Computer Networks
@CS.NCTU

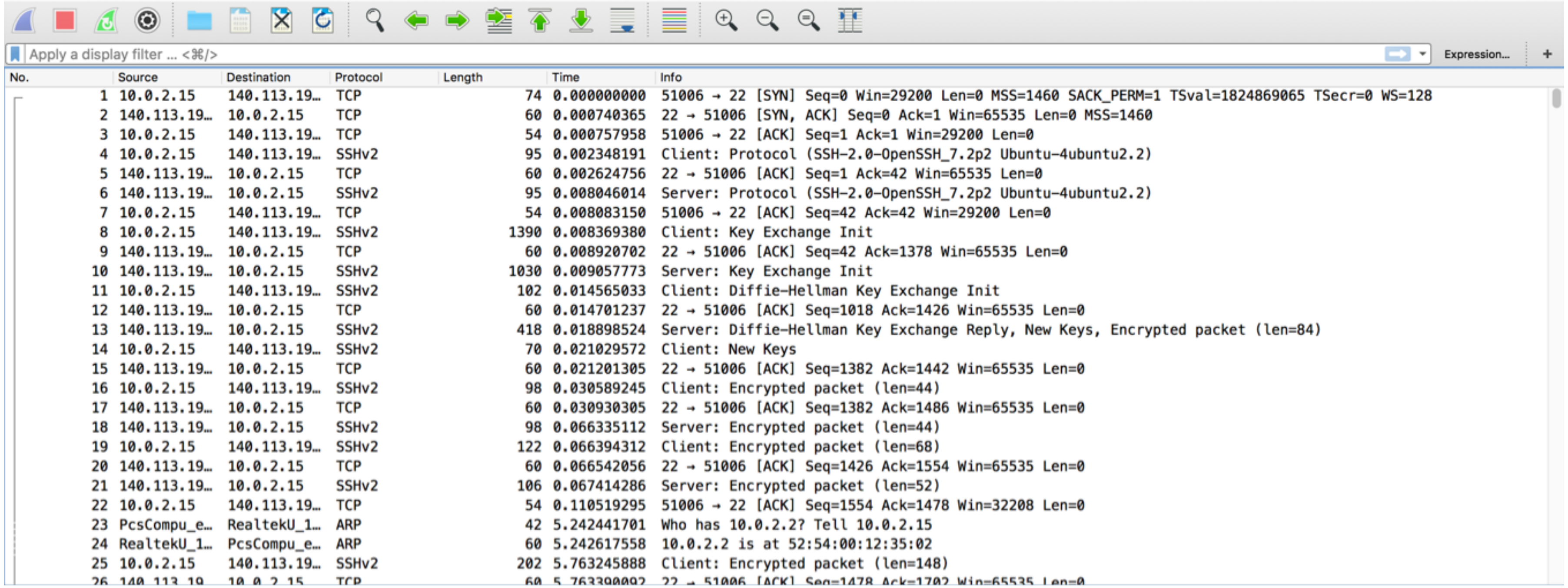
Lab. 1: packet sniffing via WireShark

Location: EC-315, 316

Instructor: 戴子鈞 孫造鴻

Wireshark

- https://www.wireshark.org/
- Foremost and widely-used network protocol analyzer → Free
- Work for both wired and wireless interfaces



```
No.   Source         Destination    Protocol  Length  Time         Info
   1 10.0.2.15      140.113.19…    TCP         74 0.000000000  51006 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1824869065 TSecr=0 WS=128
   2 140.113.19…    10.0.2.15      TCP         60 0.000740365  22 → 51006 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   3 10.0.2.15      140.113.19…    TCP         54 0.000757958  51006 → 22 [ACK] Seq=1 Ack=1 Win=29200 Len=0
   4 10.0.2.15      140.113.19…    SSHv2       95 0.002348191  Client: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
   5 140.113.19…    10.0.2.15      TCP         60 0.002624756  22 → 51006 [ACK] Seq=1 Ack=42 Win=65535 Len=0
   6 140.113.19…    10.0.2.15      SSHv2       95 0.008046014  Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
   7 10.0.2.15      140.113.19…    TCP         54 0.008083150  51006 → 22 [ACK] Seq=42 Ack=42 Win=29200 Len=0
   8 10.0.2.15      140.113.19…    SSHv2     1390 0.008369380  Client: Key Exchange Init
   9 140.113.19…    10.0.2.15      TCP         60 0.008920702  22 → 51006 [ACK] Seq=42 Ack=1378 Win=65535 Len=0
  10 140.113.19…    10.0.2.15      SSHv2     1030 0.009057773  Server: Key Exchange Init
  11 10.0.2.15      140.113.19…    SSHv2      102 0.014565033  Client: Diffie-Hellman Key Exchange Init
  12 140.113.19…    10.0.2.15      TCP         60 0.014701237  22 → 51006 [ACK] Seq=1018 Ack=1426 Win=65535 Len=0
  13 140.113.19…    10.0.2.15      SSHv2      418 0.018898524  Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
  14 10.0.2.15      140.113.19…    SSHv2       70 0.021029572  Client: New Keys
  15 140.113.19…    10.0.2.15      TCP         60 0.021201305  22 → 51006 [ACK] Seq=1382 Ack=1442 Win=65535 Len=0
  16 10.0.2.15      140.113.19…    SSHv2       98 0.030589245  Client: Encrypted packet (len=44)
  17 140.113.19…    10.0.2.15      TCP         60 0.030930305  22 → 51006 [ACK] Seq=1382 Ack=1486 Win=65535 Len=0
  18 140.113.19…    10.0.2.15      SSHv2       98 0.066335112  Server: Encrypted packet (len=44)
  19 10.0.2.15      140.113.19…    SSHv2      122 0.066394312  Client: Encrypted packet (len=68)
  20 140.113.19…    10.0.2.15      TCP         60 0.066542056  22 → 51006 [ACK] Seq=1426 Ack=1554 Win=65535 Len=0
  21 140.113.19…    10.0.2.15      SSHv2      106 0.067414286  Server: Encrypted packet (len=52)
  22 10.0.2.15      140.113.19…    TCP         54 0.110519295  51006 → 22 [ACK] Seq=1554 Ack=1478 Win=32208 Len=0
  23 PcsCompu_e…    RealtekU_1…    ARP         42 5.242441701  Who has 10.0.2.2? Tell 10.0.2.15
  24 RealtekU_1…    PcsCompu_e…    ARP         60 5.242617558  10.0.2.2 is at 52:54:00:12:35:02
  25 10.0.2.15      140.113.19…    SSHv2      202 5.763245888  Client: Encrypted packet (len=148)
  26 140.113.19     10.0.2.15      TCP         60 5.763390092  22 → 51006 [ACK] Seq=1478 Ack=1702 Win=65535 Len=0
```

