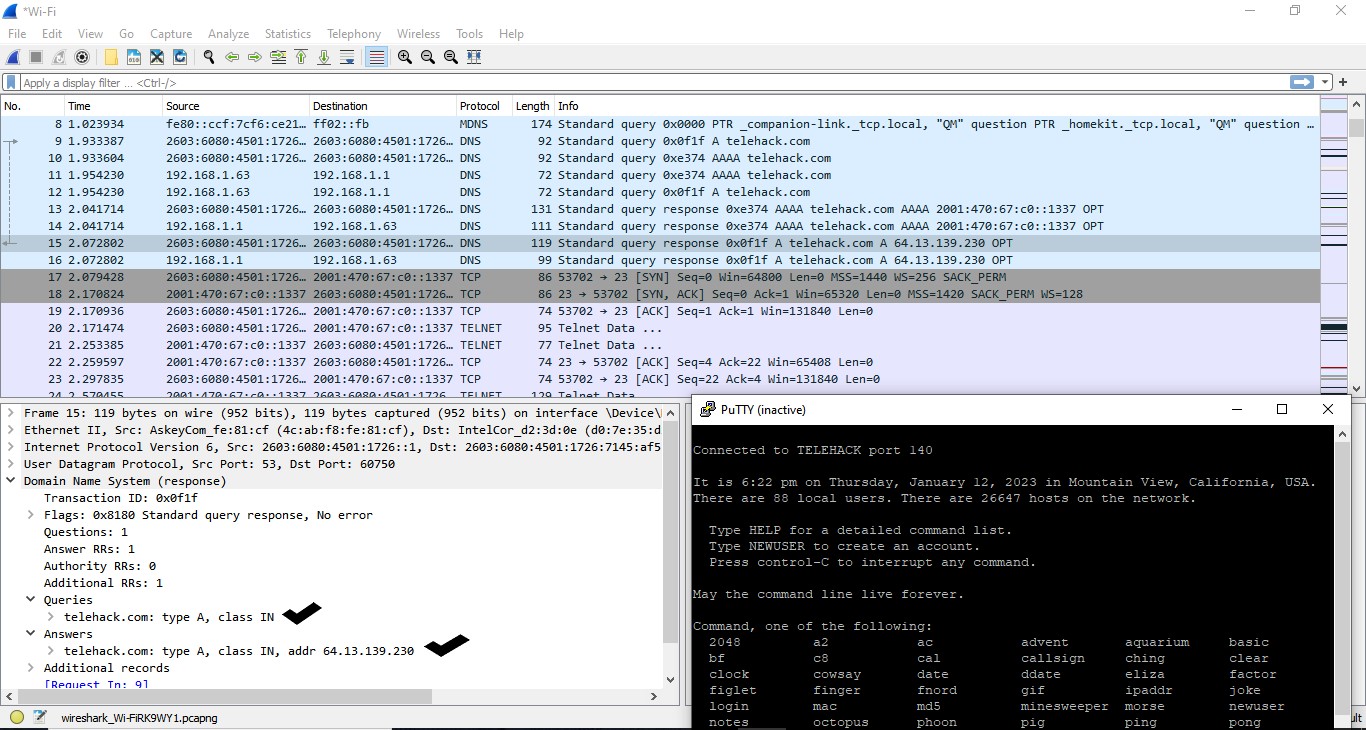
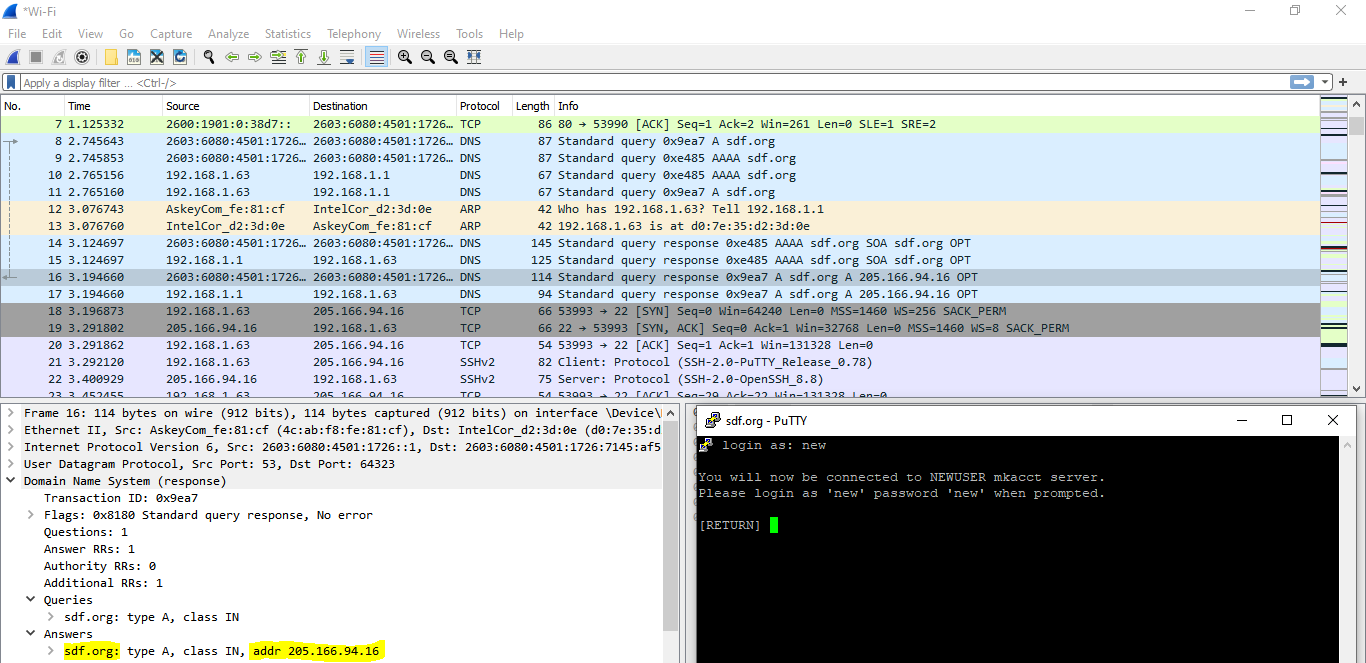
Project-1

