

ITIS-62000: Principles of Information Security & Privacy

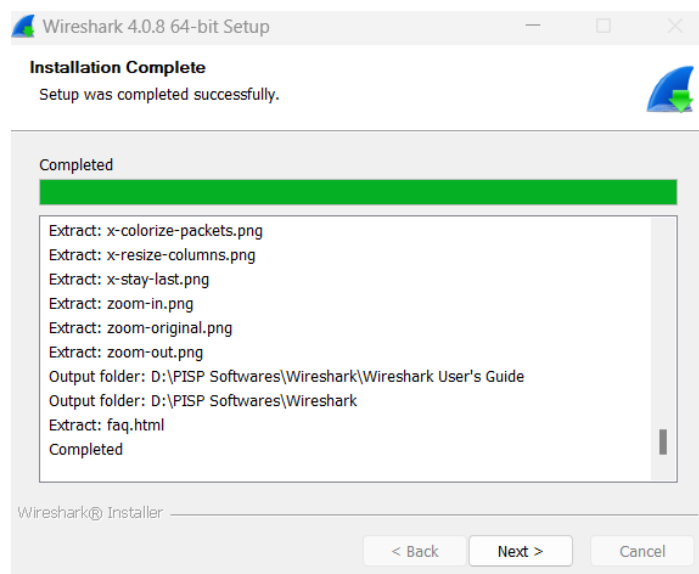
Project 1: Packet Eavesdropping and Analysis

Name: Yaswitha Sai Atluri

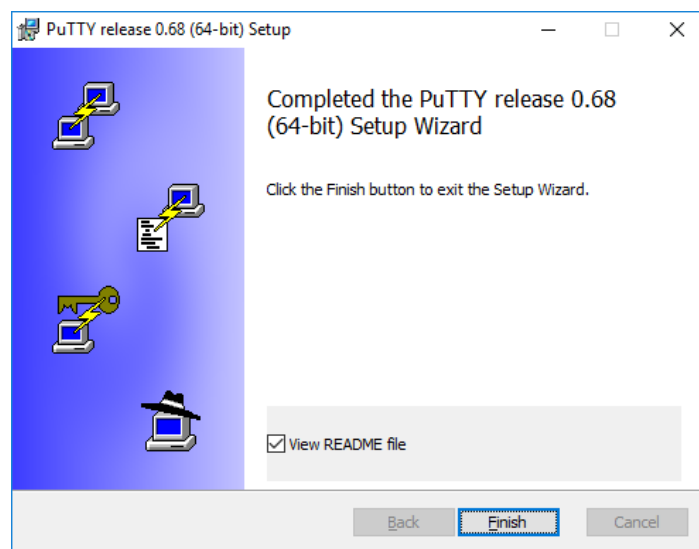
Student ID: 801366057

To do Tasks:

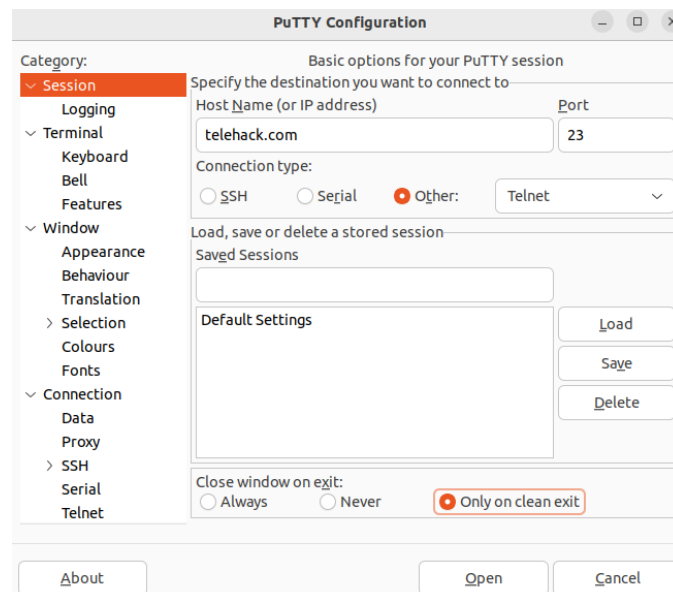
- 1) Located & installed a network monitoring or wiretap tool called Wireshark. capable of monitoring both wired and wireless networks. It's crucial to obtain this software from a trusted source, such as www.wireshark.org, to avoid potential risks. Avoid utilizing third-party websites, as they might harbour malware placed there by malicious actors.



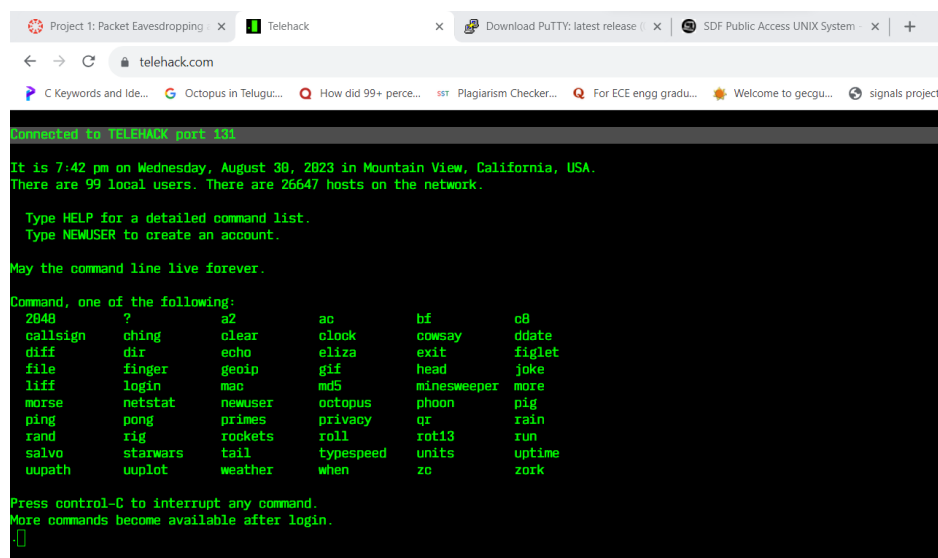
- 2) Find a software application which enables us for initiating telnet & ssh sessions. For example, consider PuTTY. It's worth noting where it is used as executable file that we can directly launch in a Windows platform. You can obtain the tool from CCI's Windows 10 machine's "Software Centre."



