Sharad Dixit

CMSC 487 Introduction to Network Security

Assignment 2

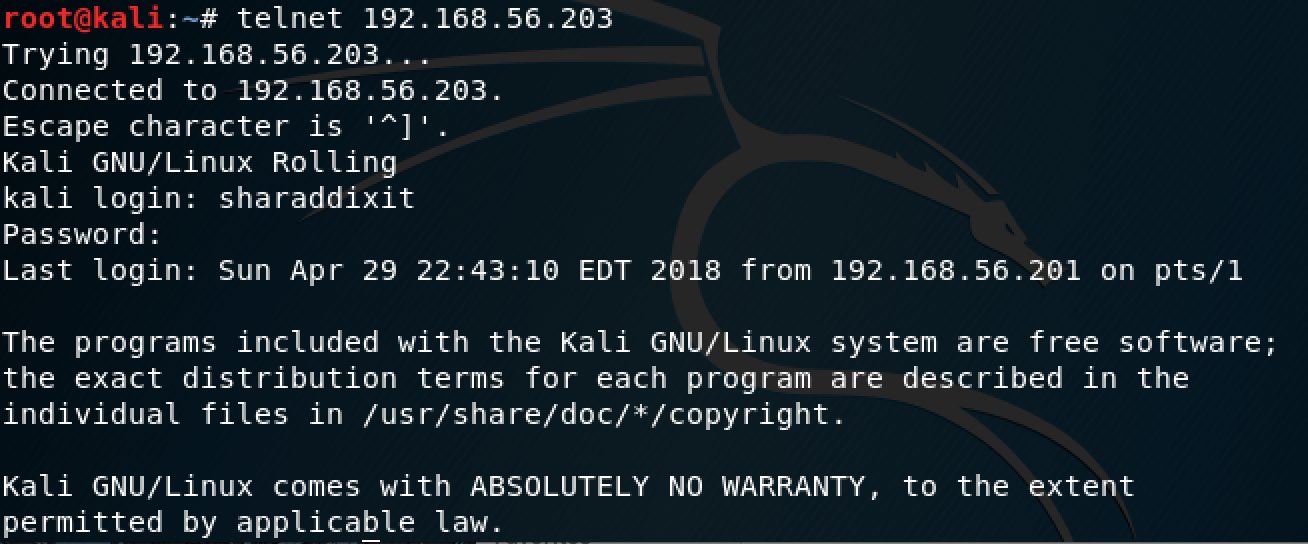
* OBJECTIVE

The objective of this project was to perform a Wireshark trace on two sessions. The first session was for the telnet session when the client on one machine performs a telnet on the telnet server on another machine. The second session was for a VPN session when the there is a VPN server and the route trace is from client to VPN server and then to telnet server. We perform a Wireshark trace for both the sessions and provide description for packets in order to verify how the route trace proceed.

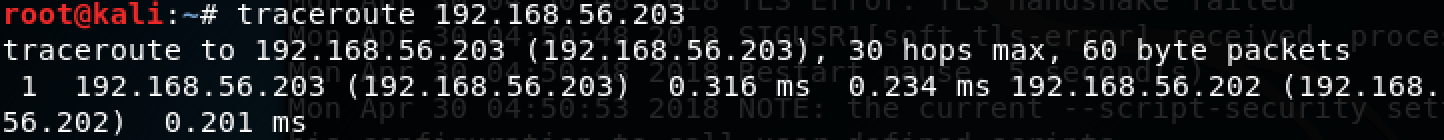
* METHODOLOGY

1. TELNET SESSION

* In this session we perform a telnet from the client with IP as 192.168.56.201 to the telnet server with IP as 192.168.56.203. After performing the telnet we get an access to the user of the telnet server. The image below provides an explanation for the process described above where after performing the telnet we provide details of the user at the telnet server and gain access to that machine.



The traceroute for this session is in below image.

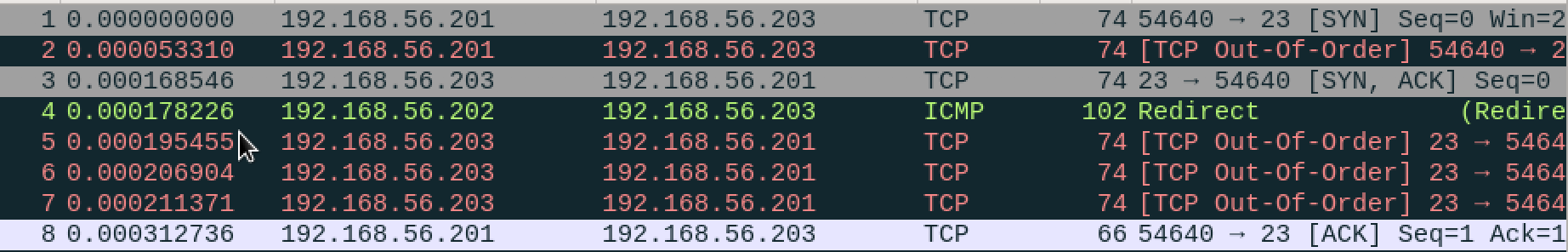


* Wireshark Trace for Telnet Session

Note:-

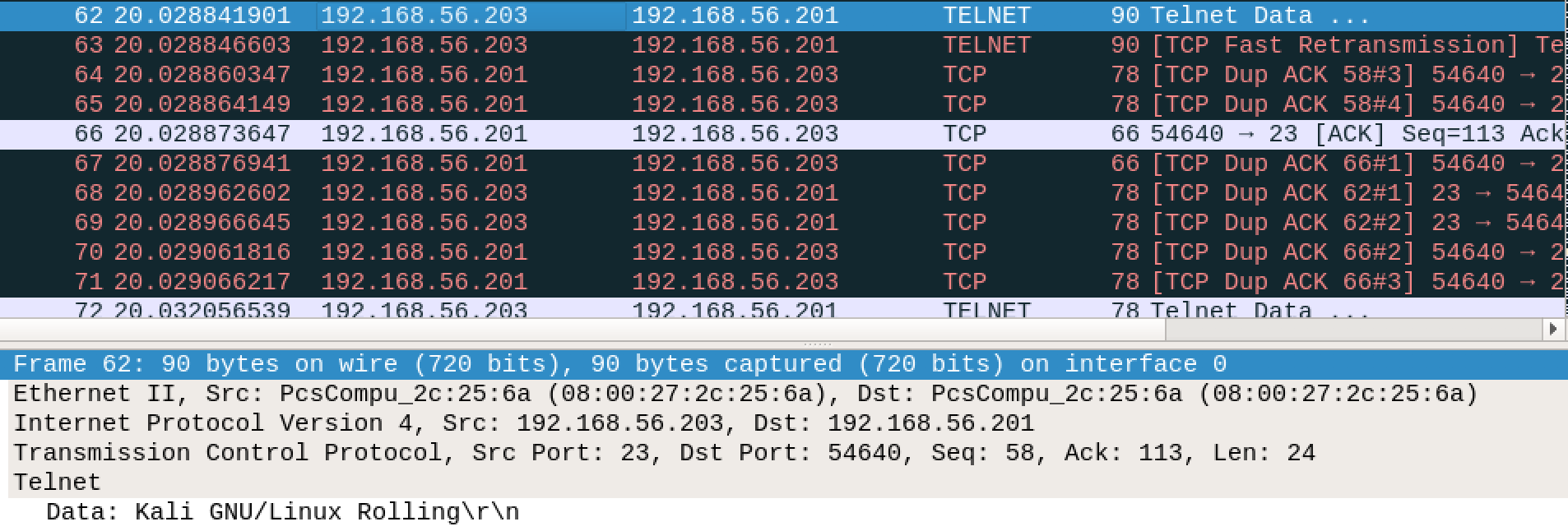
Client IP: 192.168.56.201 Telnet Server IP: 192.168.56.203

