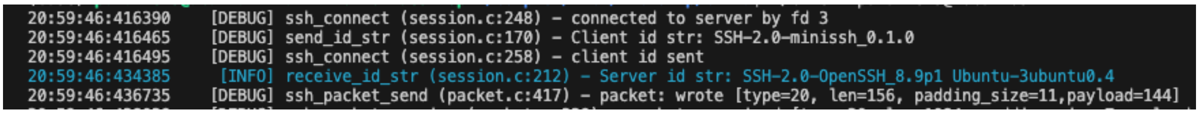
# Mini SFTP Client

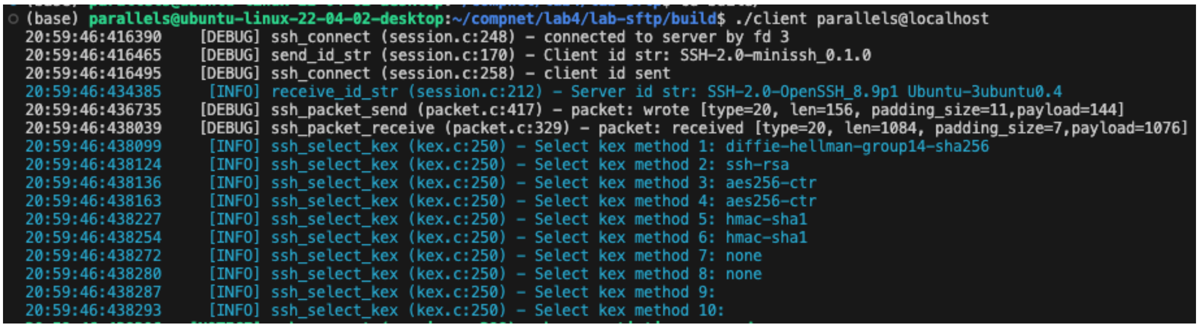
## CP1



```
20:59:46:416390    [DEBUG] ssh_connect (session.c:248) - connected to server by fd 3
20:59:46:416465    [DEBUG] send_id_str (session.c:170) - Client id str: SSH-2.0-minissh_0.1.0
20:59:46:416495    [DEBUG] ssh_connect (session.c:258) - client id sent
20:59:46:434385     [INFO] receive_id_str (session.c:212) - Server id str: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4
20:59:46:436735    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=20, len=156, padding_size=11,payload=144]
```

The server identification string is `SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4`.