- 3) Initiate your wiretapping tool, and then proceed to establish a telnet connection to the server telehack.com, utilizing port 23. If you're using Windows, refer to the image below for guidance on connecting to the telnet server using PuTTY.



- 4) Upon encountering the server's welcome message, input the command 'login' and supply your username as 'uncc2020.' When prompted for a password, make an attempt to guess a password, enter it, and take note of it. It's probable that the site will respond with "Password not correct" and request the password once more. This is expected behaviour. Simply press 'Ctrl - C' and then input 'quit.' Please refrain from making multiple password guesses, as this could result in your machine being blocked by the site. Now, conclude the packet capture operation. You will observe a cluster of packets recorded by Wireshark.



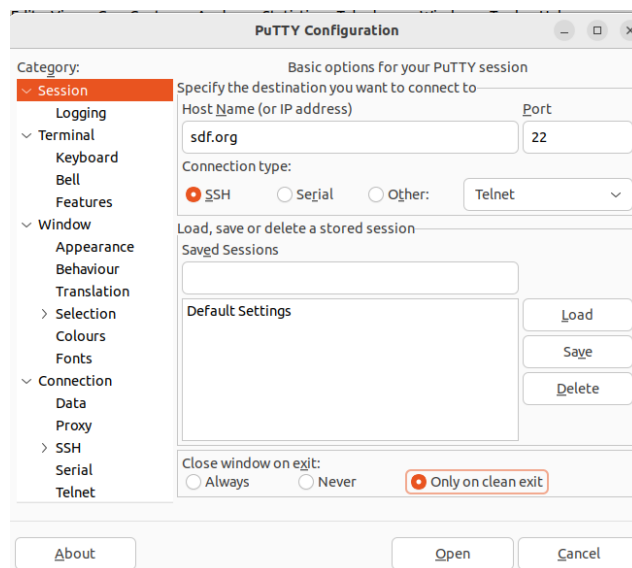
```
telehack.com - PuTTY

May the command line live forever.

Command, one of the following:
2048      ?      a2      ac      advent      aquarium
bf        cal      calc      callsign    cat      clock
cowsay    date      ddate     diff        dir      echo
exit      factor    figlet     file        finger   geoup
head      help      joke       liff        login    mac
md5        more      netstat    notes       octopus  phoon
pig        primes   privacy    qr          rain     rand
rfc        rig       rockets    roll        run      salvo
sleep     starwars  sudoku     tail        units    uptime
usenet    users      uuimap     weather     when     zork

Press control-C to interrupt any command.
More commands become available after login.
login
username? uncc2020
Password: *****
?Password not correct
Password: ^C
quit
logout user: guest port 194
```

- 5) Restart your wiretapping tool, and then utilize SSH to log in to sdf.org. Engage with the terminal window by following the on-screen instructions. Utilize the username "new." Finally, conclude the packet capture operation.



```
PuTTY (inactive)

login as: new

You will now be connected to NEWUSER mkacct server.
Please login as 'new' password 'new' when prompted.

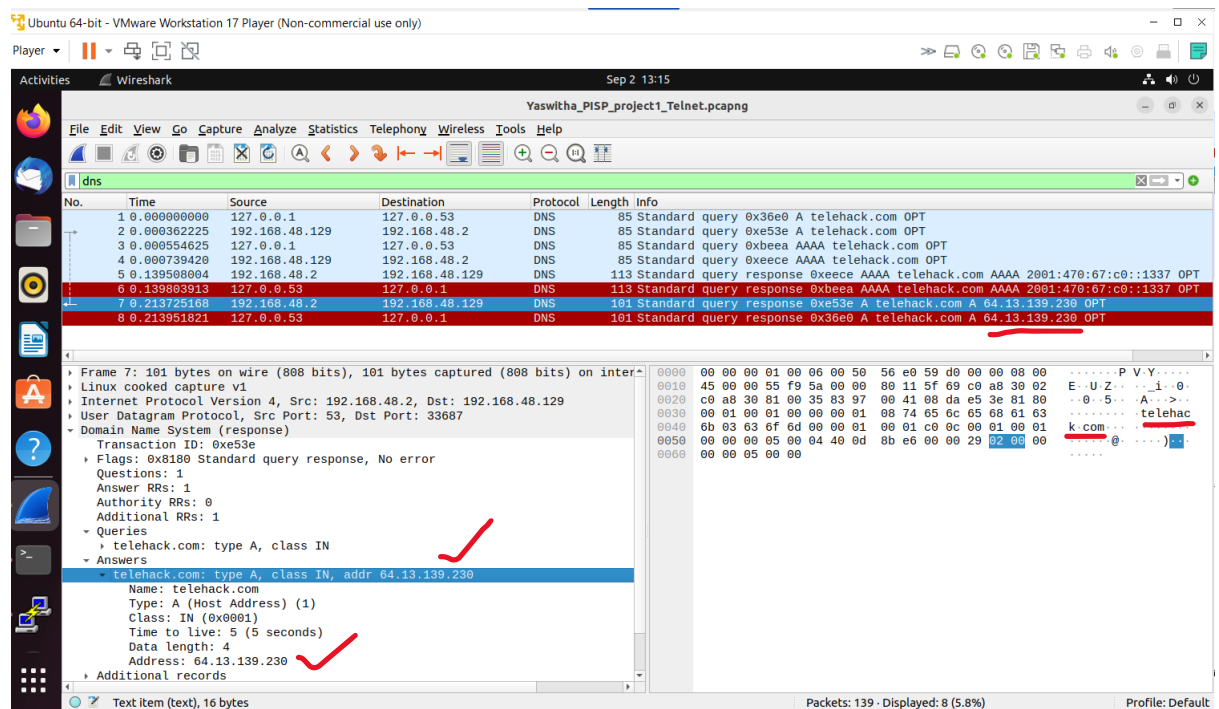
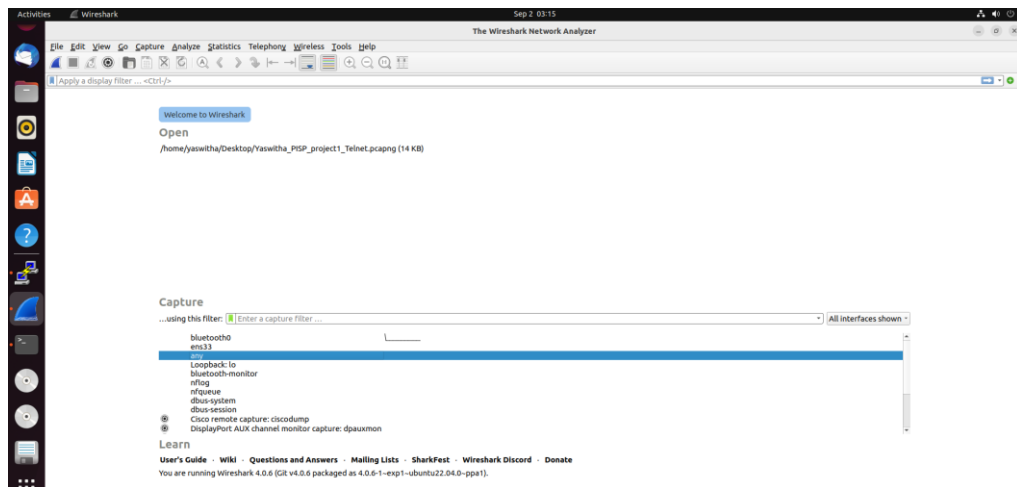
[RETURN] █
```

