

# Lab4

Cheng Yu, Yuyang Zhou

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

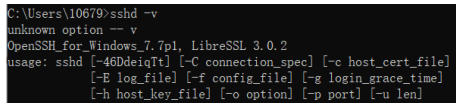
The test network is a virtual network that comes with VMware. The host IP address in the network is 192.168.230.1, the user name is 10679, and the virtual machine address is 192.168.230.231.

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

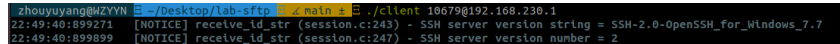
We use `sshd` command to query the software version on the host which is `OpenSSH_for_Windows_7.7` as shown in Figure.1.

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` and it doesn't have a comment. Another example is shown in Figure.3, the identification string is `SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5`



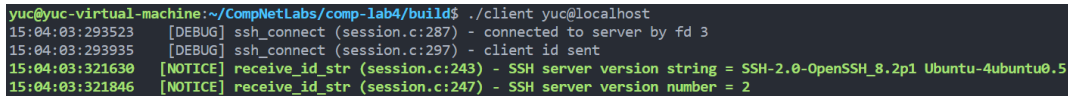
```
C:\Users\10679>sshd -v
sshd: unknown option -- v
OpenSSH_for_Windows_7.7p1, LibreSSL 3.0.2
usage: sshd [-46DdeiqTt] [-C connection_spec] [-c host_cert_file]
           [-E log_file] [-f config_file] [-g login_grace_time]
           [-h host_key_file] [-o option] [-p port] [-u len]
```

Figure 1: server software version



```
zhouyuyang@NZVYN:~/CompNetLabs/lab4/sftp$ ./client 10679@192.168.230.1
22:49:40:899271 [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_for_Windows_7.7
22:49:40:899899 [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
```

Figure 2: identification string on Windows server



```
yuc@yuc-virtual-machine:~/CompNetLabs/comp-lab4/build$ ./client yuc@localhost
15:04:03:293523 [DEBUG] ssh_connect (session.c:287) - connected to server by fd 3
15:04:03:293935 [DEBUG] ssh_connect (session.c:297) - client id sent
15:04:03:321630 [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
15:04:03:321846 [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
```

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.

```
z.houyuyang@WZYNN ~ -/Desktop/lab-sftp 2 main # ./client 10679@192.168.230.1
22:49:40:899271 [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_for_Windows_7.7
22:49:40:899899 [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
22:49:41:46536 [NOTICE] ssh_select_kex (kex.c:297) - 0-th negotiated kex method name = diffie-hellman-group14-sha256
22:49:41:46842 [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiated kex method name = ssh-rsa
22:49:41:46946 [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiated kex method name = aes256-ctr
22:49:41:47736 [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiated kex method name = aes256-ctr
22:49:41:48636 [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiated kex method name = hmac-sha1
22:49:41:48951 [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiated kex method name = hmac-sha1
22:49:41:49758 [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiated kex method name = none
22:49:41:50105 [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiated kex method name = none
22:49:41:51101 [NOTICE] ssh_select_kex (kex.c:248) - 8-th kex method name =
22:49:41:51752 [NOTICE] ssh_select_kex (kex.c:248) - 9-th kex method name =
```

