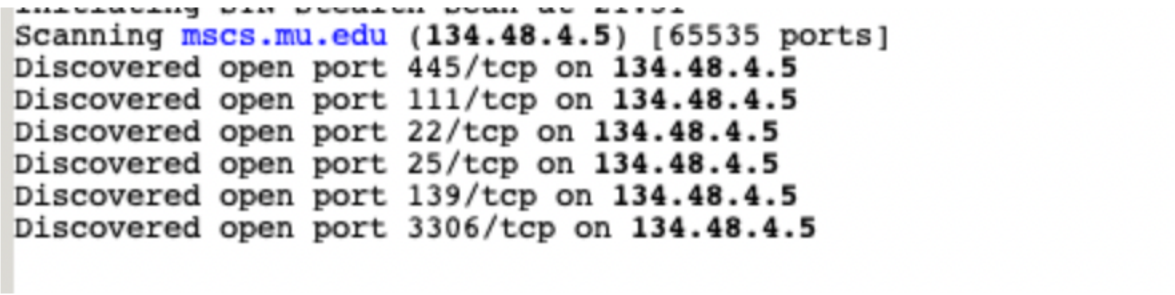
Homework 8 Solutions

Problem 1

Zenmap gives the following output for a TCP-scan:



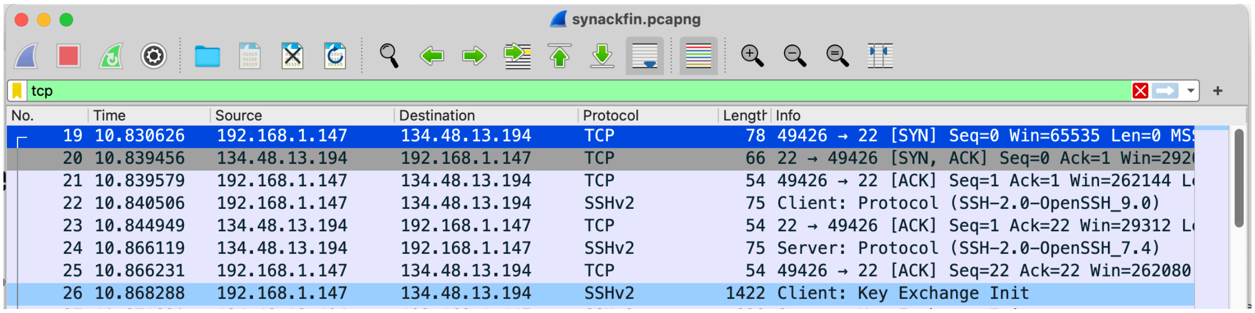
```
Scanning mscs.mu.edu (134.48.4.5) [65535 ports]
Discovered open port 445/tcp on 134.48.4.5
Discovered open port 111/tcp on 134.48.4.5
Discovered open port 22/tcp on 134.48.4.5
Discovered open port 25/tcp on 134.48.4.5
Discovered open port 139/tcp on 134.48.4.5
Discovered open port 3306/tcp on 134.48.4.5
```

We can look up the ports and obtain:

Port 22: ssh, sftp, ftp: remote shell, file transfer
Port 25: SMTP: mail protocol
Port 111: Remote procedure calls
Port 139: Netbios session
Port 445: Microsoft directory, SMB
Port 3306: MySQL database system

Problem 2:

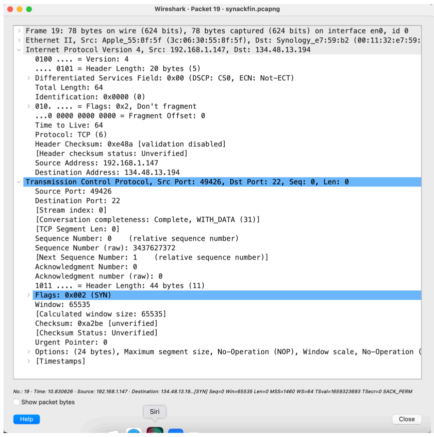
When we open up the capture window, we use tcp as the filter. This will get rid of a lot of annoying noise.



```
No.  Time       Source          Destination     Protocol  Length Info
  19 10.830626  192.168.1.147   134.48.13.194   TCP         78  49426 → 22 [SYN] Seq=0 Win=65535 Len=0 MS
  20 10.839456  134.48.13.194   192.168.1.147   TCP         66  22 → 49426 [SYN, ACK] Seq=0 Ack=1 Win=292
  21 10.839579  192.168.1.147   134.48.13.194   TCP         54  49426 → 22 [ACK] Seq=1 Ack=1 Win=262144 L
  22 10.840506  192.168.1.147   134.48.13.194   SSHv2       75  Client: Protocol (SSH-2.0-OpenSSH_9.0)
  23 10.844949  134.48.13.194   192.168.1.147   TCP         54  22 → 49426 [ACK] Seq=1 Ack=22 Win=29312 L
  24 10.866119  134.48.13.194   192.168.1.147   SSHv2       75  Server: Protocol (SSH-2.0-OpenSSH_7.4)
  25 10.866231  192.168.1.147   134.48.13.194   TCP         54  49426 → 22 [ACK] Seq=22 Ack=22 Win=262080
  26 10.868288  192.168.1.147   134.48.13.194   SSHv2     1422  Client: Key Exchange Init
```