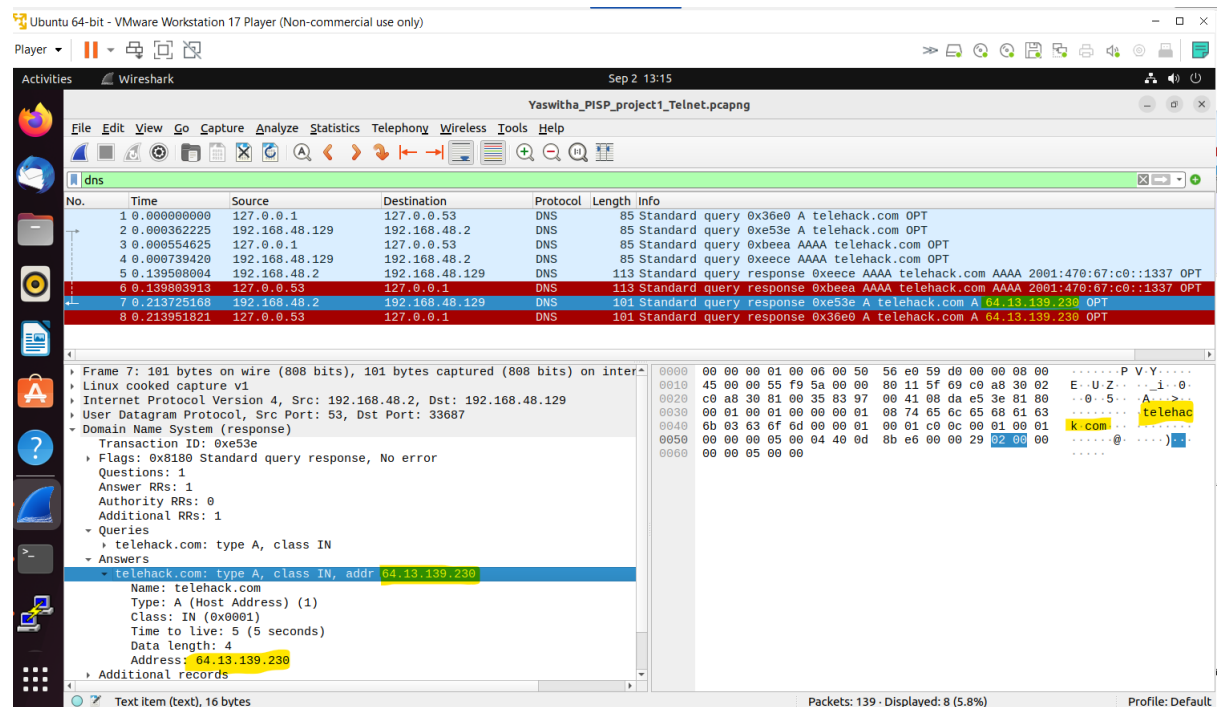
Turn-ins: (Tasks)

The packet capture tool has the capability to extract the packet contents in steps (3), (4), and (5) and save them as individual files. Store these captured data sets separately for your future analysis. You are required to submit the following:

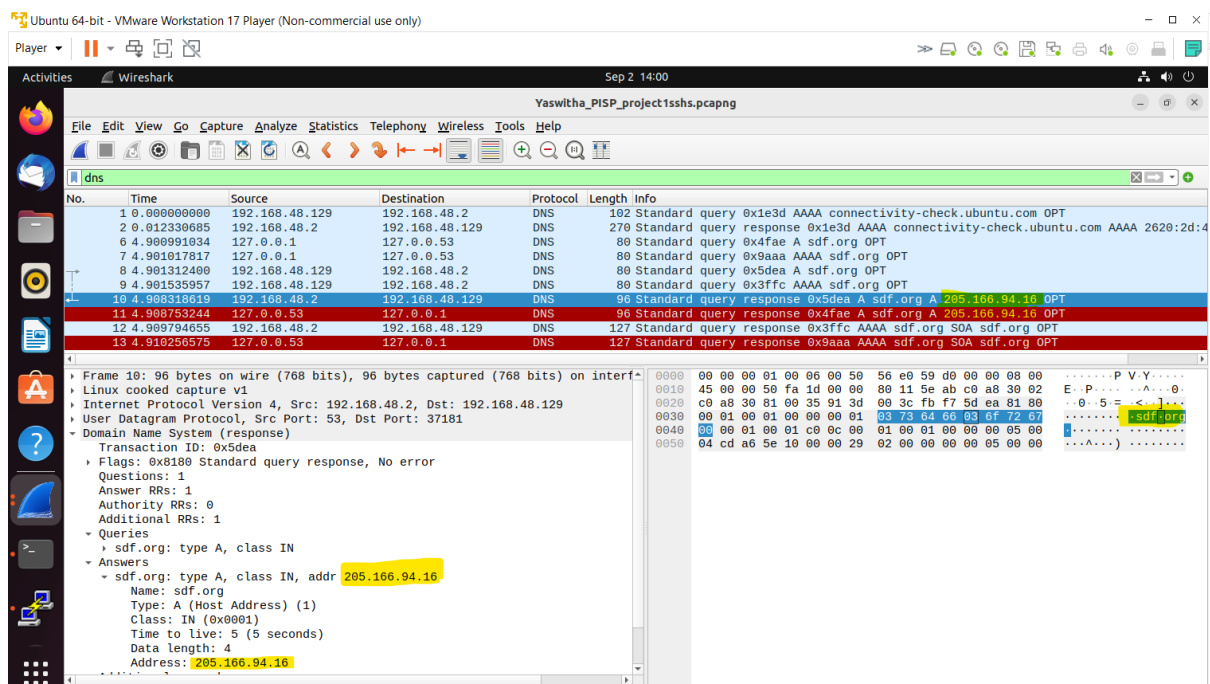
A. Indicate the set of IP address of the following websites telehack.com & sdf.org

Telehack.com: To find out the IP Address of Telehack.com, we need to filter out the DNS protocol packets using filter window in Wireshark. So, after filtering it found that the IP address of Telehack is as follows: The IP address for telehack.com, as evident from the DNS query in the packet capture, is **64.13.139.230**.





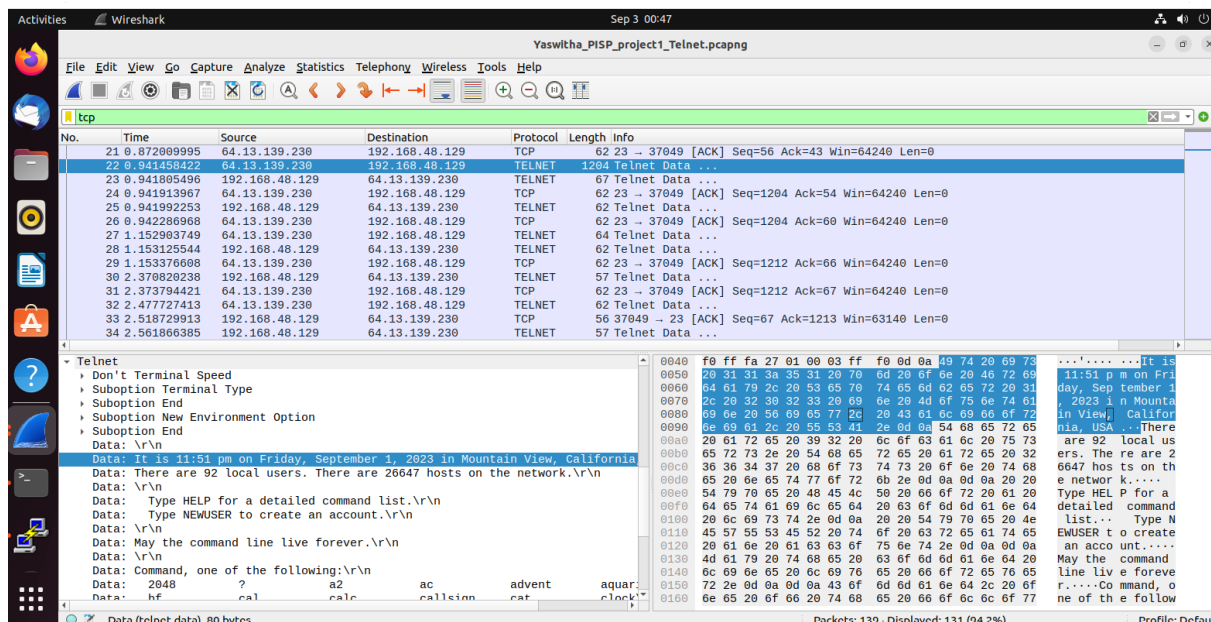
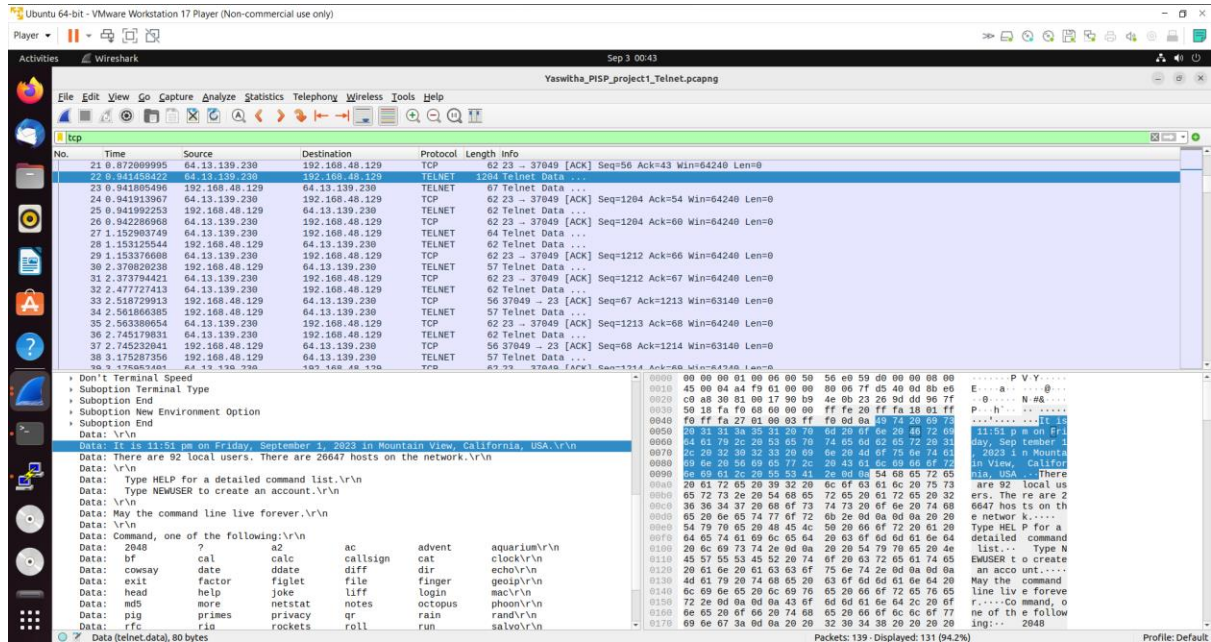
Sdf.org: To find out the IP Address of sdf.org, we need to filter out the DNS protocol packets using filter window in Wireshark. So, after filtering it found that the IP address of Telehack is as follows: The IP address for telehack.com, as evident from the DNS query in the packet capture, is **205.166. 94.16**



