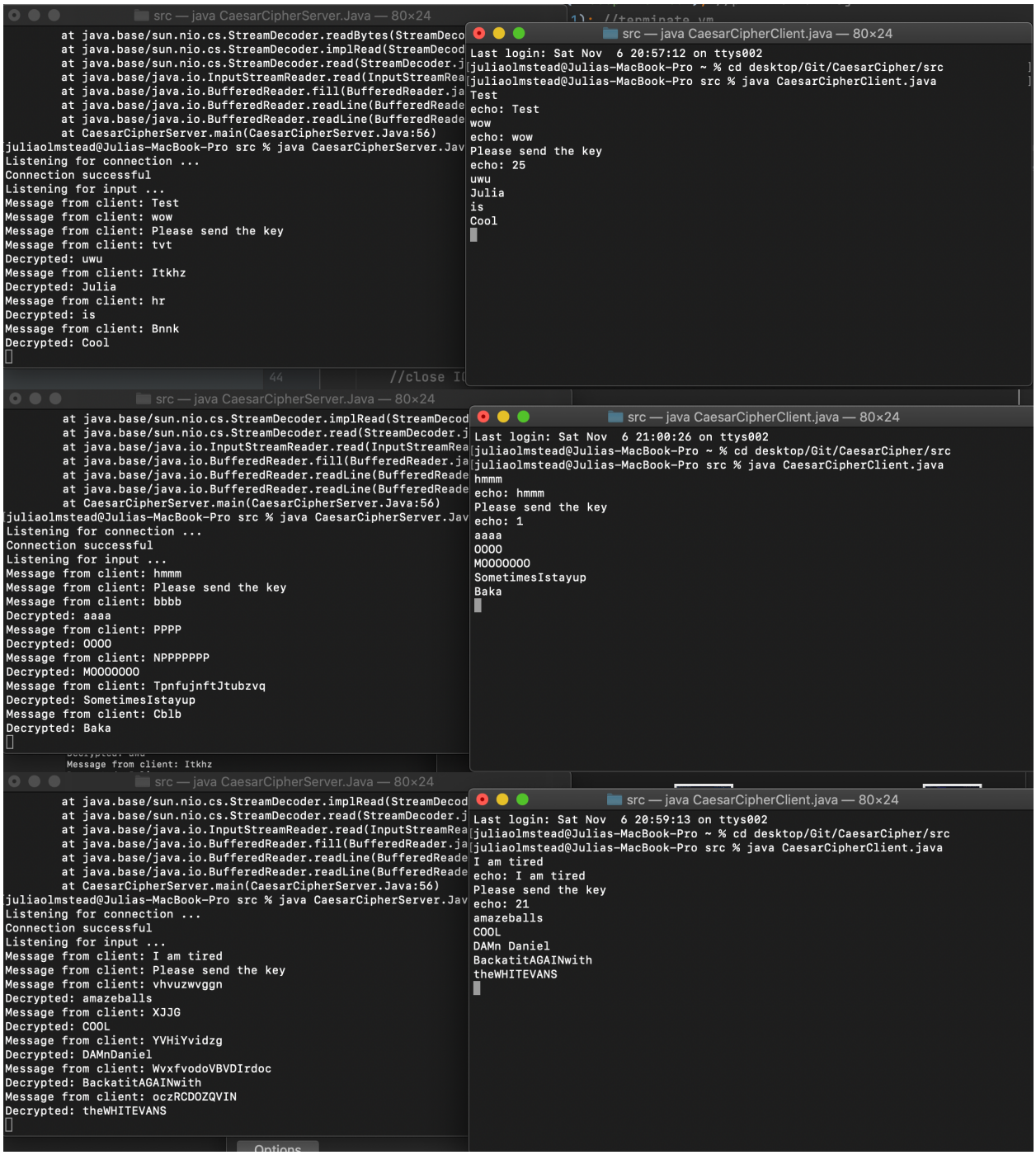
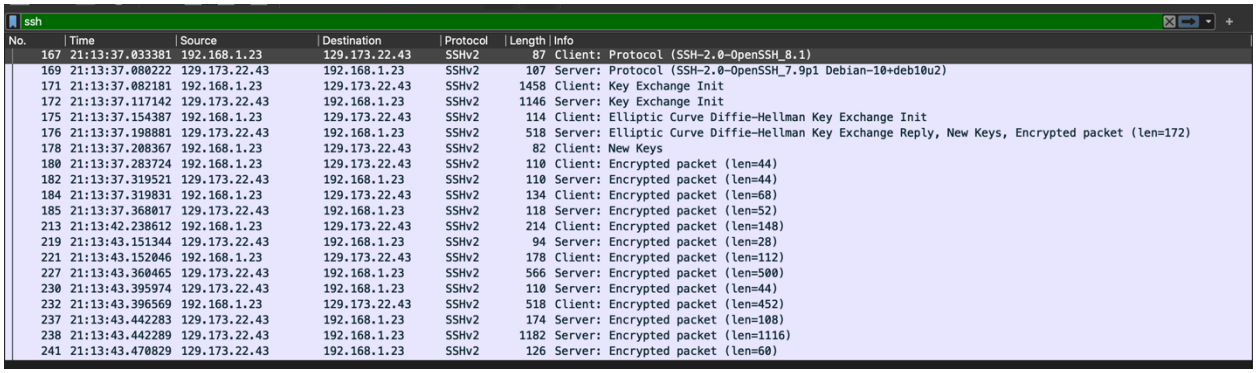
B00780639
Julia Olmstead