Wireshark

- User guide
  - https://www.wireshark.org/docs/wsug_html_chunked/
- Command-line manual page
  - https://www.wireshark.org/docs/man-pages/
- Wireshark from Linux command line
  - https://www.wireshark.org/docs/wsug_html_chunked/ChCustCommandLine.html
- Training video
  - https://riverbed11.app.box.com/s/9q2ucnnjk52im10nj53ykh26rzz7skbd

Tasks

1. Record the sending trace of one “scp” connection
   - scp id@140.113.xxx.xx:/tmp/student_ID
   - Plot the sequence-time figure
   - Use WireShark GUI

2. Record the receiving trace of two simultaneous “wget” connections
   - wget http://140.113.xxx.xxx/testfile&
   - Plot the throughput of two connections over time
   - Implement in Python (with an example code)

Tasks

- For **non-EECS** students, if you are not familiar with Python, you could alternatively use
    - C/C++
    - MATLAB
    - (talk to TA)

Filtering Rules

- Filter the packets that satisfy some conditions
  - For example, to find TCP packets with a port number of 80, you can use **tcp.port == 80**

- For more filter instructions, please reference to: https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html https://wiki.wireshark.org/DisplayFilters

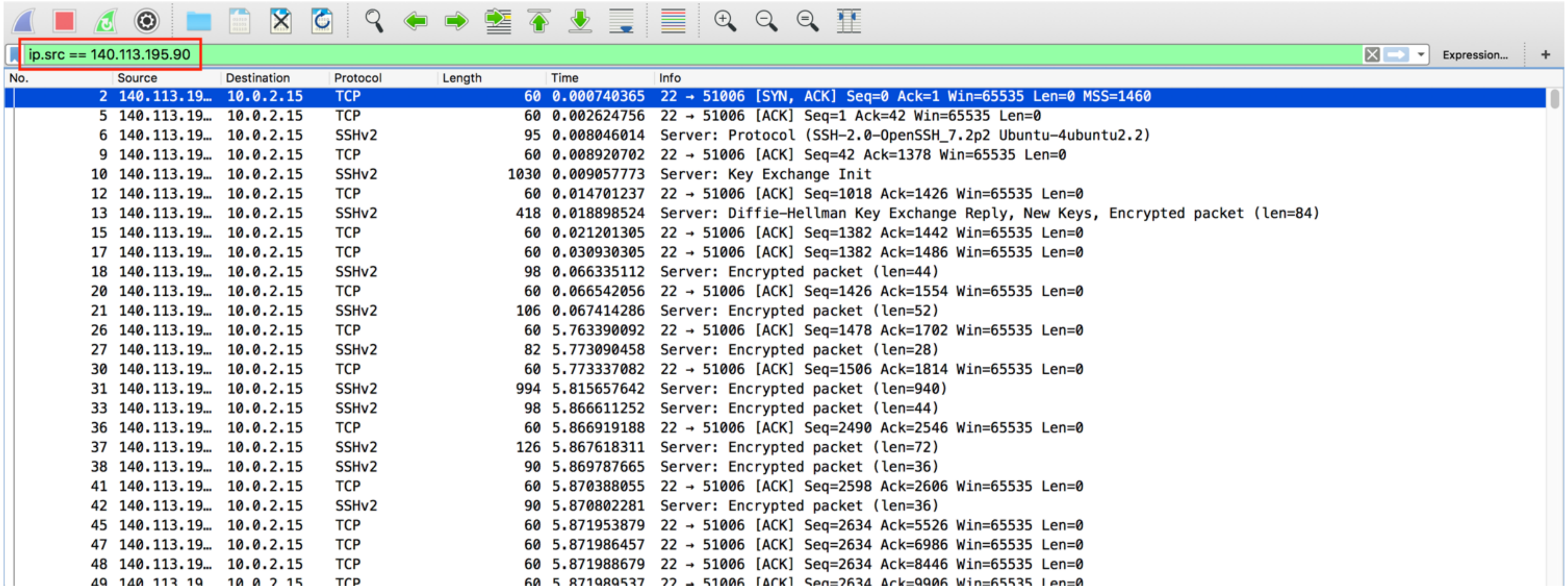
- Frequently used:
  - ip.src, ip.dst, ip.addr, …(IP address)
  - tcp.port, tcp.srcport, tcp.dstport, … (port)
  - eth.src, eth.dst, eth.addr, ... (MAC address)

Output 1: time-seq.

- Generate "uploadfile"
  - dd if=/dev/zero of=test bs=1M count=300
- Open Wireshark and start sniffing
- Upload file to server...
  - Choose one to execute
  - scp uploadfile user@140.113.195.91:/tmp/XXXXXX (XXXXX=student id)
  - scp uploadfile user@140.113.195.70:/tmp/XXXXXX
- Save Wireshark as "lab1_ID_tx_scp.pcapng"

Output 1: time-seq.

- Filter the packets captured from Wireshark
  - Use src IP and dst IP (maybe also the port)

