Lab4

Cheng Yu, Yuyang Zhou

The test environment is an Ubuntu 18.04 virtual machine running on a Windows 10 host using software VMware.

The test network is a virtual network that comes with VMware. The host IP address in the network is 192.168.230.1, the user name is 10679, and the virtual machine address is 192.168.230.231.

The server is the Win10 host machine, and the client is the Ubuntu virtual machine. We enable sftp on the server by setting the openssh server on Win10.

1 CP1

We use `sshd` command to query the software version on the host which is `OpenSSH_for_Windows_7.7` as shown in Figure.1.

We print the server identification string during version exchange as shown in Figure.2. The identification string is `SSH-2.0-OpenSSH_for_Windows_7.7<CR><LF>` and it doesn't have a comment. Another example is shown in Figure.3, the identification string is `SSH-2.0-OpenSSH_8.2p1<SP>Ubuntu-4ubuntu0.5<CR><LF>`

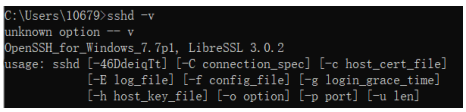


Figure 1: server software version

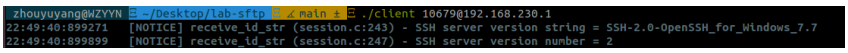


Figure 2: identification string on Windows server

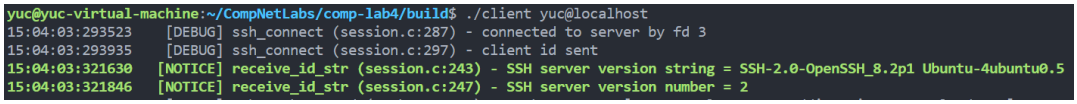


Figure 3: identification string on a Ubuntu server

2 CP2

Figure.4 is from the same running record as Figure.2, it shows the negotiated cipher suite. We find that except for the language (the 8th and 9th kex method) that is explicitly allowed to be ignored in the protocol, the rest are the only encryption methods allowed on the server side.

Figure 4: negotiated cipher suite

3 CP3

We run our mini-sftp with wireshark capturing the packets in the background. The operation in client side is shown in Figure.5. We save the wireshark record in checkpoint as `CP3.pcap`. The screenshot of packets in Figure.6 shows that the messages are encrypted.