Exercise 1:

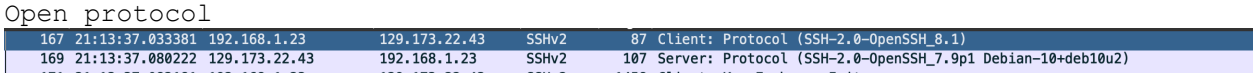


Exercise 2



No.	Time	Source	Destination	Protocol	Length	Info
167	21:13:37.033381	192.168.1.23	129.173.22.43	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_8.1)
169	21:13:37.080222	129.173.22.43	192.168.1.23	SSHv2	107	Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2)
171	21:13:37.082181	192.168.1.23	129.173.22.43	SSHv2	1458	Client: Key Exchange Init
172	21:13:37.117142	129.173.22.43	192.168.1.23	SSHv2	1146	Server: Key Exchange Init
175	21:13:37.154387	192.168.1.23	129.173.22.43	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
176	21:13:37.198881	129.173.22.43	192.168.1.23	SSHv2	518	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
178	21:13:37.208367	192.168.1.23	129.173.22.43	SSHv2	82	Client: New Keys
180	21:13:37.283724	192.168.1.23	129.173.22.43	SSHv2	110	Client: Encrypted packet (len=44)
182	21:13:37.319521	129.173.22.43	192.168.1.23	SSHv2	110	Server: Encrypted packet (len=44)
184	21:13:37.319831	192.168.1.23	129.173.22.43	SSHv2	134	Client: Encrypted packet (len=68)
185	21:13:37.368017	129.173.22.43	192.168.1.23	SSHv2	118	Server: Encrypted packet (len=52)
213	21:13:42.238612	192.168.1.23	129.173.22.43	SSHv2	214	Client: Encrypted packet (len=148)
219	21:13:43.151344	129.173.22.43	192.168.1.23	SSHv2	94	Server: Encrypted packet (len=28)
221	21:13:43.152046	192.168.1.23	129.173.22.43	SSHv2	178	Client: Encrypted packet (len=112)
227	21:13:43.360465	129.173.22.43	192.168.1.23	SSHv2	566	Server: Encrypted packet (len=500)
230	21:13:43.395974	129.173.22.43	192.168.1.23	SSHv2	110	Server: Encrypted packet (len=44)
232	21:13:43.396569	192.168.1.23	129.173.22.43	SSHv2	518	Client: Encrypted packet (len=452)
237	21:13:43.442283	129.173.22.43	192.168.1.23	SSHv2	174	Server: Encrypted packet (len=108)
238	21:13:43.442289	129.173.22.43	192.168.1.23	SSHv2	1182	Server: Encrypted packet (len=1116)
241	21:13:43.470829	129.173.22.43	192.168.1.23	SSHv2	126	Server: Encrypted packet (len=60)

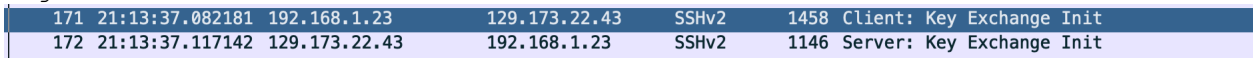
Open protocol



167	21:13:37.033381	192.168.1.23	129.173.22.43	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_8.1)
169	21:13:37.080222	129.173.22.43	192.168.1.23	SSHv2	107	Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2)

Open the ssh connec.