1. What are the IP addresses of “telehack.com” and “sdf.org”?
2. The IP Address of **telehack.com is 64.13.139.230**. We can see that clearly in Wireshark. PFB Screenshots of PuTTy and Wireshark for your reference.

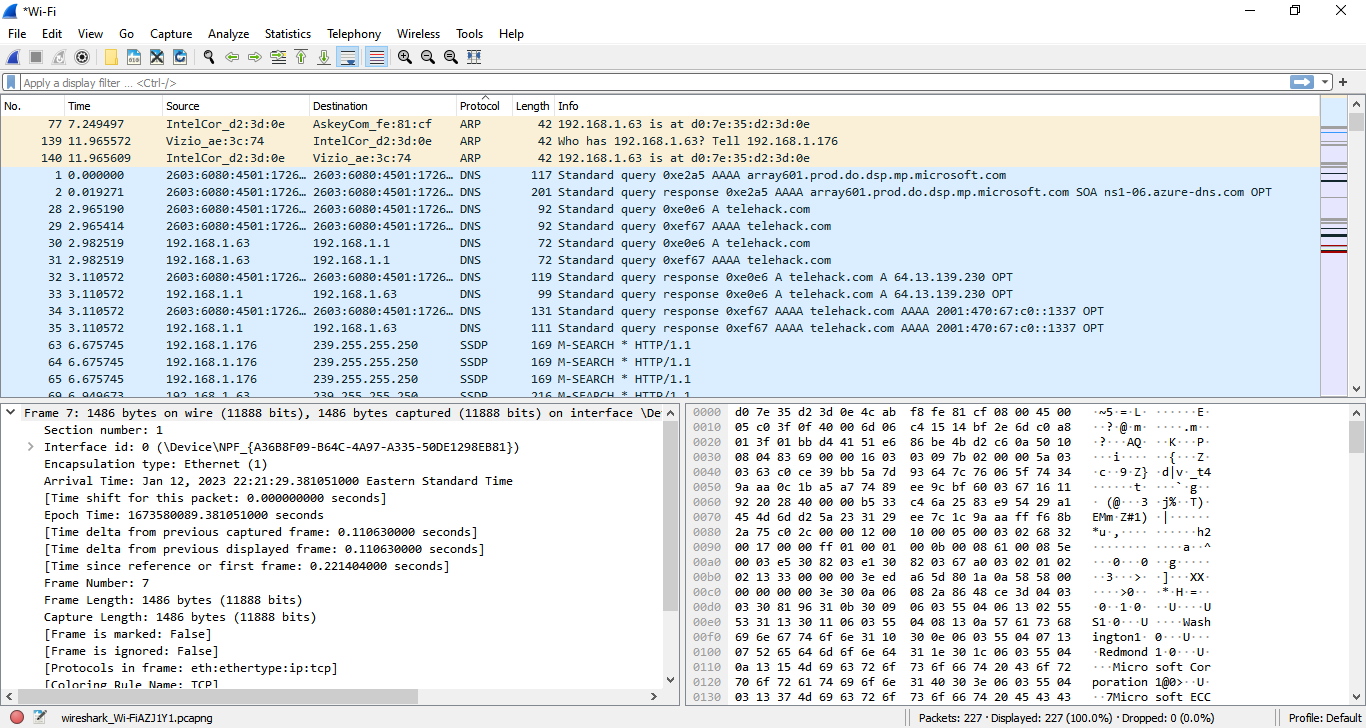


The IP Address of **sdf.org is 205.166.94.16**. We can