1. TCP connection establish

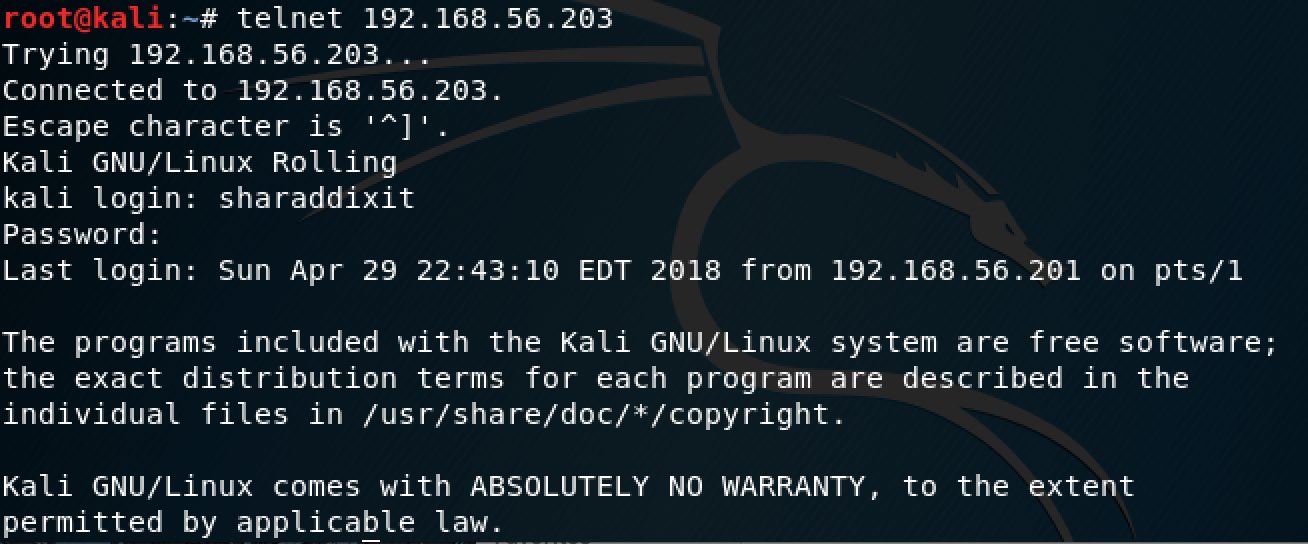


The above figure shows the Wireshark trace of TCP establishment between client (192.168.56.201) and telnet server (192.168.56.203) at port 23. The packets 1-8 describe TCP connection between the client and the telnet server, where first the client sends the [SYN] request to telnet server and the telnet server sends the [SYN, ACK] and then the client sends the [ACK] resulting in the establishment of TCP connection between the client and telnet server.

1. Message to client from telnet server

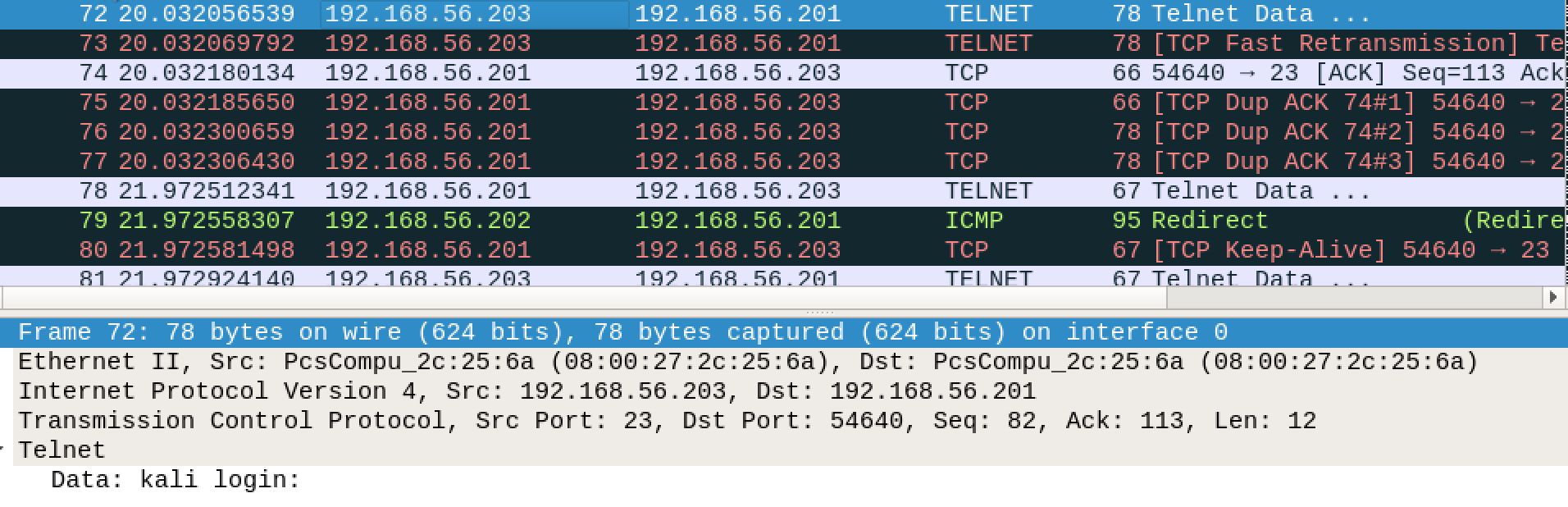


The above image shows the data from the telnet server to the client. The telnet server request with user and password from the client machine. The following terminal view shown below in image provides an explanation of the telnet packets in more detail. The packet 62 depicts above procedure. Packet 66 depicts the request to telnet server, by port 23.



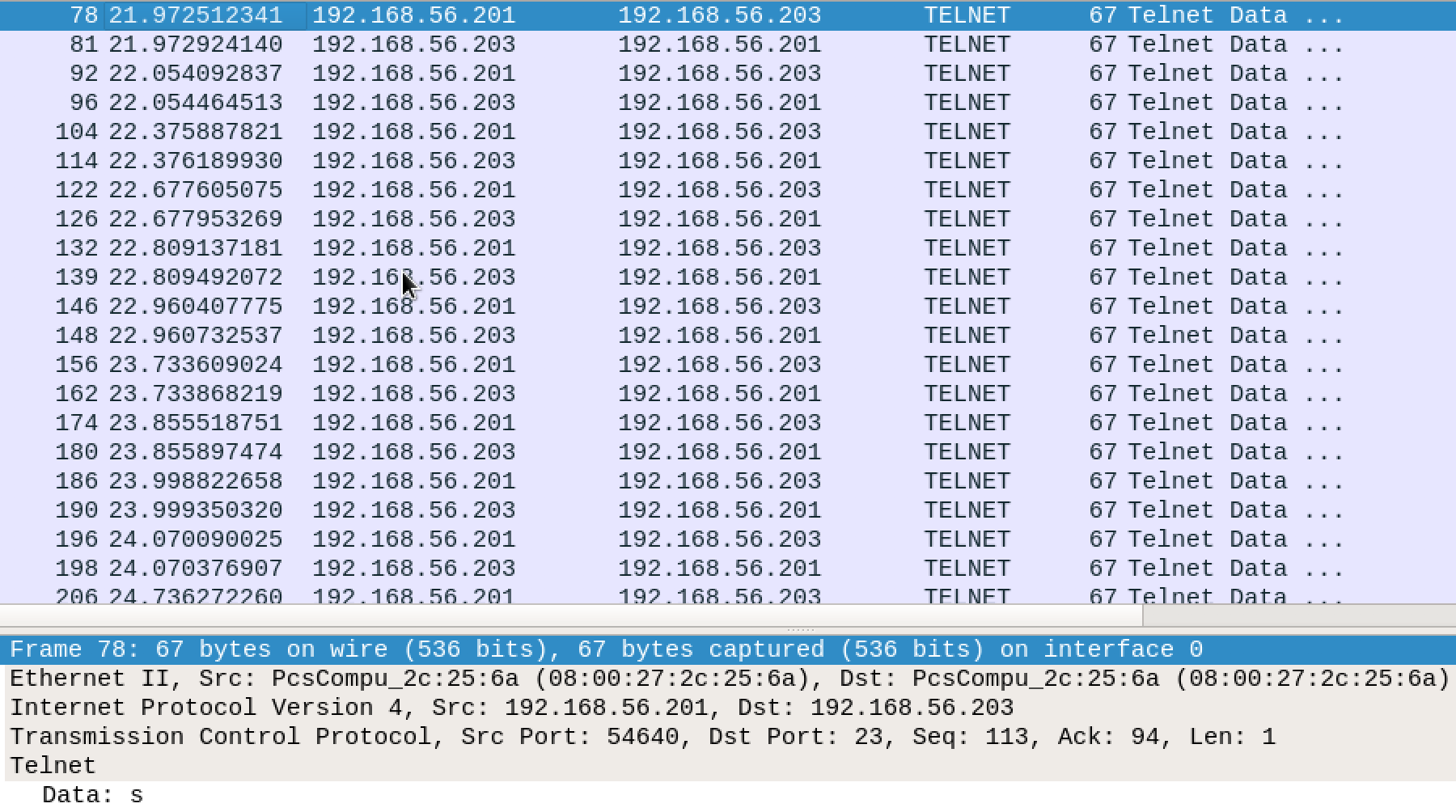
The above image shows the successful login and password from the client to the telnet server machine.

