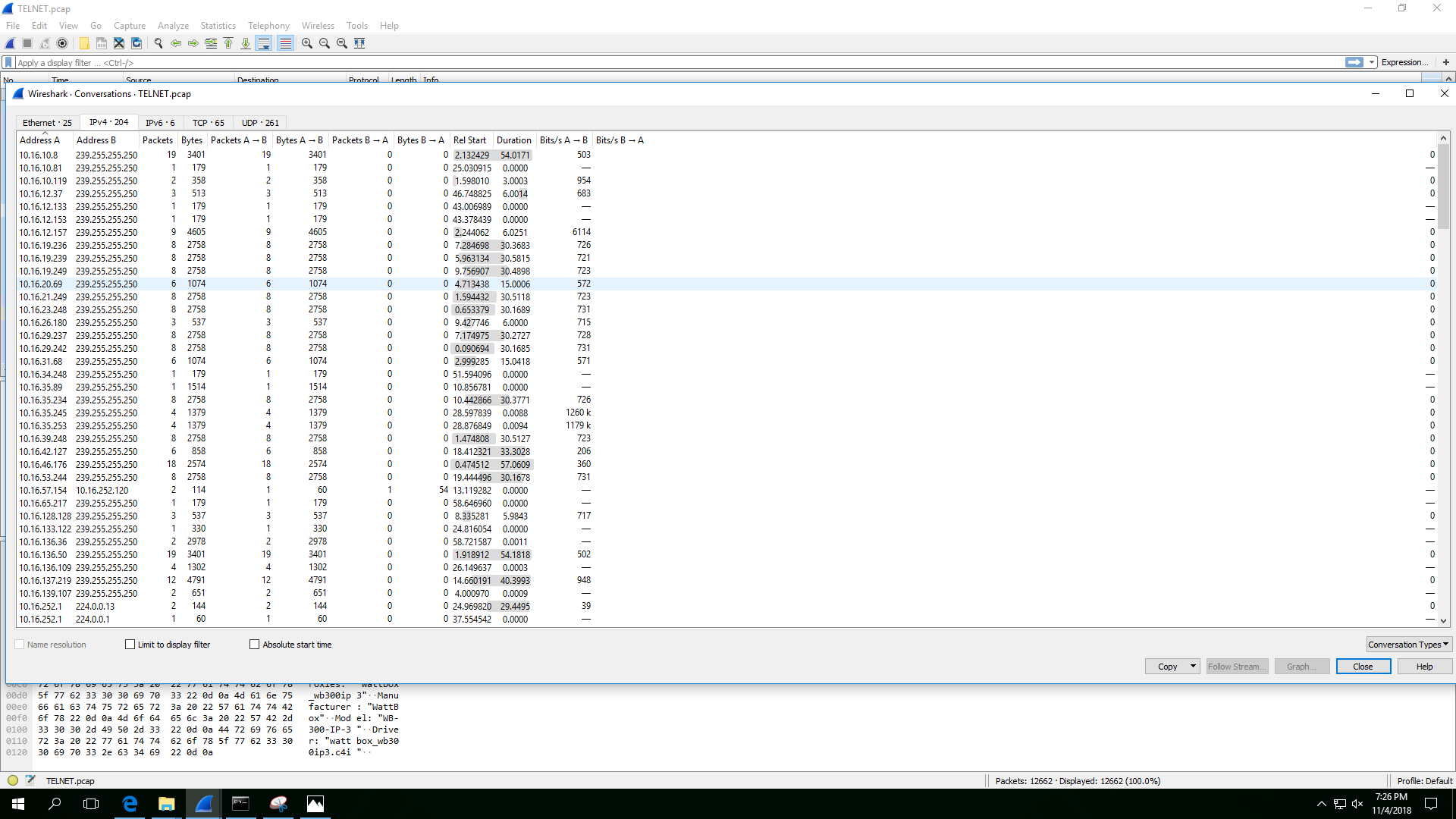


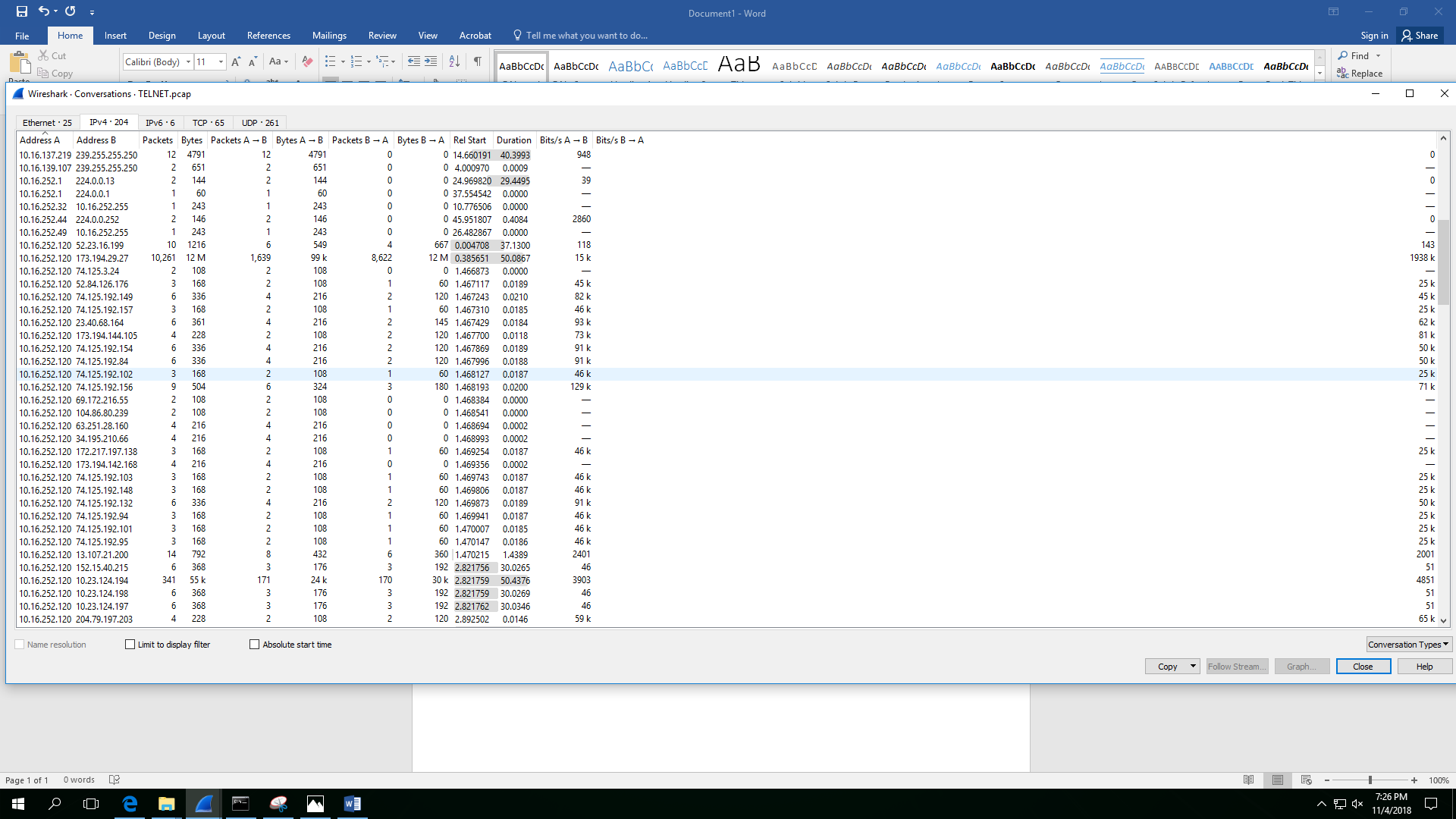
**(e) Now open the packet capture for the TELNET operations again. You