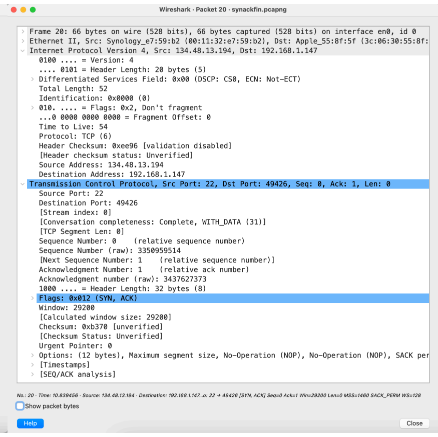
We can look at the right side under Info, to find the three packages (19, 20, 21) that make up the three way handshake.

We can now select on all three of them, expand the TCP tab and see what we get:



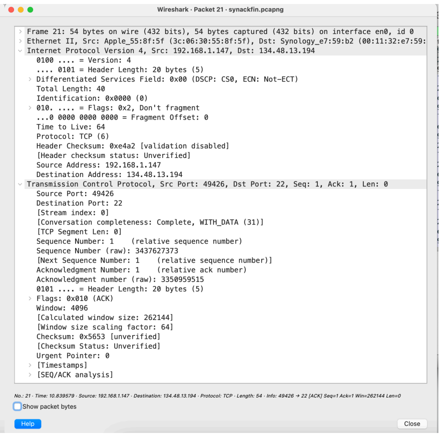
Wireshark · Packet 19 · synackfin.pcapng

```
> Frame 19: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0
> Ethernet II, Src: Apple_55:8f:5f (3c:06:30:55:8f:5f), Dst: Synology_e7:59:b2 (00:11:32:e7:59:
v Internet Protocol Version 4, Src: 192.168.1.147, Dst: 134.48.13.194
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 64
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xe48a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.147
    Destination Address: 134.48.13.194
v Transmission Control Protocol, Src Port: 49426, Dst Port: 22, Seq: 0, Len: 0
    Source Port: 49426
    Destination Port: 22
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3437627372
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1011 .... = Header Length: 44 bytes (11)
  > Flags: 0x002 (SYN)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0xa2be [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (
  > [Timestamps]

No.: 19 · Time: 10.830626 · Source: 192.168.1.147 · Destination: 134.48.13.19...[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1659323693 TSecr=0 SACK_PERM
```



Wireshark · Packet 20 · synackfin.pcapng

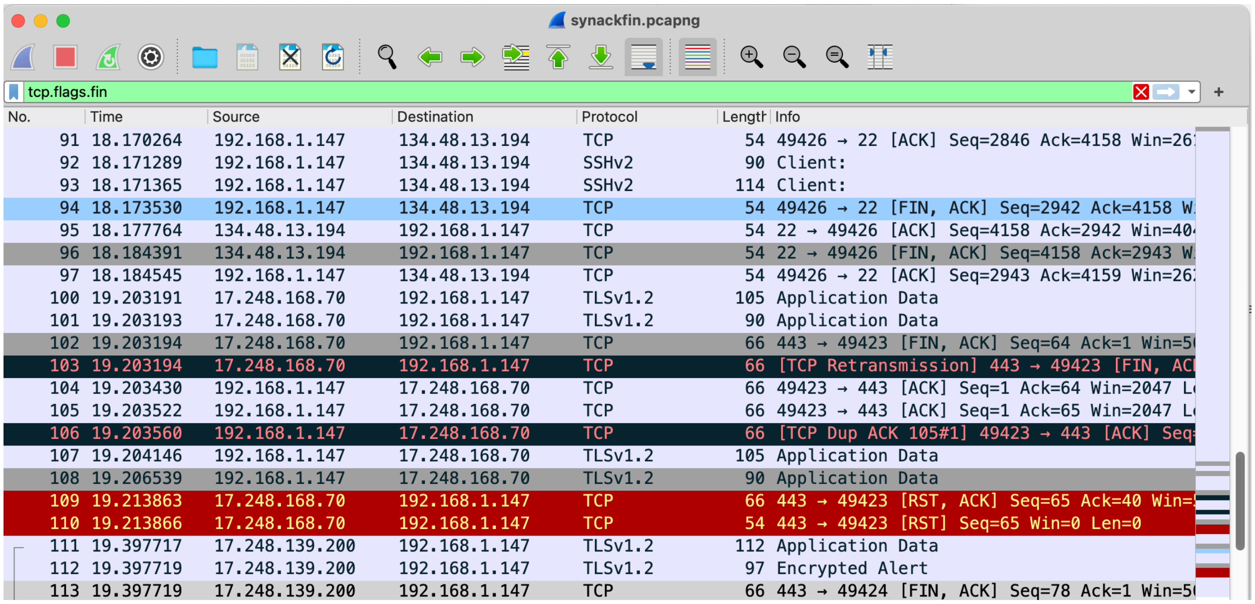
```
> Frame 20: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: Synology_e7:59:b2 (00:11:32:e7:59:b2), Dst: Apple_55:8f:5f (3c:06:30:55:8f:
v Internet Protocol Version 4, Src: 134.48.13.194, Dst: 192.168.1.147
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 54
    Protocol: TCP (6)
    Header Checksum: 0xee96 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 134.48.13.194
    Destination Address: 192.168.1.147
v Transmission Control Protocol, Src Port: 22, Dst Port: 49426, Seq: 0, Ack: 1, Len: 0
    Source Port: 22
    Destination Port: 49426
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3350959514
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3437627373
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 29200
    [Calculated window size: 29200]
    Checksum: 0xb370 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK per
  > [Timestamps]
  > [SEQ/ACK analysis]

No.: 20 · Time: 10.839456 · Source: 134.48.13.194 · Destination: 192.168.1.147...o: 22 → 49426 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
```



