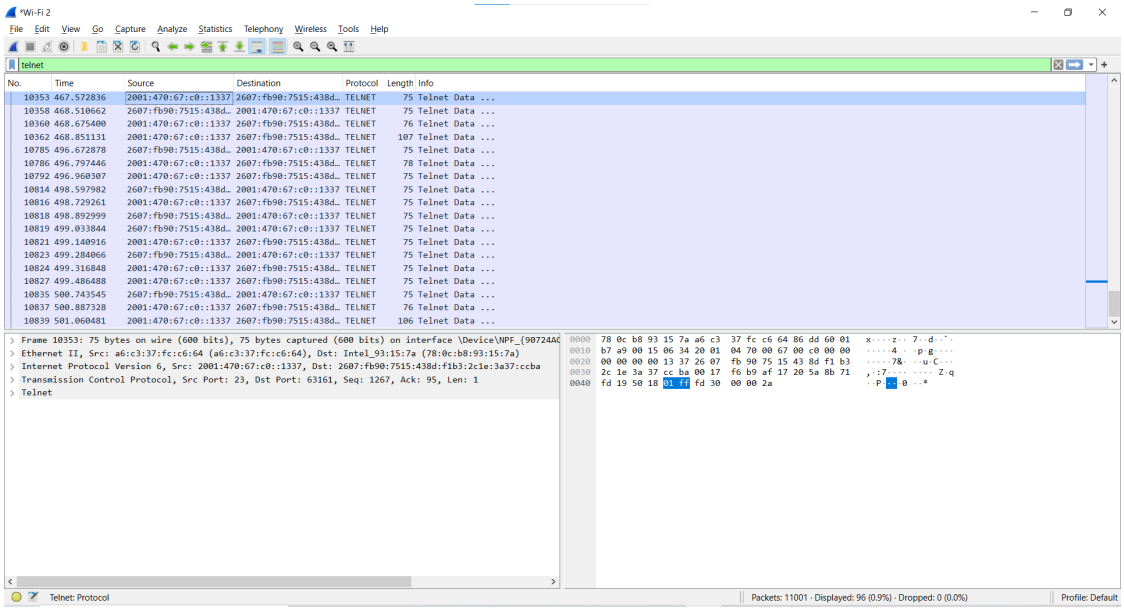
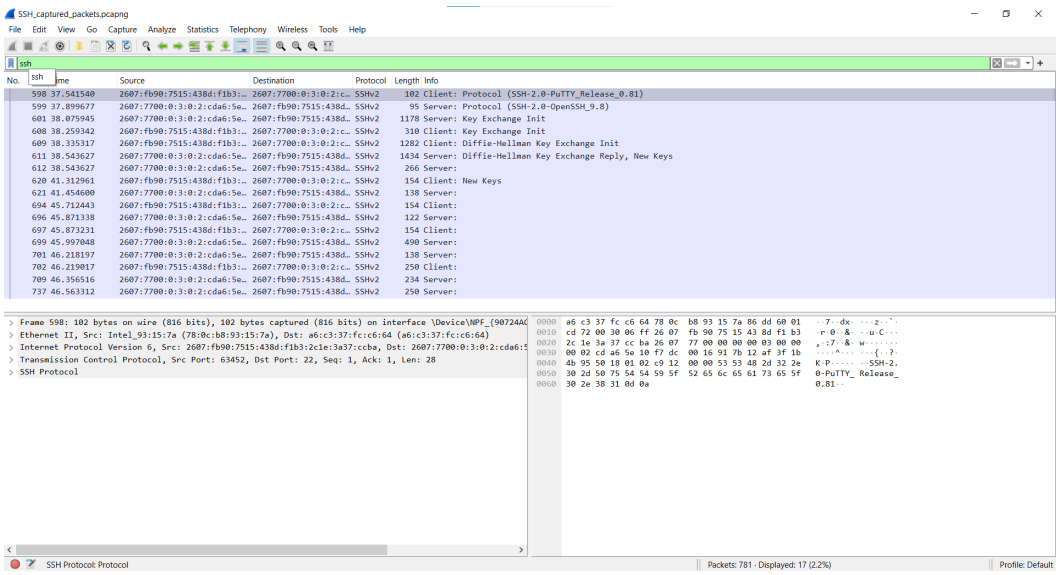
# Project:01