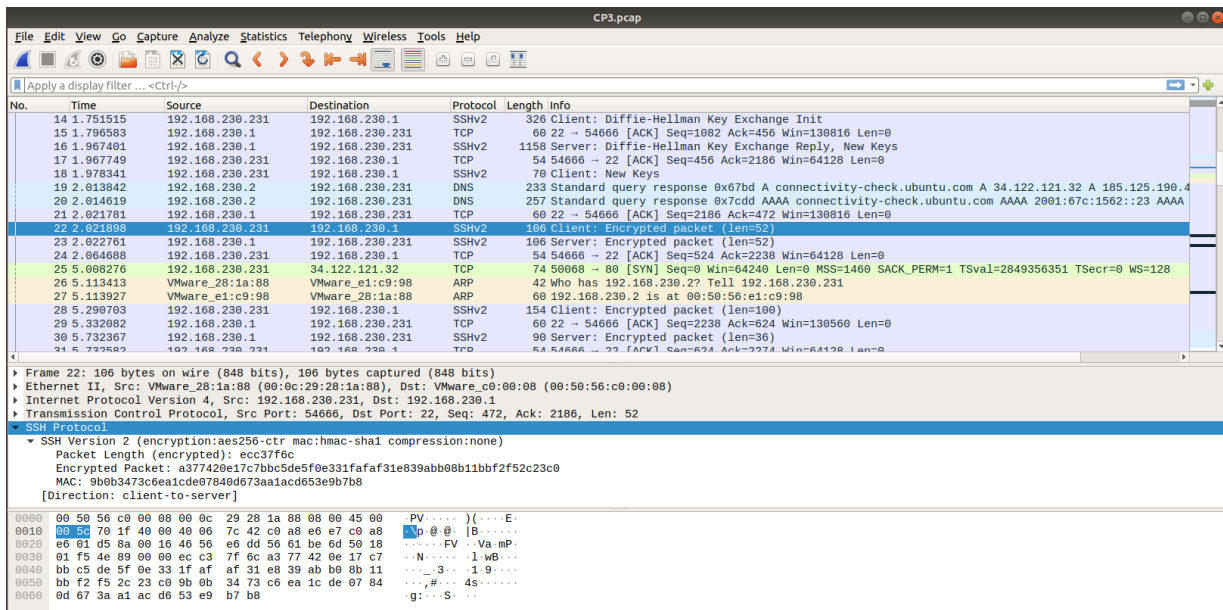
Figure 4: negotiated cipher suite

## 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.

```
z.houyuyang@WZYNN ~ -/Desktop/lab-sftp 2 main # ./client 10679@192.168.230.1
23:22:56:92692 [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_for_Windows_7.7
23:22:56:93231 [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
23:22:56:93586 [NOTICE] ssh_select_kex (kex.c:297) - 0-th negotiated kex method name = diffie-hellman-group14-sha256
23:22:56:93795 [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiated kex method name = ssh-rsa
23:22:56:94353 [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiated kex method name = aes256-ctr
23:22:56:94585 [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiated kex method name = aes256-ctr
23:22:56:94781 [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiated kex method name = hmac-sha1
23:22:56:95141 [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiated kex method name = hmac-sha1
23:22:56:95317 [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiated kex method name = none
23:22:56:95654 [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiated kex method name = none
23:22:56:95896 [NOTICE] ssh_select_kex (kex.c:248) - 8-th kex method name =
23:22:56:96256 [NOTICE] ssh_select_kex (kex.c:248) - 9-th kex method name =
23:22:56:96393 [NOTICE] ssh_connect (session.c:337) - kex negotiation succeed
23:22:56:96627 [NOTICE] ssh_connect (session.c:350) - key exchange succeed
password: 23:23:00:275152 [NOTICE] ssh_userauth_password (auth.c:147) - connection success!
23:23:00:500179 [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 directory
sftp> bye
```

Figure 5: running record on client



No.	Time	Source	Destination	Protocol	Length	Info
14	1.751515	192.168.230.231	192.168.230.1	SSHv2	326	Client: Diffie-Hellman Key Exchange Init
15	1.796583	192.168.230.1	192.168.230.231	TCP	60	22 → 54666 [ACK] Seq=1082 Ack=456 Win=130816 Len=0
16	1.967401	192.168.230.1	192.168.230.231	SSHv2	1158	Server: Diffie-Hellman Key Exchange Reply, New Keys
17	1.967749	192.168.230.231	192.168.230.1	TCP	54	54666 → 22 [ACK] Seq=456 Ack=2186 Win=64128 Len=0
18	1.978341	192.168.230.231	192.168.230.1	SSHv2	70	Client: New Keys
19	2.013842	192.168.230.2	192.168.230.231	DNS	233	Standard query response 0x67bd A connectivity-check.ubuntu.com A 34.122.121.32 A 185.125.190.4
20	2.014619	192.168.230.2	192.168.230.231	DNS	257	Standard query response 0x7cdd AAAA connectivity-check.ubuntu.com AAAA 2001:67c:1562::23 AAAA
21	2.021781	192.168.230.1	192.168.230.231	TCP	60	22 → 54666 [ACK] Seq=2186 Ack=472 Win=130816 Len=0
22	2.021898	192.168.230.231	192.168.230.1	SSHv2	106	Client: Encrypted packet (len=52)
23	2.022761	192.168.230.1	192.168.230.231	SSHv2	106	Server: Encrypted packet (len=52)
24	2.064688	192.168.230.231	192.168.230.1	TCP	54	54666 → 22 [ACK] Seq=524 Ack=2238 Win=64128 Len=0
25	5.008276	192.168.230.231	34.122.121.32	TCP	74	50008 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2849356351 TSecr=0 WS=128
26	5.113413	VMware_28:1a:88	VMware_e1:c9:98	ARP	42	Who has 192.168.230.2? Tell 192.168.230.231
27	5.113927	VMware_e1:c9:98	VMware_28:1a:88	ARP	60	192.168.230.2 is at 00:50:56:e1:c9:98
28	5.290703	192.168.230.231	192.168.230.1	SSHv2	154	Client: Encrypted packet (len=100)
29	5.332082	192.168.230.1	192.168.230.231	TCP	60	22 → 54666 [ACK] Seq=2238 Ack=624 Win=130560 Len=0
30	5.732367	192.168.230.1	192.168.230.231	SSHv2	90	Server: Encrypted packet (len=36)
31	6.732582	192.168.230.231	192.168.230.1	TCP	64	54666 → 22 [ACK] Seq=524 Ack=2274 Win=64128 Len=0