will notice that there are many other types of packets such as DNS, TCP, etc.**

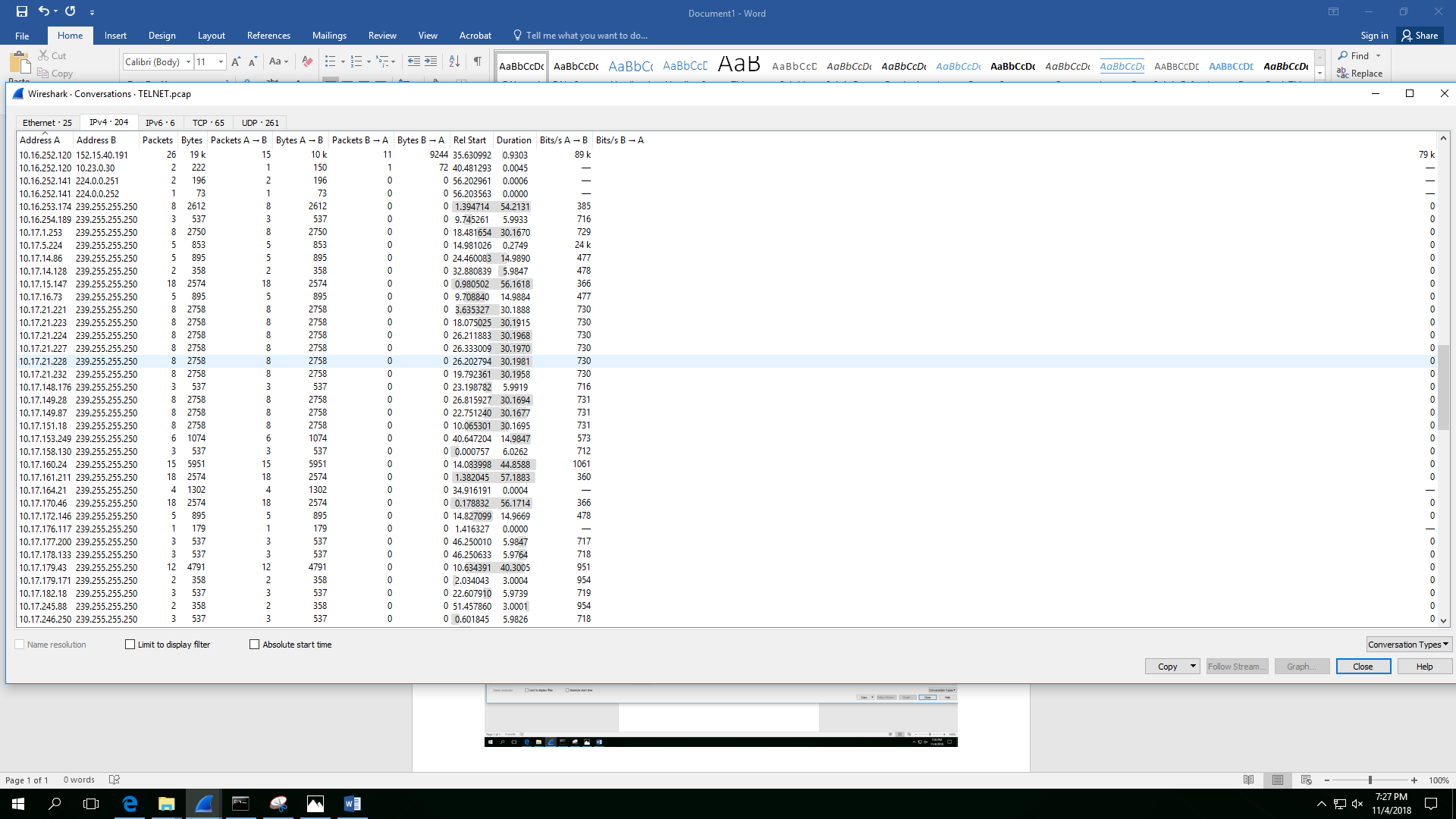
**Please answer:**