## A. What are the IP addresses of **telehack.com** and **sdf.org**?

**IP of telehack.com** - 64.13.139.230

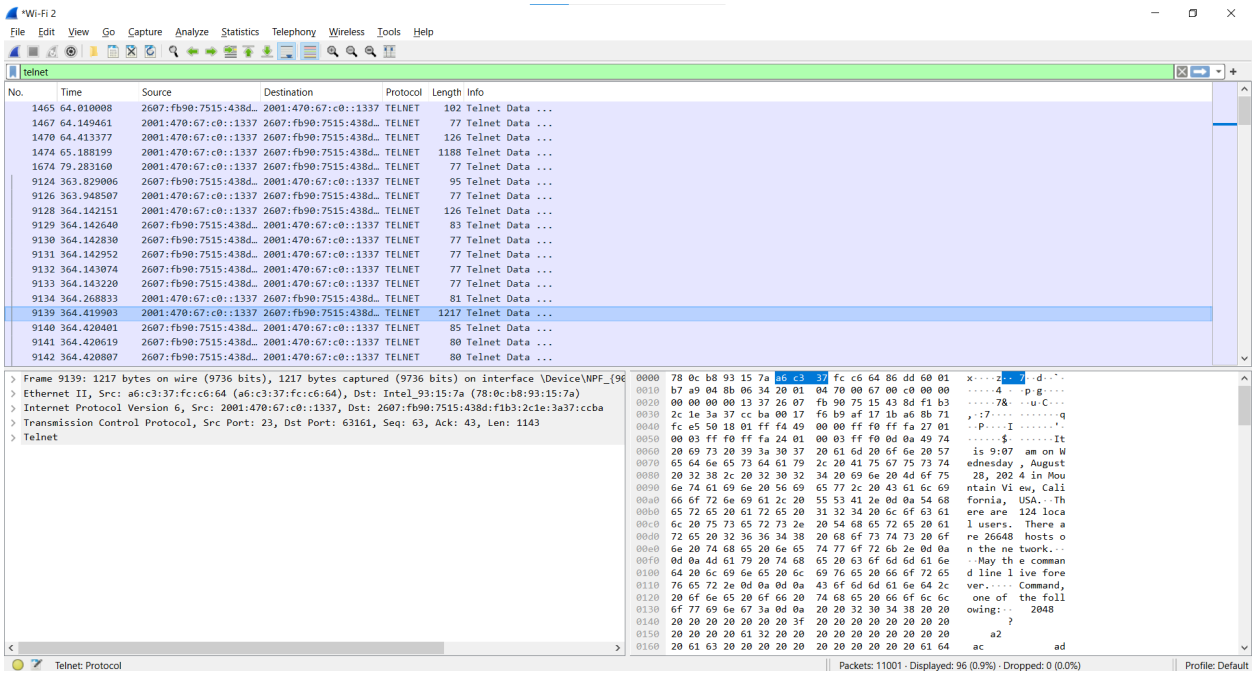



**IP of sdf.org** - 205.166.94.16

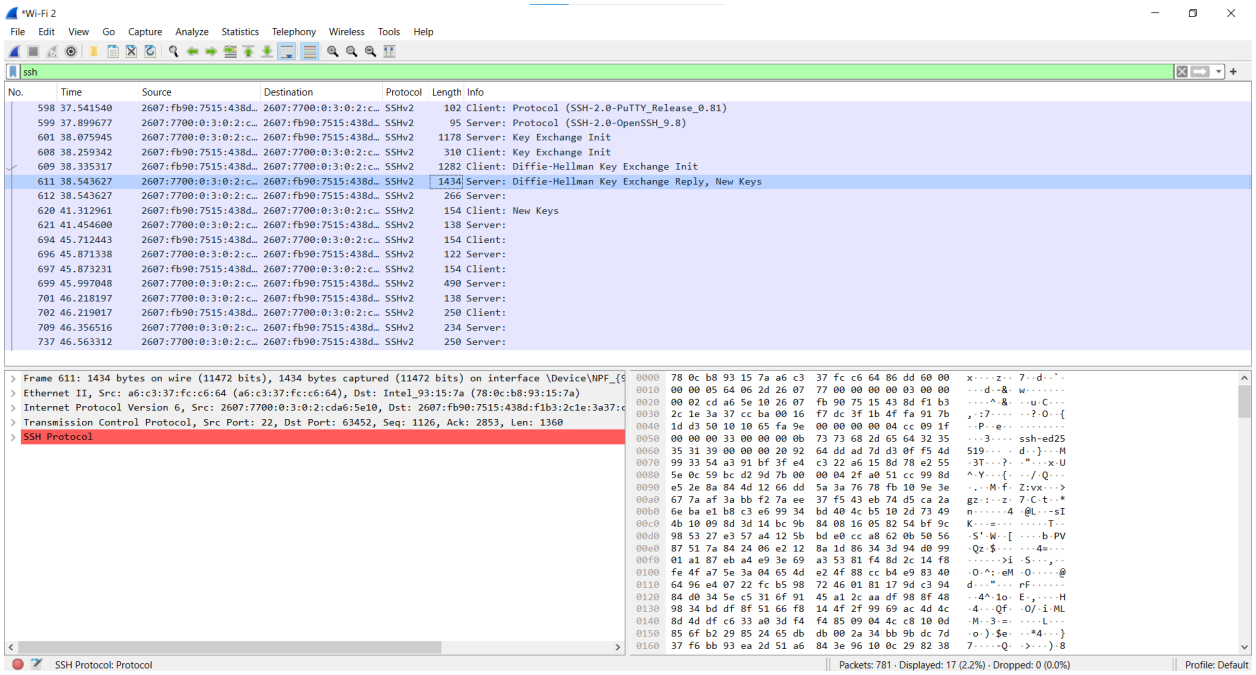


**B.** Screenshots of the packet dump for the TELNET operation and the SSH operation. Please choose the packets with relatively large size (i.e., greater than 300 bytes) so that we can see the data contents.