Frame 22: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0  
Ethernet II, Src: VMware\_28:1a:88 (00:0c:29:28:1a:88), Dst: VMware\_e1:c9:98 (00:50:56:e1:c9:98)  
Internet Protocol Version 4, Src: 192.168.230.231, Dst: 192.168.230.1  
Transmission Control Protocol, Src Port: 54666, Dst Port: 22, Seq: 472, Ack: 2186, Len: 52  
SSH (Protocol)  
SSH Version 2 (encryption:aes256-ctr mac:hmac-sha1 compression:none)  
Packet Length (encrypted): ecc37f6c  
Encrypted Packet: a377420e17c7bb5de5f0e331fafaf31e839abb08b11bbf2f52c230  
MAC: 9b0b3473c6e1cde07840d673a1acd653e9b7b8  
[Direction: client-to-server]  
0000 00 50 56 c0 00 08 00 c0 29 28 1a 88 00 00 45 00 ..PV....)....E  
0010 30 5c 70 1f 40 00 40 00 7c 42 c0 a8 e6 e7 c0 a8 ..p.@.@|B....  
0020 e6 01 d5 8a 00 16 46 56 e6 dd 56 01 be 6d 56 18 .....FV..Va.mP.  
0030 01 f5 4e 89 00 00 ec c3 7f 6c a3 77 42 0e 17 c7 .....N....1..wS..  
0040 bb c5 de 5f 0e 33 1f af af 31 e8 39 ab b0 8b 11 .....3...1.9...  
0050 bb f2 f5 2c 23 c0 9b 0b 34 73 c6 ea 1c de 07 84 ....,###.4s.....  
0060 0d 67 3a a1 ac d6 53 e9 b7 b8 .....g:...S..