see that clearly in Wireshark. PFB Screenshots of PuTTy and Wireshark for your reference

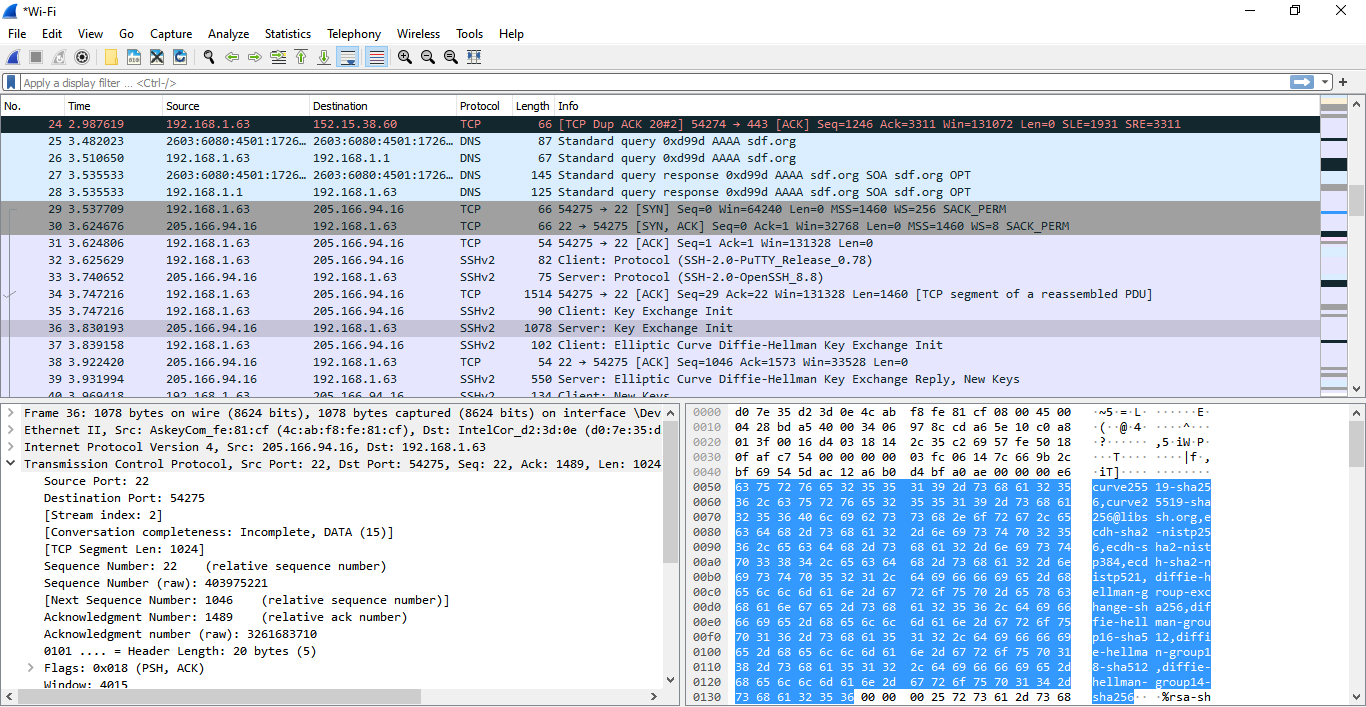


1. Screenshots of the packet dump for the TELNET operation and the SSH operation. Please  
   choose the packets with relatively large size so that we can see the data contents.