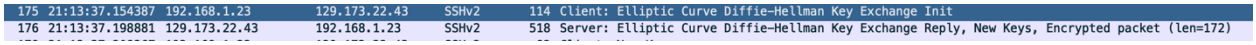
Negotiations start



171	21:13:37.082181	192.168.1.23	129.173.22.43	SSHv2	1458	Client: Key Exchange Init
172	21:13:37.117142	129.173.22.43	192.168.1.23	SSHv2	1146	Server: Key Exchange Init

Client sends several parameters negotiation, compression, and cryptography algorithms.
The server replies to these.

DH



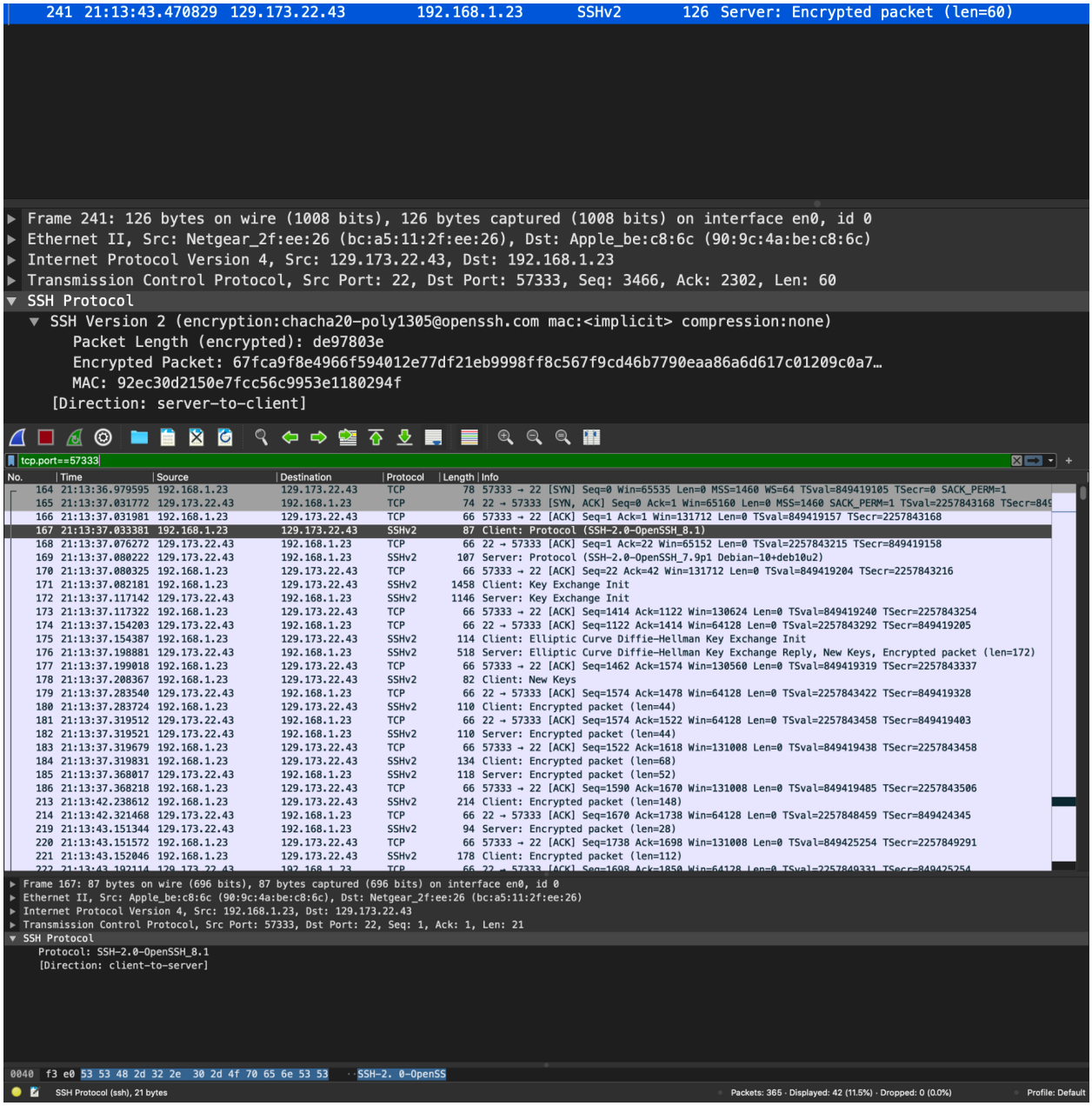
175	21:13:37.154387	192.168.1.23	129.173.22.43	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
176	21:13:37.198881	129.173.22.43	192.168.1.23	SSHv2	518	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)