Figure 6: screenshot 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.

```
zhouyuyang@WZYIN ~ -/Desktop/lab-sftp % ./main + B ./client 10679@192.168.230.1
23:15:11:755517 [DEBUG] ssh_connect (session.c:287) - connected to server by fd 3
23:15:11:756936 [DEBUG] ssh_connect (session.c:297) - client id sent
23:15:12:165592 [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_for_Windows_7.7
23:15:12:166001 [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
23:15:12:168147 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=20, len=156, padding_size=11,payload=144]
23:15:12:353440 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=20, len=1044, padding_size=8,payload=1035]
23:15:12:354034 [NOTICE] ssh_select_kex (kex.c:297) - 0-th negotiated kex method name = diffie-hellman-group14-sha256
23:15:12:354389 [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiated kex method name = ssh-rsa
23:15:12:354627 [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiated kex method name = aes256-ctr
23:15:12:354975 [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiated kex method name = aes256-ctr
23:15:12:355433 [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiated kex method name = hmac-sha1
23:15:12:355589 [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiated kex method name = hmac-sha1
23:15:12:356086 [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiated kex method name = none
23:15:12:356439 [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiated kex method name = none
23:15:12:356615 [NOTICE] ssh_select_kex (kex.c:248) - 8-th kex method name =
23:15:12:356692 [NOTICE] ssh_select_kex (kex.c:248) - 9-th kex method name =
23:15:12:357193 [NOTICE] ssh_connect (session.c:337) - kex negotiation succeed
23:15:12:369552 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=30, len=268, padding_size=5,payload=262]
23:15:12:559488 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=31, len=1084, padding_size=7,payload=1076]
23:15:12:570493 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=21, len=12, padding_size=10,payload=1]
23:15:12:570902 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=21, len=12, padding_size=10,payload=1]
23:15:12:571043 [NOTICE] ssh_connect (session.c:350) - key exchange succeed
23:15:12:572073 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=5, len=28, padding_size=10,payload=17]
23:15:12:572073 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=6, len=28, padding_size=10,payload=17]
password: 23:15:16:969111 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=50, len=76, padding_size=17,payload=58]
23:15:17:342659 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=52, len=12, padding_size=10,payload=1]
23:15:17:343095 [DEBUG] ssh_log_hexdump (util.c:152) - authorized message: (1 bytes):
23:15:17:343981 [DEBUG] ssh_log_hexdump (util.c:234) - 00000000 34
23:15:17:344208 [NOTICE] ssh_userauth_password (auth.c:147) - connection success!
```

Figure 7: input correct password

```
zhouyuyang@WZYIN ~ -/Desktop/lab-ftp % ./main + B ./client 10679@192.168.230.1
23:18:55:895002 [DEBUG] ssh_connect (session.c:287) - connected to server by fd 3
23:18:55:896701 [DEBUG] ssh_connect (session.c:297) - client id sent
23:18:56:292245 [NOTICE] receive_id_str (session.c:243) - SSH server version string = SSH-2.0-OpenSSH_for_Windows_7.7
23:18:56:292592 [NOTICE] receive_id_str (session.c:247) - SSH server version number = 2
23:18:56:293814 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=20, len=156, padding_size=11,payload=144]
23:18:56:439474 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=20, len=1044, padding_size=8,payload=1035]
23:18:56:439901 [NOTICE] ssh_select_kex (kex.c:297) - 0-th negotiated kex method name = diffie-hellman-group14-sha256
23:18:56:440117 [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiated kex method name = ssh-rsa
23:18:56:440440 [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiated kex method name = aes256-ctr
23:18:56:440627 [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiated kex method name = aes256-ctr
23:18:56:440803 [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiated kex method name = hmac-sha1
23:18:56:440978 [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiated kex method name = hmac-sha1