1. Username request from telnet server to client (Kali login)



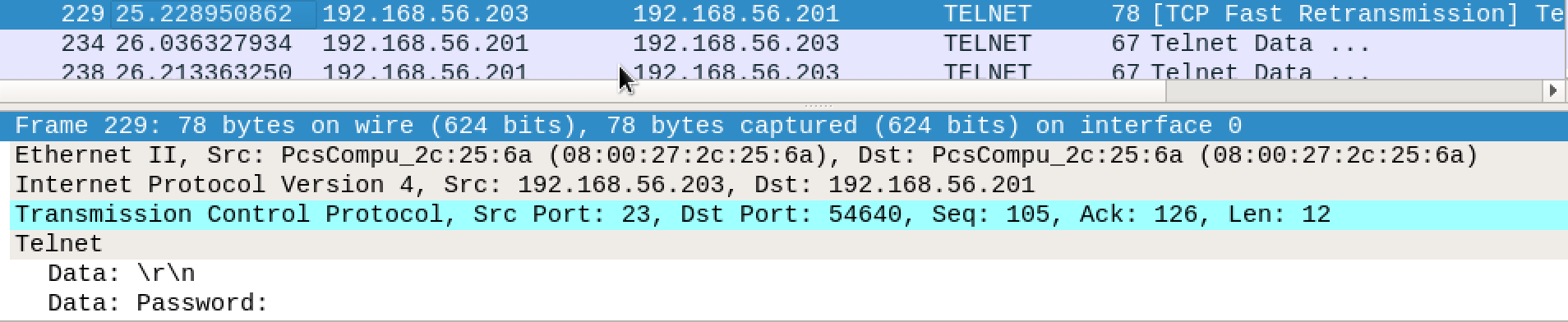
The above image depicts when the telnet server request for login details from the client in order to proceed further. The data can be seen that is “Kali login:”, The packet number 72 depicts the above, with the message for login.

1. Username entry by the client



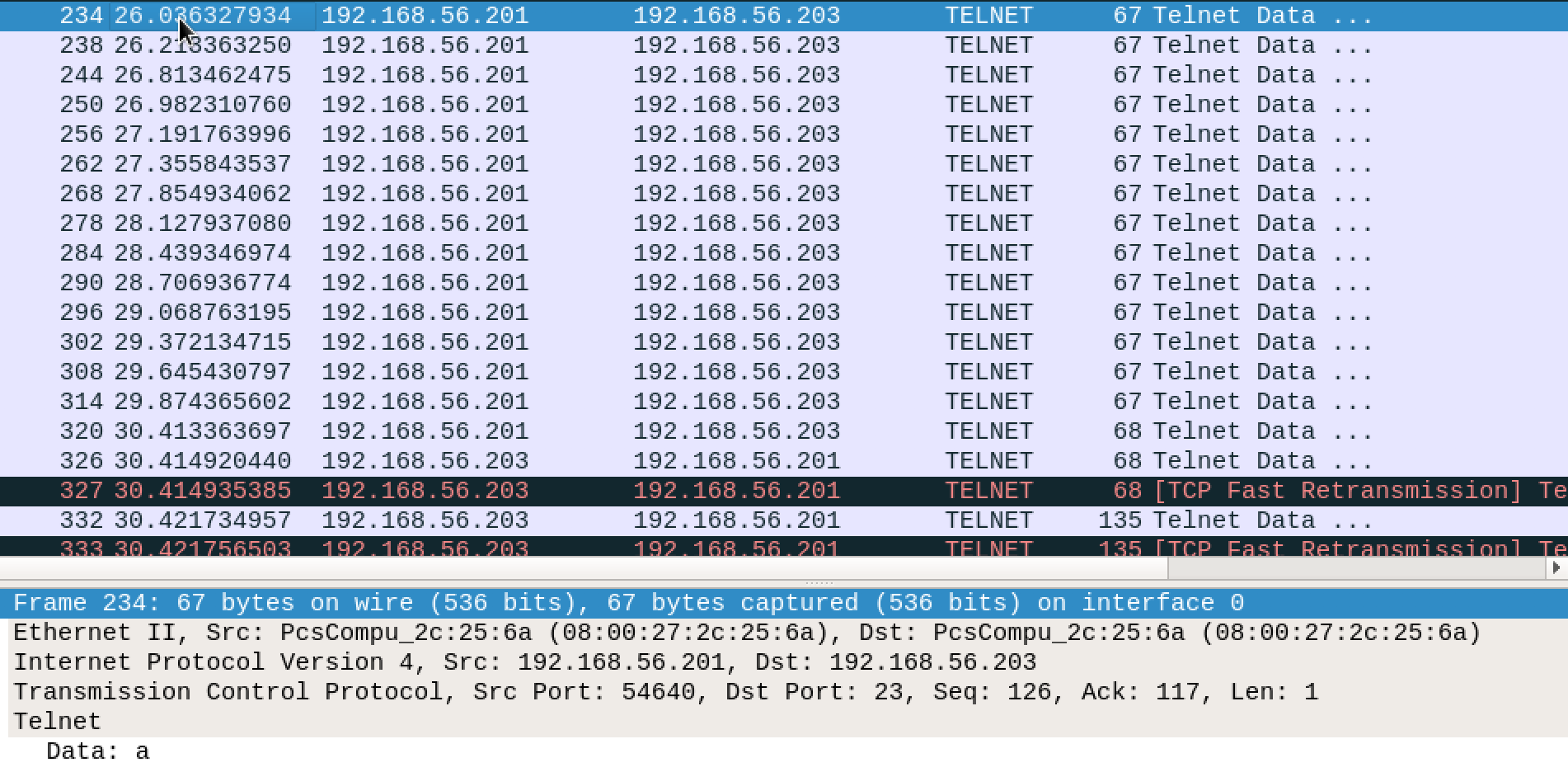
The above image depicts when the client enters the user name, as we can see data here is “s” which is the first letter of the username “sharaddixit”, each packet depicts each username letter, that is from packet number 78-206 depicts the user name entered by the client.

1. Password request from the telnet server to client (Password)



The above figure depicts the password request from the telnet server to the client where we can see the packet 229 in the above figure depicts that from telnet server to client request for password comes. The data here can be seen as “Password:”.

