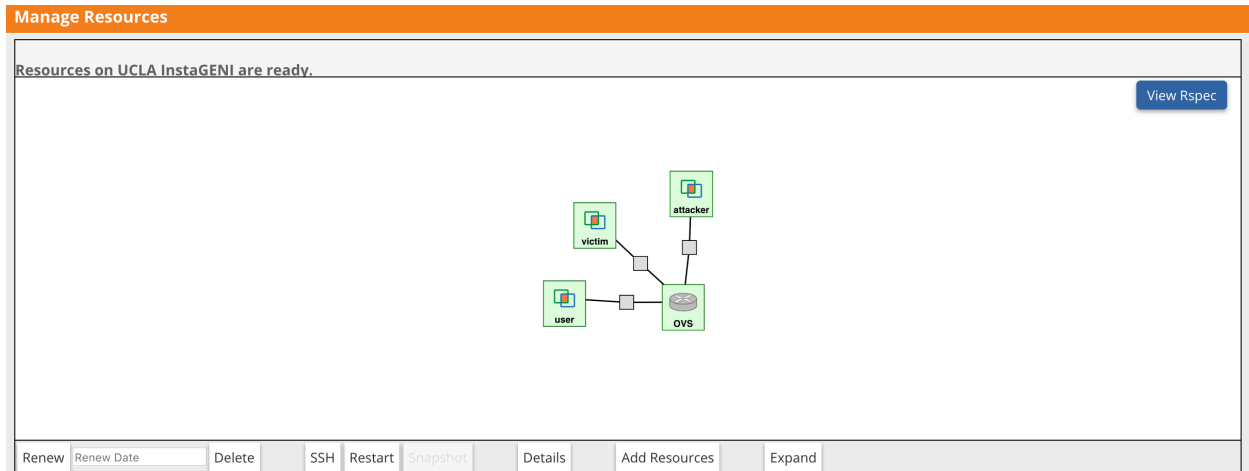


## Lab 1 – Yu Qiu, Xu Cheng

### Set Up

We set up the topology step by step following the instruction, and then we get:



### Part 1

1. There are four machines in our topology and their names are attacker, victim, user and OVS respectively. As the topology shown, attacker, victim and user are connected by OVS.
2. User refers to machines behave regularly on a network; such as browsing the internet.

Attackers will create and send attacks, such as DoS attack, to other users in the network.

Victims are the users who are compromised by attacks, such as DoS attack, from attackers.

3. A network switch is a computer networking device that connects devices together on a computer network. It works as the network connection point by using packet switching to receive, process, and forward data to the destination device.

## Part 2

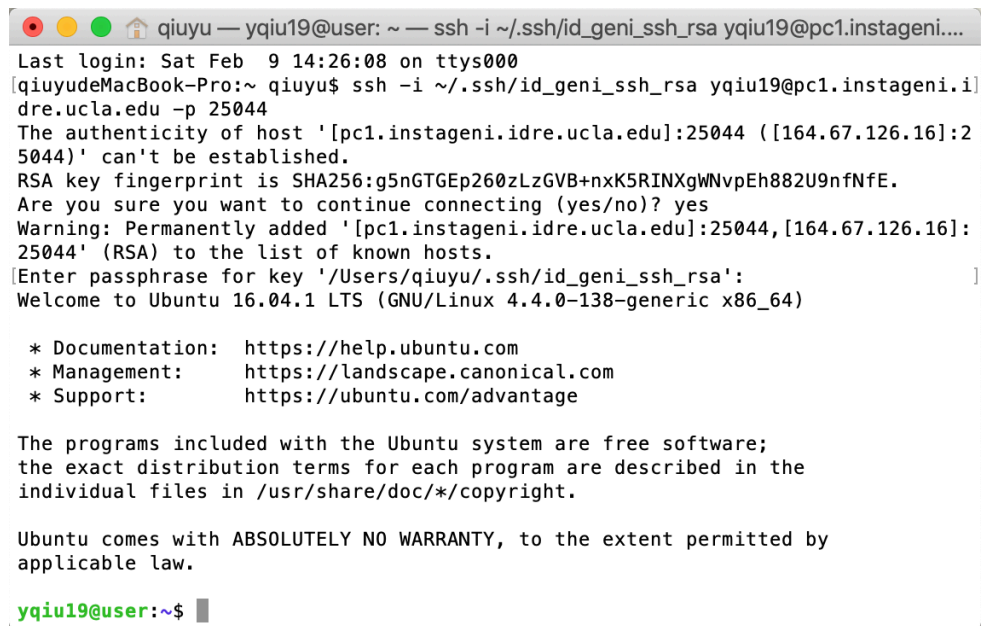
1. Network protocols are formal standards and policies made up of rules, procedures and formats that defines communication between two or more devices over a network. Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. SSH provides a secure channel over an unsecured network in a client–server architecture, connecting an SSH client application with an SSH server. Tare some malicious users on the network and they will compromise other users, for example, these malicious users will eavesdrop or tamper communication between other users. Hence, protocols like SSH are needed to offer a secure network environment for regular users.

Reference:

[https://en.wikipedia.org/wiki/Secure\\_Shell](https://en.wikipedia.org/wiki/Secure_Shell)

<https://www.interserver.net/tips/kb/common-network-protocols-ports/>

4. We generate and download our private key, and then open ssh connection to the user node:



```
qiuyu — yqiu19@user: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni...
Last login: Sat Feb  9 14:26:08 on ttys000
[qiuyudeMacBook-Pro:~ qiuyu$ ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.i]
dre.ucla.edu -p 25044
The authenticity of host '[pc1.instageni.idre.ucla.edu]:25044 ([164.67.126.16]:25044)' can't be established.
RSA key fingerprint is SHA256:g5nGTGEp260zLzGVB+nxK5RINXgWNvpEh882U9nfNfE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[pc1.instageni.idre.ucla.edu]:25044,[164.67.126.16]:25044' (RSA) to the list of known hosts.
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa': ]
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-138-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

yqiu19@user:~$
```