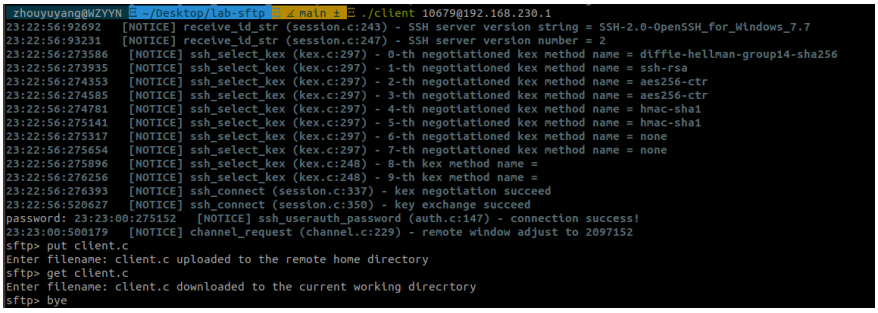


Figure 5: running record on client

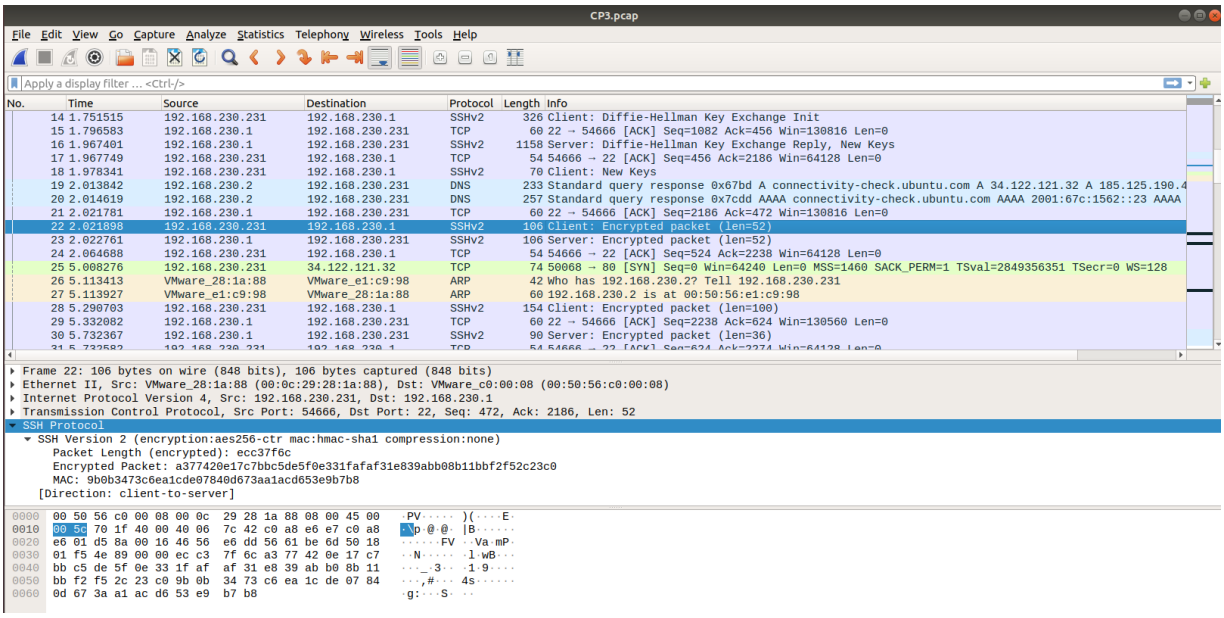


Figure 6: sreenshot of wireshark

4 CP4

During authentication process, we hexdump the response packet after sending the password. Figure.7 shows the result when we enter correct password. The response is a byte `0x34` which represents `SSH_MSG_USERAUTH_SUCCESS`, and we successfully setup the connection. Figure.8 shows the result when we enter incorrect password. The first byte of response is `0x34` which represents `SSH_MSG_USERAUTH_FAILURE`, and we have a second chance to try.