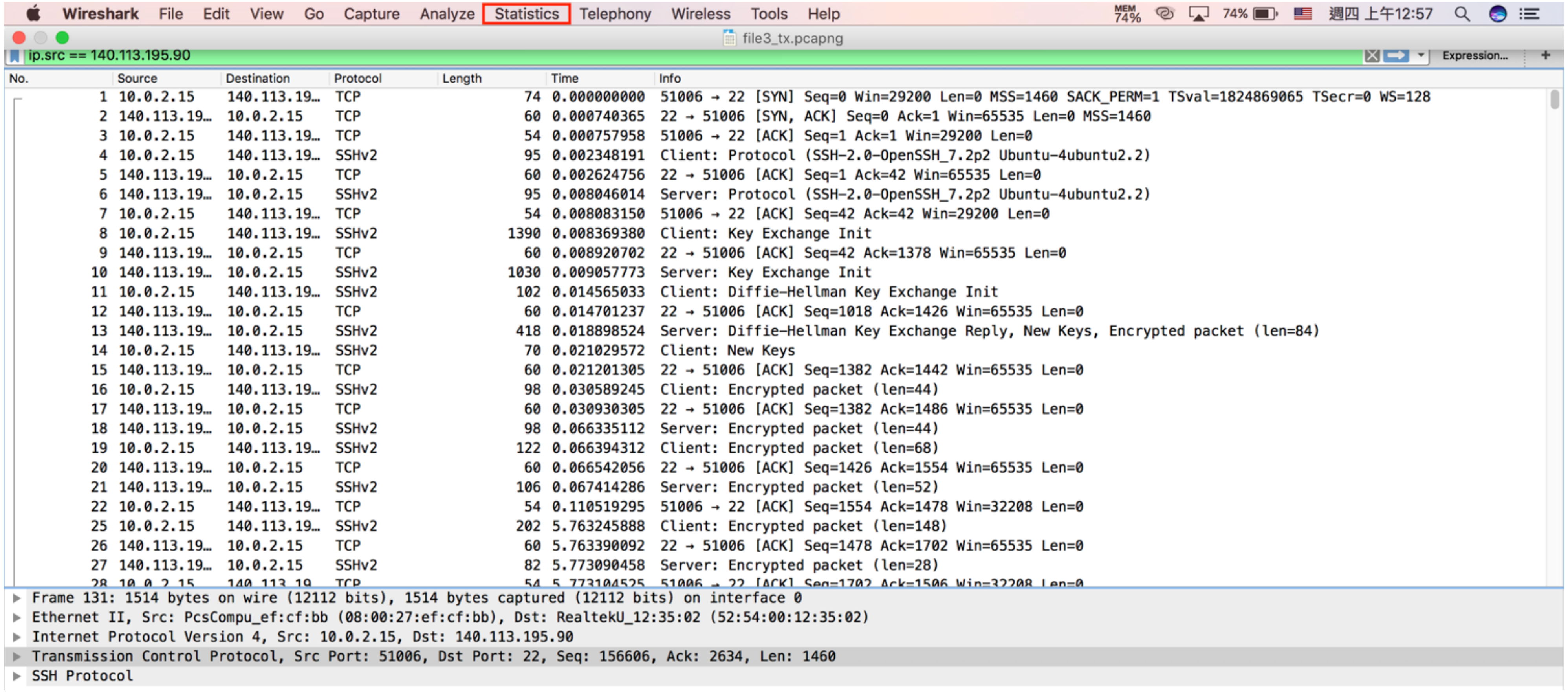


ip.src == 140.113.195.90

```
No.   Source          Destination  Protocol  Length  Time         Info
    2 140.113.19…    10.0.2.15    TCP           60 0.000740365  22 → 51006 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
    5 140.113.19…    10.0.2.15    TCP           60 0.002624756  22 → 51006 [ACK] Seq=1 Ack=42 Win=65535 Len=0
    6 140.113.19…    10.0.2.15    SSHv2         95 0.008046014  Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
    9 140.113.19…    10.0.2.15    TCP           60 0.008920702  22 → 51006 [ACK] Seq=42 Ack=1378 Win=65535 Len=0
   10 140.113.19…    10.0.2.15    SSHv2       1030 0.009057773  Server: Key Exchange Init
   12 140.113.19…    10.0.2.15    TCP           60 0.014701237  22 → 51006 [ACK] Seq=1018 Ack=1426 Win=65535 Len=0
   13 140.113.19…    10.0.2.15    SSHv2        418 0.018898524  Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
   15 140.113.19…    10.0.2.15    TCP           60 0.021201305  22 → 51006 [ACK] Seq=1382 Ack=1442 Win=65535 Len=0
   17 140.113.19…    10.0.2.15    TCP           60 0.030930305  22 → 51006 [ACK] Seq=1382 Ack=1486 Win=65535 Len=0
   18 140.113.19…    10.0.2.15    SSHv2         98 0.066335112  Server: Encrypted packet (len=44)
   20 140.113.19…    10.0.2.15    TCP           60 0.066542056  22 → 51006 [ACK] Seq=1426 Ack=1554 Win=65535 Len=0
   21 140.113.19…    10.0.2.15    SSHv2        106 0.067414286  Server: Encrypted packet (len=52)
   26 140.113.19…    10.0.2.15    TCP           60 5.763390092  22 → 51006 [ACK] Seq=1478 Ack=1702 Win=65535 Len=0
   27 140.113.19…    10.0.2.15    SSHv2         82 5.773090458  Server: Encrypted packet (len=28)
   30 140.113.19…    10.0.2.15    TCP           60 5.773337082  22 → 51006 [ACK] Seq=1506 Ack=1814 Win=65535 Len=0
   31 140.113.19…    10.0.2.15    SSHv2        994 5.815657642  Server: Encrypted packet (len=940)
   33 140.113.19…    10.0.2.15    SSHv2         98 5.866611252  Server: Encrypted packet (len=44)
   36 140.113.19…    10.0.2.15    TCP           60 5.866919188  22 → 51006 [ACK] Seq=2490 Ack=2546 Win=65535 Len=0
   37 140.113.19…    10.0.2.15    SSHv2        126 5.867618311  Server: Encrypted packet (len=72)
   38 140.113.19…    10.0.2.15    SSHv2         90 5.869787665  Server: Encrypted packet (len=36)
   41 140.113.19…    10.0.2.15    TCP           60 5.870388055  22 → 51006 [ACK] Seq=2598 Ack=2606 Win=65535 Len=0
   42 140.113.19…    10.0.2.15    SSHv2         90 5.870802281  Server: Encrypted packet (len=36)
   45 140.113.19…    10.0.2.15    TCP           60 5.871953879  22 → 51006 [ACK] Seq=2634 Ack=5526 Win=65535 Len=0
   47 140.113.19…    10.0.2.15    TCP           60 5.871986457  22 → 51006 [ACK] Seq=2634 Ack=6986 Win=65535 Len=0
   48 140.113.19…    10.0.2.15    TCP           60 5.871988679  22 → 51006 [ACK] Seq=2634 Ack=8446 Win=65535 Len=0
   49 140.113.19     10.0.2.15    TCP           60 5.871989537  22 → 51006 [ACK] Seq=2634 Ack=9906 Win=65535 Len=0
```

Output 1: time-seq.