5. We repeat the above operation to open ssh connection to all the other nodes in our topology:

```
qiuyu — yqiu19@victim: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instage...
[qiuyudeMacBook-Pro:~ qiuyu$
[qiuyudeMacBook-Pro:~ qiuyu$ ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.i]
dre.ucla.edu -p 25045
The authenticity of host '[pc1.instageni.idre.ucla.edu]:25045 ([164.67.126.16]:2]
5045)' can't be established.
RSA key fingerprint is SHA256:g5nGTGEp260zLzGVB+nxK5RINXgWNvpEh882U9nfNfE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[pc1.instageni.idre.ucla.edu]:25045,[164.67.126.16]:]
25045' (RSA) to the list of known hosts.
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa':
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-138-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

yqiu19@victim:~$
```

```
qiuyu — yqiu19@attacker: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instag...
Connection to pc1.instageni.idre.ucla.edu closed.
[qiuyudeMacBook-Pro:~ qiuyu$ ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.i]
dre.ucla.edu -p 25043
The authenticity of host '[pc1.instageni.idre.ucla.edu]:25043 ([164.67.126.16]:2]
5043)' can't be established.
RSA key fingerprint is SHA256:g5nGTGEp260zLzGVB+nxK5RINXgWNvpEh882U9nfNfE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[pc1.instageni.idre.ucla.edu]:25043,[164.67.126.16]:]
25043' (RSA) to the list of known hosts.
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa':
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-138-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

yqiu19@attacker:~$
```

```

qiu19 — yqiu19@ovs: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.i...
[yqiu19@attacker:~$ exit
logout
Connection to pc1.instageni.idre.ucla.edu closed.
[qiuyudeMacBook-Pro:~ qiuyu$ ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.i]
dre.ucla.edu -p 25042
The authenticity of host '[pc1.instageni.idre.ucla.edu]:25042 ([164.67.126.16]:2
5042)' can't be established.
RSA key fingerprint is SHA256:g5nGTGEp260zLzGVB+nxK5RINXgWNvpEh882U9nfNfE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[pc1.instageni.idre.ucla.edu]:25042,[164.67.126.16]:
25042' (RSA) to the list of known hosts.
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa':
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

yqiu19@ovs:~$

```

## Part 3

### 1. We type 'ping victim' in the terminal of user machine:

```

qiu19 — yqiu19@user: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni...
[qiuyudeMacBook-Pro:~ qiuyu$ ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.i]
dre.ucla.edu -p 25044
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa':
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-138-generic x86_64)

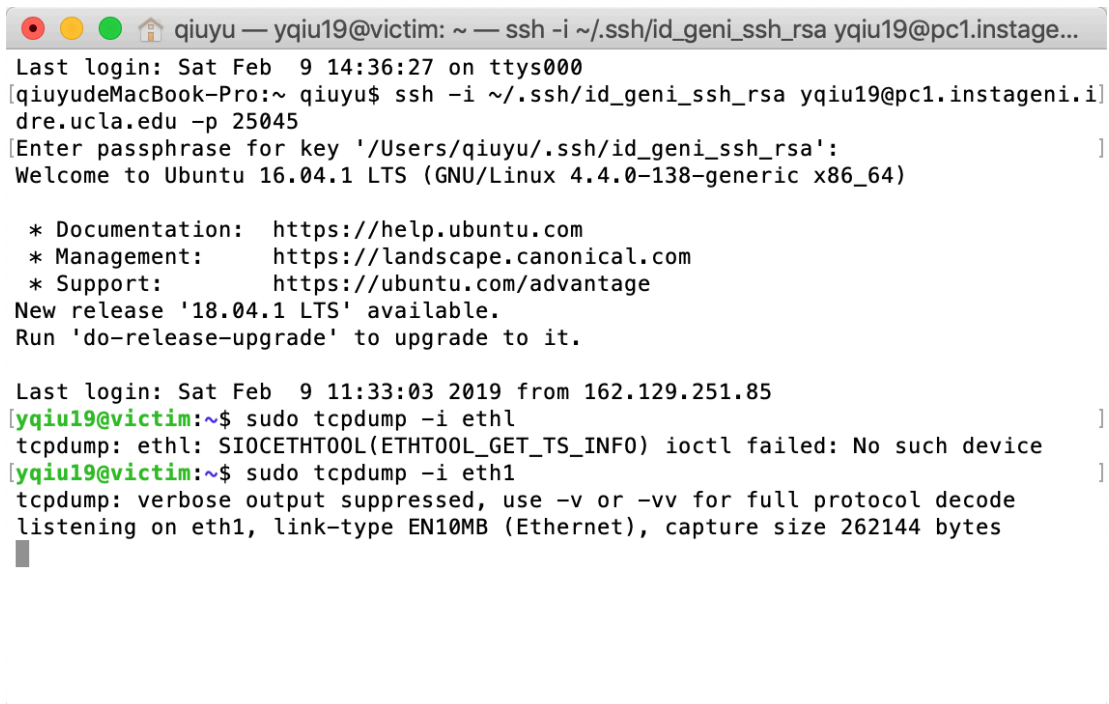
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Sat Feb  9 11:36:14 2019 from 162.129.251.85
[yqiu19@user:~$ ping victim
PING victim-link-0 (10.10.1.1) 56(84) bytes of data.
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=1 ttl=63 time=1.91 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=2 ttl=63 time=0.938 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=3 ttl=63 time=0.831 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=4 ttl=63 time=0.826 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=5 ttl=63 time=0.873 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=6 ttl=63 time=0.821 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=7 ttl=63 time=0.876 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=8 ttl=63 time=0.956 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=9 ttl=63 time=0.825 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=10 ttl=63 time=0.867 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=11 ttl=63 time=0.953 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=12 ttl=63 time=0.875 ms
^C

```

2. These are the three lines we copy from the user terminal:

```
PING victim-link-0 (10.10.1.1) 56(84) bytes of data.  
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=1 ttl=63 time=1.91  
ms  
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=2 ttl=63 time=0.938  
ms
```

3.