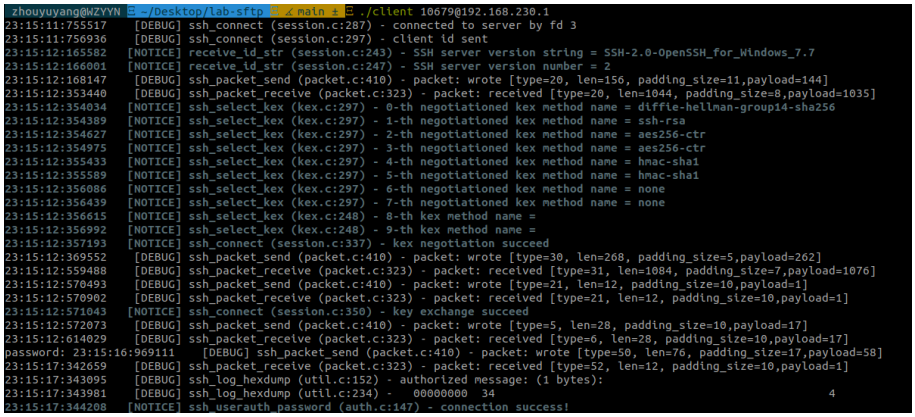


Figure 7: input correct password

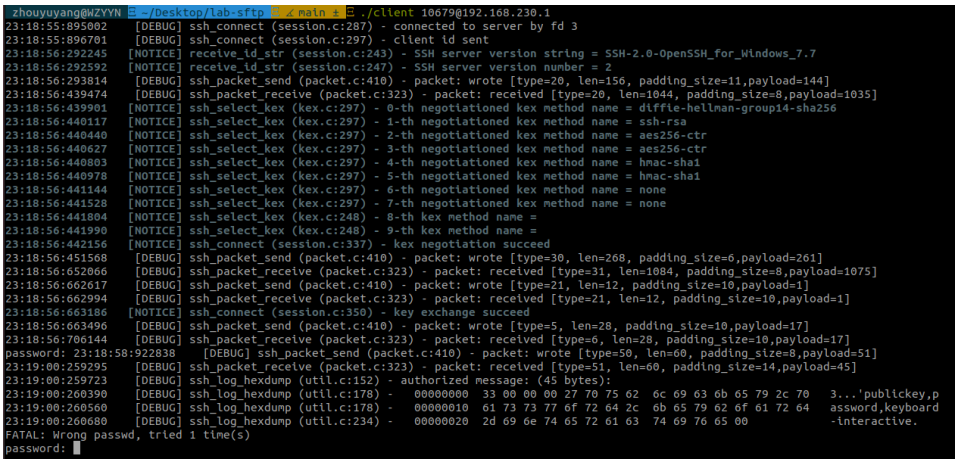
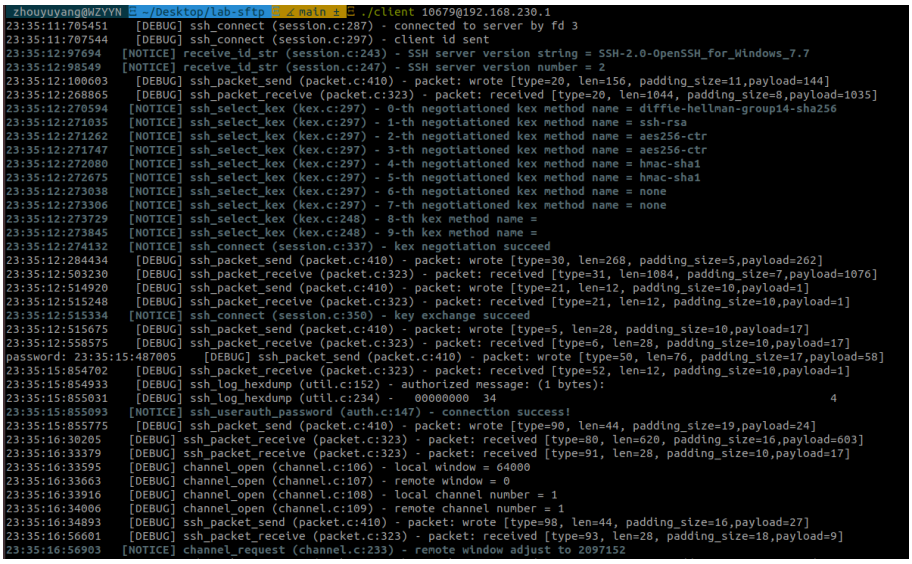


Figure 8: input incorrect password

5 CP5

We print important information in the packet during opening a channel. Figure.9 shows that the server and the client have the same channel id 1. The client has window size 64000, but the server's window size is 0. It will wait for subsequent operations to increase its window size.



```
zhouyuyang@WZYYN ~/Desktop/lab-sftp main ± ./client 10679@192.168.230.1
23:35:11:705451    [DEBUG] ssh_connect (session.c:287) - connected to server by fd 3
23:35:11:707544    [DEBUG] ssh_connect (session.c:297) - client id sent
23:35:12:97694   [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_for_Windows_7.7
23:35:12:98549   [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
23:35:12:100603    [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=20, len=156, padding_size=11,payload=144]
23:35:12:268865    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=20, len=1044, padding_size=8,payload=1035]
23:35:12:270594   [NOTICE] ssh_select_kex (kex.c:297) - 0-th negotiationed kex method name = diffie-hellman-group14-sha256
23:35:12:271035   [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiationed kex method name = ssh-rsa
23:35:12:271262   [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiationed kex method name = aes256-ctr
23:35:12:271747   [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiationed kex method name = aes256-ctr
23:35:12:272080   [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiationed kex method name = hmac-sha1
23:35:12:272675   [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiationed kex method name = hmac-sha1
23:35:12:273038   [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiationed kex method name = none
23:35:12:273306   [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiationed kex method name = none
23:35:12:273729   [NOTICE] ssh_select_kex (kex.c:248) - 8-th kex method name =
23:35:12:273845   [NOTICE] ssh_select_kex (kex.c:248) - 9-th kex method name =
23:35:12:274132   [NOTICE] ssh_connect (session.c:337) - kex negotiation succeed
23:35:12:284434    [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=30, len=268, padding_size=5,payload=262]
23:35:12:503230    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=31, len=1084, padding_size=7,payload=1076]
23:35:12:514920    [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=21, len=12, padding_size=10,payload=1]
23:35:12:515248    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=21, len=12, padding_size=10,payload=1]
23:35:12:515334   [NOTICE] ssh_connect (session.c:350) - key exchange succeed
23:35:12:515675    [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=5, len=28, padding_size=10,payload=17]
23:35:12:558575    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=6, len=28, padding_size=10,payload=17]
password: 23:35:15:487005    [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=50, len=76, padding_size=17,payload=58]
23:35:15:854702    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=52, len=12, padding_size=10,payload=1]
23:35:15:854933    [DEBUG] ssh_log_hexdump (util.c:152) - authorized message: (1 bytes):
23:35:15:855031    [DEBUG] ssh_log_hexdump (util.c:234) -   00000000  34                                                4
23:35:15:855093   [NOTICE] ssh_userauth_password (auth.c:147) - connection success!
23:35:15:855775    [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=90, len=44, padding_size=19,payload=24]
23:35:16:30205    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=80, len=620, padding_size=16,payload=603]
23:35:16:33379    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=91, len=28, padding_size=10,payload=17]
23:35:16:33595    [DEBUG] channel_open (channel.c:106) - local window = 64000
23:35:16:33663    [DEBUG] channel_open (channel.c:107) - remote window = 0
23:35:16:33916    [DEBUG] channel_open (channel.c:108) - local channel number = 1
23:35:16:34006    [DEBUG] channel_open (channel.c:109) - remote channel number = 1
23:35:16:34893    [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=98, len=44, padding_size=16,payload=27]
23:35:16:56601    [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=93, len=28, padding_size=18,payload=9]
23:35:16:56903   [NOTICE] channel_request (channel.c:233) - remote window adjust to 2097152
```