- Draw the time-sequence number graph

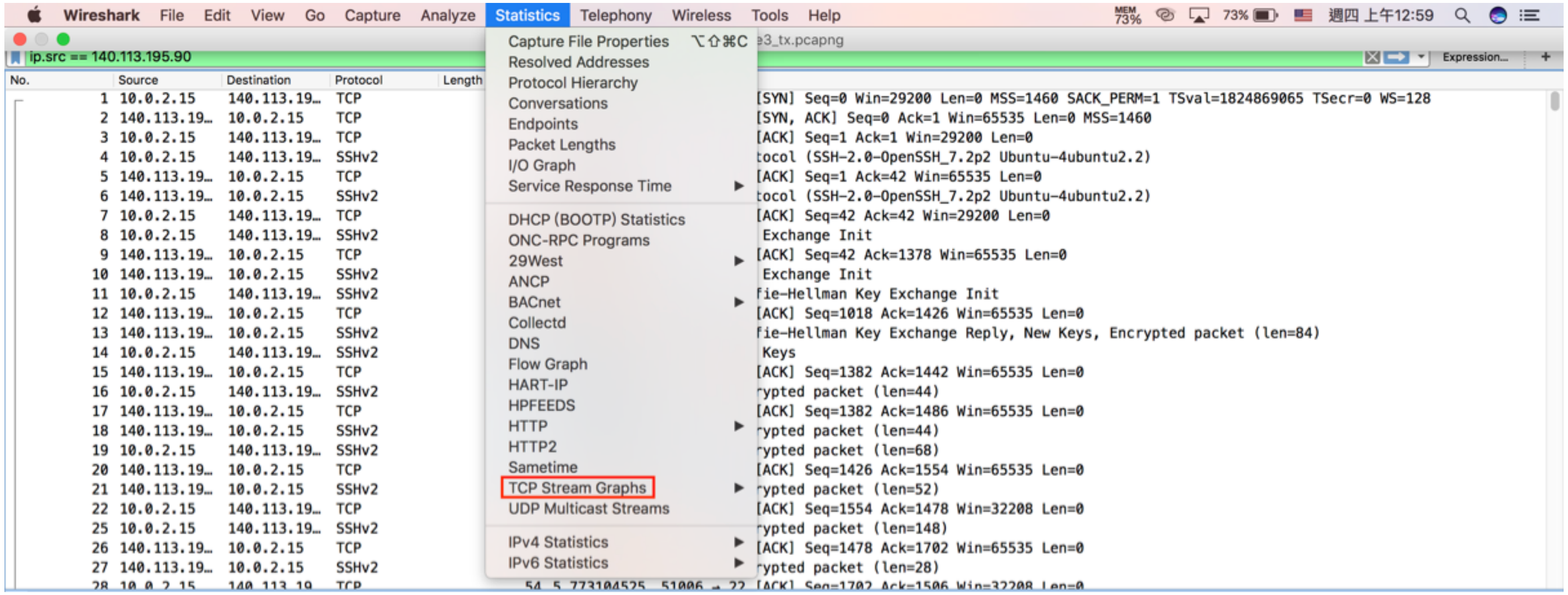


```
ip.src == 140.113.195.90
```

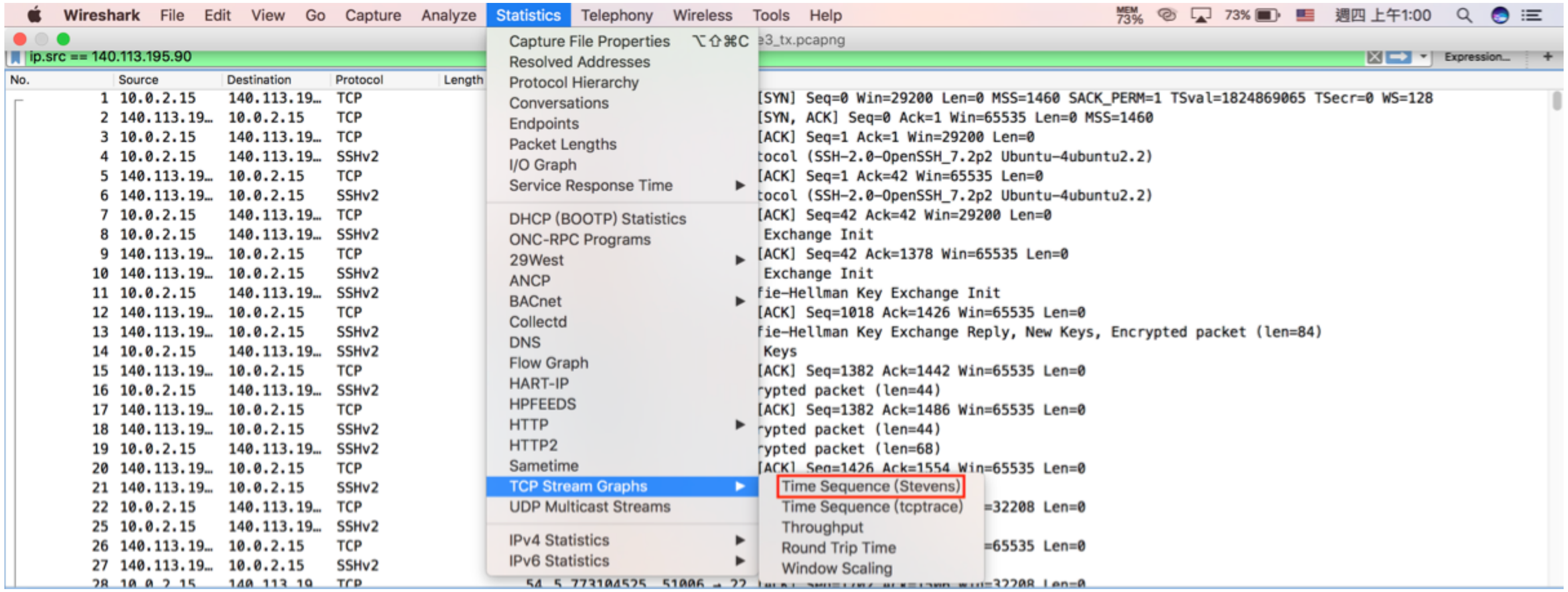
```
No.  Source        Destination   Protocol  Length  Time         Info
  1  10.0.2.15     140.113.19…   TCP           74  0.000000000  51006 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1824869065 TSecr=0 WS=128
  2  140.113.19…   10.0.2.15     TCP           60  0.000740365  22 → 51006 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  3  10.0.2.15     140.113.19…   TCP           54  0.000757958  51006 → 22 [ACK] Seq=1 Ack=1 Win=29200 Len=0
  4  10.0.2.15     140.113.19…   SSHv2         95  0.002348191  Client: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
  5  140.113.19…   10.0.2.15     TCP           60  0.002624756  22 → 51006 [ACK] Seq=1 Ack=42 Win=65535 Len=0
  6  140.113.19…   10.0.2.15     SSHv2         95  0.008046014  Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
  7  10.0.2.15     140.113.19…   TCP           54  0.008083150  51006 → 22 [ACK] Seq=42 Ack=42 Win=29200 Len=0
  8  10.0.2.15     140.113.19…   SSHv2       1390  0.008369380  Client: Key Exchange Init
  9  140.113.19…   10.0.2.15     TCP           60  0.008920702  22 → 51006 [ACK] Seq=42 Ack=1378 Win=65535 Len=0
 10  140.113.19…   10.0.2.15     SSHv2       1030  0.009057773  Server: Key Exchange Init
 11  10.0.2.15     140.113.19…   SSHv2        102  0.014565033  Client: Diffie-Hellman Key Exchange Init
 12  140.113.19…   10.0.2.15     TCP           60  0.014701237  22 → 51006 [ACK] Seq=1018 Ack=1426 Win=65535 Len=0
 13  140.113.19…   10.0.2.15     SSHv2        418  0.018898524  Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
 14  10.0.2.15     140.113.19…   SSHv2         70  0.021029572  Client: New Keys
 15  140.113.19…   10.0.2.15     TCP           60  0.021201305  22 → 51006 [ACK] Seq=1382 Ack=1442 Win=65535 Len=0
 16  10.0.2.15     140.113.19…   SSHv2         98  0.030589245  Client: Encrypted packet (len=44)
 17  140.113.19…   10.0.2.15     TCP           60  0.030930305  22 → 51006 [ACK] Seq=1382 Ack=1486 Win=65535 Len=0
 18  140.113.19…   10.0.2.15     SSHv2         98  0.066335112  Server: Encrypted packet (len=44)
 19  10.0.2.15     140.113.19…   SSHv2        122  0.066394312  Client: Encrypted packet (len=68)
 20  140.113.19…   10.0.2.15     TCP           60  0.066542056  22 → 51006 [ACK] Seq=1426 Ack=1554 Win=65535 Len=0
 21  140.113.19…   10.0.2.15     SSHv2        106  0.067414286  Server: Encrypted packet (len=52)
 22  10.0.2.15     140.113.19…   TCP           54  0.110519295  51006 → 22 [ACK] Seq=1554 Ack=1478 Win=32208 Len=0
 25  10.0.2.15     140.113.19…   SSHv2        202  5.763245888  Client: Encrypted packet (len=148)
 26  140.113.19…   10.0.2.15     TCP           60  5.763390092  22 → 51006 [ACK] Seq=1478 Ack=1702 Win=65535 Len=0
 27  140.113.19…   10.0.2.15     SSHv2         82  5.773090458  Server: Encrypted packet (len=28)
 28  10.0.2.15     140.113.19…   TCP           54  5.773104525  51006 → 22 [ACK] Seq=1702 Ack=1506 Win=32208 Len=0
```

```
▶ Frame 131: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_ef:cf:bb (08:00:27:ef:cf:bb), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 140.113.195.90
▶ Transmission Control Protocol, Src Port: 51006, Dst Port: 22, Seq: 156606, Ack: 2634, Len: 1460
▶ SSH Protocol
```