A terminal window titled 'qiuyu — yqiu19@victim: ~ — ssh -i ~/.ssh/id\_geni\_ssh\_rsa yqiu19@pc1.instage...' shows a session from a MacBook-Pro. The user runs 'ssh -i ~/.ssh/id\_geni\_ssh\_rsa yqiu19@pc1.instage...' and enters a passphrase. The terminal displays Ubuntu 16.04.1 LTS login messages, system updates, and support links. The user then runs 'sudo tcpdump -i eth1', which fails with 'ioctl failed: No such device'. Finally, the user runs 'sudo tcpdump -i eth1' again, which starts listening on eth1 with a capture size of 262144 bytes.

```
qiuyu — yqiu19@victim: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instage...  
Last login: Sat Feb  9 14:36:27 on ttys000  
[qiuyudeMacBook-Pro:~ qiuyu$ ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instage.i]  
dre.ucla.edu -p 25045  
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa':  
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-138-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
New release '18.04.1 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Sat Feb  9 11:33:03 2019 from 162.129.251.85  
[yqiu19@victim:~$ sudo tcpdump -i eth1  
tcpdump: eth1: SIOCETHTOOL(ETHTOOL_GET_TS_INFO) ioctl failed: No such device  
[yqiu19@victim:~$ sudo tcpdump -i eth1  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
```

4/5.

```
qiyu — yqiu19@user: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni...
yqiu19@user:~$ ping victim
PING victim-link-0 (10.10.1.1) 56(84) bytes of data.
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=1 ttl=63 time=1.09 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=2 ttl=63 time=1.20 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=3 ttl=63 time=1.30 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=4 ttl=63 time=1.05 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=5 ttl=63 time=1.07 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=6 ttl=63 time=0.899 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=7 ttl=63 time=1.14 ms
^C
--- victim-link-0 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.899/1.110/1.303/0.121 ms
yqiu19@user:~$

qiyu — yqiu19@victim: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instage...
yqiu19@victim:~$ sudo tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:46:28.440591 IP user-link-2 > victim-link-0: ICMP echo request, id 499, seq 1
, length 64
11:46:28.440648 IP victim-link-0 > user-link-2: ICMP echo reply, id 499, seq 1,
length 64
11:46:29.442117 IP user-link-2 > victim-link-0: ICMP echo request, id 499, seq 2
, length 64
11:46:29.442154 IP victim-link-0 > user-link-2: ICMP echo reply, id 499, seq 2,
length 64
11:46:30.443717 IP user-link-2 > victim-link-0: ICMP echo request, id 499, seq 3
, length 64
11:46:30.443772 IP victim-link-0 > user-link-2: ICMP echo reply, id 499, seq 3,
length 64
11:46:31.444366 IP user-link-2 > victim-link-0: ICMP echo request, id 499, seq 4
, length 64
11:46:31.444395 IP victim-link-0 > user-link-2: ICMP echo reply, id 499, seq 4,
length 64
11:46:32.445811 IP user-link-2 > victim-link-0: ICMP echo request, id 499, seq 5
, length 64
11:46:32.445842 IP victim-link-0 > user-link-2: ICMP echo reply, id 499, seq 5,
length 64
```

6. These are lines from victim terminal:

```
listening on eth1, link-type EN10MB (Ethernet), capture size 262144
bytes
11:46:28.440591 IP user-link-2 > victim-link-0: ICMP echo request,
id 499, seq 1, length 64
11:46:28.440648 IP victim-link-0 > user-link-2: ICMP echo reply, id
499, seq 1, length 64
11:46:29.442117 IP user-link-2 > victim-link-0: ICMP echo request,
id 499, seq 2, length 64
11:46:29.442154 IP victim-link-0 > user-link-2: ICMP echo reply, id
499, seq 2, length 64
11:46:30.443717 IP user-link-2 > victim-link-0: ICMP echo request,
id 499, seq 3, length 64
11:46:30.443772 IP victim-link-0 > user-link-2: ICMP echo reply, id
499, seq 3, length 64
11:46:31.444366 IP user-link-2 > victim-link-0: ICMP echo request,
id 499, seq 4, length 64
11:46:31.444395 IP victim-link-0 > user-link-2: ICMP echo reply, id
499, seq 4, length 64
```

```
11:46:32.445811 IP user-link-2 > victim-link-0: ICMP echo request,
id 499, seq 5, length 64
11:46:32.445842 IP victim-link-0 > user-link-2: ICMP echo reply, id
499, seq 5, length 64
11:46:33.447103 ARP, Request who-has OVS-link-0 tell victim-link-0,
length 28
11:46:33.447232 IP user-link-2 > victim-link-0: ICMP echo request,
id 499, seq 6, length 64
11:46:33.447255 IP victim-link-0 > user-link-2: ICMP echo reply, id
499, seq 6, length 64
11:46:33.447412 ARP, Reply OVS-link-0 is-at 02:f2:81:13:f7:9d (oui
Unknown), length 28
11:46:34.448613 IP user-link-2 > victim-link-0: ICMP echo request,
id 499, seq 7, length 64
11:46:34.448654 IP victim-link-0 > user-link-2: ICMP echo reply, id
499, seq 7, length 64
11:46:39.454753 ARP, Request who-has victim-link-0 tell OVS-link-0,
length 28
11:46:39.454785 ARP, Reply victim-link-0 is-at 02:21:ee:0f:ab:e0
(oui Unknown), length 28
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
```

The 'ping victim' command is used to check whether the network between user and victim is connected. After entering this command in user terminal, the user machine sent several 'ICMP echo request' to victim machine and then victim reply these requests to user. Hence, lines showed above mean network between these two machine is connected.

#### 7. Lines from the user terminal:

```
PING victim-link-0 (10.10.1.1) 56(84) bytes of data.
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=1 ttl=63
time=1.09 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=2 ttl=63
time=1.20 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=3 ttl=63
time=1.30 ms
```



```
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=4 ttl=63
time=1.05 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=5 ttl=63
time=1.07 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=6 ttl=63
time=0.899 ms
64 bytes from victim-link-0 (10.10.1.1): icmp_seq=7 ttl=63
time=1.14 ms
^C
--- victim-link-0 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.899/1.110/1.303/0.121 ms
```

The time unit used in the ping statistics is ms.

8. Round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgement of that signal to be received. In the context of computer networks, the signal is generally a data packet, and the RTT is also known as the ping time. An internet user can determine the RTT by using the ping command.

Reference: [https://en.wikipedia.org/wiki/Round-trip\\_delay\\_time](https://en.wikipedia.org/wiki/Round-trip_delay_time)

9. The average RTT in this experiment is 1.110ms. What we search online claims that a lower number, around less than 20 ms or better, is ideal. Hence, this network is very fast and we think because it is an ethernet.