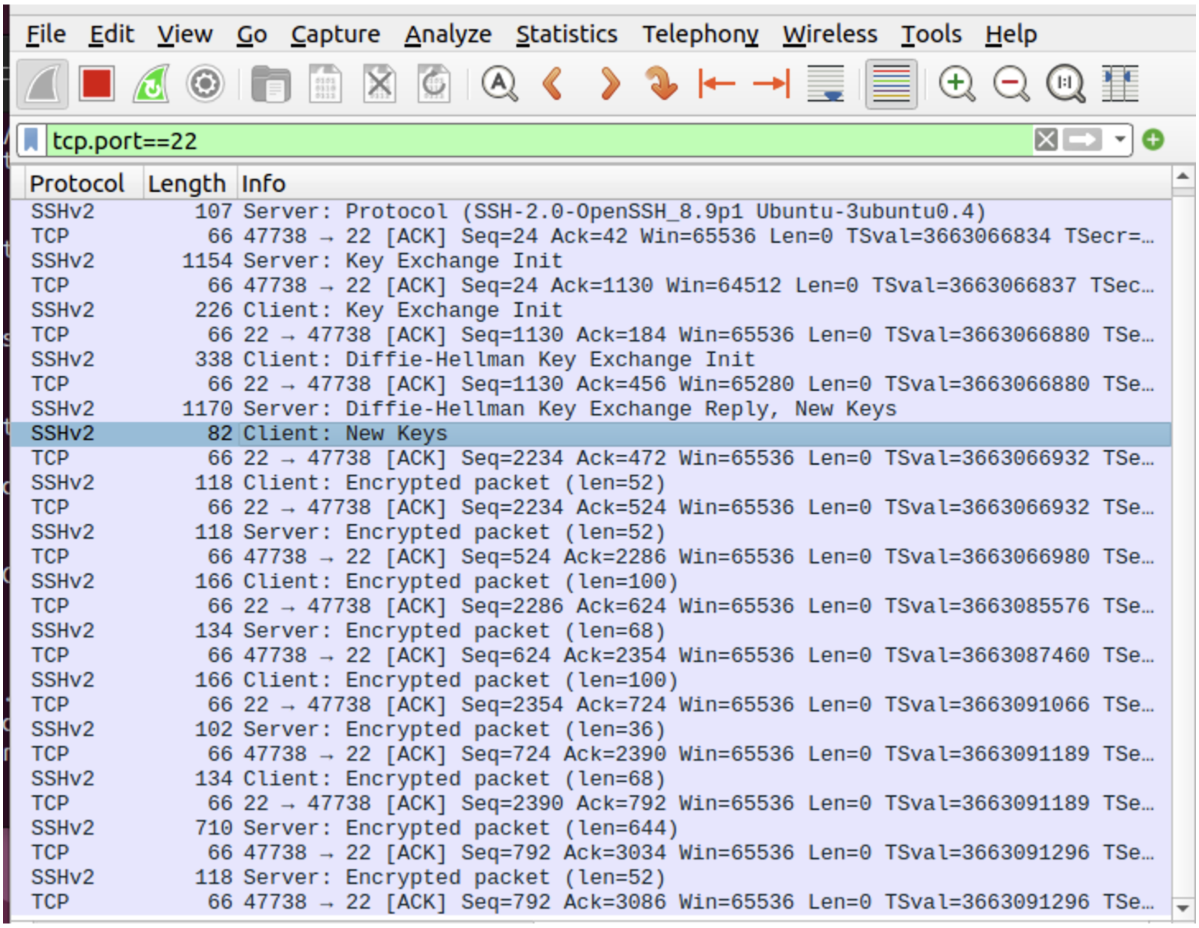
## CP2



```
○ (base) parallels@ubuntu-linux-22-04-02-desktop:~/compnet/lab4/lab-sftp/build$ ./client parallels@localhost
  20:59:46:416390    [DEBUG] ssh_connect (session.c:248) - connected to server by fd 3
  20:59:46:416465    [DEBUG] send_id_str (session.c:170) - Client id str: SSH-2.0-minissh_0.1.0
  20:59:46:416495    [DEBUG] ssh_connect (session.c:258) - client id sent
  20:59:46:434385     [INFO] receive_id_str (session.c:212) - Server id str: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4
  20:59:46:436735    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=20, len=156, padding_size=11,payload=144]
  20:59:46:438039    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=20, len=1084, padding_size=7,payload=1076]
  20:59:46:438099     [INFO] ssh_select_kex (kex.c:250) - Select kex method 1: diffie-hellman-group14-sha256
  20:59:46:438124     [INFO] ssh_select_kex (kex.c:250) - Select kex method 2: ssh-rsa
  20:59:46:438136     [INFO] ssh_select_kex (kex.c:250) - Select kex method 3: aes256-ctr
  20:59:46:438163     [INFO] ssh_select_kex (kex.c:250) - Select kex method 4: aes256-ctr
  20:59:46:438227     [INFO] ssh_select_kex (kex.c:250) - Select kex method 5: hmac-sha1
  20:59:46:438254     [INFO] ssh_select_kex (kex.c:250) - Select kex method 6: hmac-sha1
  20:59:46:438272     [INFO] ssh_select_kex (kex.c:250) - Select kex method 7: none
  20:59:46:438280     [INFO] ssh_select_kex (kex.c:250) - Select kex method 8: none
  20:59:46:438287     [INFO] ssh_select_kex (kex.c:250) - Select kex method 9:
  20:59:46:438293     [INFO] ssh_select_kex (kex.c:250) - Select kex method 10:
```

We can see the negotiate cipher suite in above figure.