Output 1: time-seq.



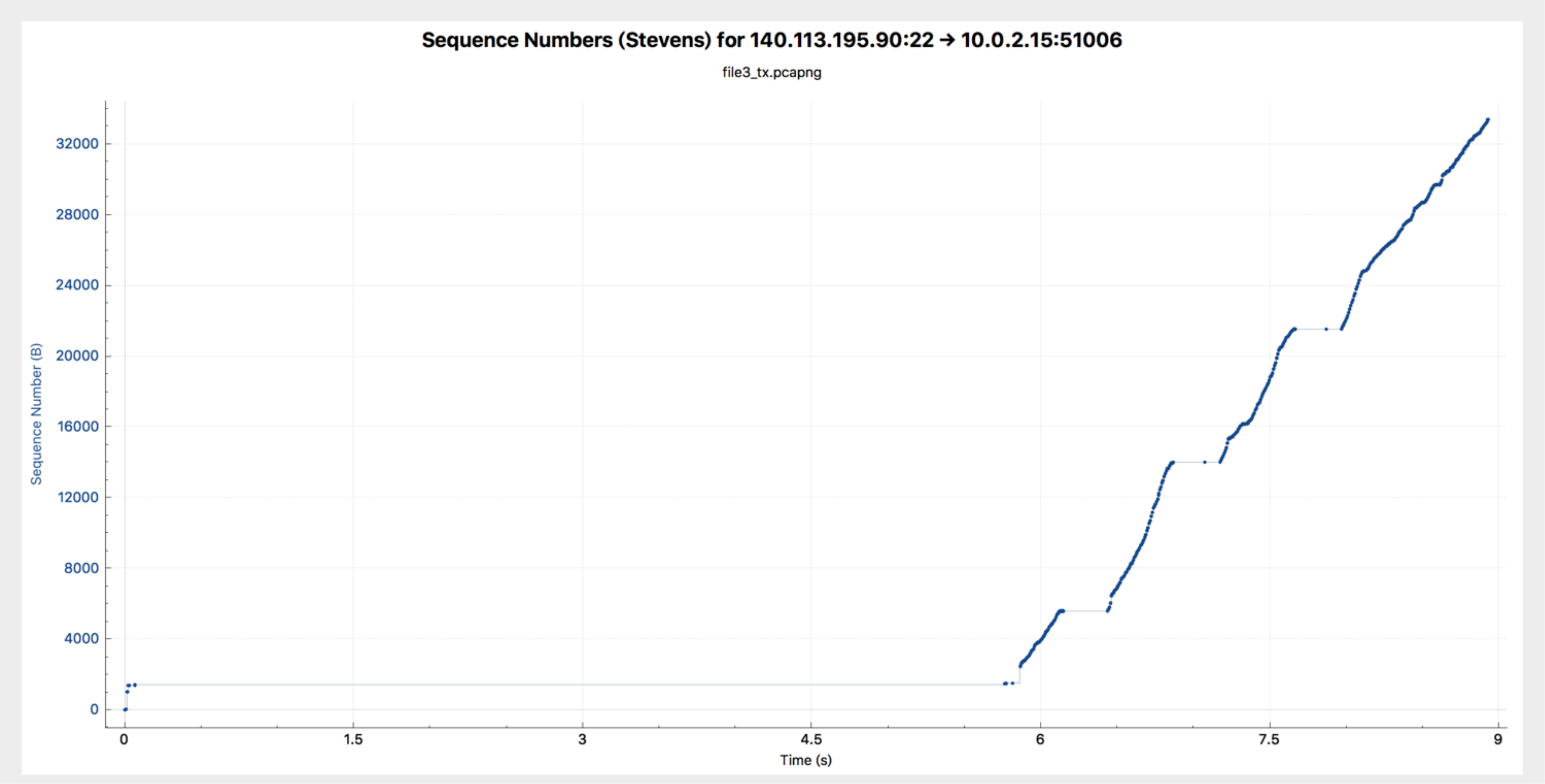
```
 1 10.0.2.15      140.113.19… TCP     [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1824869065 TSecr=0 WS=128
 2 140.113.19… 10.0.2.15      TCP     [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 3 10.0.2.15      140.113.19… TCP     [ACK] Seq=1 Ack=1 Win=29200 Len=0
 4 10.0.2.15      140.113.19… SSHv2   tocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
 5 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1 Ack=42 Win=65535 Len=0
 6 140.113.19… 10.0.2.15      SSHv2   tocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
 7 10.0.2.15      140.113.19… TCP     [ACK] Seq=42 Ack=42 Win=29200 Len=0
 8 10.0.2.15      140.113.19… SSHv2    Exchange Init
 9 140.113.19… 10.0.2.15      TCP     [ACK] Seq=42 Ack=1378 Win=65535 Len=0
10 140.113.19… 10.0.2.15      SSHv2    Exchange Init
11 10.0.2.15      140.113.19… SSHv2   fie-Hellman Key Exchange Init
12 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1018 Ack=1426 Win=65535 Len=0
13 140.113.19… 10.0.2.15      SSHv2   fie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
14 10.0.2.15      140.113.19… SSHv2    Keys
15 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1382 Ack=1442 Win=65535 Len=0
16 10.0.2.15      140.113.19… SSHv2   rypted packet (len=44)
17 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1382 Ack=1486 Win=65535 Len=0
18 140.113.19… 10.0.2.15      SSHv2   rypted packet (len=44)
19 10.0.2.15      140.113.19… SSHv2   rypted packet (len=68)
20 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1426 Ack=1554 Win=65535 Len=0
21 140.113.19… 10.0.2.15      SSHv2   rypted packet (len=52)
22 10.0.2.15      140.113.19… TCP     [ACK] Seq=1554 Ack=1478 Win=32208 Len=0
25 10.0.2.15      140.113.19… SSHv2   rypted packet (len=148)
26 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1478 Ack=1702 Win=65535 Len=0
27 140.113.19… 10.0.2.15      SSHv2   rypted packet (len=28)
28 10.0.2.15      140.113.19  TCP     54 5.773104525 51006 → 22 [ACK] Seq=1702 Ack=1506 Win=32208 Len=0
```



```
 1 10.0.2.15      140.113.19… TCP     [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1824869065 TSecr=0 WS=128
 2 140.113.19… 10.0.2.15      TCP     [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 3 10.0.2.15      140.113.19… TCP     [ACK] Seq=1 Ack=1 Win=29200 Len=0
 4 10.0.2.15      140.113.19… SSHv2   tocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
 5 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1 Ack=42 Win=65535 Len=0
 6 140.113.19… 10.0.2.15      SSHv2   tocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
 7 10.0.2.15      140.113.19… TCP     [ACK] Seq=42 Ack=42 Win=29200 Len=0
 8 10.0.2.15      140.113.19… SSHv2    Exchange Init
 9 140.113.19… 10.0.2.15      TCP     [ACK] Seq=42 Ack=1378 Win=65535 Len=0
10 140.113.19… 10.0.2.15      SSHv2    Exchange Init
11 10.0.2.15      140.113.19… SSHv2   fie-Hellman Key Exchange Init
12 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1018 Ack=1426 Win=65535 Len=0
13 140.113.19… 10.0.2.15      SSHv2   fie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
14 10.0.2.15      140.113.19… SSHv2    Keys
15 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1382 Ack=1442 Win=65535 Len=0
16 10.0.2.15      140.113.19… SSHv2   rypted packet (len=44)
17 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1382 Ack=1486 Win=65535 Len=0
18 140.113.19… 10.0.2.15      SSHv2   rypted packet (len=44)
19 10.0.2.15      140.113.19… SSHv2   rypted packet (len=68)
20 140.113.19… 10.0.2.15      TCP     [ACK] Seq=1426 Ack=1554 Win=65535 Len=0
21 140.113.19… 10.0.2.15      SSHv2
22 10.0.2.15      140.113.19… TCP     =32208 Len=0
25 10.0.2.15      140.113.19… SSHv2
26 140.113.19… 10.0.2.15      TCP     =65535 Len=0
27 140.113.19… 10.0.2.15      SSHv2
28 10.0.2.15      140.113.19  TCP     54 5.773104525 51006 → 22 =32208 Len=0
```