Wireshark · Packet 21 · synackfin.pcapng

```
> Frame 21: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
> Ethernet II, Src: Apple_55:8f:5f (3c:06:30:55:8f:5f), Dst: Synology_e7:59:b2 (00:11:32:e7:59:
v Internet Protocol Version 4, Src: 192.168.1.147, Dst: 134.48.13.194
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xe4a2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.147
    Destination Address: 134.48.13.194
v Transmission Control Protocol, Src Port: 49426, Dst Port: 22, Seq: 1, Ack: 1, Len: 0
    Source Port: 49426
    Destination Port: 22
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3437627373
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3350959515
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 4096
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0x5653 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]

No.: 21 · Time: 10.839579 · Source: 192.168.1.147 · Destination: 134.48.13.194 · Protocol: TCP · Length: 54 · Info: 49426 → 22 [ACK] Seq=1 Ack=1 Win=262144 Len=0
```

To look for the closing, we can use the filter tcp.flags.fin, and find that packets 94 to 97 contain the termination protocol. Double-click on these and you will find the details.



synackfin.pcapng

tcp.flags.fin

```
No.  Time       Source          Destination     Protocol  Length Info
  91 18.170264  192.168.1.147   134.48.13.194   TCP         54 49426 → 22 [ACK] Seq=2846 Ack=4158 Win=26
  92 18.171289  192.168.1.147   134.48.13.194   SSHv2       90 Client:
  93 18.171365  192.168.1.147   134.48.13.194   SSHv2      114 Client:
  94 18.173530  192.168.1.147   134.48.13.194   TCP         54 49426 → 22 [FIN, ACK] Seq=2942 Ack=4158 W
  95 18.177764  134.48.13.194   192.168.1.147   TCP         54 22 → 49426 [ACK] Seq=4158 Ack=2942 Win=40
  96 18.184391  134.48.13.194   192.168.1.147   TCP         54 22 → 49426 [FIN, ACK] Seq=4158 Ack=2943 W
  97 18.184545  192.168.1.147   134.48.13.194   TCP         54 49426 → 22 [ACK] Seq=2943 Ack=4159 Win=26
 100 19.203191  17.248.168.70   192.168.1.147   TLSv1.2    105 Application Data
 101 19.203193  17.248.168.70   192.168.1.147   TLSv1.2     90 Application Data
 102 19.203194  17.248.168.70   192.168.1.147   TCP         66 443 → 49423 [FIN, ACK] Seq=64 Ack=1 Win=5
 103 19.203194  17.248.168.70   192.168.1.147   TCP         66 [TCP Retransmission] 443 → 49423 [FIN, AC
 104 19.203430  192.168.1.147   17.248.168.70   TCP         66 49423 → 443 [ACK] Seq=1 Ack=64 Win=2047 L
 105 19.203522  192.168.1.147   17.248.168.70   TCP         66 49423 → 443 [ACK] Seq=1 Ack=65 Win=2047 L
 106 19.203560  192.168.1.147   17.248.168.70   TCP         66 [TCP Dup ACK 105#1] 49423 → 443 [ACK] Seq
 107 19.204146  192.168.1.147   17.248.168.70   TLSv1.2    105 Application Data
 108 19.206539  192.168.1.147   17.248.168.70   TLSv1.2     90 Application Data
 109 19.213863  17.248.168.70   192.168.1.147   TCP         66 443 → 49423 [RST, ACK] Seq=65 Ack=40 Win=
 110 19.213866  17.248.168.70   192.168.1.147   TCP         54 443 → 49423 [RST] Seq=65 Win=0 Len=0
 111 19.397717  17.248.139.200  192.168.1.147   TLSv1.2    112 Application Data
 112 19.397719  17.248.139.200  192.168.1.147   TLSv1.2     97 Encrypted Alert
 113 19.397719  17.248.139.200  192.168.1.147   TCP         66 443 → 49424 [FIN, ACK] Seq=78 Ack=1 Win=5
```