## CP3

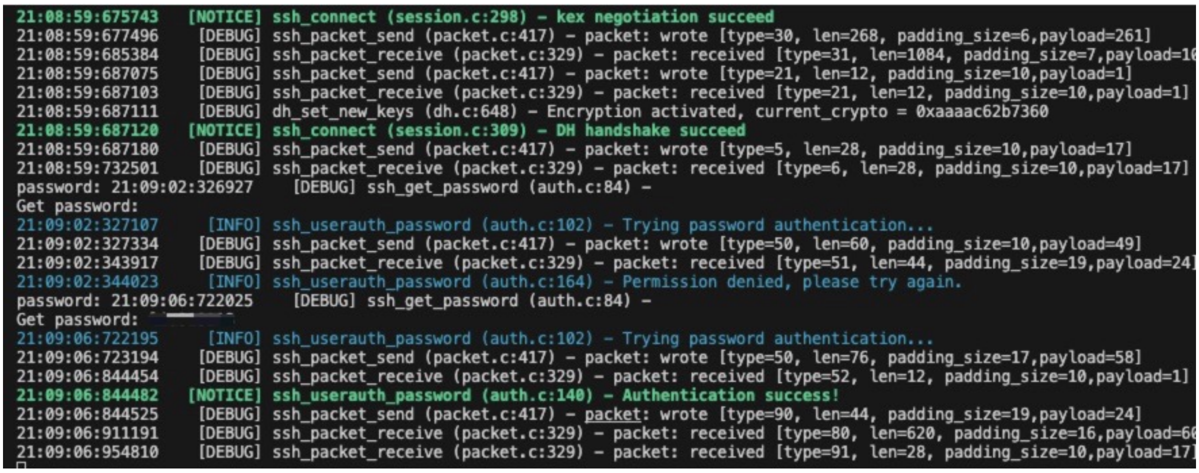


```
tcp.port==22
```

```
Protocol  Length Info
SSHv2       107 Server: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4)
TCP          66 47738 → 22 [ACK] Seq=24 Ack=42 Win=65536 Len=0 TSval=3663066834 TSecr=…
SSHv2      1154 Server: Key Exchange Init
TCP          66 47738 → 22 [ACK] Seq=24 Ack=1130 Win=64512 Len=0 TSval=3663066837 TSec…
SSHv2       226 Client: Key Exchange Init
TCP          66 22 → 47738 [ACK] Seq=1130 Ack=184 Win=65536 Len=0 TSval=3663066880 TSe…
SSHv2       338 Client: Diffie-Hellman Key Exchange Init
TCP          66 22 → 47738 [ACK] Seq=1130 Ack=456 Win=65280 Len=0 TSval=3663066880 TSe…
SSHv2      1170 Server: Diffie-Hellman Key Exchange Reply, New Keys
SSHv2        82 Client: New Keys
TCP          66 22 → 47738 [ACK] Seq=2234 Ack=472 Win=65536 Len=0 TSval=3663066932 TSe…
SSHv2       118 Client: Encrypted packet (len=52)
TCP          66 22 → 47738 [ACK] Seq=2234 Ack=524 Win=65536 Len=0 TSval=3663066932 TSe…
SSHv2       118 Server: Encrypted packet (len=52)
TCP          66 47738 → 22 [ACK] Seq=524 Ack=2286 Win=65536 Len=0 TSval=3663066980 TSe…
SSHv2       166 Client: Encrypted packet (len=100)
TCP          66 22 → 47738 [ACK] Seq=2286 Ack=624 Win=65536 Len=0 TSval=3663085576 TSe…
SSHv2       134 Server: Encrypted packet (len=68)
TCP          66 47738 → 22 [ACK] Seq=624 Ack=2354 Win=65536 Len=0 TSval=3663087460 TSe…
SSHv2       166 Client: Encrypted packet (len=100)
TCP          66 22 → 47738 [ACK] Seq=2354 Ack=724 Win=65536 Len=0 TSval=3663091066 TSe…
SSHv2       102 Server: Encrypted packet (len=36)
TCP          66 47738 → 22 [ACK] Seq=724 Ack=2390 Win=65536 Len=0 TSval=3663091189 TSe…
SSHv2       134 Client: Encrypted packet (len=68)
TCP          66 22 → 47738 [ACK] Seq=2390 Ack=792 Win=65536 Len=0 TSval=3663091189 TSe…
SSHv2       710 Server: Encrypted packet (len=644)
TCP          66 47738 → 22 [ACK] Seq=792 Ack=3034 Win=65536 Len=0 TSval=3663091296 TSe…
SSHv2       118 Server: Encrypted packet (len=52)
TCP          66 47738 → 22 [ACK] Seq=792 Ack=3086 Win=65536 Len=0 TSval=3663091296 TSe…
```

The above figure is the screenshot from wireshark. We can see that after the New Keys message, all messages are encrypted.