Output 1: time-seq.

- Example figure



Output 2: average throughput

- Plot the average throughput of each window of every connection

- Window size: 0.1s

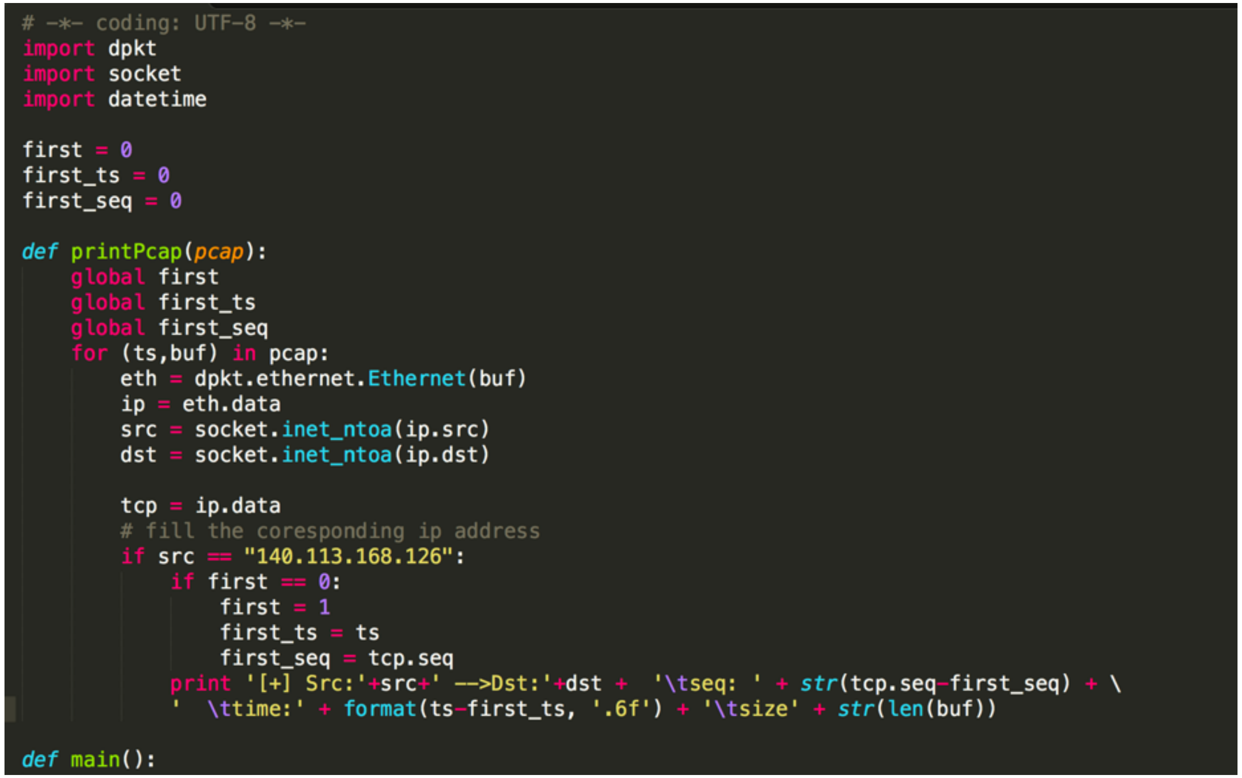
- Calculate the average throughput of each window: (number of bits)/0.1s

Output 2: average throughput

- Download "two_connection.sh" from e3
- Open Wireshark and start sniffing
- Use "two_connection.sh" to download two files concurrently
  - Choose one of below to execute
  - ./two_connection.sh http://140.113.195.91/testfile
  - ./two_connection.sh http://140.113.195.70/testfile
- Save Wireshark as ”lab1_ID_rx_wget.pcap”
  - .pcap format for Python