Reference: <https://go.frontier.com/best-internet-for-gaming>

## Part 4

1.

```
yqiu19@victim:~$ iperf -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
█
```

2.

```
yqiu19@user:~$ iperf -c victim
-----
Client connecting to victim, TCP port 5001
TCP window size: 85.0 KByte (default)
-----
[ 3] local 10.10.3.2 port 38256 connected with 10.10.1.1 port 5001
█

yqiu19@victim:~$ iperf -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
[ 4] local 10.10.1.1 port 5001 connected with 10.10.3.2 port 38256
[ ID] Interval      Transfer    Bandwidth
[ 4]  0.0-10.2 sec  116 MBytes  95.6 Mbits/sec
□
```


4. The lines in user terminal:

```
-----
Client connecting to victim, TCP port 5001
TCP window size: 85.0 KByte (default)
-----
[ 3] local 10.10.3.2 port 38256 connected with 10.10.1.1 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3]  0.0-10.0 sec  116 MBytes  97.2 Mbits/sec
```

6.

```
[^Cyqiu19@victim:~$ ping ovs
PING OVS-link-0 (10.10.1.2) 56(84) bytes of data.
64 bytes from OVS-link-0 (10.10.1.2): icmp_seq=1 ttl=64 time=0.599 ms
64 bytes from OVS-link-0 (10.10.1.2): icmp_seq=2 ttl=64 time=0.485 ms
64 bytes from OVS-link-0 (10.10.1.2): icmp_seq=3 ttl=64 time=0.527 ms
64 bytes from OVS-link-0 (10.10.1.2): icmp_seq=4 ttl=64 time=0.453 ms
64 bytes from OVS-link-0 (10.10.1.2): icmp_seq=5 ttl=64 time=0.472 ms
^C
--- OVS-link-0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.453/0.507/0.599/0.053 ms
```

7.



A terminal window titled 'qiuyu — yqiu19@ovs: ~ — ssh -i ~/.ssh/id\_geni\_ssh\_rsa yqiu19@pc1.instageni.i...' shows the following content:

```
Last login: Sat Feb 9 14:41:39 on ttys001
[qiuyudeMacBook-Pro:~ qiuyu$ ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.i]
dre.ucla.edu -p 25042
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa':
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Sat Feb 9 11:34:50 2019 from 162.129.251.85
[yqiu19@ovs:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:6e:49:59:df:51
          inet addr:172.17.1.1  Bcast:172.31.255.255  Mask:255.240.0.0
          inet6 addr: fe80::6e:49ff:fe59:df51/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4584 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4726 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:368249 (368.2 KB)  TX bytes:378058 (378.0 KB)

eth1      Link encap:Ethernet  HWaddr 02:f2:81:13:f7:9d
          inet addr:10.10.1.2  Bcast:10.10.1.255  Mask:255.255.255.0
          inet6 addr: fe80::f2:81ff:fe13:f79d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9630 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9658 errors:0 dropped:0 overruns:0 carrier:0
```

8. We find out that it is 10.10.1.2 and it is located beside 'eth1':

```

eth1      Link encap:Ethernet  HWaddr 02:f2:81:13:f7:9d
          inet addr:10.10.1.2  Bcast:10.10.1.255  Mask:255.255.255.0
          inet6 addr: fe80::f2:81ff:fe13:f79d/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9630 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9658 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:512640 (512.6 KB)  TX bytes:122575200 (122.5 MB)

```

9. We repeat step one and step two, and then we can observe this at OVS. This

traffic comes from user to victim:

```

qiu19@ovs: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa qiu19@pc1.instageni.i...
), length 724)
  user-link-2.38352 > victim-link-0.5001: Flags [FP.], cksum 0x1add (incorrect
-> 0x6f16), seq 121765241:121765913, ack 1, win 229, options [nop,nop,TS val 45
771401 ecr 45758918], length 672
22:40:40.252357 IP (tos 0x0, ttl 64, id 36816, offset 0, flags [DF], proto TCP (
6), length 52)
  victim-link-0.5001 > user-link-2.38352: Flags [.], cksum 0x183d (incorrect -
> 0xd38c), seq 1, ack 121765914, win 7745, options [nop,nop,TS val 45758924 ecr
45771401], length 0
22:40:40.254702 IP (tos 0x0, ttl 64, id 36817, offset 0, flags [DF], proto TCP (
6), length 52)
  victim-link-0.5001 > user-link-2.38352: Flags [F.], cksum 0x183d (incorrect
-> 0xd38b), seq 1, ack 121765914, win 7745, options [nop,nop,TS val 45758924 ecr
45771401], length 0
22:40:40.254954 IP (tos 0x0, ttl 63, id 14188, offset 0, flags [DF], proto TCP (
6), length 52)
  user-link-2.38352 > victim-link-0.5001: Flags [.], cksum 0xf0e1 (correct), s
eq 121765914, ack 2, win 229, options [nop,nop,TS val 45771407 ecr 45758924], le
ngth 0
^C
18880 packets captured
18880 packets received by filter
0 packets dropped by kernel
qiu19@ovs:~$