23:18:56:441144 [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiated kex method name = none
23:18:56:441528 [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiated kex method name = none
23:18:56:441804 [NOTICE] ssh_select_kex (kex.c:248) - 8-th kex method name =
23:18:56:441990 [NOTICE] ssh_select_kex (kex.c:248) - 9-th kex method name =
23:18:56:442156 [NOTICE] ssh_connect (session.c:337) - kex negotiation succeed
23:18:56:451508 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=30, len=268, padding_size=6,payload=261]
23:18:56:652066 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=31, len=1084, padding_size=8,payload=1075]
23:18:56:662617 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=21, len=12, padding_size=10,payload=1]
23:18:56:662994 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=21, len=12, padding_size=10,payload=1]
23:18:56:663186 [NOTICE] ssh_connect (session.c:350) - key exchange succeed
23:18:56:663496 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=5, len=28, padding_size=10,payload=17]
23:18:56:706144 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=6, len=28, padding_size=10,payload=17]
password: 23:18:58:922838 [DEBUG] ssh_packet_send (packet.c:410) - packet: wrote [type=50, len=60, padding_size=8,payload=51]
23:19:00:259295 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=51, len=60, padding_size=14,payload=45]
23:19:00:259723 [DEBUG] ssh_log_hexdump (util.c:152) - authorized message: (45 bytes):
23:19:00:260390 [DEBUG] ssh_log_hexdump (util.c:178) - 00000000 33 00 00 00 27 70 75 62 6c 69 63 6b 65 79 2c 70 3...'publickey,p
23:19:00:260560 [DEBUG] ssh_log_hexdump (util.c:178) - 00000010 61 73 73 77 6f 72 64 2c 6b 65 79 62 6f 61 72 64 assword,keyboard
23:19:00:260680 [DEBUG] ssh_log_hexdump (util.c:234) - 00000020 2d 69 6e 74 65 72 61 63 74 69 76 65 00 -Interactive.
FATAL: Wrong passwd, tried 1 time(s)
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@WZYNYN ~ -/Desktop/lab-sftp - z main + B ./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:248) - 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]
23:35:12:208865 [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 negotiated kex method name = diffie-hellman-group14-sha256
23:35:12:271035 [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiated kex method name = ssh-rsa
23:35:12:271262 [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiated kex method name = aes256-ctr
23:35:12:271747 [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiated kex method name = aes256-ctr
23:35:12:272080 [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiated kex method name = hmac-sha1
23:35:12:272675 [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiated kex method name = hmac-sha1
23:35:12:273038 [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiated kex method name = none
23:35:12:273306 [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiated 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]
23:35:12:515805 [DEBUG] ssh_packet_receive (packet.c:323) - packet: received [type=6, len=20, 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=50]
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-sftp/) 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. Opening 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@WZYNYN ~ -/Desktop/lab-sftp - z main + B ./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:243) - SSH server version number = 2
22:53:51:254952 [NOTICE] ssh_select_kex (kex.c:297) - 0-th negotiated kex method name = diffie-hellman-group14-sha256
22:53:51:255271 [NOTICE] ssh_select_kex (kex.c:297) - 1-th negotiated kex method name = ssh-rsa
22:53:51:255488 [NOTICE] ssh_select_kex (kex.c:297) - 2-th negotiated kex method name = aes256-ctr
22:53:51:255789 [NOTICE] ssh_select_kex (kex.c:297) - 3-th negotiated kex method name = aes256-ctr
22:53:51:256260 [NOTICE] ssh_select_kex (kex.c:297) - 4-th negotiated kex method name = hmac-sha1
22:53:51:256462 [NOTICE] ssh_select_kex (kex.c:297) - 5-th negotiated kex method name = hmac-sha1
22:53:51:256708 [NOTICE] ssh_select_kex (kex.c:297) - 6-th negotiated kex method name = none
22:53:51:256985 [NOTICE] ssh_select_kex (kex.c:297) - 7-th negotiated 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 directory
sftp>
```