### TELNET packet Dumps




### Ssh Packet dumps

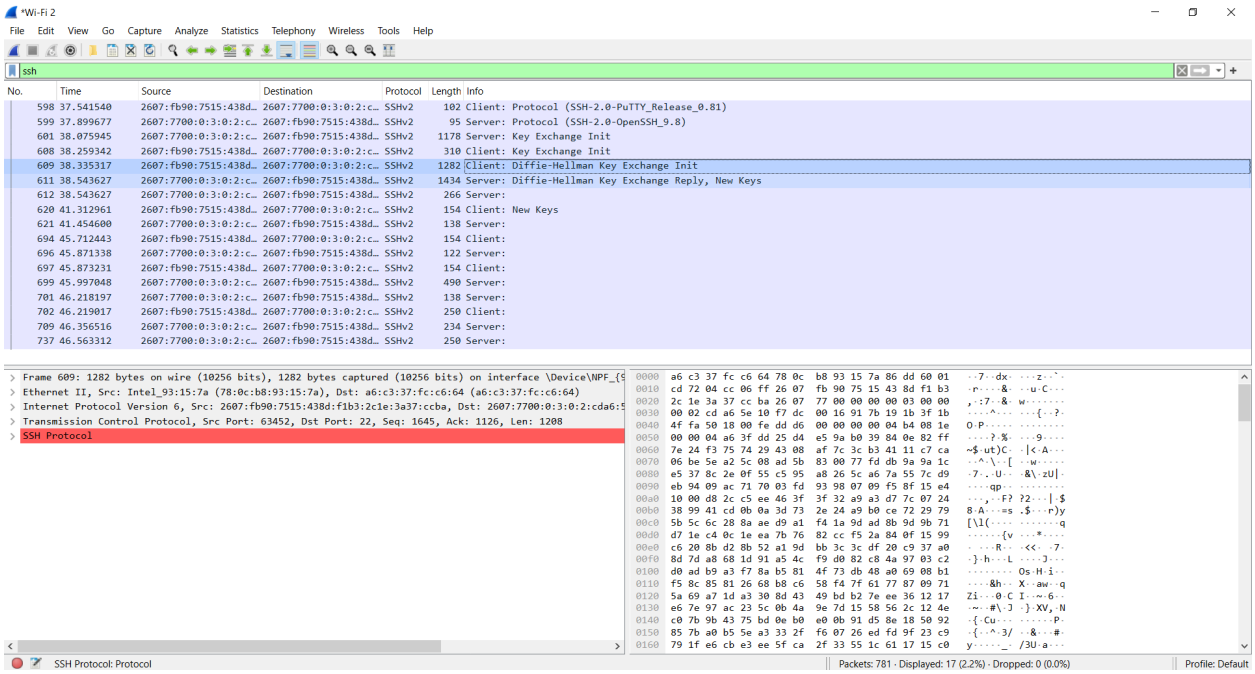


**C.** Please answer, which protocol does PuTTY use to establish encryption key with the SSH server (i.e., which key exchange algorithm is used)? It is okay to consult external sources such as textbooks, online videos, or the web to find the answer to this question ?