Figure 9: opening a channel

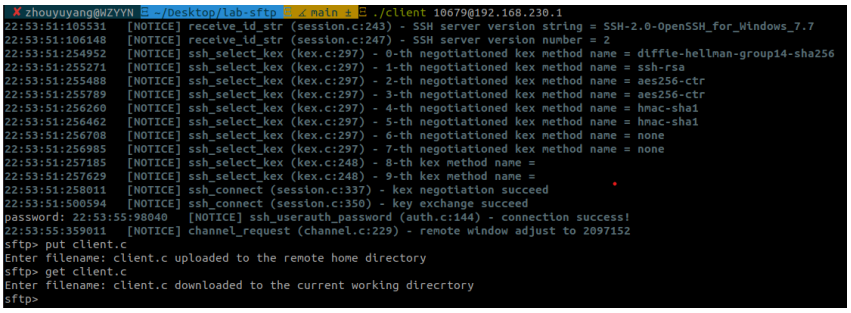
6 CP6

We run our mini-sftp (note that the current work directory is `lab-stfp/`) and first upload `client.c` then download `client.c` as shown in Figure.10.

After perform the put command, the file `client.c` is shown in home directory of server as shown in Figure.11 and 12.

Then we modify the `client.c` in the server. We add a few comments as shown in Figure.13.

We perform the get command and the file gets from server in shown in Figure.14. Openning the file as shown in Figure.15 we find the modification we added is there which indicates that we successfully gets the file from the server and covers the original file.



```
zhouyuyang@WZYYN ~/Desktop/lab-sftp main ± ./client 10679@192.168.230.1
22:53:51:105531   [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_for_Windows_7.7
22:53:51:106148   [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
22:53:51:254952   [NOTICE] ssh_select_kex (kex.c:297) - 0-th negotiationed kex method name = diffie-hellman-group14-sha256
22:53:51:255271   [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiationed kex method name = ssh-rsa
22:53:51:255488   [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiationed kex method name = aes256-ctr
22:53:51:255789   [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiationed kex method name = aes256-ctr
22:53:51:256260   [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiationed kex method name = hmac-sha1
22:53:51:256462   [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiationed kex method name = hmac-sha1
22:53:51:256708   [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiationed kex method name = none
22:53:51:256985   [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiationed kex method name = none
22:53:51:257185   [NOTICE] ssh_select_kex (kex.c:248) - 8-th kex method name =
22:53:51:257629   [NOTICE] ssh_select_kex (kex.c:248) - 9-th kex method name =
22:53:51:258011   [NOTICE] ssh_connect (session.c:337) - kex negotiation succeed
22:53:51:500594   [NOTICE] ssh_connect (session.c:350) - key exchange succeed
password: 22:53:55:98040   [NOTICE] ssh_userauth_password (auth.c:144) - connection success!
22:53:55:359011   [NOTICE] channel_request (channel.c:229) - remote window adjust to 2097152
sftp> put client.c
Enter filename: client.c uploaded to the remote home directory
sftp> get client.c
Enter filename: client.c downloaded to the current working direcrtory
sftp>
```