Output 2: average throughput

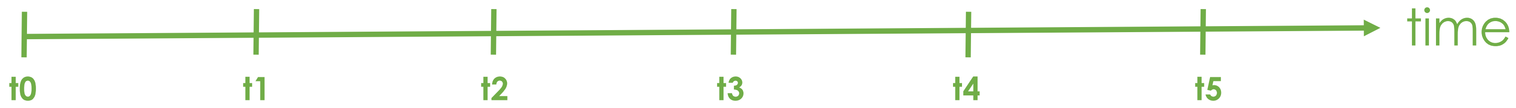
- Save the packet trace as a “pcap” file
- Use Python parser to get the packet information
  - Download the example code from e3



```
# -*- coding: UTF-8 -*-
import dpkt
import socket
import datetime

first = 0
first_ts = 0
first_seq = 0

def printPcap(pcap):
    global first
    global first_ts
    global first_seq
    for (ts,buf) in pcap:
        eth = dpkt.ethernet.Ethernet(buf)
        ip = eth.data
        src = socket.inet_ntoa(ip.src)
        dst = socket.inet_ntoa(ip.dst)

        tcp = ip.data
        # fill the coresponding ip address
        if src == "140.113.168.126":
            if first == 0:
                first = 1
                first_ts = ts
                first_seq = tcp.seq
            print '[+] Src:'+src+' -->Dst:'+dst +  '\tseq: ' + str(tcp.seq-first_seq) + \
            '  \ttime:' + format(ts-first_ts, '.6f') + '\tsize' + str(len(buf))

def main():
```

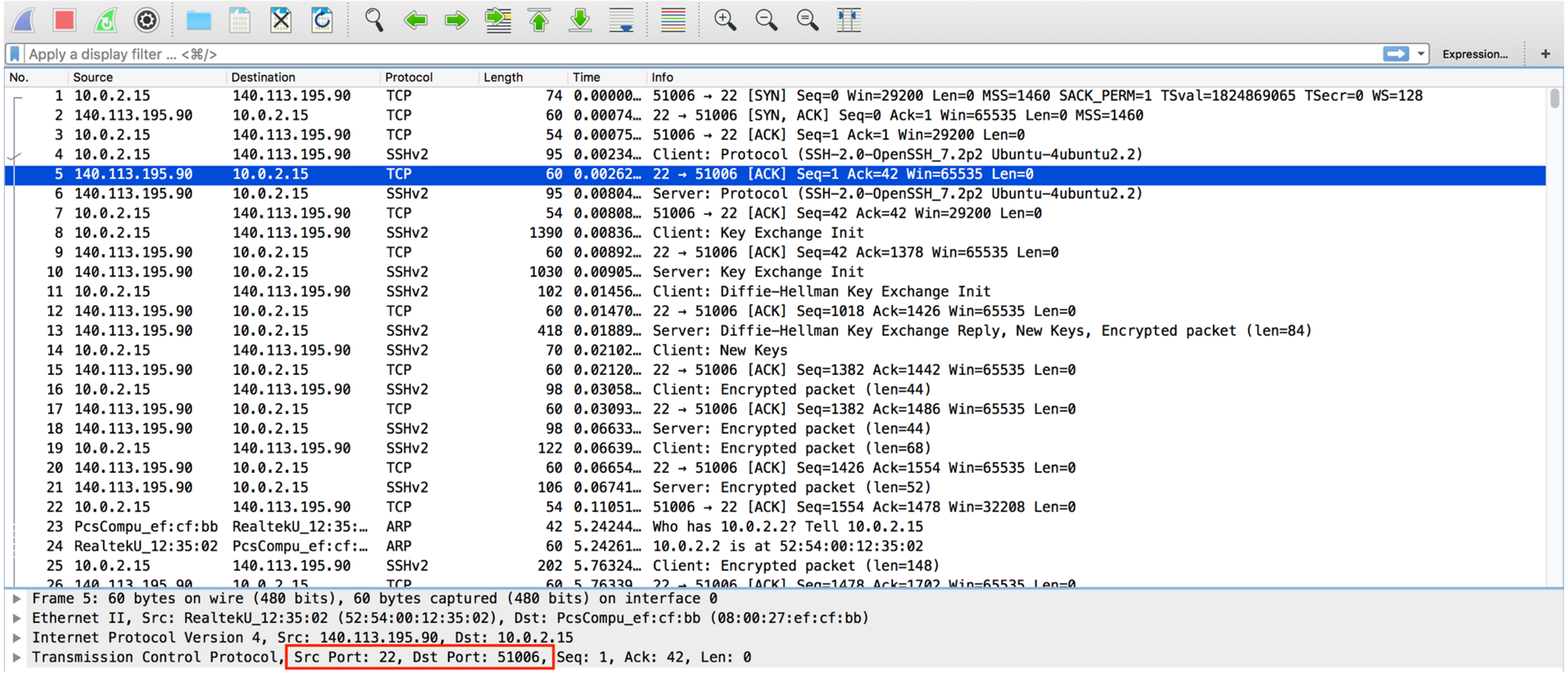
Output 2: average throughput

- How to calculate the average throughput over time?
  - Set time interval, e.g. 0.1s
  - throughput = sent bits / time-interval
    - Throughput =
      (total # of bits for all packets in t0~t1)/(t1-t0)