The protocol which PuTTY use to establish encryption key with the SSH server (i.e., which key exchange algorithm is used) is the Diffie-Hellman Key Exchange .

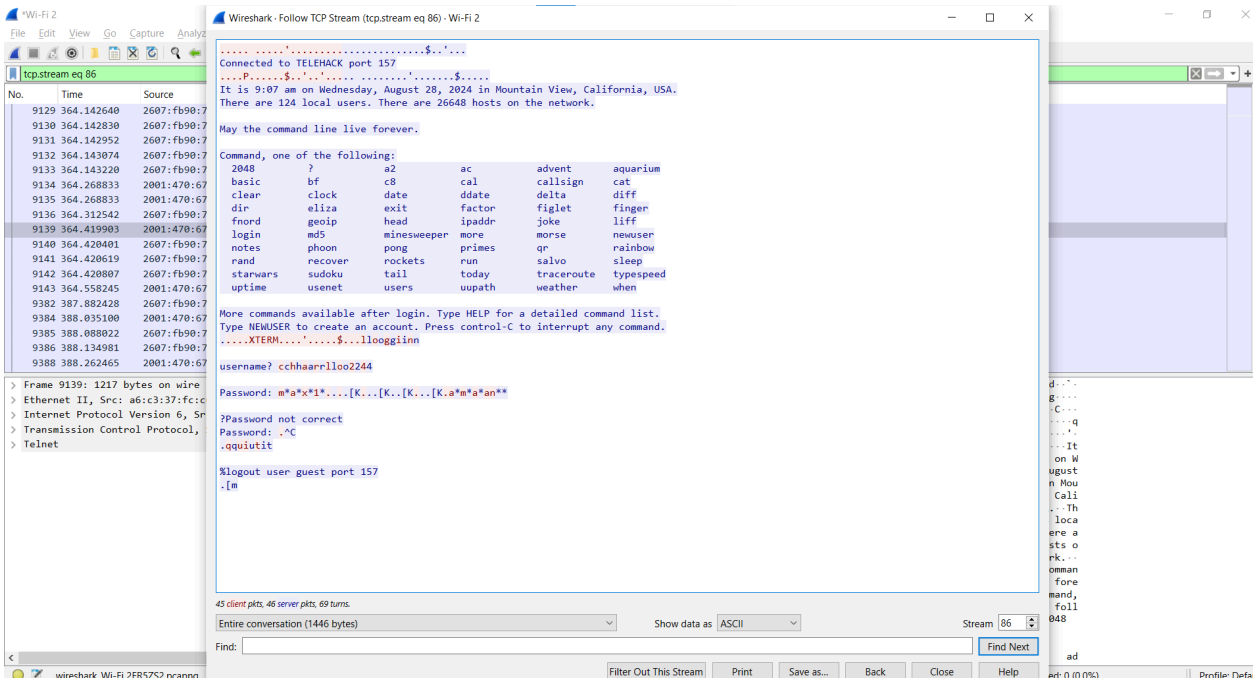
This algorithm allows two parties to securely share a secret key over an insecure channel without actually transmitting the key itself.