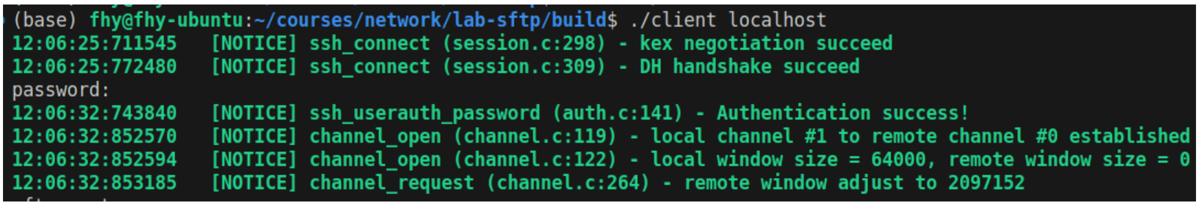
## CP4



```
21:08:59:675743   [NOTICE] ssh_connect (session.c:298) - kex negotiation succeed
21:08:59:677496    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=30, len=268, padding_size=6,payload=261]
21:08:59:685384    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=31, len=1084, padding_size=7,payload=1
21:08:59:687075    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=21, len=12, padding_size=10,payload=1]
21:08:59:687103    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=21, len=12, padding_size=10,payload=1]
21:08:59:687111    [DEBUG] dh_set_new_keys (dh.c:648) - Encryption activated, current_crypto = 0xaaaac62b7360
21:08:59:687120   [NOTICE] ssh_connect (session.c:309) - DH handshake succeed
21:08:59:687180    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=5, len=28, padding_size=10,payload=17]
21:08:59:732501    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=6, len=28, padding_size=10,payload=17]
password: 21:09:02:326927    [DEBUG] ssh_get_password (auth.c:84) -
Get password:
21:09:02:327107     [INFO] ssh_userauth_password (auth.c:102) - Trying password authentication...
21:09:02:327334    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=50, len=60, padding_size=10,payload=49]
21:09:02:343917    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=51, len=44, padding_size=19,payload=24]
21:09:02:344023     [INFO] ssh_userauth_password (auth.c:164) - Permission denied, please try again.
password: 21:09:06:722025    [DEBUG] ssh_get_password (auth.c:84) -
Get password: [redacted]
21:09:06:722195     [INFO] ssh_userauth_password (auth.c:102) - Trying password authentication...
21:09:06:723194    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=50, len=76, padding_size=17,payload=58]
21:09:06:844454    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=52, len=12, padding_size=10,payload=1]
21:09:06:844482   [NOTICE] ssh_userauth_password (auth.c:140) - Authentication success!
21:09:06:844525    [DEBUG] ssh_packet_send (packet.c:417) - packet: wrote [type=90, len=44, padding_size=19,payload=24]
21:09:06:911191    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=80, len=620, padding_size=16,payload=6
21:09:06:954810    [DEBUG] ssh_packet_receive (packet.c:329) - packet: received [type=91, len=28, padding_size=10,payload=17]
```

When we input wrong password, the terminal will show `Permission denied, please try again.`. When we input correct password, the server grants access to the client.