Output 2: average throughput

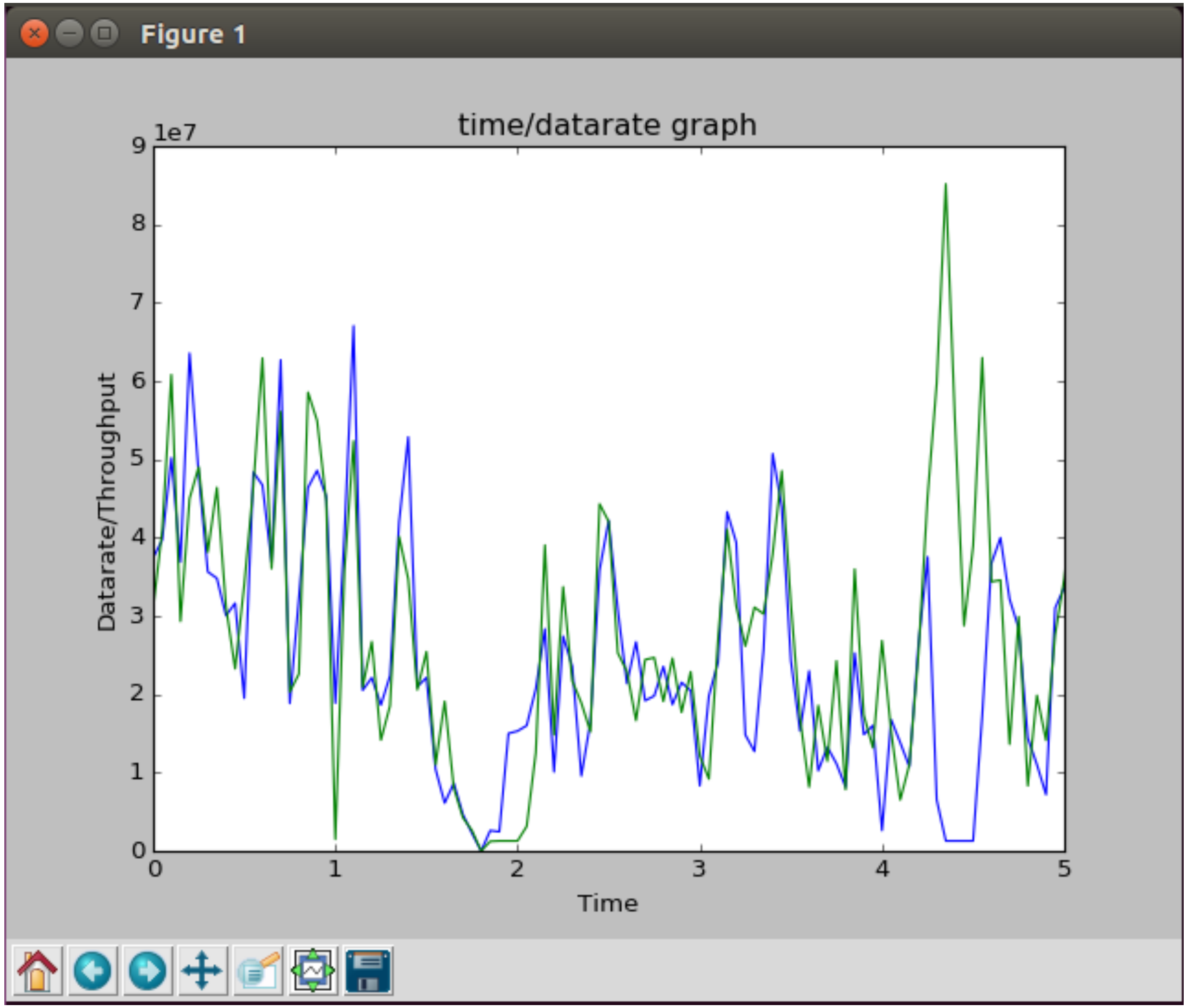
- Hint
  - How to discriminate two connections?
    - Different connections using different ports



```
No.  Source            Destination       Protocol  Length Time        Info
  1  10.0.2.15         140.113.195.90    TCP           74 0.00000…  51006 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1824869065 TSecr=0 WS=128
  2  140.113.195.90    10.0.2.15         TCP           60 0.00074…  22 → 51006 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  3  10.0.2.15         140.113.195.90    TCP           54 0.00075…  51006 → 22 [ACK] Seq=1 Ack=1 Win=29200 Len=0
  4  10.0.2.15         140.113.195.90    SSHv2         95 0.00234…  Client: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
  5  140.113.195.90    10.0.2.15         TCP           60 0.00262…  22 → 51006 [ACK] Seq=1 Ack=42 Win=65535 Len=0
  6  140.113.195.90    10.0.2.15         SSHv2         95 0.00804…  Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
  7  10.0.2.15         140.113.195.90    TCP           54 0.00808…  51006 → 22 [ACK] Seq=42 Ack=42 Win=29200 Len=0
  8  10.0.2.15         140.113.195.90    SSHv2       1390 0.00836…  Client: Key Exchange Init
  9  140.113.195.90    10.0.2.15         TCP           60 0.00892…  22 → 51006 [ACK] Seq=42 Ack=1378 Win=65535 Len=0
 10  140.113.195.90    10.0.2.15         SSHv2       1030 0.00905…  Server: Key Exchange Init
 11  10.0.2.15         140.113.195.90    SSHv2        102 0.01456…  Client: Diffie-Hellman Key Exchange Init
 12  140.113.195.90    10.0.2.15         TCP           60 0.01470…  22 → 51006 [ACK] Seq=1018 Ack=1426 Win=65535 Len=0
 13  140.113.195.90    10.0.2.15         SSHv2        418 0.01889…  Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
 14  10.0.2.15         140.113.195.90    SSHv2         70 0.02102…  Client: New Keys
 15  140.113.195.90    10.0.2.15         TCP           60 0.02120…  22 → 51006 [ACK] Seq=1382 Ack=1442 Win=65535 Len=0
 16  10.0.2.15         140.113.195.90    SSHv2         98 0.03058…  Client: Encrypted packet (len=44)
 17  140.113.195.90    10.0.2.15         TCP           60 0.03093…  22 → 51006 [ACK] Seq=1382 Ack=1486 Win=65535 Len=0
 18  140.113.195.90    10.0.2.15         SSHv2         98 0.06633…  Server: Encrypted packet (len=44)
 19  10.0.2.15         140.113.195.90    SSHv2        122 0.06639…  Client: Encrypted packet (len=68)
 20  140.113.195.90    10.0.2.15         TCP           60 0.06654…  22 → 51006 [ACK] Seq=1426 Ack=1554 Win=65535 Len=0
 21  140.113.195.90    10.0.2.15         SSHv2        106 0.06741…  Server: Encrypted packet (len=52)
 22  10.0.2.15         140.113.195.90    TCP           54 0.11051…  51006 → 22 [ACK] Seq=1554 Ack=1478 Win=32208 Len=0
 23  PcsCompu_ef:cf:bb RealtekU_12:35:…  ARP           42 5.24244…  Who has 10.0.2.2? Tell 10.0.2.15
 24  RealtekU_12:35:02 PcsCompu_ef:cf:…  ARP           60 5.24261…  10.0.2.2 is at 52:54:00:12:35:02
 25  10.0.2.15         140.113.195.90    SSHv2        202 5.76324…  Client: Encrypted packet (len=148)
 26  140.113.195.90    10.0.2.15         TCP           60 5.76339…  22 → 51006 [ACK] Seq=1478 Ack=1702 Win=65535 Len=0
▶ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_ef:cf:bb (08:00:27:ef:cf:bb)
▶ Internet Protocol Version 4, Src: 140.113.195.90, Dst: 10.0.2.15
▶ Transmission Control Protocol, Src Port: 22, Dst Port: 51006, Seq: 1, Ack: 42, Len: 0
```

Output 2: average throughput

- Example figure



Output

- Trace files
  - lab1_ID_tx_scp.pcapng
  - lab1_ID_rx_wget.pcap
- Report (lab1_ID.pdf) including
  - Figure 1 (time-sequence of scp)
    - Step-by-step instruction (e.g., which bottoms you click, what are the filtering rules, etc)
    - Your observation from the figure
  - Figure 2 (average throughput of wget)
    - How do you calculate the throughput
    - Your observation from the figure
- Python code (lab1_ID.py)
- Submit to E3 by Oct. 13, 23:59
  - Delay policy: see syllabus