I personally believe that it is not required to consult external sources such as textbooks, online videos, or the web to find the answer to this question because when you perform the practicals, all the details are mentioned as shown in figure below.



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

### Analyzed packet dump




Why SSH is more secure than Telnet?

**SSH**: Encrypts all information that's transmitted between the client and the server. This encryption guarantees that indeed on the off chance that the information is captured, it cannot be effortlessly studied or altered by an assailant.

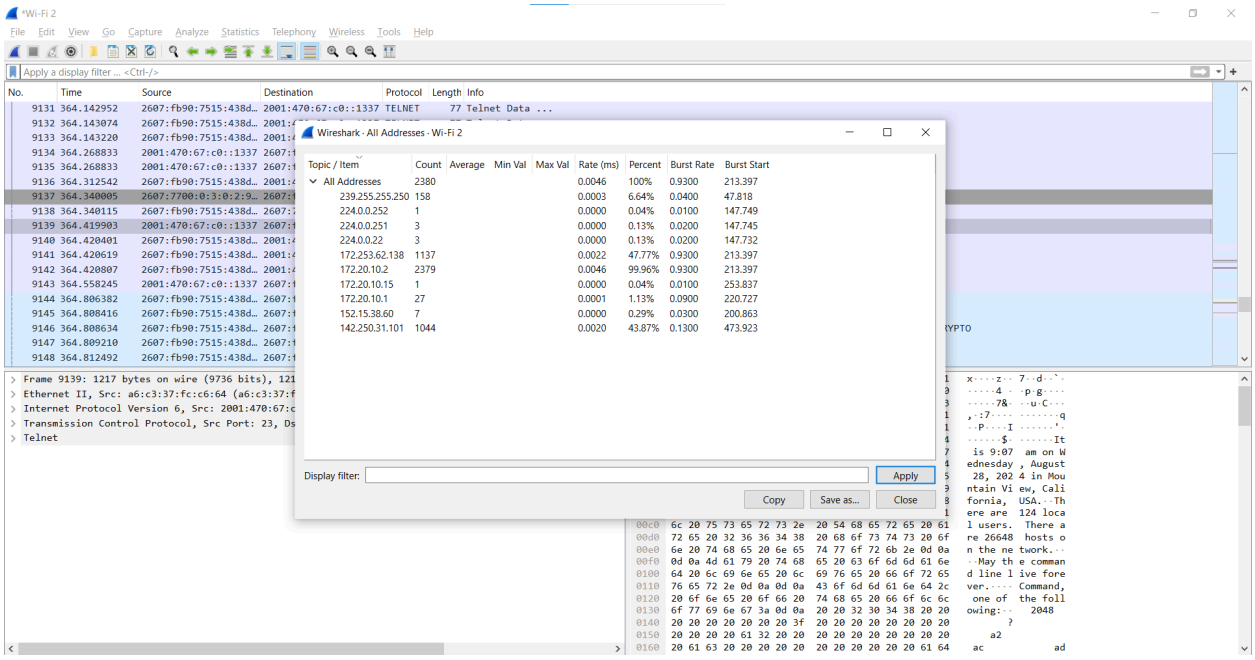
SSH gives information judgment checks utilizing Message Verification Codes (MACs), guaranteeing that the information has not been altered amid transmission. In case the information is changed, the communication session will be ended.