```

10. We type 'sudo hping3 -S --flood victim' in attacker terminal and we observe

what happen in OVS:

```
[yqiu19@attacker:~$ sudo hping3 -S --flood victim
HPING victim (eth1 10.10.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
qiuyu — yqiu19@ovs: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa yqiu19@pc1.instageni.idre.ucla.edu
13:36:57.472943 IP (tos 0x0, ttl 64, id 52248, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54041: Flags [R.], cksum 0x0a0e (correct), seq 0, ack 1427465853, win 0, length 0
13:36:57.472950 IP (tos 0x0, ttl 64, id 52249, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54042: Flags [R.], cksum 0x3d7e (correct), seq 0, ack 83985184, win 0, length 0
13:36:57.472952 IP (tos 0x0, ttl 64, id 52250, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54043: Flags [R.], cksum 0x47ba (correct), seq 0, ack 1838944328, win 0, length 0
13:36:57.472954 IP (tos 0x0, ttl 64, id 52251, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54044: Flags [R.], cksum 0x9e3d (correct), seq 0, ack 1110304050, win 0, length 0
13:36:57.472961 IP (tos 0x0, ttl 63, id 3770, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54052 > victim-link-0.0: Flags [S], cksum 0x8a18 (correct), seq 1237113383, win 512, length 0
13:36:57.472976 IP (tos 0x0, ttl 63, id 63666, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54053 > victim-link-0.0: Flags [S], cksum 0x1ae8 (correct), seq 1888625822, win 512, length 0
13:36:57.472982 IP (tos 0x0, ttl 64, id 52252, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54045: Flags [R.], cksum 0xa52d (correct), seq 0, ack 784200113, win 0, length 0
13:36:57.472989 IP (tos 0x0, ttl 64, id 52253, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54046: Flags [R.], cksum 0x1f24 (correct), seq 0, ack 1454067660, win 0, length 0
13:36:57.472992 IP (tos 0x0, ttl 64, id 52254, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54047: Flags [R.], cksum 0xa41e (correct), seq 0, ack 1276852273, win 0, length 0
13:36:57.472994 IP (tos 0x0, ttl 64, id 52255, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54048: Flags [R.], cksum 0x35bd (correct), seq 0, ack 1924996383, win 0, length 0
13:36:57.473003 IP (tos 0x0, ttl 64, id 52256, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54049: Flags [R.], cksum 0xd518 (correct), seq 0, ack 2050979392, win 0, length 0
13:36:57.473009 IP (tos 0x0, ttl 63, id 62034, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54054 > victim-link-0.0: Flags [S], cksum 0xdf28 (correct), seq 140943657, win 512, length 0
13:36:57.473018 IP (tos 0x0, ttl 63, id 14511, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54055 > victim-link-0.0: Flags [S], cksum 0x906c (correct), seq 2015748023, win 512, length 0
13:36:57.473021 IP (tos 0x0, ttl 63, id 15478, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54056 > victim-link-0.0: Flags [S], cksum 0x618b (correct), seq 542326771, win 512, length 0
13:36:57.473047 IP (tos 0x0, ttl 63, id 57252, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54057 > victim-link-0.0: Flags [S], cksum 0x8b36 (correct), seq 835092616, win 512, length 0
13:36:57.473052 IP (tos 0x0, ttl 63, id 26345, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54058 > victim-link-0.0: Flags [S], cksum 0x4718 (correct), seq 1458540448, win 512, length 0
13:36:57.473058 IP (tos 0x0, ttl 63, id 45624, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54059 > victim-link-0.0: Flags [S], cksum 0x6c1f (correct), seq 730080645, win 512, length 0
13:36:57.473068 IP (tos 0x0, ttl 64, id 52257, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54050: Flags [R.], cksum 0x7cc1 (correct), seq 0, ack 1095501706, win 0, length 0
13:36:57.473078 IP (tos 0x0, ttl 64, id 52258, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54051: Flags [R.], cksum 0xef83 (correct), seq 0, ack 1364821177, win 0, length 0
13:36:57.473081 IP (tos 0x0, ttl 64, id 52259, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54052: Flags [R.], cksum 0xa1b0 (correct), seq 0, ack 1237113384, win 0, length 0
13:36:57.473086 IP (tos 0x0, ttl 64, id 52260, offset 0, flags [DF], proto TCP (6), length 40)
    victim-link-0.0 > attacker-link-1.54053: Flags [R.], cksum 0x3063 (correct), seq 0, ack 1888625823, win 0, length 0
13:36:57.473096 IP (tos 0x0, ttl 63, id 36534, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54060 > victim-link-0.0: Flags [S], cksum 0x504b (correct), seq 1571931733, win 512, length 0
13:36:57.473149 IP (tos 0x0, ttl 63, id 53679, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54061 > victim-link-0.0: Flags [S], cksum 0x6080 (correct), seq 1426352314, win 512, length 0
13:36:57.473156 IP (tos 0x0, ttl 63, id 38856, offset 0, flags [none], proto TCP (6), length 40)
    attacker-link-1.54062 > victim-link-0.0: Flags [S], cksum 0xf655 (correct), seq 862605466, win 512, length 0

16362 packets captured
1232984 packets received by filter
1202590 packets dropped by kernel
```

The attacker was trying to implement flood attack to victim by sending a lot of packets to victim. Because OVS is listening on this network, it captured those packets.

11. Yes, the traffic generated by attacker machine look like it goes through much faster than the traffic generated in task 3. Because DoS attack just keep sending packets to victim no matter there is acknowledge or not.