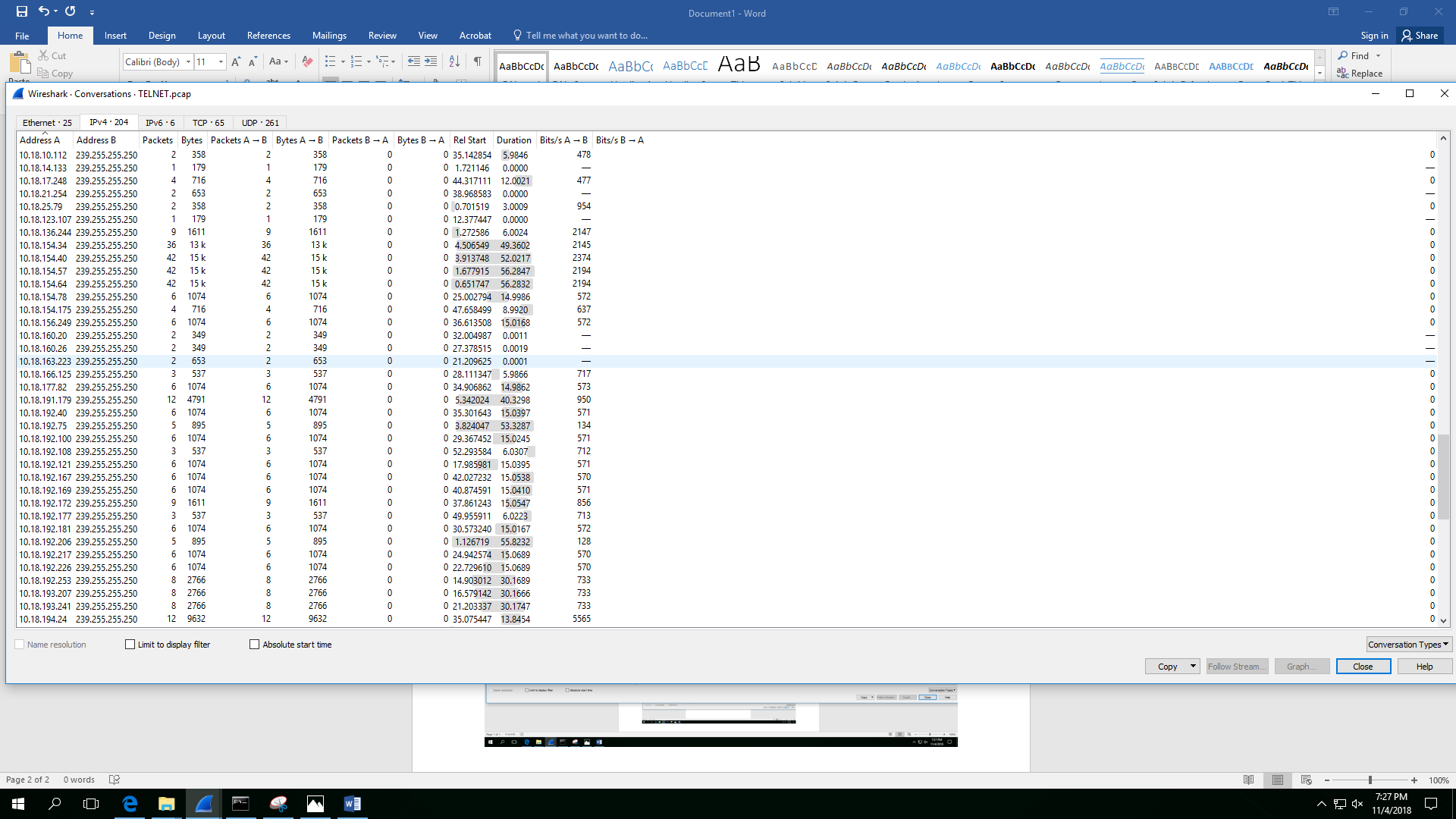
**(1) List all different IP addresses that you see in these captured packets;**

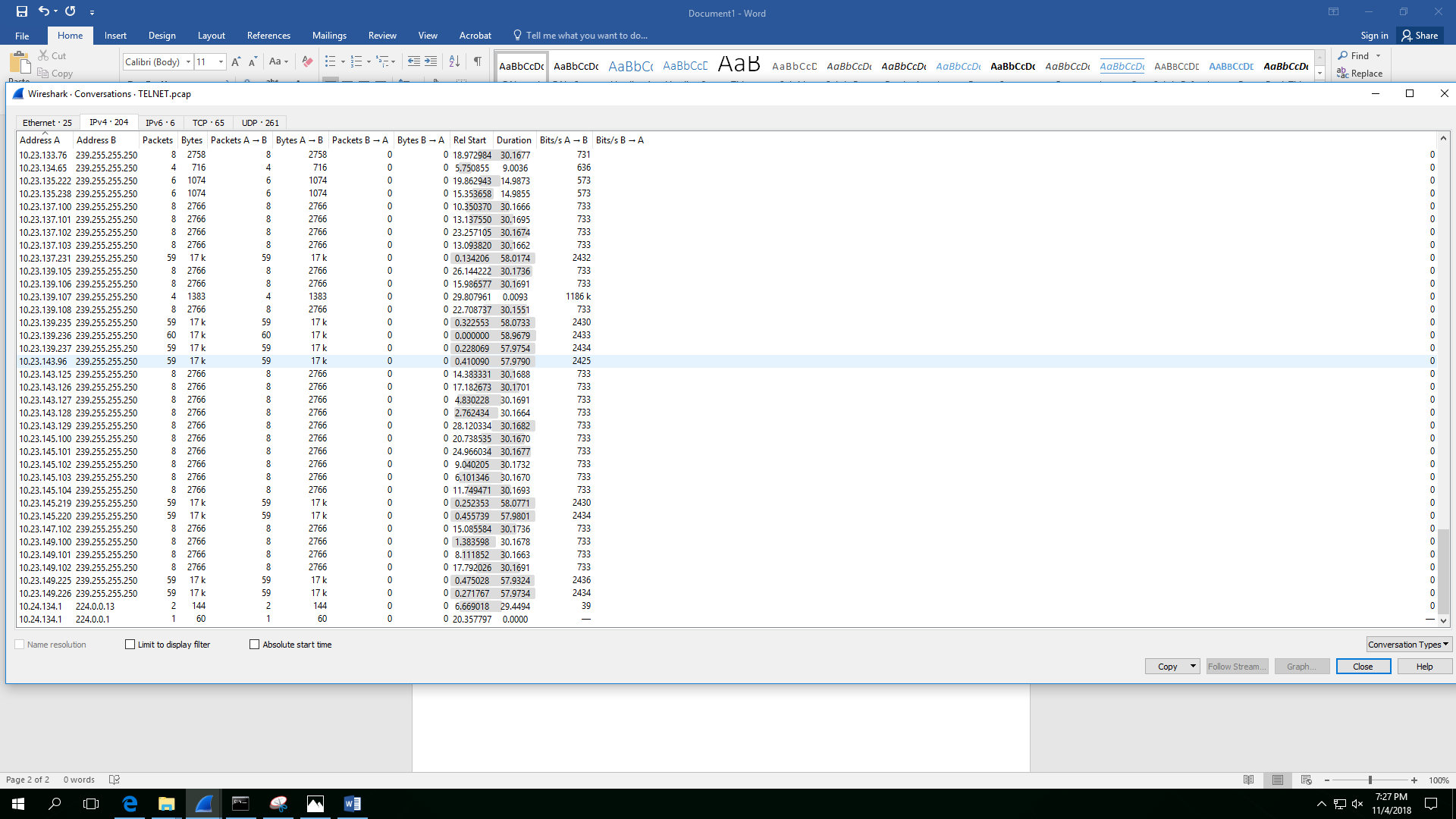