**TELNET:** Transmits data in plaintext, meaning that all communication, including usernames, passwords, and any commands or data sent over the network, can be easily intercepted and read by anyone who has access to the network traffic.

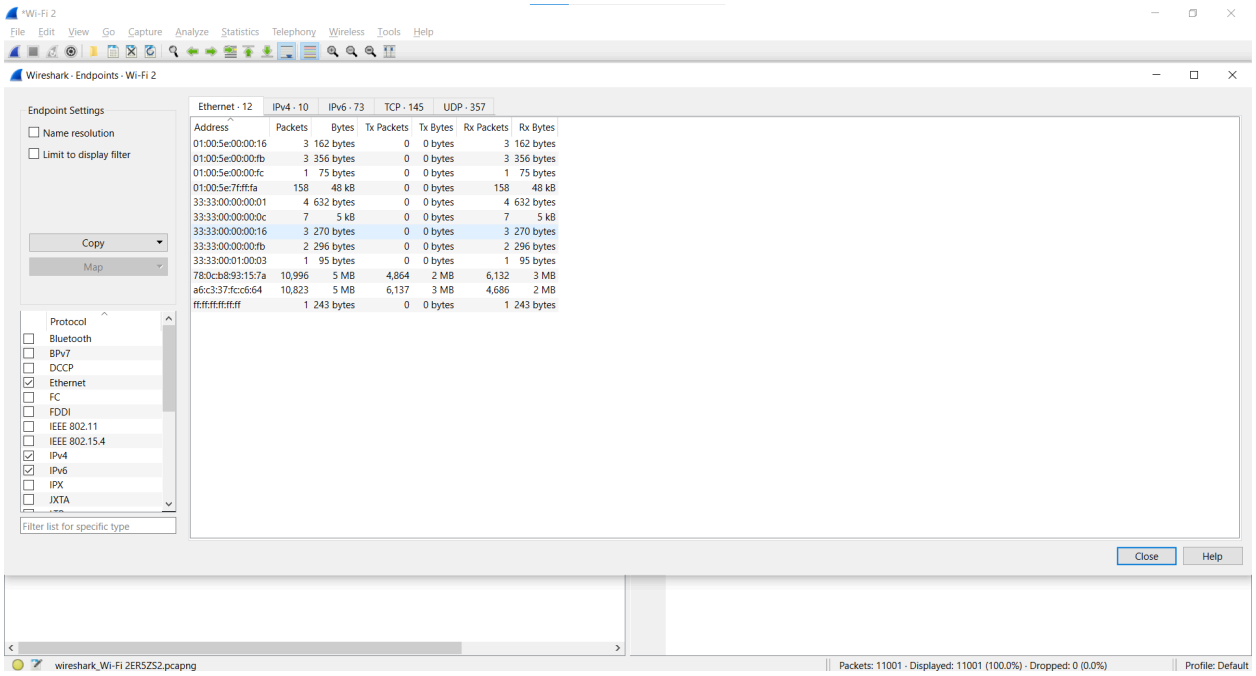
Telnet does not provide any mechanisms to ensure the integrity of the data being transmitted. This means that data can be altered in transit without detection.

**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; (2) List all the MAC addresses that you see in these captured packets; (3) 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).

## 1. All different IP addresses in the captured packets.



## 2. All different MAC addresses in the captured packets.




## 3. All TCP connections between the captured IP addresses.