Figure 10: client operations

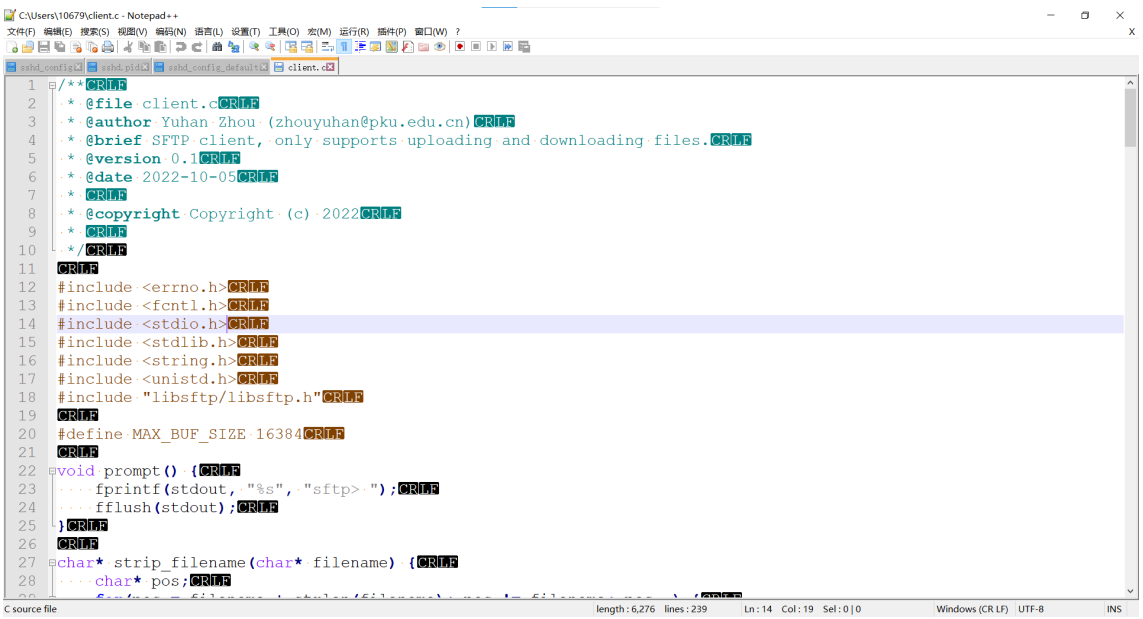


Figure 11: server receive file

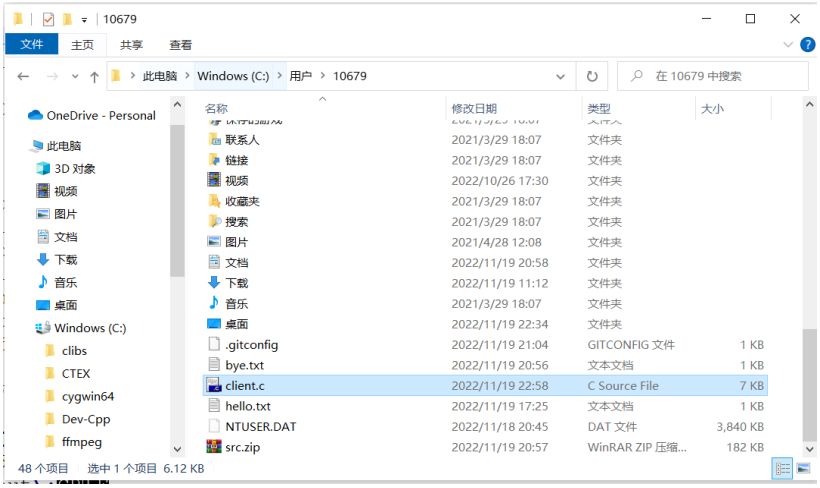


Figure 12: the time server receives the file