* The list of all the IPs that I can see in these captured packets are in the screenshot below:

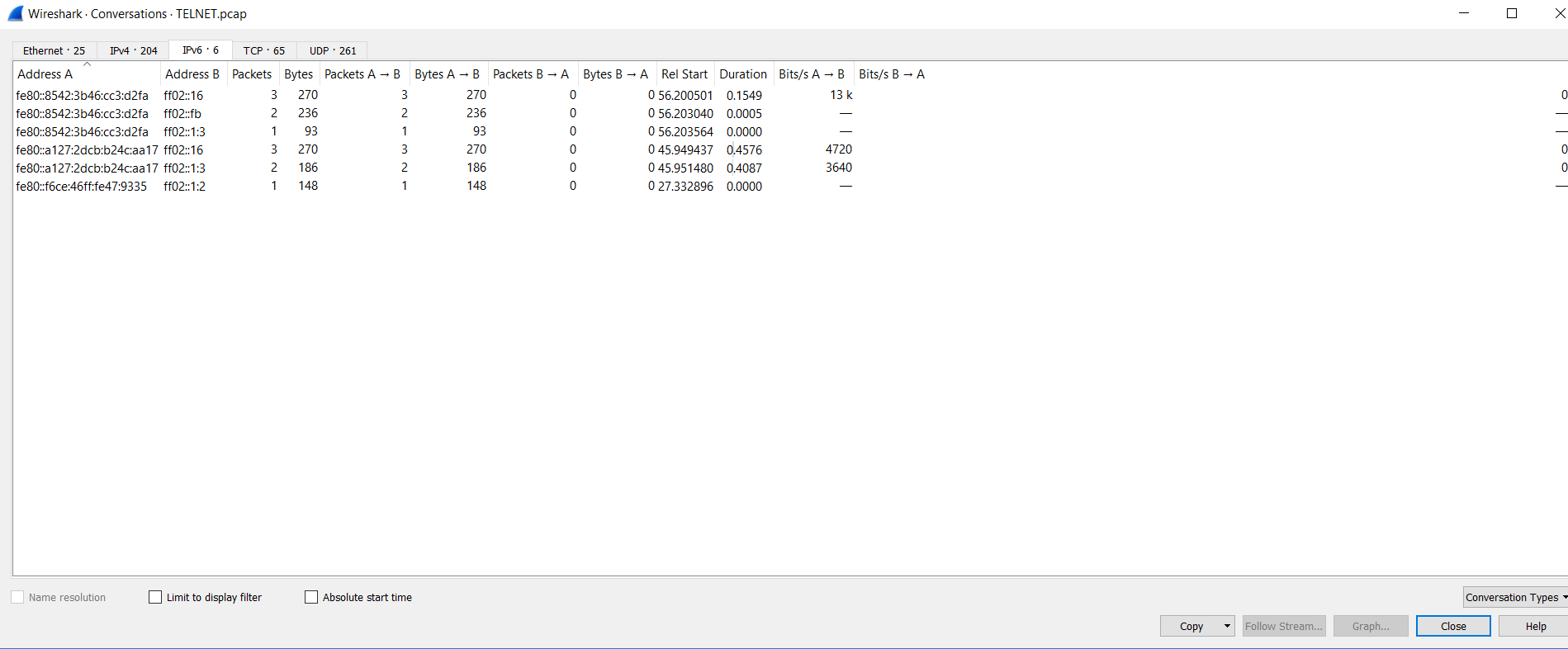