B. Capture snapshots of packet's dumps during the TELNET and SSH operations. Please select packets with relatively substantial sizes (exceeding 300 bytes) to ensure visibility of their data contents.

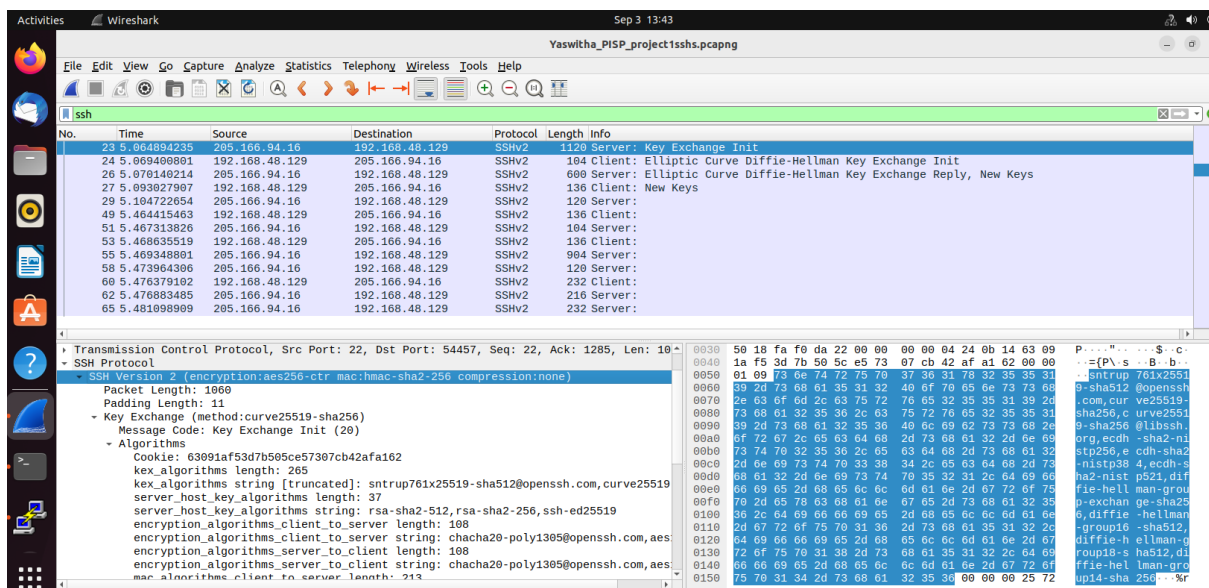
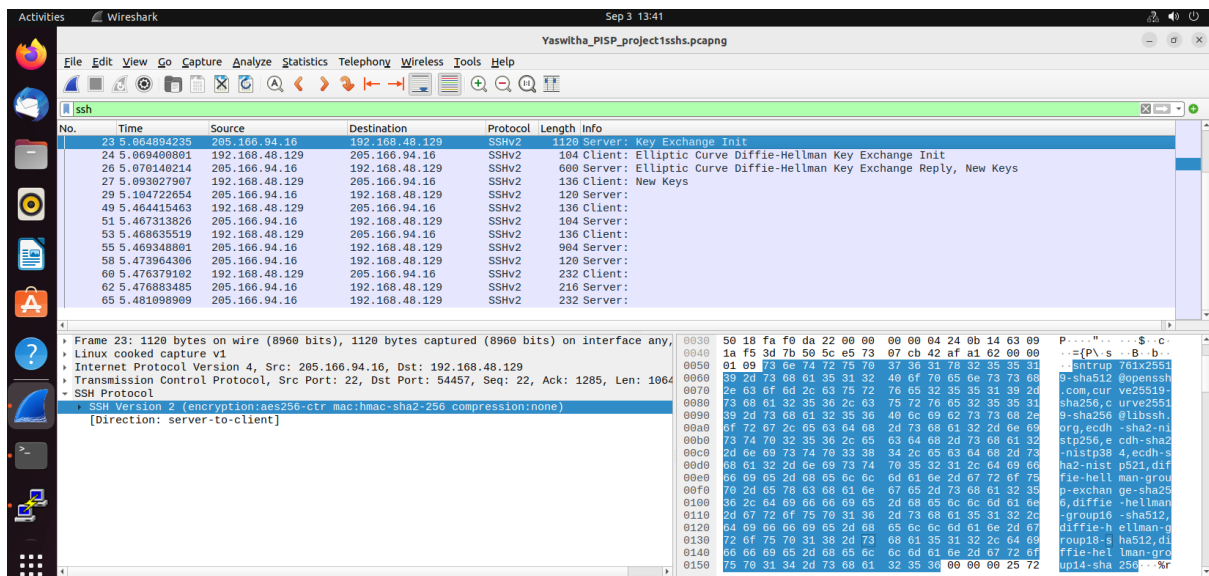
The following is the screenshot of packet dump of TELNET/ TCP operation

TCP:



The following is the screenshot of packet dump of SSH operation

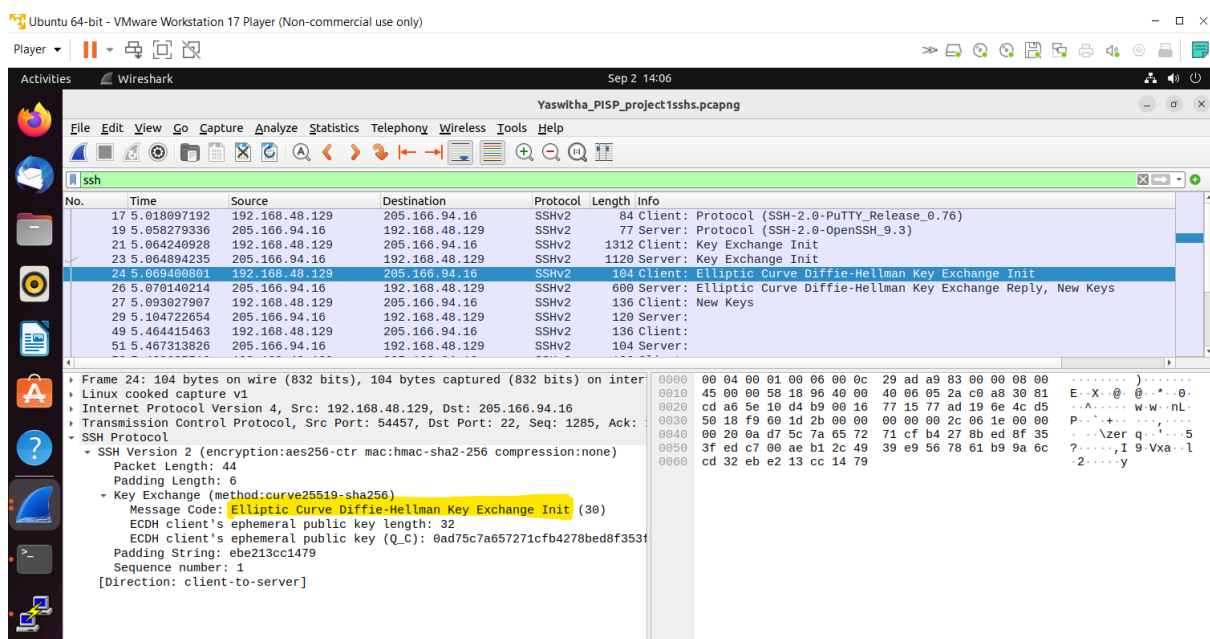
SSH:



C. Answer the following question: What protocol do PuTTY employ to form an encryption key to the SSH server, specifically, what key-exchange-algorithm was utilized? You are welcome to refer to external resources like online video/ textbook/ web for obtaining solution for this query.

Utilized the terminal to establish a connection with sdf.org. The encryption algorithm employed should remain consistent.

Algorithm: Elliptic Curve Diffie-Hellman Key Exchange



D. Conduct a brief analysis of packet dump and elucidate the reasons behind SSH's superior security compared to TELNET.

I've noticed that TELNET lacks encryption, while SSH employs the AES encryption algorithm. As a result, TELNET is deemed less dependable for maintaining data confidentiality over the internet. This is the reason, SSH is considered a more secure choice compared to TELNET and is recommended option.

SSH (Secure Shell) is significantly more secure than TELNET. Here's why:

1. Encryption:

SSH encrypts all data, including credentials and commands, while TELNET exposes data to eavesdropping, allowing attackers to intercept and read it.

2. Authentication:

- SSH offers robust methods like passwords, keys, and multi-factor authentication.
- TELNET relies mainly on basic username-password authentication, vulnerable to brute-force and password-sniffing attacks.

3. Data Integrity:

- SSH maintains data integrity with cryptographic hashes.
- TELNET lacks this data integrity protection.

4. Portability:

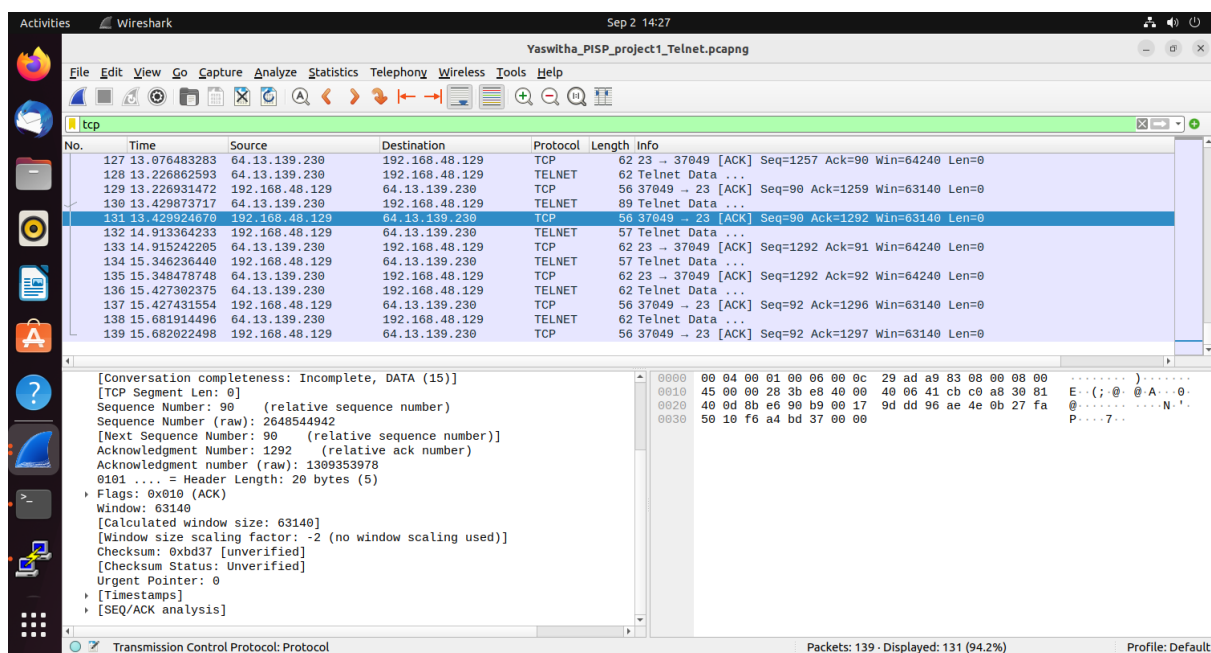
- SSH is secure for use over untrusted networks, like the internet.
- TELNET is insecure without additional safeguards like VPNs.