**TELNET Packet Dump**.

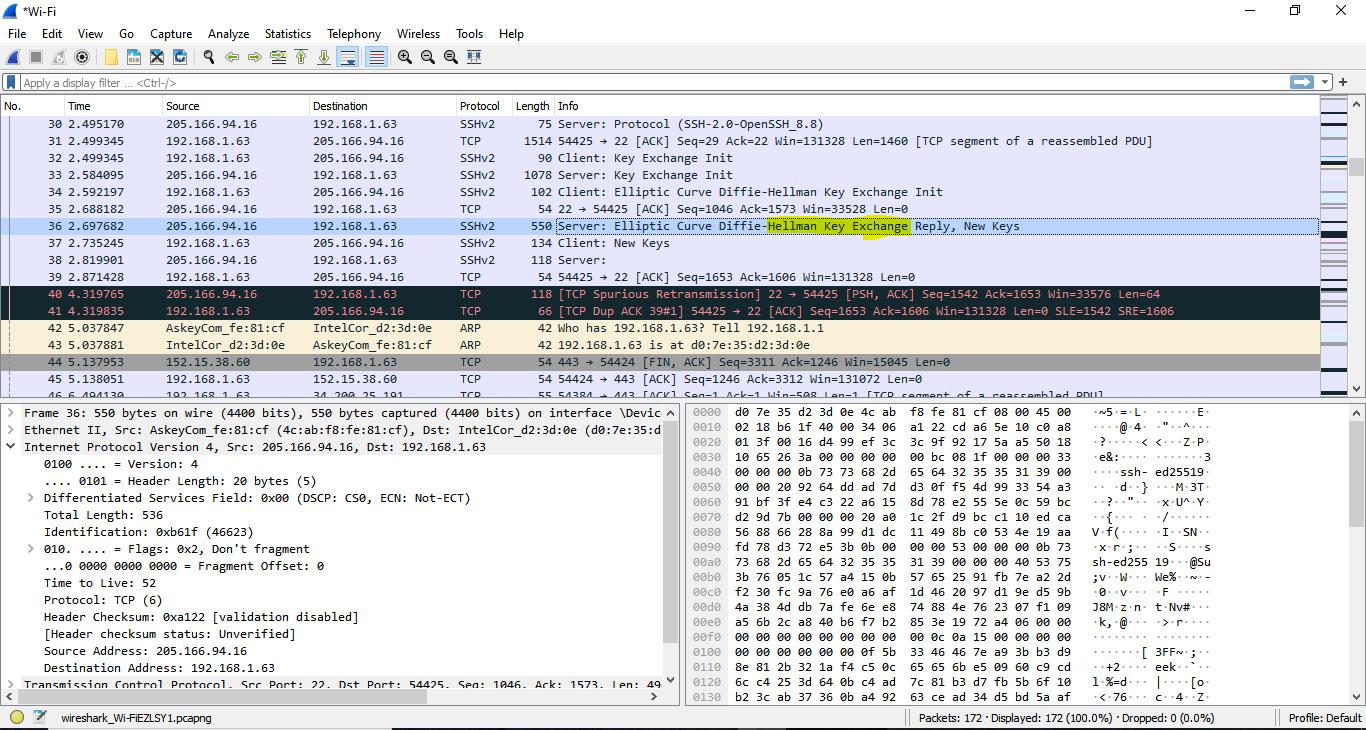


**SSH Packet Dump**.



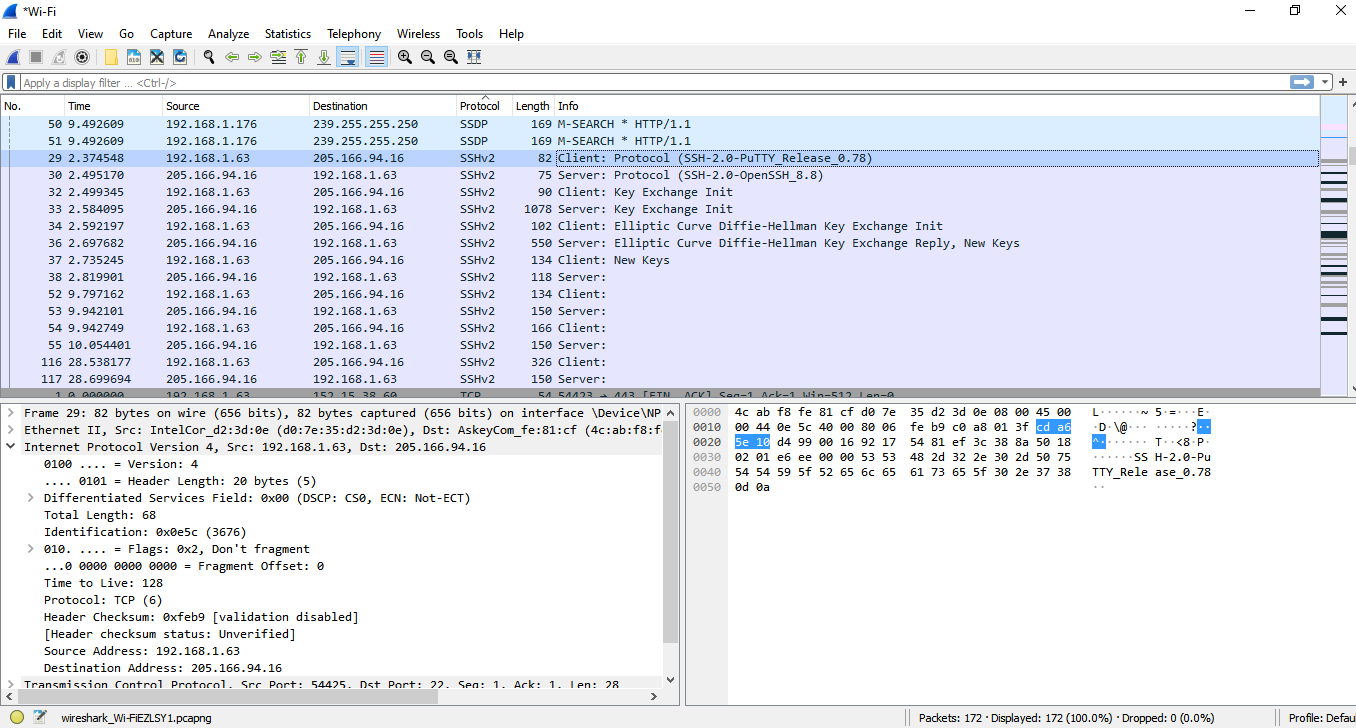
1. which protocol does PuTTY use to establish encryption key with the SSH  
   server?

As we can in the below screenshot by using puTTY SSH, Algorithm used is **Elliptic Curve Diffie-Hellman Key Exchange.**