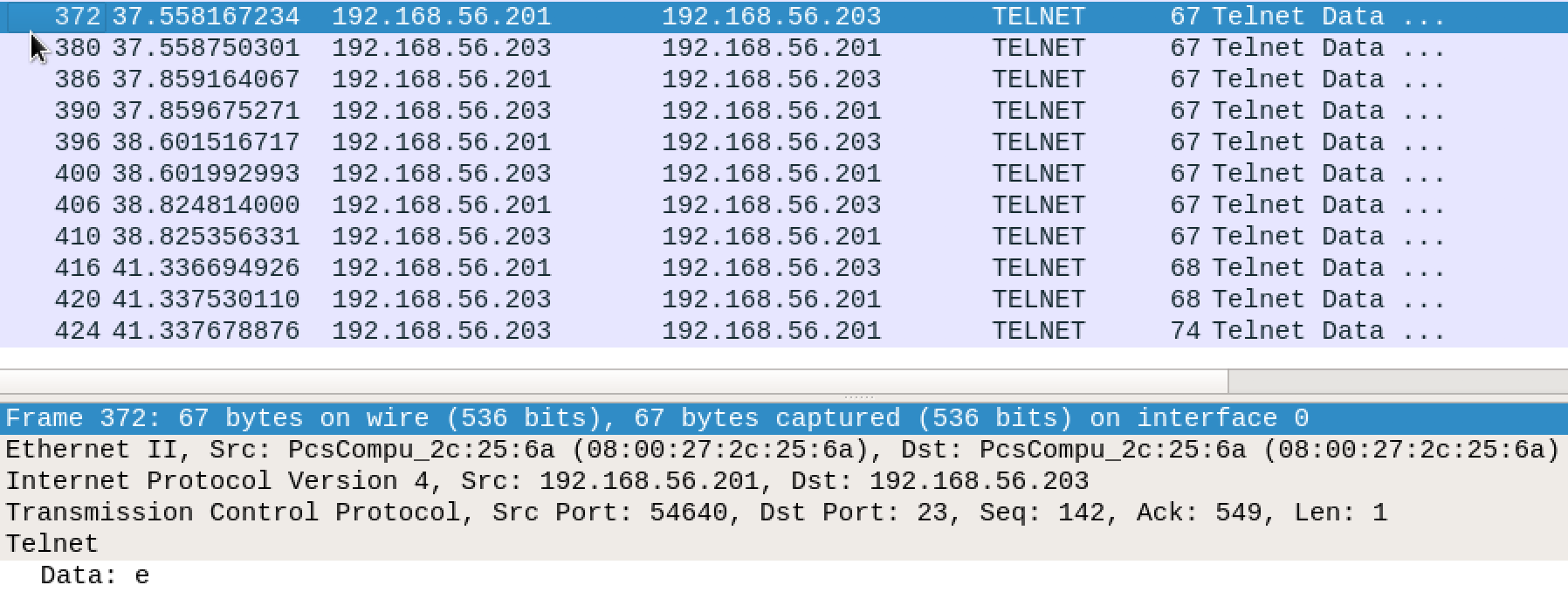
1. Password entry by client



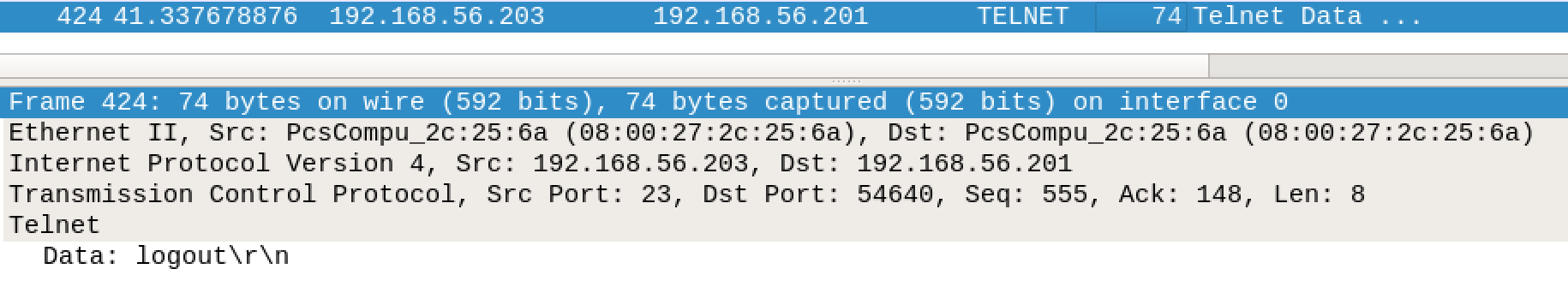
The image depicts that the client enters the password which goes from the client to telnet server. The packets from 234 to 326 depicts the client entry of password for the telnet server.

After entering the correct password the client enters in a telnet session in the telnet server machine.

1. Exit message for telnet session between client and telnet server

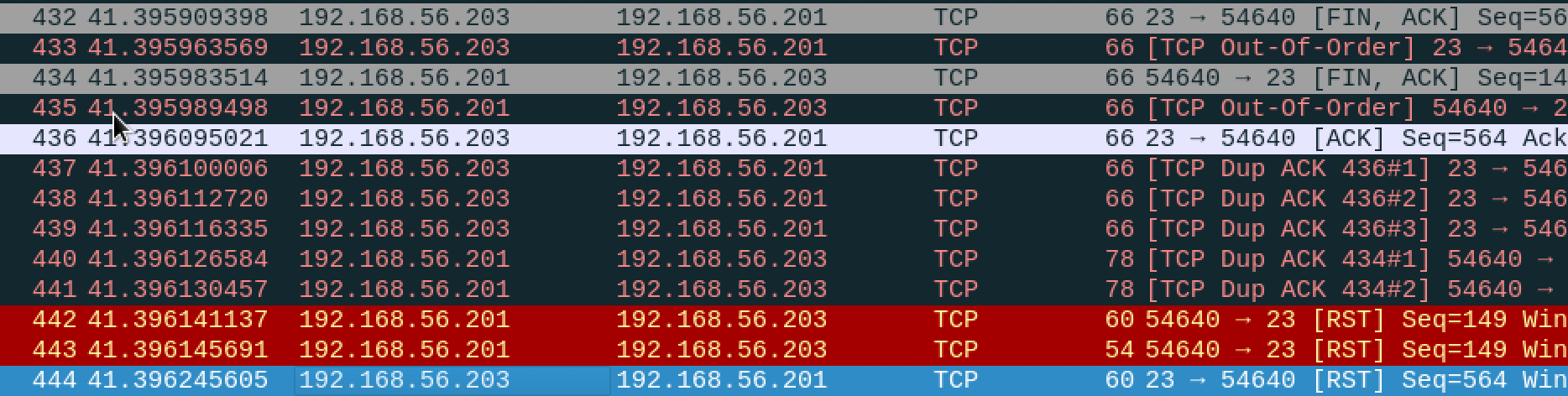
The above image depicts the exit message from the telnet session where client disconnects the telnet session by providing exit command which is done from packets 372 to 420 where data of packet 372 can be seen as “e” of the exit from client to telnet server.

1. Logout message from telnet server to client for exiting the telnet session



The above image depicts the packet 424 from the telnet server to the client for the logout message after the client sent exit message to the telnet server.

1. TCP teardown after ending of telnet session.



The above figure depicts the TCP teardown from packet 432- packet 444 where the server sends a [FIN] to client and the client sends a [FIN] to the server and with the [RST] in order to for TCP breakdown and ending the session. The server also sends an [ACK] to the client for receiving of the [FIN] from the client.