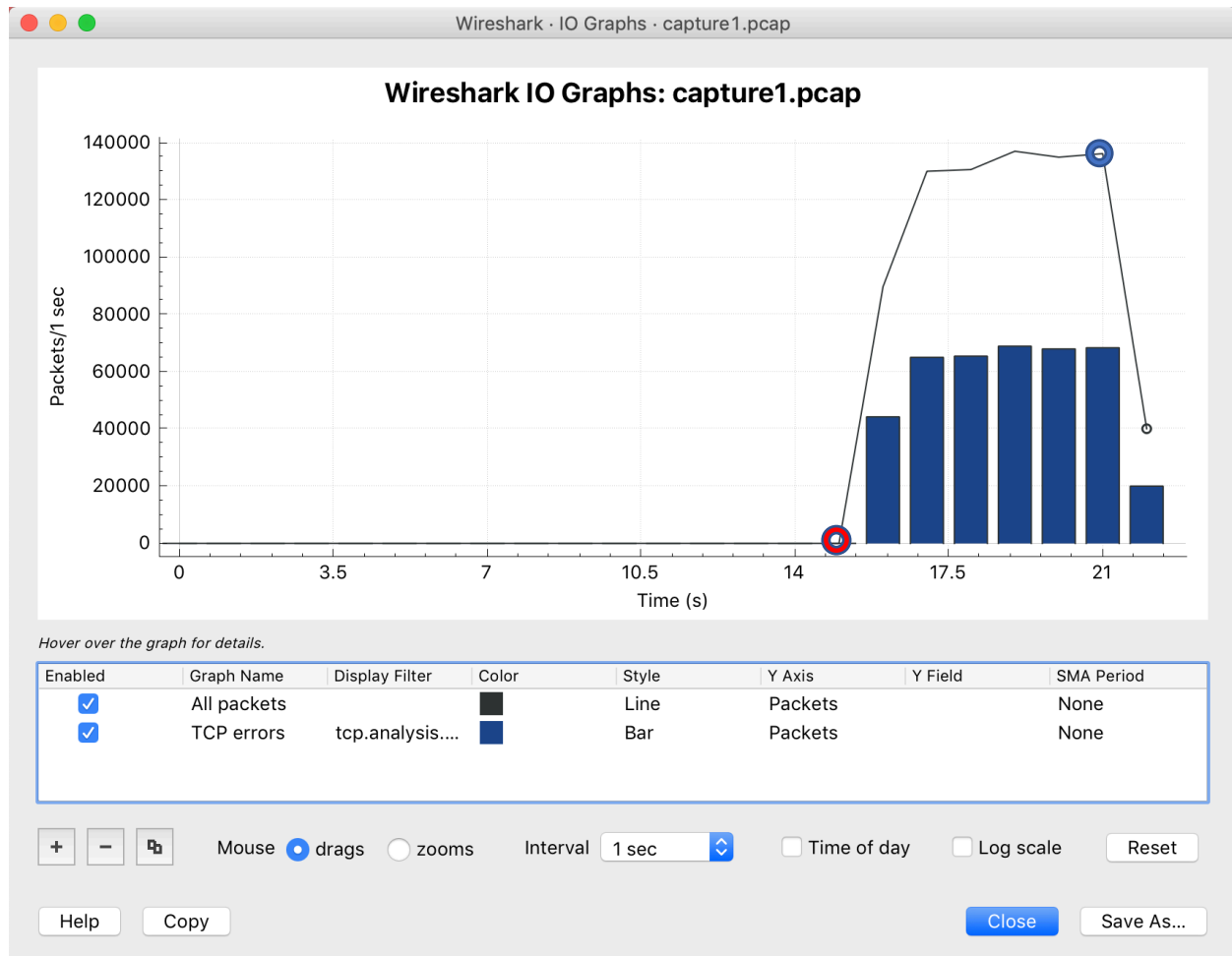
## Part 5

After completing all the steps in instruction, we get our capture1.pcap file:

```
[qiuyudeMacBook-Pro:~ qiuyu$ sftp -i ~/.ssh/id_geni_ssh_rsa -oPort=25042 yqiu19@pc1.instageni.idre.ucla.edu  
[Enter passphrase for key '/Users/qiuyu/.ssh/id_geni_ssh_rsa':  
Connected to yqiu19@pc1.instageni.idre.ucla.edu.  
sftp> mget capture1.pcap  
Fetching /users/yqiu19/capture1.pcap to capture1.pcap  
/users/yqiu19/capture1.pcap          100% 343MB 10.6MB/s 00:32  
sftp> █
```

## Part 6

1. This is the graph we get from wireshark:



2. From the very beginning to the red point, the traffic is almost 0. From the read point, attacker starts to conduct flood attack so the number of packets through the network increase. Finally, this attack terminate at blue point so packets through network decrease again. What's more, we the see the TCP error also increase during the DoS attack.

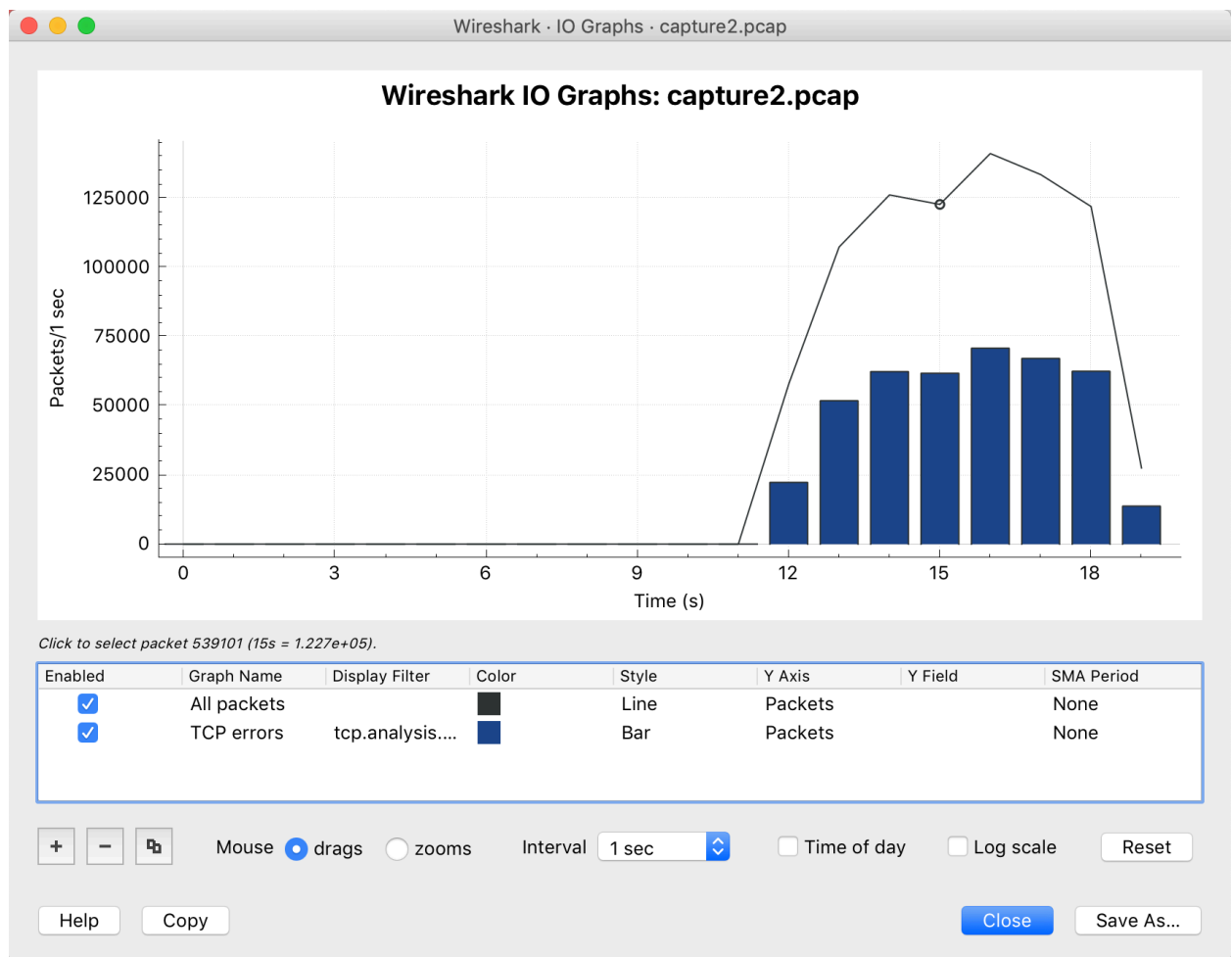
3. As the graph shown above, the attack end at blue point because the number of packets throughout the network and TCP errors decrease obviously after this point.