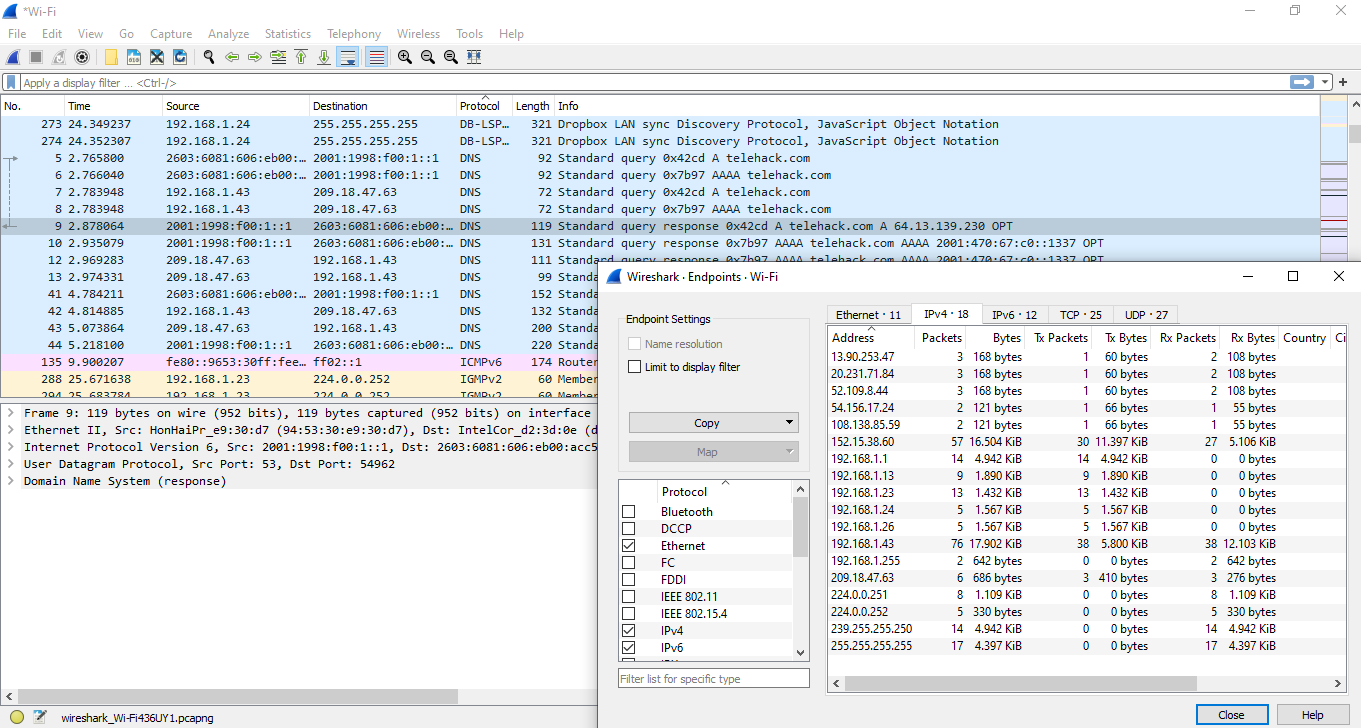


1. Analysis – packet dump out and explain why SSH is more secure than TELNET.

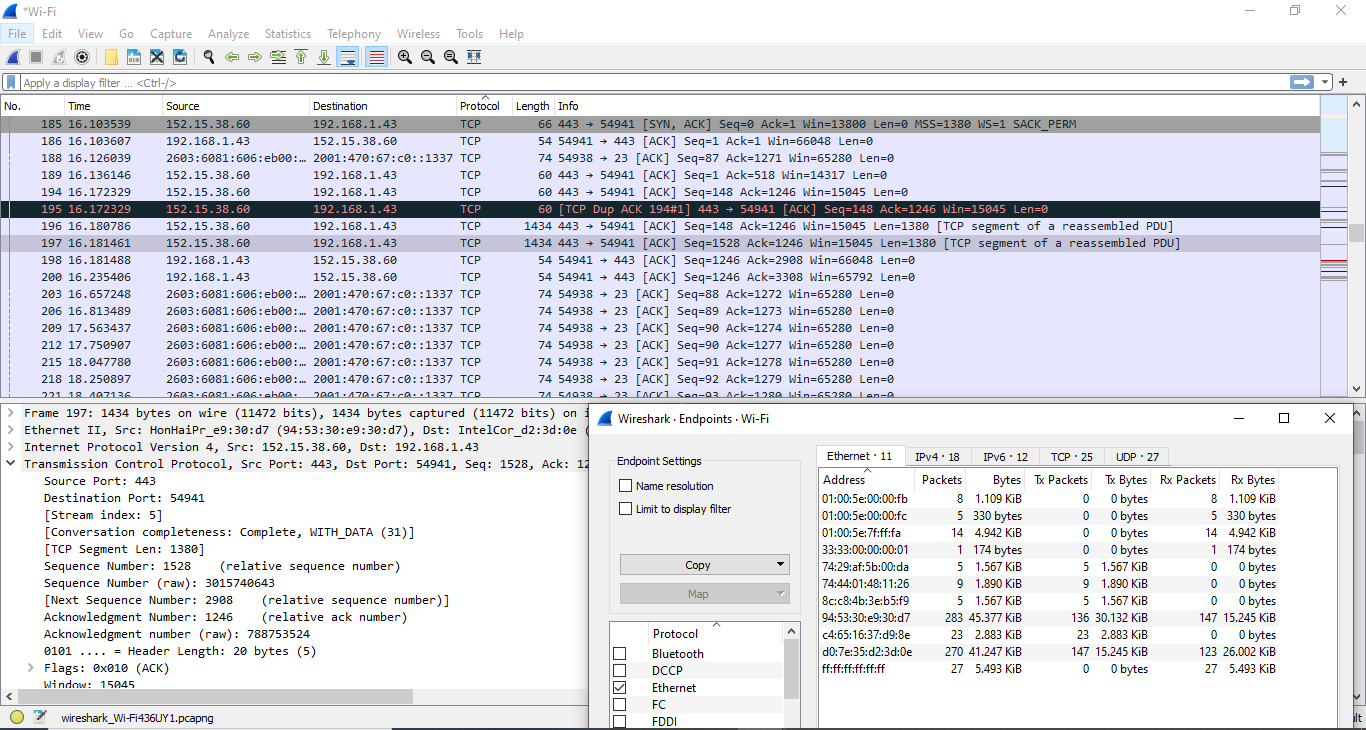
As per the Analysis from the TELNET and SSH, SSH Uses Encryption which means all data transferred on the network is protected from eavesdropping which makes it hard to decrypt. Data sent into the internet using this protocol will be out of confidentiality. SSH Protocol uses public key encryption for authentication.