Figure 10: client operations

```
C:\Users\10679\client.c - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(O) 工具(T) 宏(M) 运行(R) 插件(P) 窗口(W) ?
ssh_config sshd.pid sshd_config_default client.c

1 1 /** @brief
2 2  * @file client.c
3 3  * @author Yuhua Zhou (zhouyuhua@pku.edu.cn)
4 4  * @brief SFTP client, only supports uploading and downloading files.
5 5  * @version 0.1
6 6  * @date 2022-10-05
7 7  *
8 8  * @copyright Copyright (c) 2022
9 9  *
10 10 */
11
12 #include <errno.h>
13 #include <fcntl.h>
14 #include <stdio.h>
15 #include <stdlib.h>
16 #include <string.h>
17 #include <unistd.h>
18 #include "libsftp/libsftp.h"
19
20 #define MAX_BUF_SIZE 16384
21
22 void prompt() {
23     fprintf(stdout, "%s", "sftp>");
24     fflush(stdout);
25 }
26
27 char* strip_filename(char* filename) {
28     char* pos;
29     pos = strrchr(filename, '/');
30     if (pos != NULL)
31         *pos = '\0';
32 }
```

Figure 11: server receive file

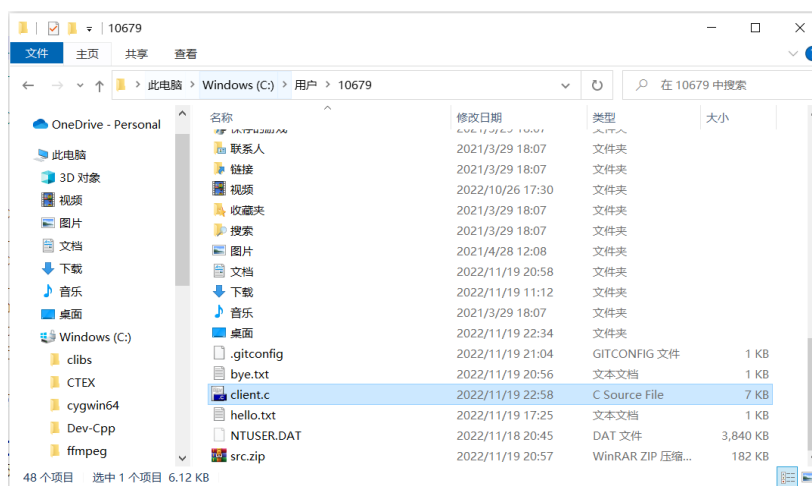


Figure 12: the time server receives the file

```
ssh_config sshd.pid sshd_config_default client.c bye.txt
1 1 /** @brief
2 2  * @file client.c
3 3  * @author Yuhua Zhou (zhouyuhua@pku.edu.cn)
4 4  * @brief SFTP client, only supports uploading and downloading files.
5 5  * @version 0.1
6 6  * @date 2022-10-05
7 7  *
8 8  * @copyright Copyright (c) 2022
9 9  *
10 10 */
11
12 /** Copied from bye.txt, another test file for our mini-sftp.
13 13  *
14 14  * Goodbye world!
15 15  * I like the lab, but it seems that the README.md omit lots of details.
16 16  * So that writing is easy, but debugging is really hard.
17 17  * A cup of water, A pack of cigar, A silly bug, A fully day!
18 18  */
19
20 #include <errno.h>
21 #include <fcntl.h>
22 #include <stdio.h>
23 #include <stdlib.h>
24 #include <string.h>
25 #include <unistd.h>
26 #include "libsftp/libsftp.h"
27
28 #define MAX_BUF_SIZE 16384
```

Figure 13: modify the file at server

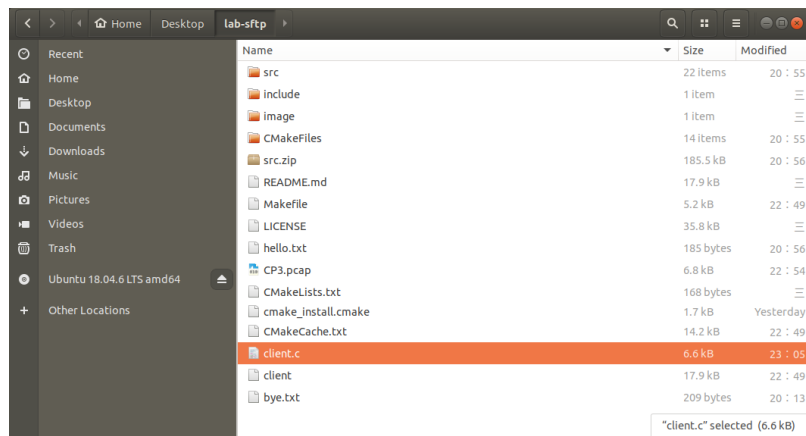


Figure 14: the time clients gets the file

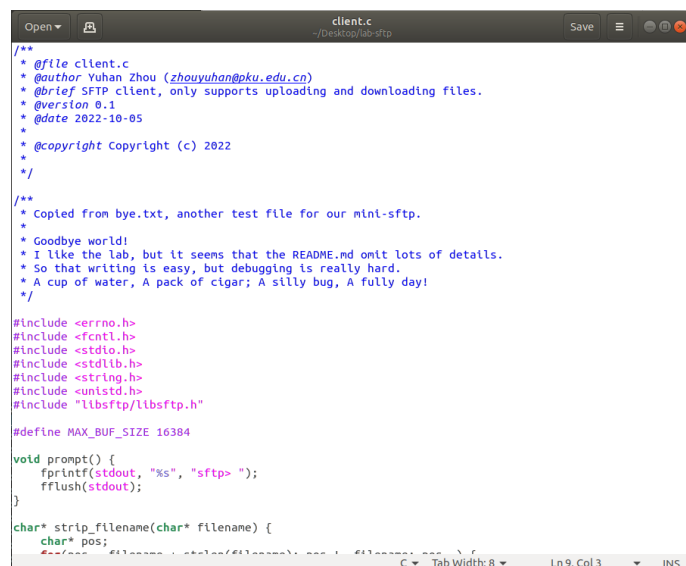


Figure 15: ns4 perf server