## CP5

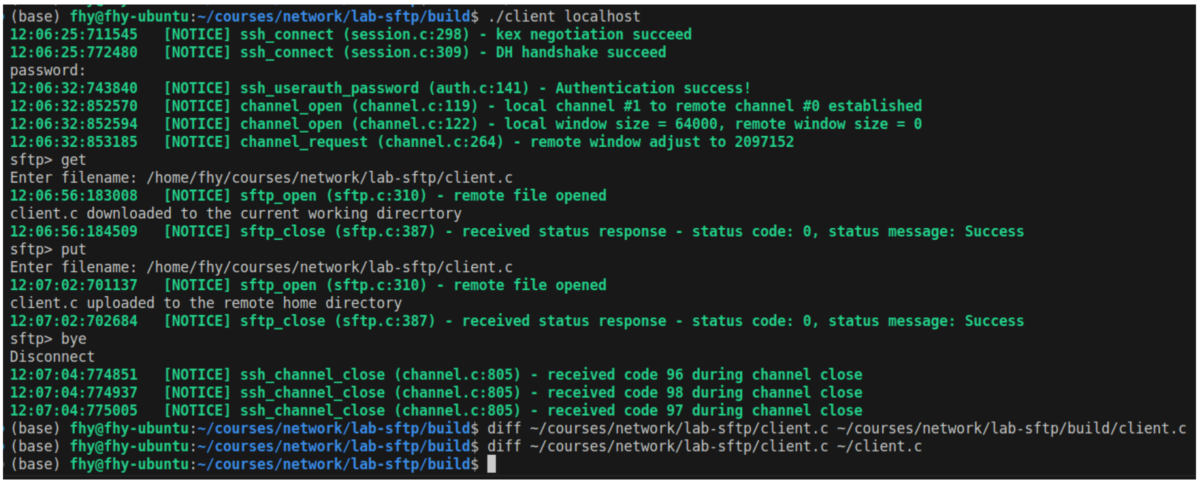


```
(base) fhy@fhy-ubuntu:~/courses/network/lab-sftp/build$ ./client localhost
12:06:25:711545   [NOTICE] ssh_connect (session.c:298) - kex negotiation succeed
12:06:25:772480   [NOTICE] ssh_connect (session.c:309) - DH handshake succeed
password:
12:06:32:743840   [NOTICE] ssh_userauth_password (auth.c:141) - Authentication success!
12:06:32:852570   [NOTICE] channel_open (channel.c:119) - local channel #1 to remote channel #0 established
12:06:32:852594   [NOTICE] channel_open (channel.c:122) - local window size = 64000, remote window size = 0
12:06:32:853185   [NOTICE] channel_request (channel.c:264) - remote window adjust to 2097152
```

Local channel number was 1, and remote channel number was 0.

Local window size was 64000, and remote window size was 0 when the channel was firstly established. After the client requested an SFTP subsystem, the remote window was adjusted to 2097152.

## CP6



```
(base) fhy@fhy-ubuntu:~/courses/network/lab-sftp/build$ ./client localhost
12:06:25:711545   [NOTICE] ssh_connect (session.c:298) - kex negotiation succeed
12:06:25:772480   [NOTICE] ssh_connect (session.c:309) - DH handshake succeed
password:
12:06:32:743840   [NOTICE] ssh_userauth_password (auth.c:141) - Authentication success!
12:06:32:852570   [NOTICE] channel_open (channel.c:119) - local channel #1 to remote channel #0 established
12:06:32:852594   [NOTICE] channel_open (channel.c:122) - local window size = 64000, remote window size = 0
12:06:32:853185   [NOTICE] channel_request (channel.c:264) - remote window adjust to 2097152
sftp> get
Enter filename: /home/fhy/courses/network/lab-sftp/client.c
12:06:56:183008   [NOTICE] sftp_open (sftp.c:310) - remote file opened
client.c downloaded to the current working direcrtory
12:06:56:184509   [NOTICE] sftp_close (sftp.c:387) - received status response - status code: 0, status message: Success
sftp> put
Enter filename: /home/fhy/courses/network/lab-sftp/client.c
12:07:02:701137   [NOTICE] sftp_open (sftp.c:310) - remote file opened
client.c uploaded to the remote home directory
12:07:02:702684   [NOTICE] sftp_close (sftp.c:387) - received status response - status code: 0, status message: Success
sftp> bye
Disconnect
12:07:04:774851   [NOTICE] ssh_channel_close (channel.c:805) - received code 96 during channel close
12:07:04:774937   [NOTICE] ssh_channel_close (channel.c:805) - received code 98 during channel close
12:07:04:775005   [NOTICE] ssh_channel_close (channel.c:805) - received code 97 during channel close
(base) fhy@fhy-ubuntu:~/courses/network/lab-sftp/build$ diff ~/courses/network/lab-sftp/client.c ~/courses/network/lab-sftp/build/client.c
(base) fhy@fhy-ubuntu:~/courses/network/lab-sftp/build$ diff ~/courses/network/lab-sftp/client.c ~/client.c
(base) fhy@fhy-ubuntu:~/courses/network/lab-sftp/build$ █
```

The client connected to the localhost and successfully uploaded and downloaded `client.c`. We compared the downloaded and uploaded files with the original file using command `diff`. Empty outputs mean that these three files are exactly the same.