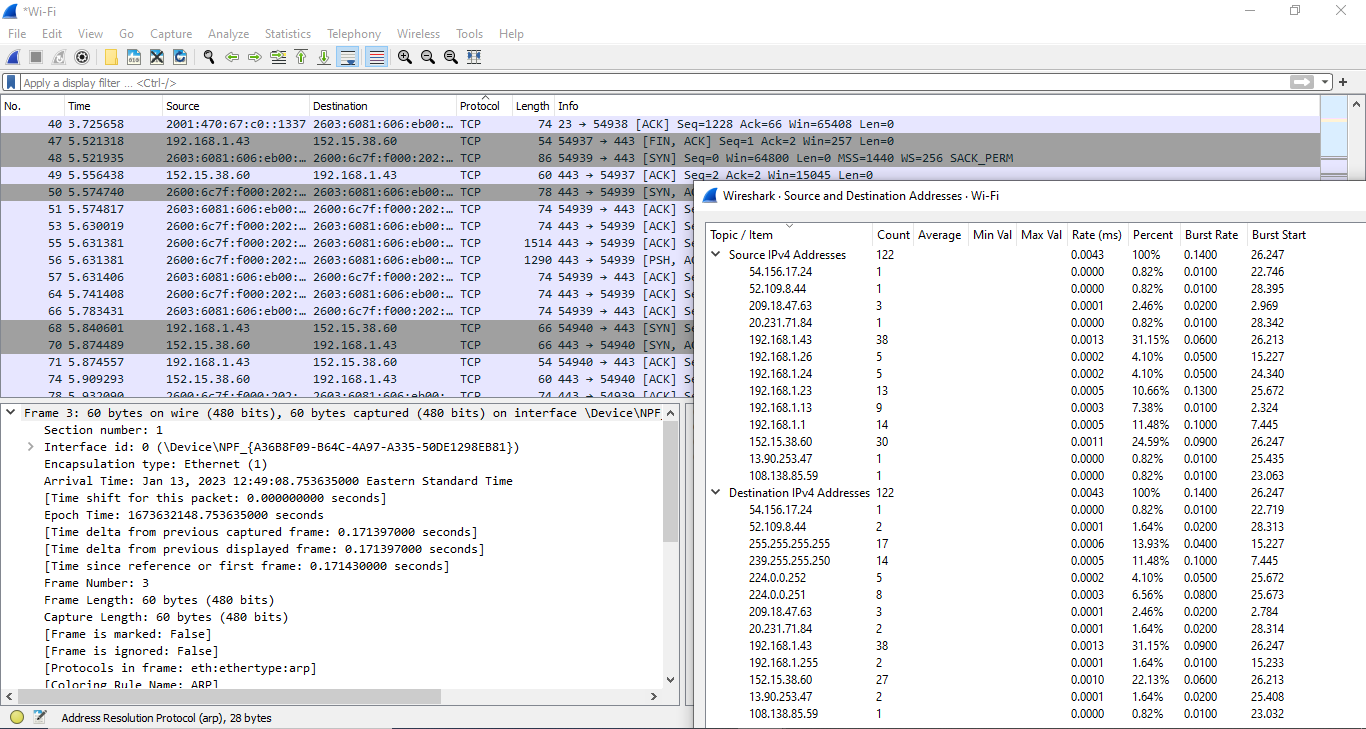
1. **IP Addresses in Captured Packets**
   * + **List all different IP addresses that you see in these captured packets:**