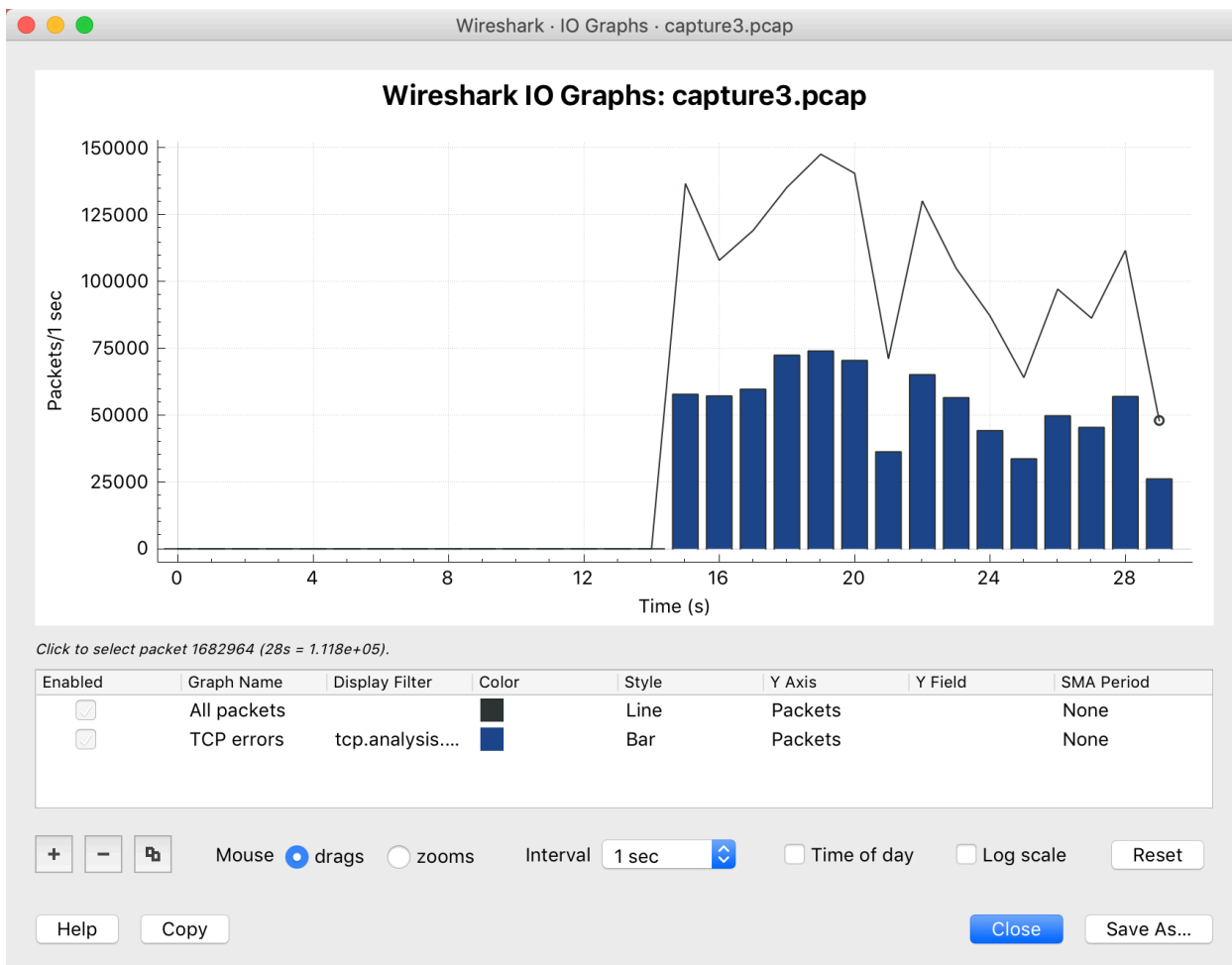


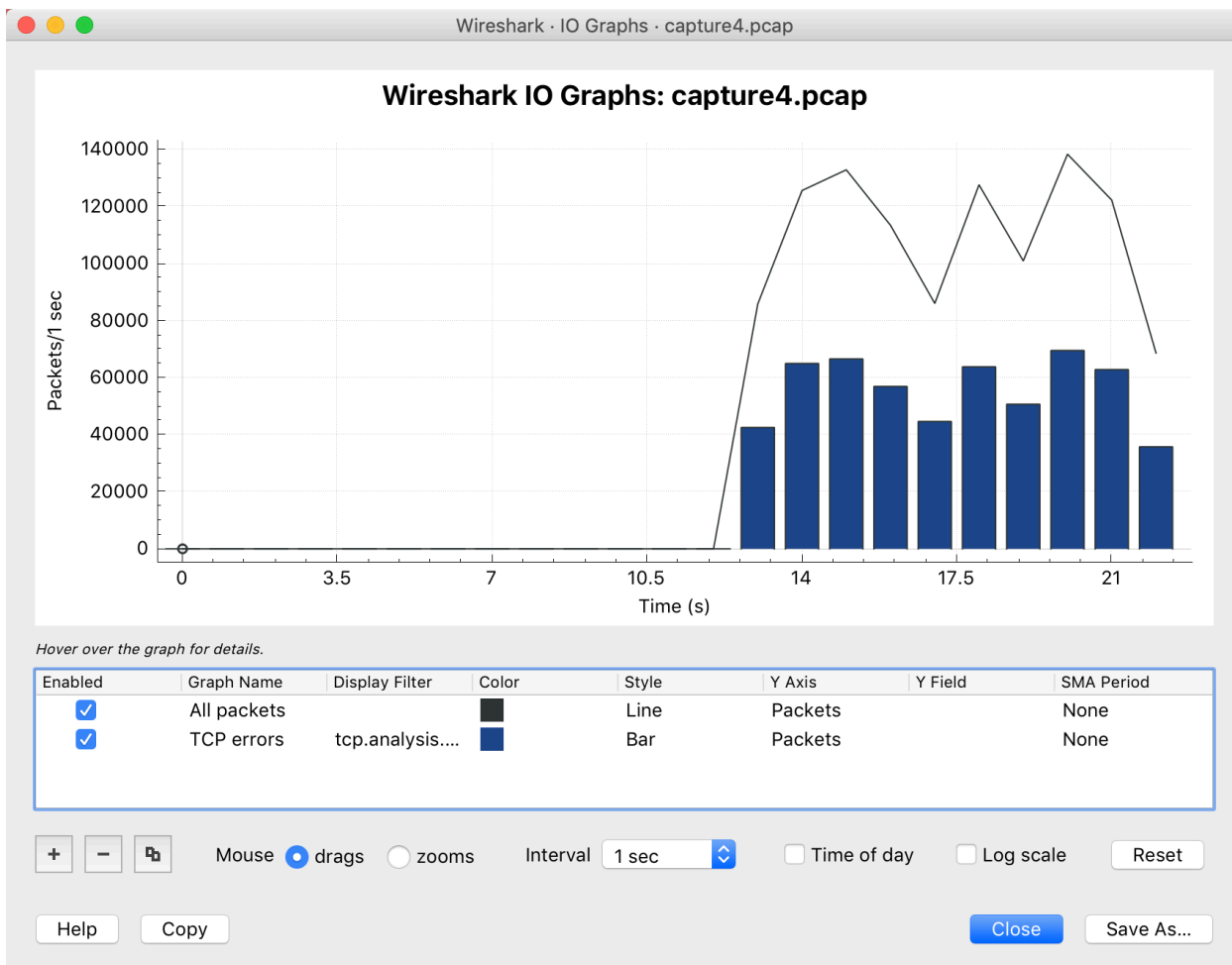
## Part 7

We repeat the experiment four times and get the following graphs. And then we find out a property called length which we think is packet size of these files.

What's more, we also find out the bandwidth and plot them by ourselves:







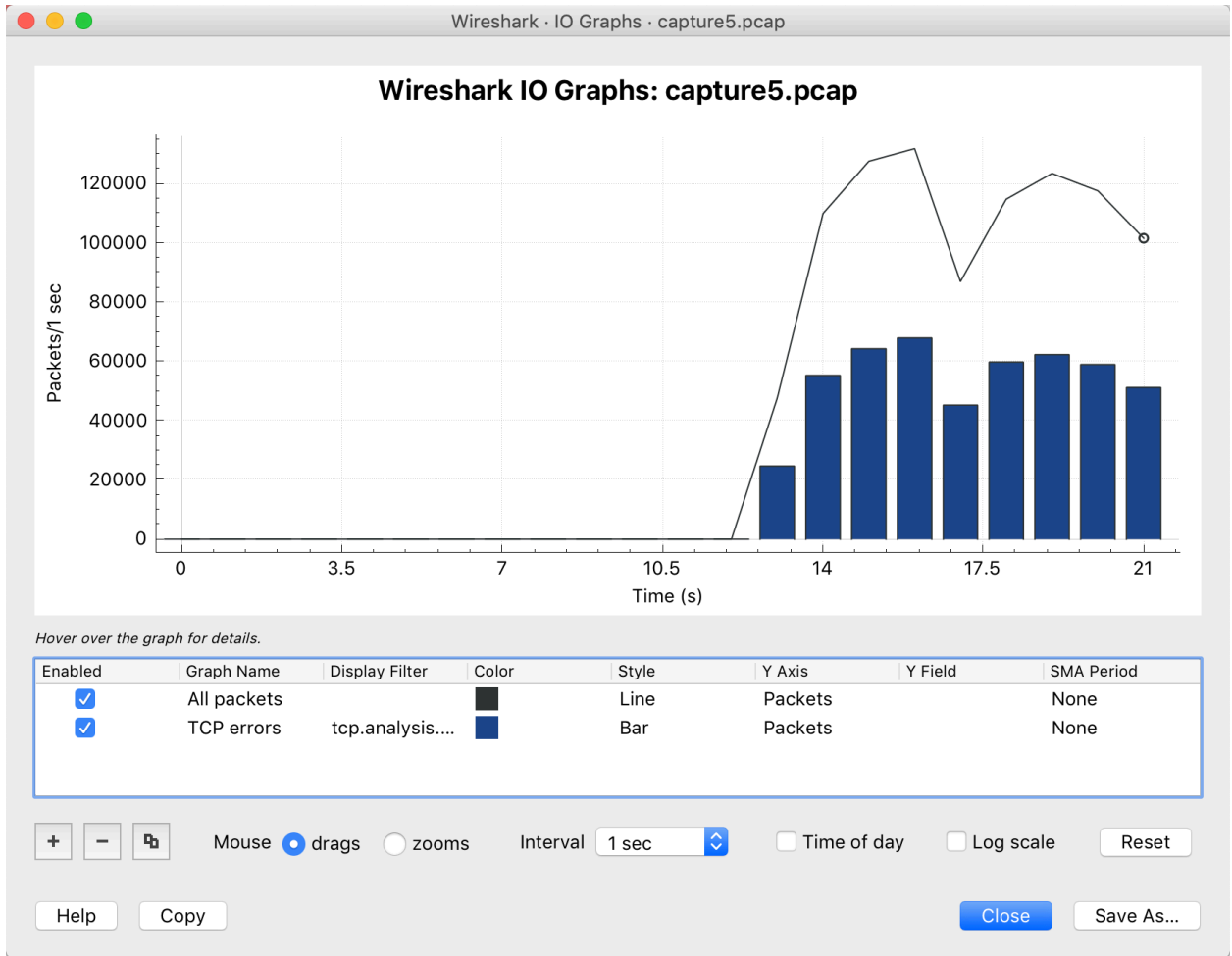


Table 1

No.	Packet Size (MB)	Average of total Packet Size	standard deviation of packet size	Bandwidth(Mbits/s)	Average Bandwidth	standard deviation of bandwidth
1	193	206.4	21.0428135	63	65.2	5.1672
2	189			72		
3	241			58		
4	211			67		
5	198			66		