1. OPENVPN SESSION

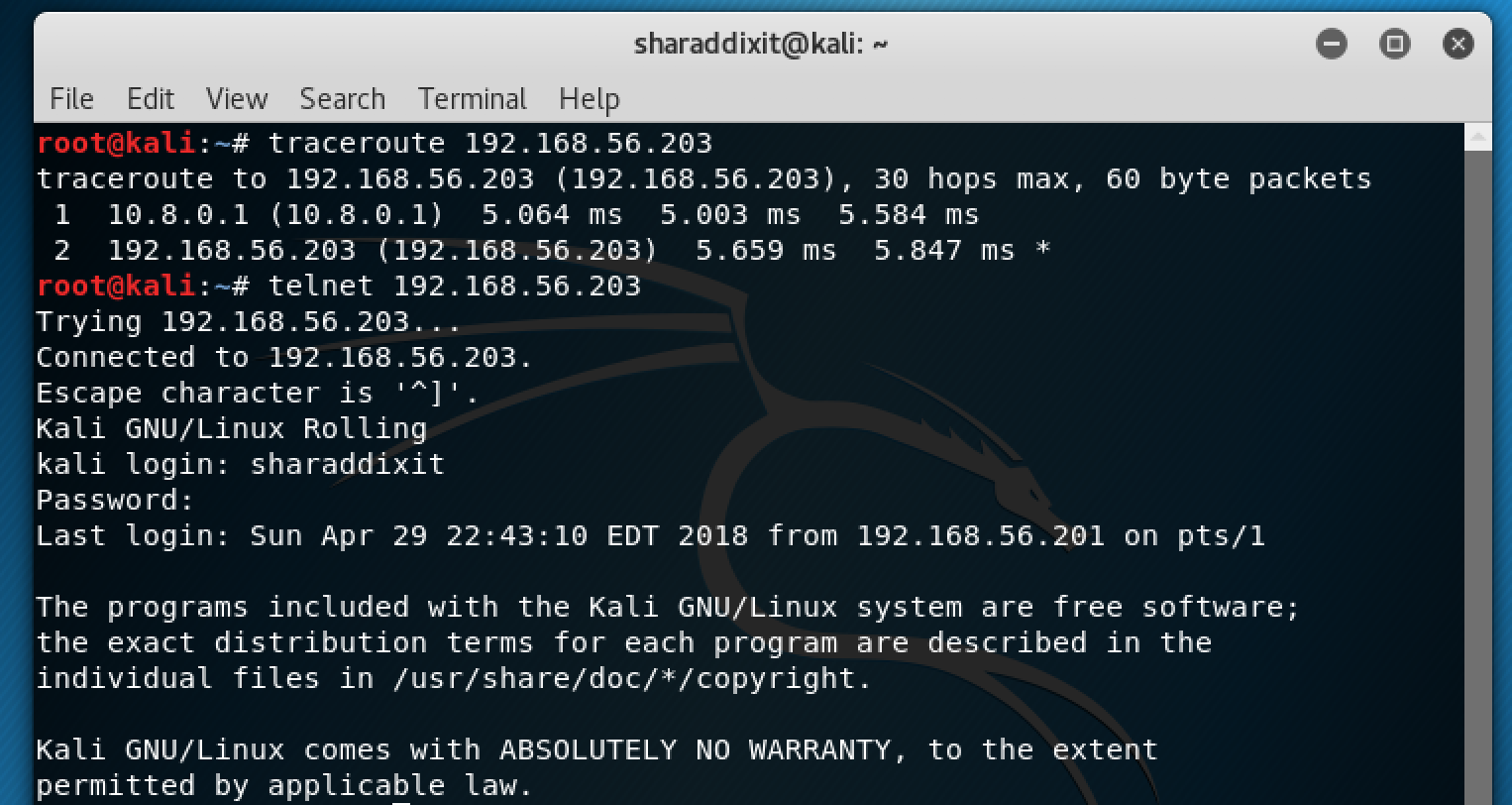
Client IP: 192.168.56.201

OPENVPN server IP: 192.168.56.202

Telnet server IP: 192.168.56.203

Tunnel: 10.8.0.6

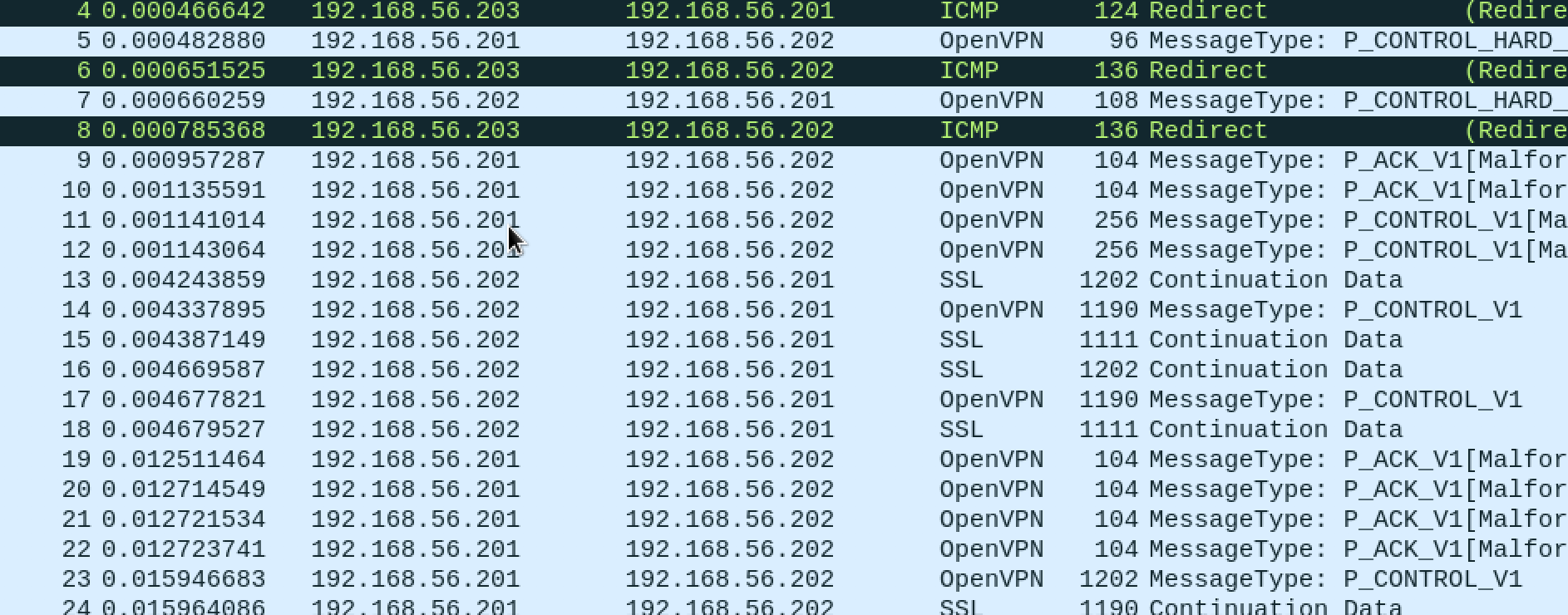
In this session we perform a telnet from the client to the telnet server but the traceroute goes from the openvpn server network and then to the telnet server as we set up a tunnel from the client to the openvpn server.



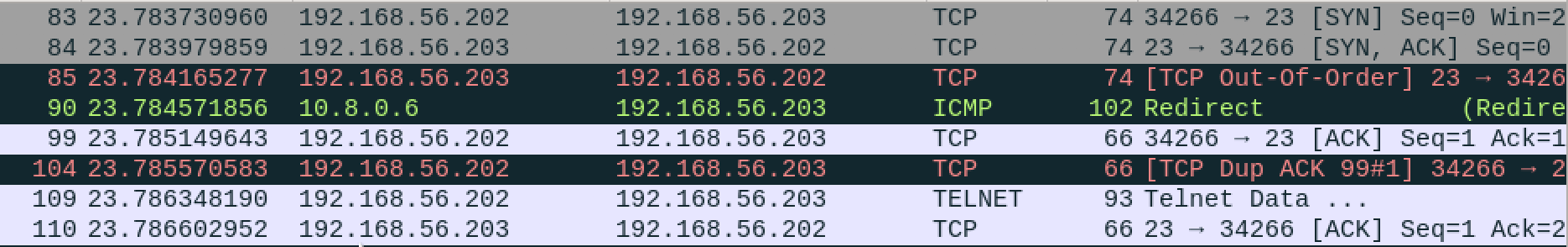
The above image depicts the traceroute and telnet for our openvpn session, where we can see that in the traceroute it first goes to the openvpn server and then to the telnet server. After performing the telnet, we get an access to the user of the telnet server.