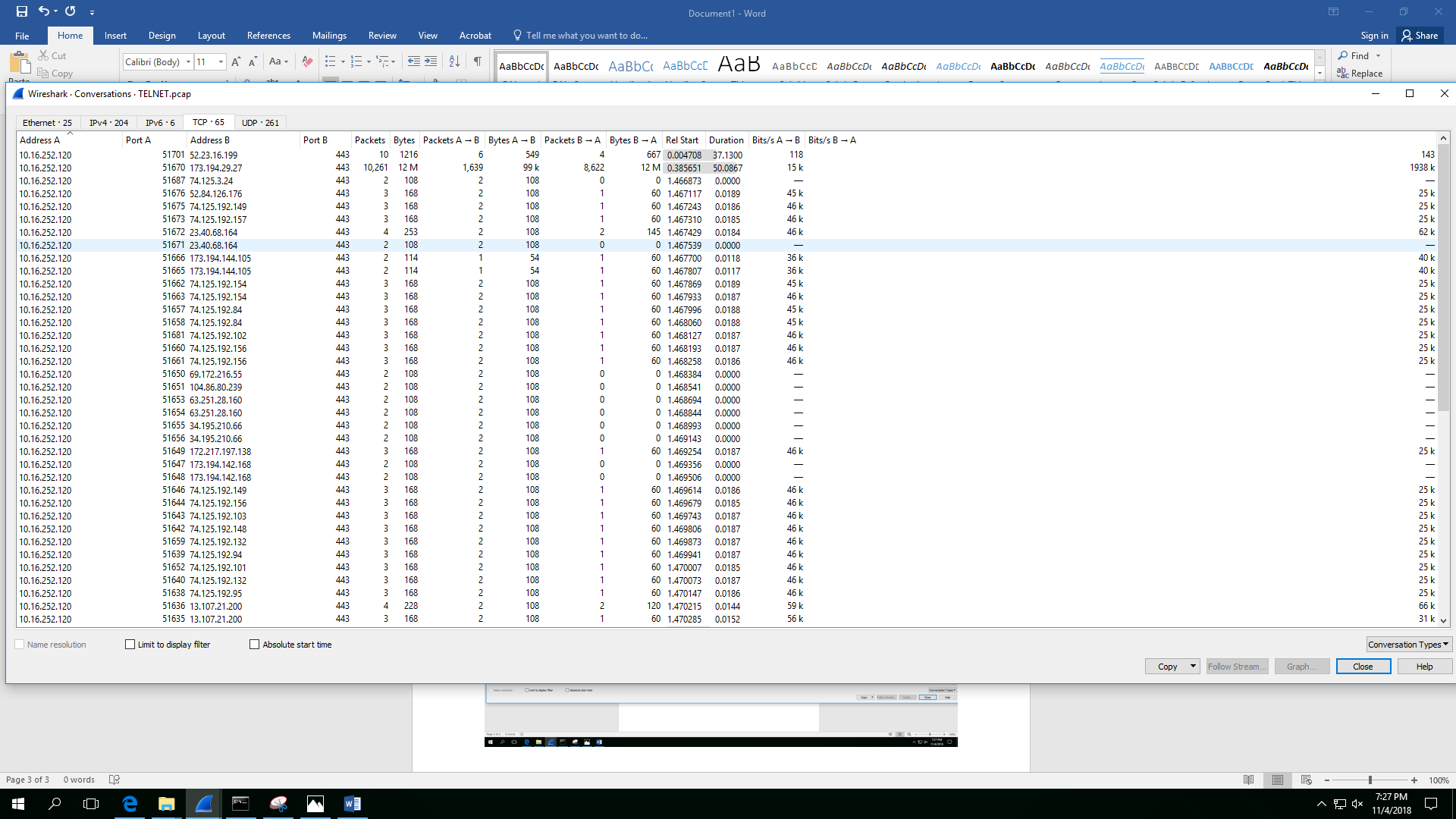


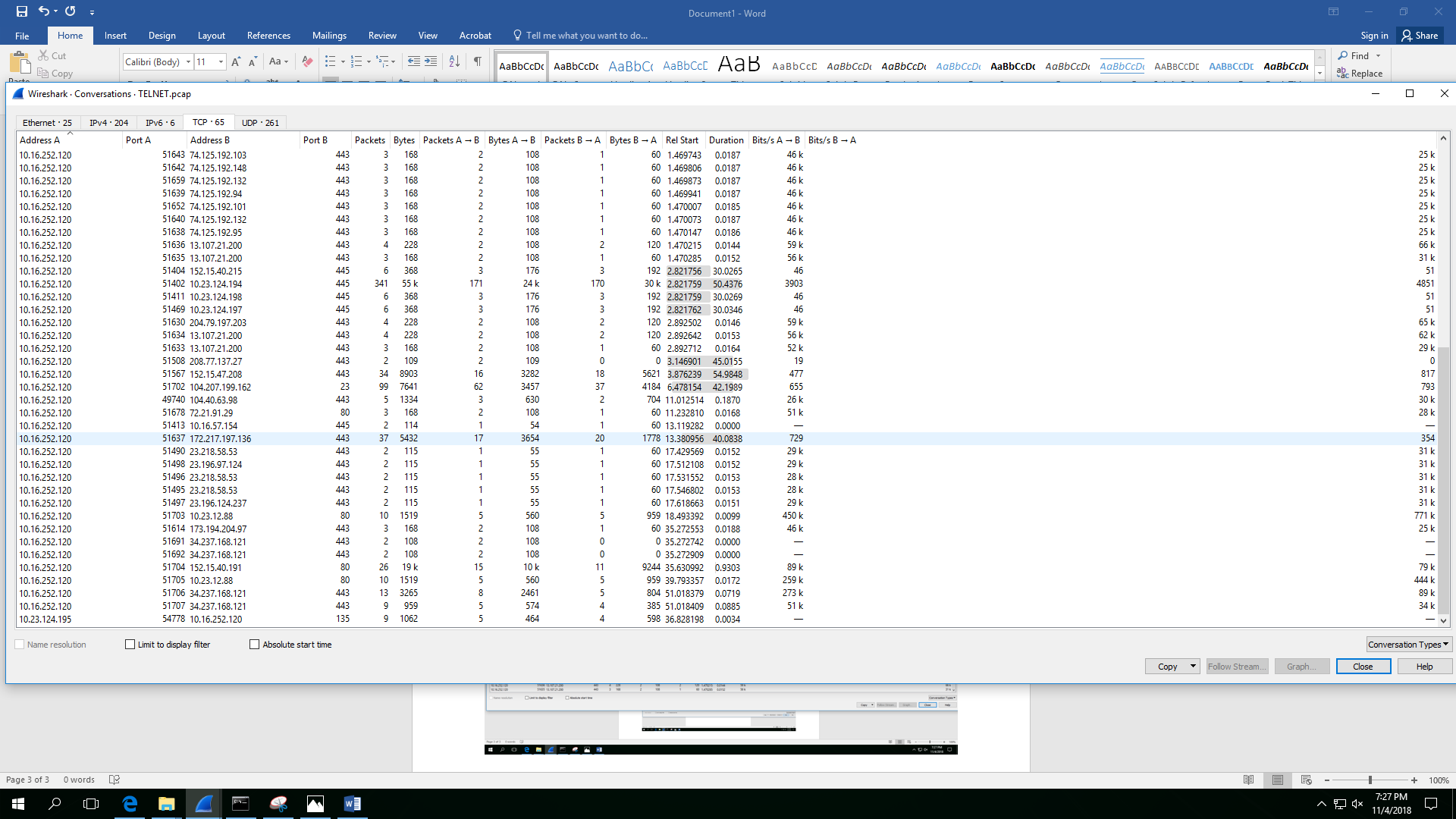


From the ‘Endpoints’ and ‘Conversation’ Tabs, As shown above, these are the IPv4 and IPv6 addresses.

**(2) List all TCP connections between the IP addresses that you capture. Please note that for a TCP connection, you need to provide (Source IP, Source PORT, Destination IP, Destination PORT).**

* A list of all TCP connections is given in the screenshots below:





As shown above, address A represents source IP, port A represents source port, address B represents destination IP and port B represents destination port.