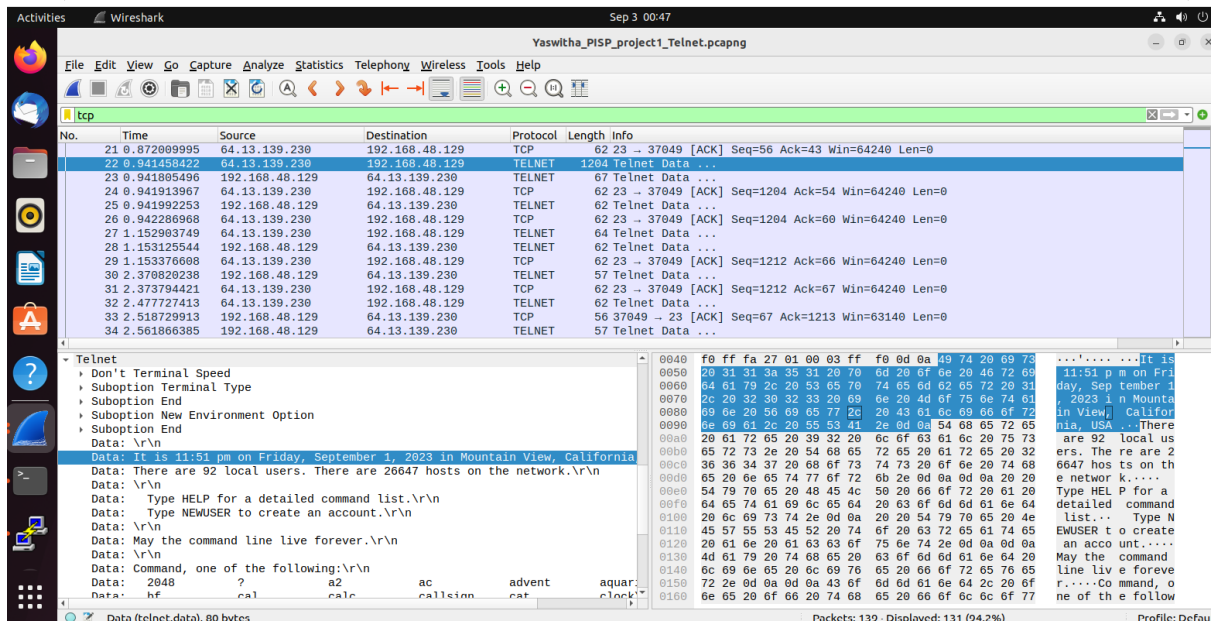
5. Vulnerabilities:

- TELNET is insecure, discouraged for sensitive tasks.
- SSH is highly secure and industry-standard for remote access.

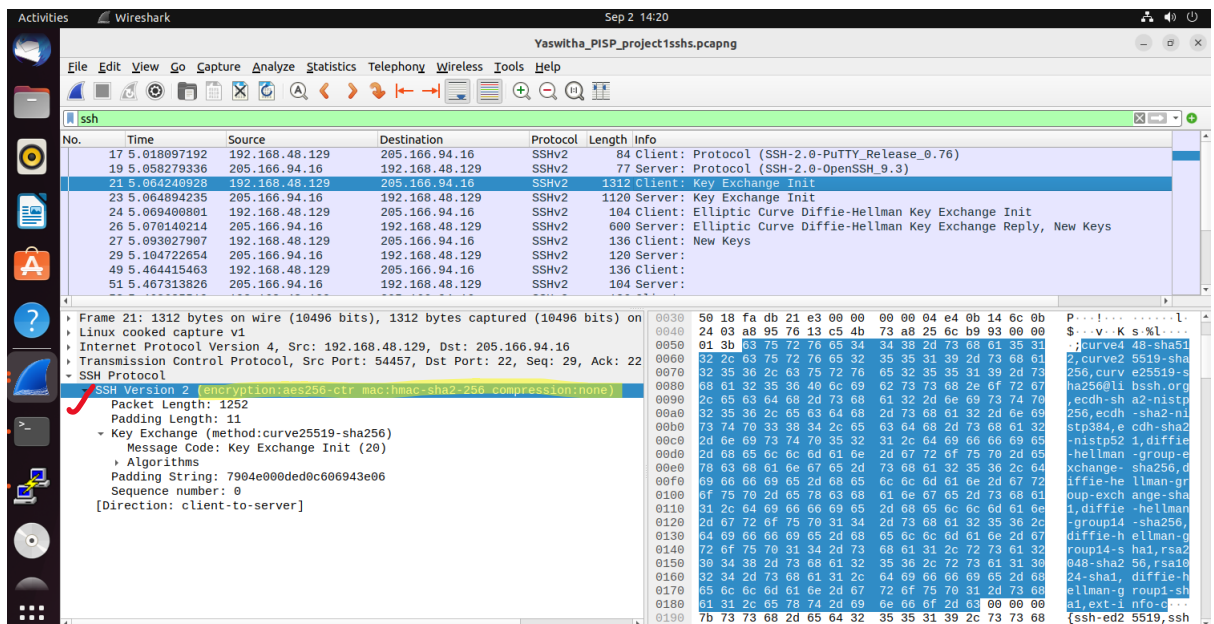
In summary, SSH is the more secure option for remote access and data transmission, offering encryption, robust authentication, data integrity protection, and a higher level of overall security compared to TELNET. It should be the preferred choice whenever security is a concern.