* Wireshark Trace for openvpn Session

1. Set up of openvpn server

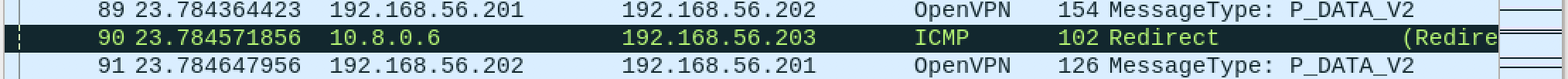
The image above depicts the packets 4-30 which shows the openvpn packets and SSL packets which are initialization of the openvpn server. As we can see the packets from telnet server to client are redirected to the tunnel that is openvpn, and are following the openvpn protocol.

1. TCP connection establish

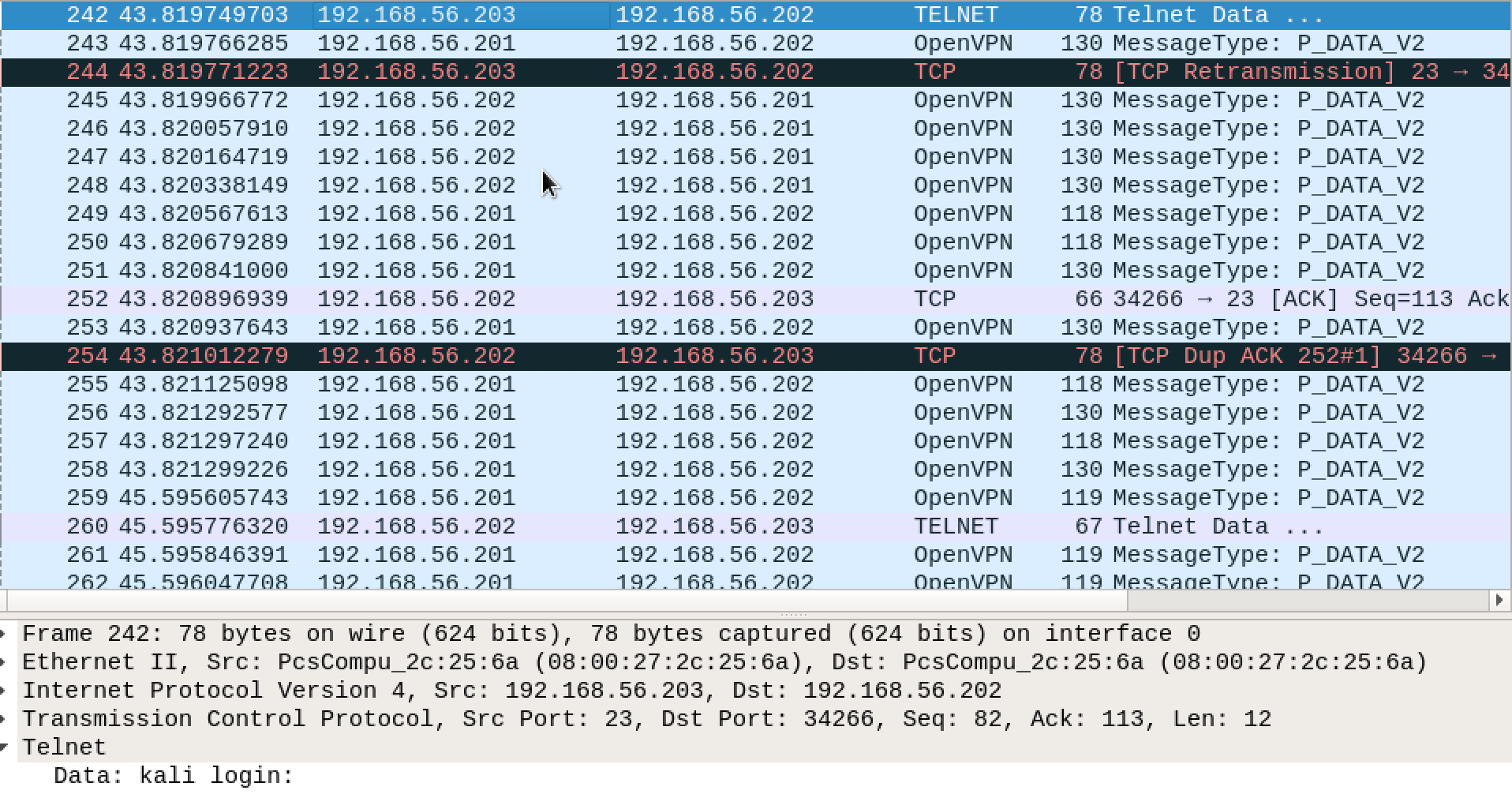


The above image depicts the TCP connection between the openvpn server and the telnet server where the openvpn server sends an [SYN] to telnet server and then receives a [SYN, ACK] and then the openvpn server an [ACK] to the telnet server. The packets above from 83 to packet 110 shows the above procedure.

NOTE:- The below screenshot is an example that shows every packet that the client sends enters the VPN tunnel through the “10” Network interface.