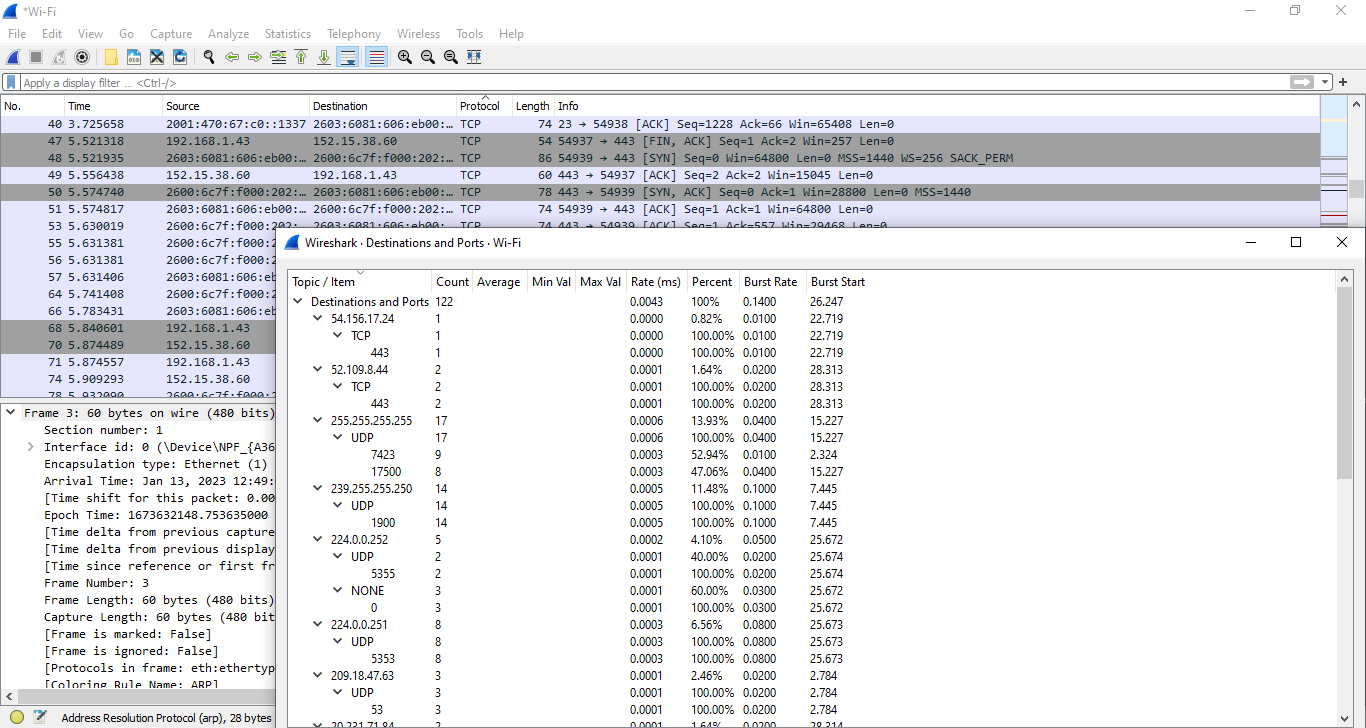


* **List all the MAC addresses that you see in these captured packets**



* **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)**





****