TELNET packet example:





SSH packet Example:



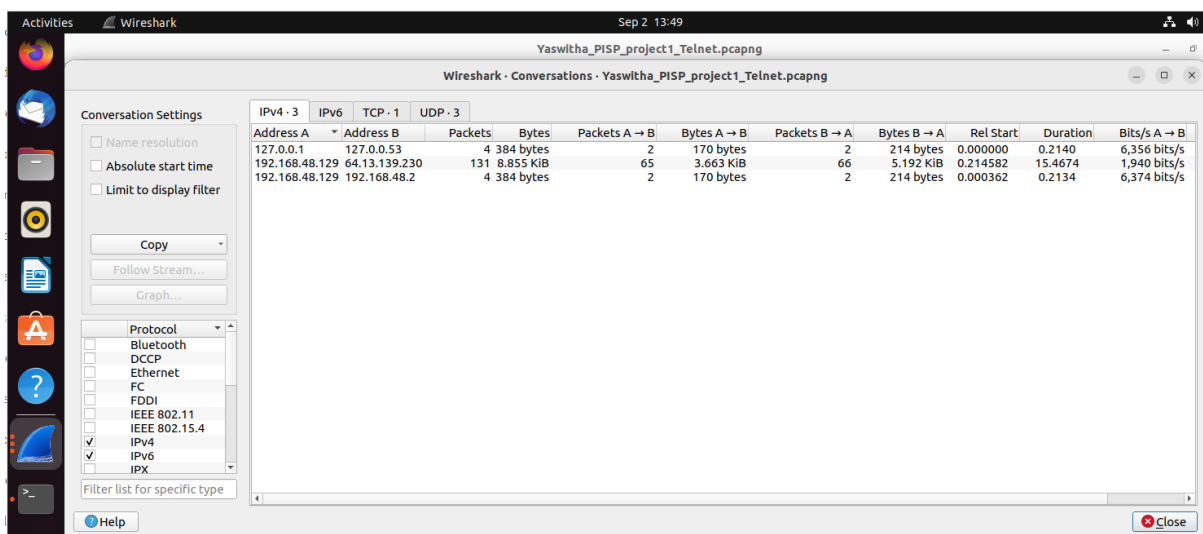
SSH is using Encryption of **aes256-ctr** mac:**hmac-sha2-256**

E. Reopen the packet capture related to the TELNET operations. You'll observe the presence of various packet types, including DNS and TCP. Please provide your response to:

1) Enumerate all distinct IP addresses identified within these captured packets.

IP addresses:

- **192.168.148.129**
- **64.13.139.230**
- 127.0.0.1
- 127.0.0.53
- 64.13.139.230
- 192.168.48.2



Wireshark - Conversations - Yaswitha_PISP_project1_Telnet.pcapng

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
127.0.0.1	127.0.0.53	4	384 bytes	2	170 bytes	2	214 bytes	0.000000	0.2140	6,356 bits/s	6,356 bits/s
192.168.48.129	64.13.139.230	131	8,855 KiB	65	3,663 KiB	66	5,192 KiB	0.214582	15.4674	1,940 bits/s	1,940 bits/s
192.168.48.129	192.168.48.2	4	384 bytes	2	170 bytes	2	214 bytes	0.000362	0.2134	6,374 bits/s	6,374 bits/s

2) Enumerate all the MAC addresses evident within these captured packets.

MAC addresses:

- **28:cd:c4:a1:28:4d**
- **8a:ee:b3:86:8c:cd**
- 3c:55:76:87:73:2d
- 01:00:5e:00:00:16
- 01:00:5e:00:00:fb
- 01:00:5e:00:00:fc
- 01:00:5e:7f:ff:fa
- 33:33:00:00:00:16
- 33:33:00:00:00:fb
- 33:33:00:01:00:03

Wireshark - Conversations - YaswithaSaiAtiuri_PISP_Project1_TELNET_ethernet.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

Filter list for specific type

Ethernet · 9IPv4 · 12IPv6 · 27TCP · 33UDP · 33

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
28:cd:c4:a1:28:4d	01:00:5e:00:00:16	5	270 bytes	5	270 bytes	0	0 bytes	5.101000	0.4715	4581 bits/s	0 bits/s
28:cd:c4:a1:28:4d	01:00:5e:00:00:fb	2	256 bytes	2	256 bytes	0	0 bytes	5.115981	0.0045		
28:cd:c4:a1:28:4d	01:00:5e:00:00:fc	1	75 bytes	1	75 bytes	0	0 bytes	5.124157	0.0000		
28:cd:c4:a1:28:4d	01:00:5e:7f:ff:fa	8	2 kB	8	2 kB	0	0 bytes	11.696694	3.0377	4571 bits/s	0 bits/s
28:cd:c4:a1:28:4d	33:33:00:00:00:16	5	450 bytes	5	450 bytes	0	0 bytes	5.102264	0.4720	7626 bits/s	0 bits/s
28:cd:c4:a1:28:4d	33:33:00:00:00:fb	2	296 bytes	2	296 bytes	0	0 bytes	5.117326	0.0041		
28:cd:c4:a1:28:4d	33:33:00:01:00:03	1	95 bytes	1	95 bytes	0	0 bytes	5.122737	0.0000		
3c:55:76:87:73:2d	01:00:5e:00:00:fb	1	105 bytes	1	105 bytes	0	0 bytes	3.382951	0.0000		
8a:ee:b3:86:8c:cd	3c:55:76:87:73:2d	1,032	325 kB	514	166 kB	518	159 kB	0.000000	34.0938	39 kbps	37 kbps

Close

Help

3) Please compile a list of all the TCP connections captured, including the following details: Destination IP; Source IP; Destination PORT; Source PORT.

All TCP connections are listed in the conversations option available in the statistics tab.
TCP connections:

Source IP	Source Port	Destination IP	Destination Port
192.168.48.129	37049	64.13.139.230	23

Activities

Wireshark

Sep 2 13:51

Yaswitha_PISP_project1_Telnet.pcapng

Wireshark - Conversations - Yaswitha_PISP_project1_Telnet.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ DCCP

☐ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

Filter list for specific type

Help

Close

IPv4 - 3		IPv6	TCP - 1	UDP - 3								
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	
192.168.48.129	37049	64.13.139.230	23	131	8.855 KiB	0	65	3.663 KiB	66	5.192 KiB	0.214582	