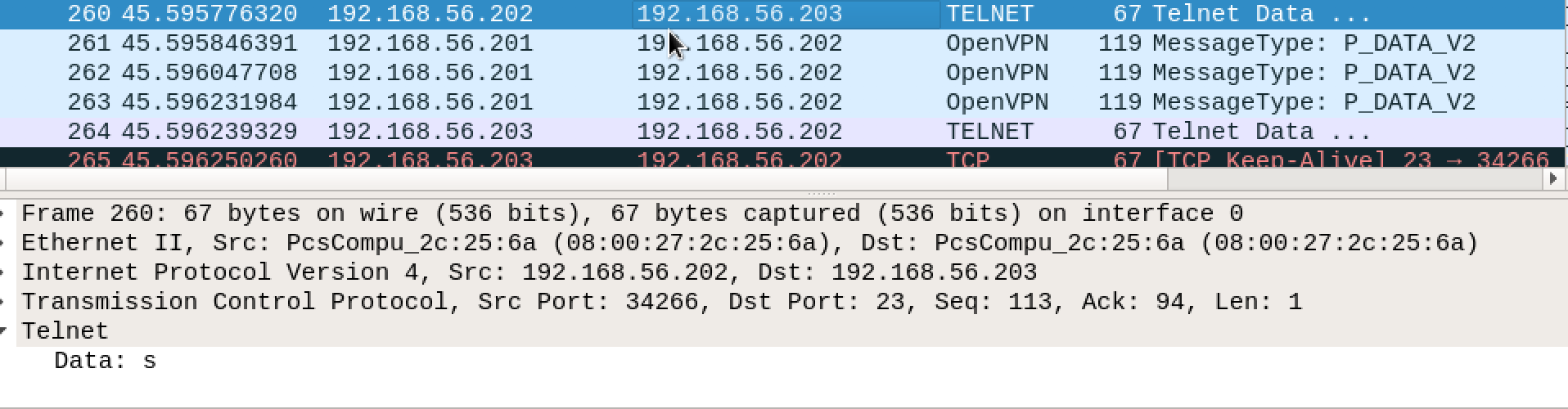


1. Username Request

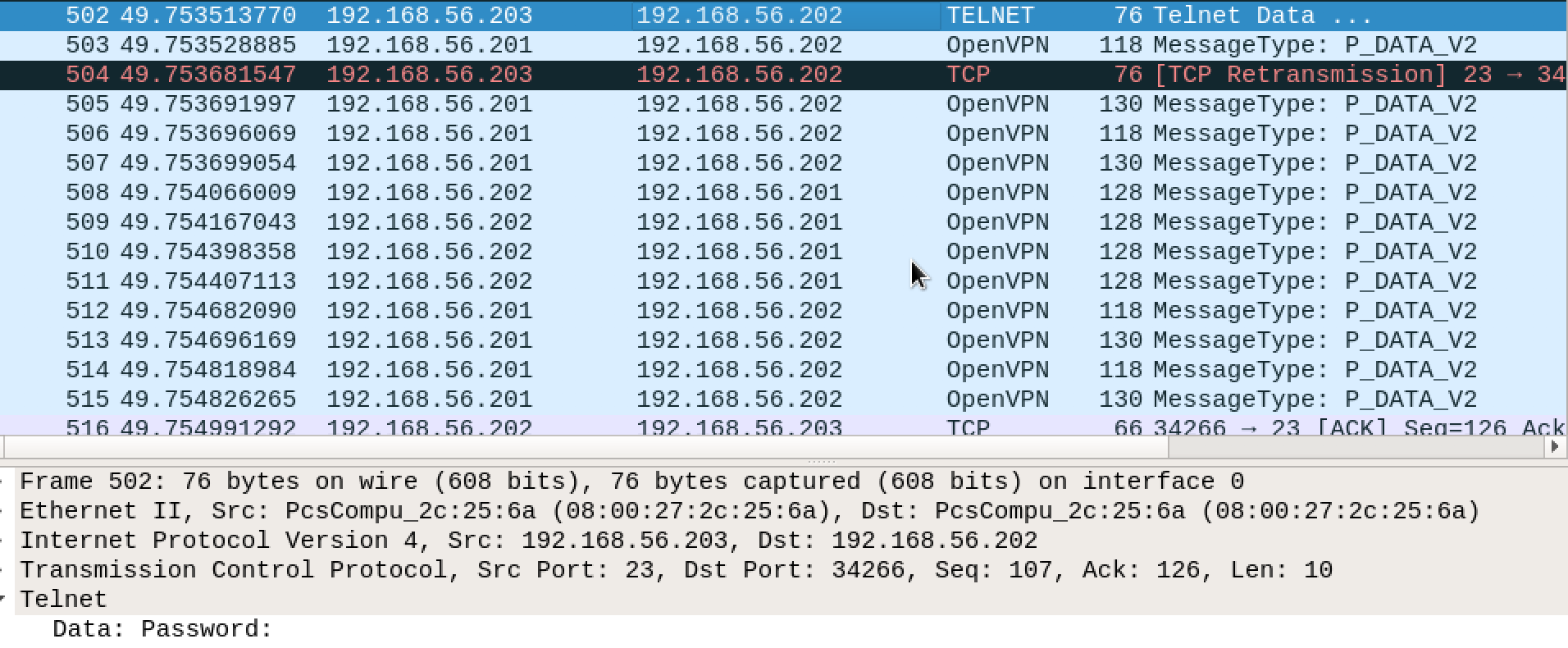
The above shows the username request in Packet 242 from the telnet server to the openvpn server. An important thing to note is that openvpn protocol is employed here in addition to which is done in part1 of the only telnet session.

Therefore, the data hence goes through the openvpn protocol.

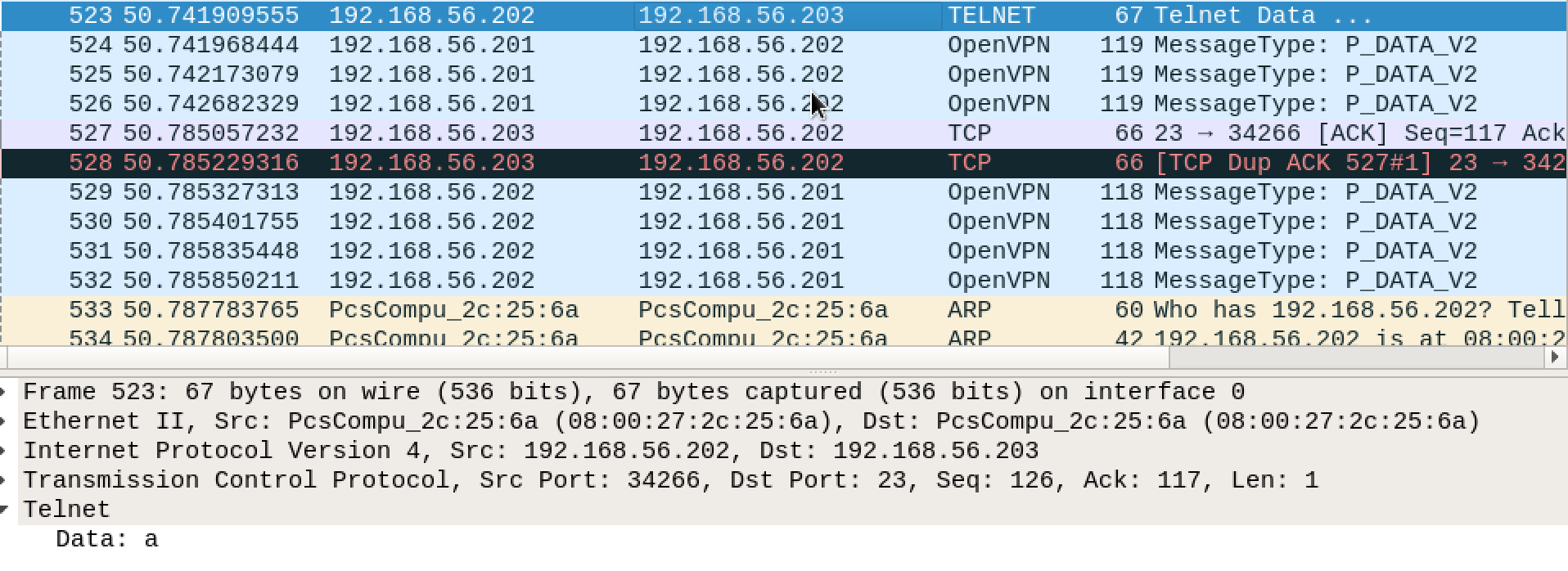
1. Username Entry

The above image depicts the username entry as the data can be seen as “s” which is first letter of the username at the telnet server “sharaddixit”. The important thing is that the openvpn protocol being employed here and the data goes through the openvpn protocol. The packets from 260 to 270 describe the above process.