Client negotiates dh params
Server replies to the above

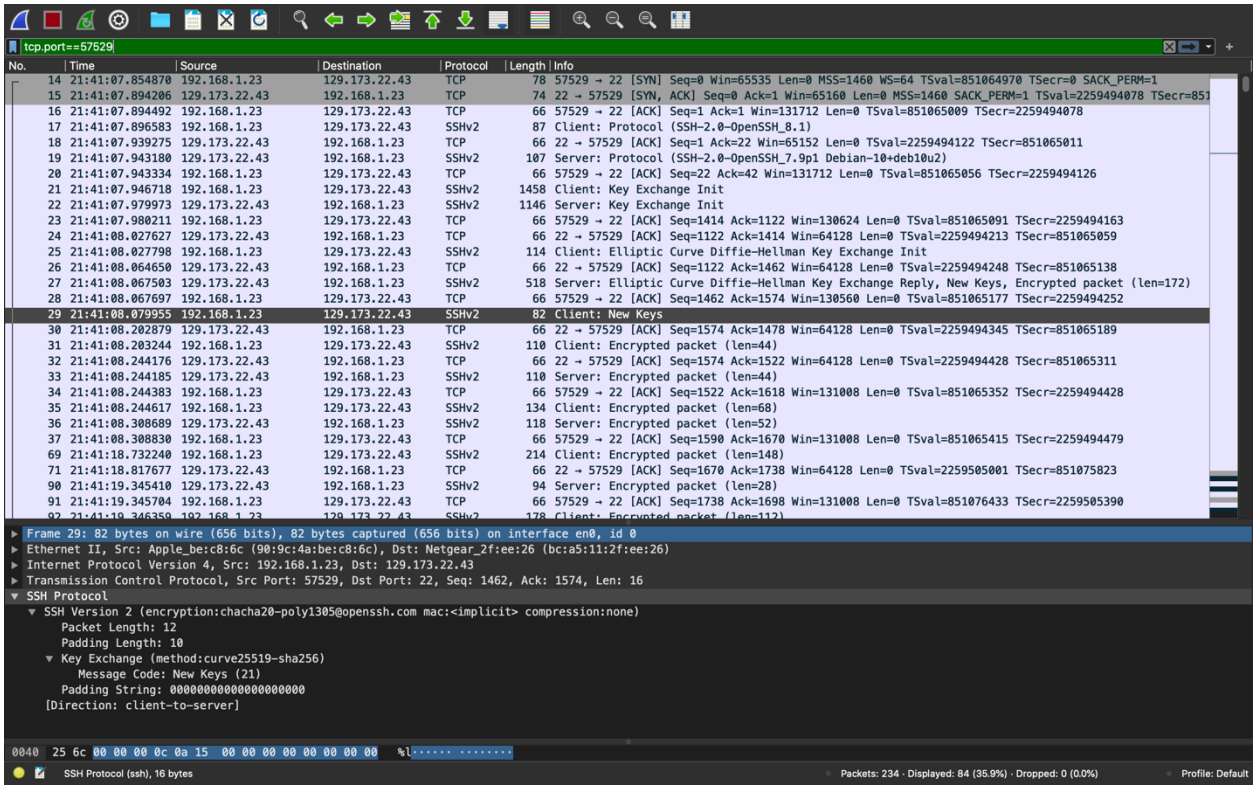
Have some keys

178	21:13:37.208367	192.168.1.23	129.173.22.43	SSHv2	82	Client: New Keys

Acknowledgement message
Encryption from here on out



New session continued below, was too tired to do assignment all at once.



Gray +blue before sshv2

```
    14 21:41:07.854870 192.168.1.23   129.173.22.43   TCP      78 57529 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=851064970 TSecr=0 SACK
    15 21:41:07.894206 129.173.22.43  192.168.1.23   TCP      74 22 → 57529 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=22594
    16 21:41:07.894492 192.168.1.23   129.173.22.43  TCP      66 57529 → 22 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=851065009 TSecr=2259494078
    17 21:41:07.896583 192.168.1.23   129.173.22.43  SSHv2    87 Client: Protocol (SSH-2.0-OpenSSH_8.1)
```

These lads

```
   182 21:41:24.825824 129.173.22.43  192.168.1.23   TCP      66 22 → 57529 [FIN, ACK] Seq=4142 Ack=2651 Win=64128 Len=0 TSval=2259511009 TSecr=85
   183 21:41:24.826068 192.168.1.23   129.173.22.43  TCP      66 57529 → 22 [ACK] Seq=2651 Ack=4143 Win=131072 Len=0 TSval=851081881 TSecr=2259511
```