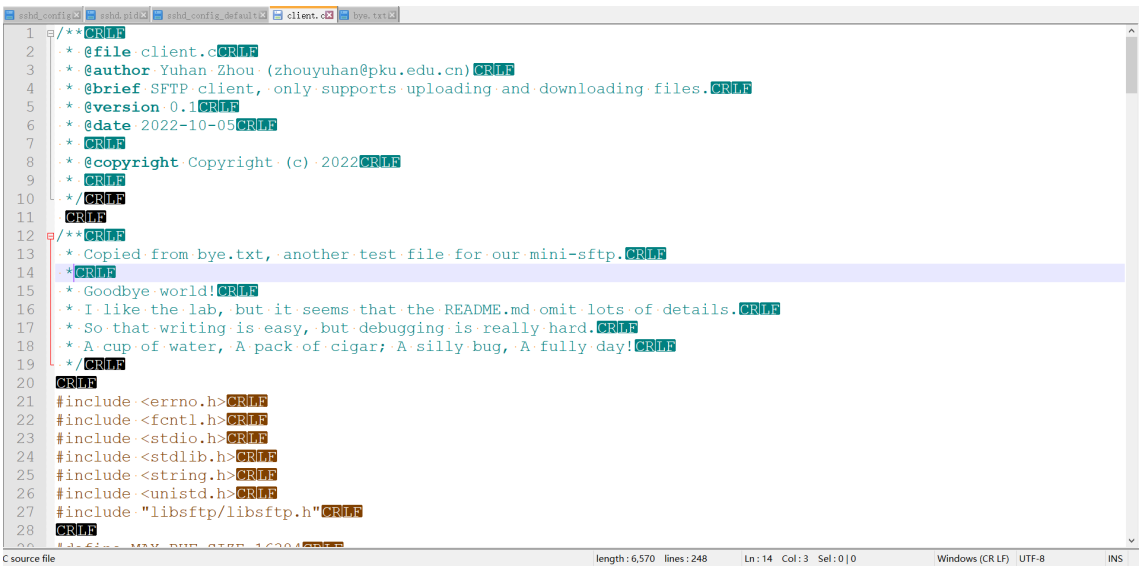


Figure 13: modify the file at server

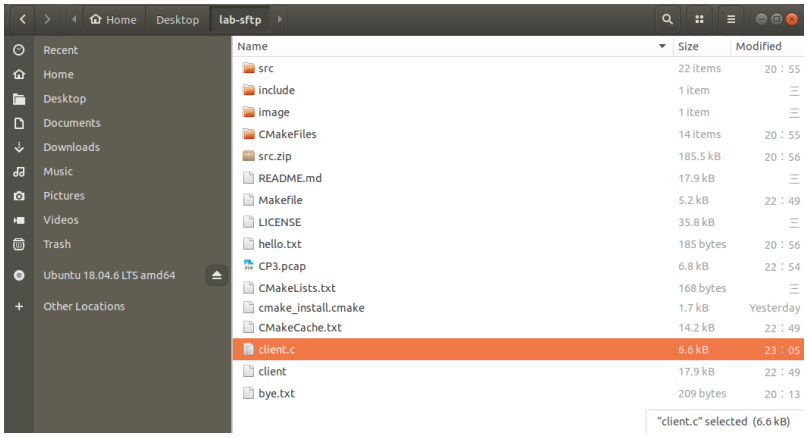


Figure 14: the time clients gets the file

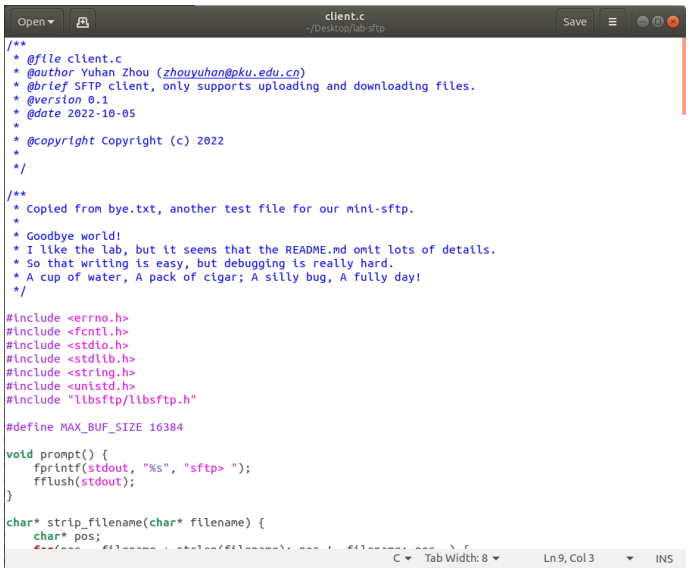


Figure 15: ns4 perf server