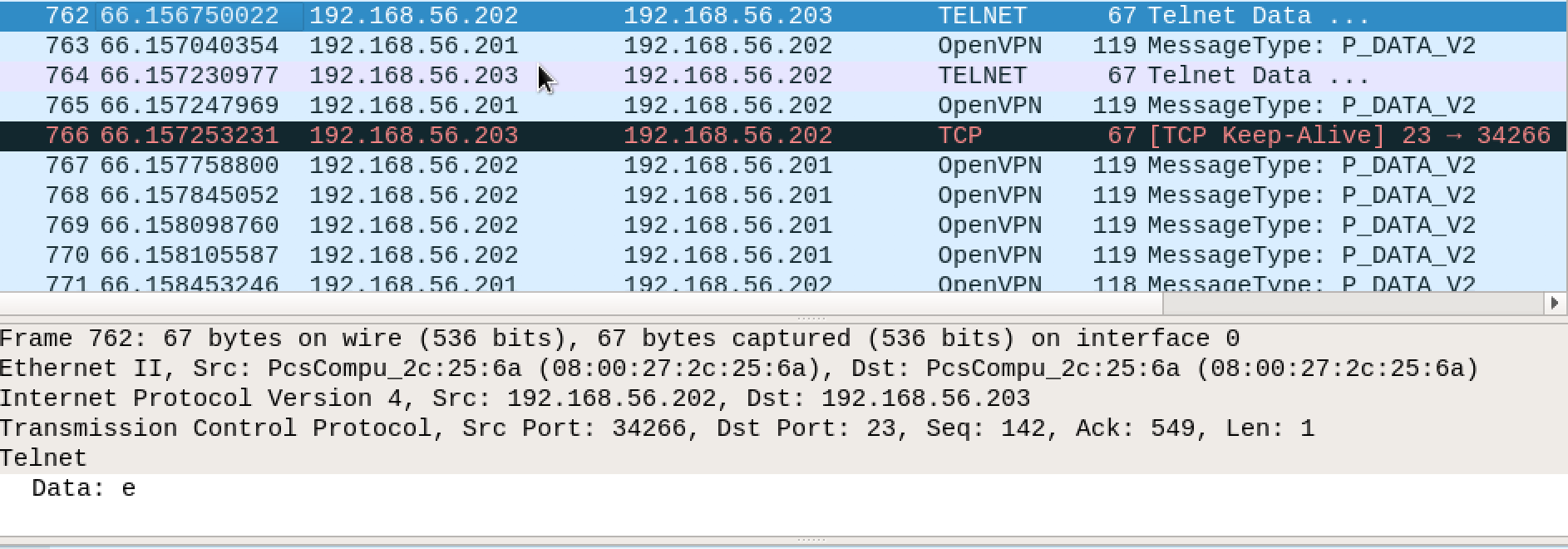
1. Password Request

The above image depicts the password request from the client as the packet 502 can be seen with the data as “Password” where its asking for the password. The openvpn protocol is employed here leading to use of openvpn server as compared to that done in part1 that is in only telnet session. The packet 502 to 503 are for the password request.

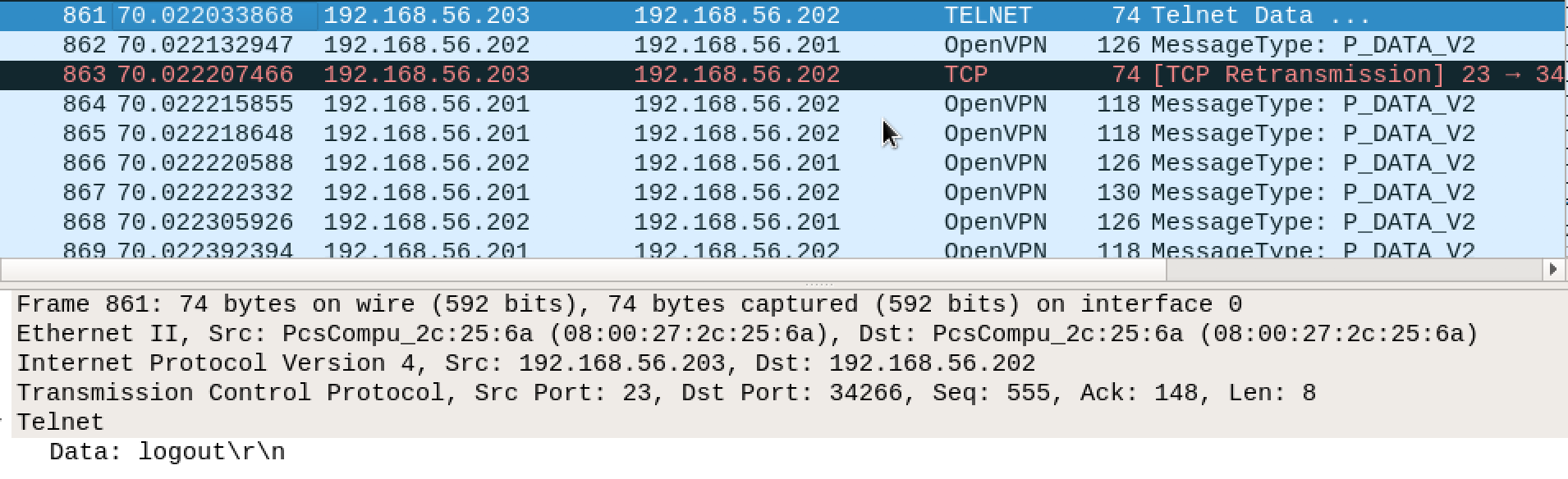
1. Password Entry

The above figure depicts the password entry after the password request from the telnet server. The data can be seen as “a” which is the start of the password. The packet 523 describes the first letter of the password and the consecutive packets show the password letters. The important thing is that the openvpn protocol being employed when the packets are being send.

1. Exit message

The above image depicts the start of the exit message in order to exit the telnet session. The packet 762 depicts the data “e” for the exit and the consecutive packets send the consecutive letter of the message. The openvpn protocol is employed which can seen from the image in contrast to that of only telnet session of part1

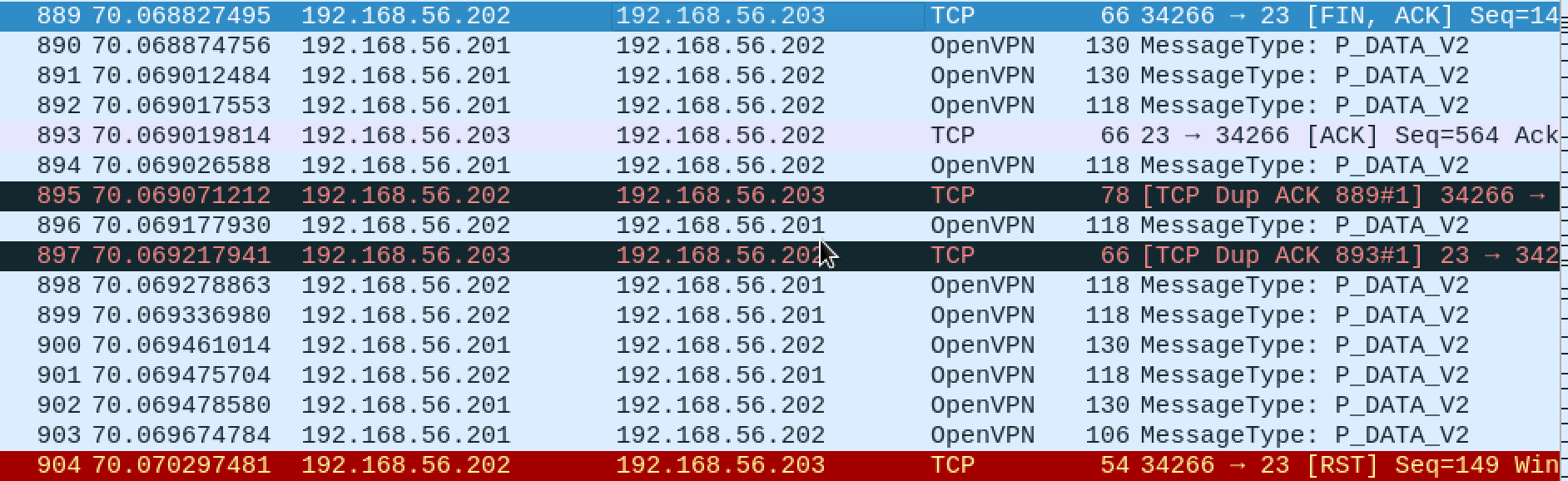
1. Logout Message



The above image depicts packet 861 where the logout message is being sent, the openvpn protocol is employed here. The packet is from the telnet server to the openvpn server.

1. TCP teardown





The above image depicts the packet 881 that has [FIN, ACK] for the openvpn server and then the packet 889 has [FIN, ACK] for the telnet server and sends [RST] to the telnet server in order to finish the session in the packet 904.