SFTP in Wireshark and Stratoshark

This exercise uses the files 5_sftp_packets.pcapng and 5_sftp_syscalls.scap. In these files, we will examine sending a file via SFTP.

1. Open 5_sftp_packets.pcapng
    a. Look at the TCP handshake in the first 3 frames.
        i. Write down the 4-tuple of this connection (source IP address, source port, destination IP address, and destination port)

192.168.64.3, 55492, 192.168.63.1, 22

b. Look at the opening Client and Server SSH packets. These often give some clues to the version of SSH on each machine.
    i. What is the Client Protocol statement?

SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13

ii. What is the Server Protocol statement?

SSH-2.0-OpenSSH_9.8

c. Assuming SSH keys are not being used, a user needs to type their password after the SSH session is established. Because this is interactive, there's usually a time gap while the user is typing.
    i. In which frame does the client likely send their password?

29

ii. How long does it take them to type their password?

4.666 seconds

d. Once the user is logged in, they need to type the statement of what they want to get from the server or put on the server.
    i. In which frame does the client likely send this statement?

55

ii. How long does it take them to type that statement?

6.94 seconds

e. Once that statement is sent, the transmission can begin.

i. Ensure the Time column is set to one of the “Seconds” options in View -> Time Display Format

ii. Right click on the frame identified in question 1.d.i and select “Set/Unset Time Reference”

iii. How long does the actual file transfer take?

0.51 seconds

iv. What is the maximum receive window achieved during the transfer?

619520

2. Open 5_sftp_syscalls.pcapng

a. Look at the SFTP session initiation

i. Build a display filter to look at the SFTP command stack (SFTP and SSH). Filter the capture with this filter.

proc.name in {"sftp","ssh"}

ii. Build a display filter for the TCP file description for this transfer using the following format. Look for events matching this filter using the Search dialog (Ctrl+F/Cmd+F).
[source IP}:[source port]->[destination IP]:[destination port]

fd.name eq "192.168.64.3:55492->192.168.64.1:22"

iii. In which event does the client send a connection request to the server?

1110

b. The SSH and SFTP processes communicate with each other using the /dev/tty file. Modify the search filter above and search for that inter-process communication.

i. In which event does SSH prompt the user for their password?

1776

ii. What is the user's password?

notmyrealpassword

c. The user is using a terminal session located at /dev/pts/0. SFTP uses this file to interact with the user. Modify the search filter to search for this file.

i. What string does the user type to initiate the file transfer?

put 50MB*

d. Once the file transfer begins, SFTP opens a file and begins reading from it.

i. What is the full path of this file?

/home/ubuntu/50MB.zip

ii. What is the maximum chunk size that SFTP uses to read from that file?

261120

iii. What is the maximum chunk size that SSH uses to write data to the network?

32804

e. When the file transfer is finished, SFTP reports statistics back to the user. At what speed does SFTP say the file transfer occurred?

117.6 MB/s