

Qianyi Feng
Asst 8

Exercise1:

Traceroute of 184.50.85.91:

```
[osboxes@osboxes:~$ sudo traceroute 184.50.85.91
traceroute to 184.50.85.91 (184.50.85.91), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  0.207 ms  0.104 ms  0.101 ms
 2 vl-4.uonet1-gw.uoregon.edu (128.223.4.2)  1.396 ms  1.309 ms  1.400 ms
 3 * * *
 4 * * 10.252.10.250 (10.252.10.250)  0.904 ms
 5 eugn-car1-gw.nero.net (207.98.68.181)  0.622 ms 10.252.253.129 (10.252.253.1
29)  0.831 ms 10.252.253.130 (10.252.253.130)  0.739 ms
 6 eugn-p2-gw.nero.net (207.98.64.202)  2.463 ms  3.027 ms 10.252.9.246 (10.252
.9.246)  0.880 ms
 7 eugn-car1-gw.nero.net (207.98.68.177)  0.637 ms eugn-core1-gw.nero.net (207.
98.64.195)  1.295 ms  1.193 ms
 8 5-1-4.bear1.Sacramento1.Level3.net (4.53.200.1)  10.479 ms  10.434 ms  10.79
0 ms
 9 eugn-core1-gw.nero.net (207.98.64.195)  1.107 ms  1.170 ms *
10 5-1-4.bear1.Sacramento1.Level3.net (4.53.200.1)  10.556 ms 4.68.63.214 (4.68
.63.214)  13.563 ms 5-1-4.bear1.Sacramento1.Level3.net (4.53.200.1)  10.527 ms
11 if-ae-1-2.tcore1.sqn-san-jose.as6453.net (63.243.205.1)  198.174 ms  197.761
ms 197.638 ms
12 if-ae-13-66.tcore2.lvw-los-angeles.as6453.net (63.243.205.15)  193.756 ms 4.
68.63.214 (4.68.63.214)  27.539 ms  13.453 ms
13 if-ae-7-2.tcore2.svw-singapore.as6453.net (180.87.15.25)  193.603 ms if-ae-1
-2.tcore1.sqn-san-jose.as6453.net (63.243.205.1)  197.348 ms if-ae-7-2.tcore2.sv
w-singapore.as6453.net (180.87.15.25)  193.608 ms
14 if-ae-18-2.tcore2.sv1-santa-clara.as6453.net (63.243.205.73)  196.377 ms if-
ae-13-2.tcore2.lvw-los-angeles.as6453.net (63.243.205.66)  192.666 ms if-ae-20-2
.tcore1.svq-singapore.as6453.net (180.87.96.21)  192.517 ms
15 if-ae-7-2.tcore2.svw-singapore.as6453.net (180.87.15.25)  193.891 ms 180.87.
96.26 (180.87.96.26)  420.996 ms if-et-5-2.hcore1.kv8-chiba.as6453.net (209.58.8
6.143)  119.169 ms
16 if-ae-7-2.tcore2.svw-singapore.as6453.net (180.87.15.25)  200.202 ms a184-50
-85-91.deploy.static.akamaitechnologies.com (184.50.85.91)  191.921 ms  192.088
ms
```

AS mapping:

Traceroute ip	AS	AS Name	Geo IP	ISP	Country	Region	City	Latitude	Longitude
10.0.2.2	NA	NA	128.223.222.133	University of Oregon	US	Oregon	Eugene	44.0385	-123.0610
128.223.4.2	3582	UONET - University of Oregon, US	128.23.4.2	University of Oregon	US	Oregon	Eugene	44.0385	-123.0610
10.252.10.250	NA	NA	128.223.222.139	University of Oregon	US	Oregon	Eugene	44.0385	-123.0610
207.98.68.181	3701	NERONET - Network for Education and Research in Oregon (NERO), US	207.98.68.181	Network for Education and Research in Oregon(NERO)	US	Oregon	Eugene	37.7510	-97.8220
207.98.64.202	3701	NERONET - Network for Education and Research in Oregon (NERO), US	207.98.64.202	Network for Education and Research in Oregon(NERO)	United States	Oregon	Eugene	37.7510	-97.8220

207.9 8.68. 177	3701	NERONET – Network for Education and Research in Oregon (NERO), US	207.9 8.68. 177	Network for Education and Research in Oregon(NERO)	US	Oregon	Eugene	37.7510	-97.8220
4.53. 200.1	3356	LEVEL3 – Level 3 Parent, LLC, US	4.53. 200.1	Level 3 Parent, LLC	US	Nevada	Smith	38.8087	-119.320
207.9 8.64. 195	3701	NERONET – Network for Education and Research in Oregon (NERO), US	207.9 8.64. 195	Network for Education and Research in Oregon(NERO)	United States	Oregon	Eugene	37.7510	-97.8220
4.53. 200.1	3356	LEVEL3 – Level 3 Parent, LLC, US	4.53. 200.1	Level 3 Parent, LLC	United States	Nevada	Smith	38.8087	-119.320
63.24 3.205 .1	6453	AS6453 – TATA COMMUNICATIONS (AMERICA) INC, US	63.24 3.205 .1	Tata Communications LTD	US	Illinois	Chicago	41.8500	-97.8220

63.24 3.205 .15	6453	AS6453 – TATA COMMUNICATIONS (AMERICA) INC, US	63.24 3.205 .15	Tata Communications LTD	US	California	San Jose	37.2297	-121.7865
180.8 7.15. 25	6453	AS6453 – TATA COMMUNICATIONS (AMERICA) INC, US	180.8 7.15. 25	Tata Communications LTD	Singapore	Singapore	Singapore	1.2897	103.8501
63.24 3.205 .73	6453	AS6453 – TATA COMMUNICATIONS (AMERICA) INC, US	63.24 3.205 .73	Tata Communications LTD	Japan	Chiba	Chiba	35.6000	140.1000
180.8 7.15. 25	6453	AS6453 – TATA COMMUNICATIONS (AMERICA) INC, US	180.8 7.15. 25	Tata Communications LTD	Singapore	Singapore	Singapore	1.2897	103.8501
180.8 7.15. 25	6453	AS6453 – TATA COMMUNICATIONS (AMERICA) INC, US	180.8 7.15. 25	Tata Communications LTD	Singapore	Singapore	Singapore	1.2897	103.8501

Traceroute of 8.8.8.8:

```
[osboxes@osboxes:~$ sudo traceroute 8.8.8.8
[sudo] password for osboxes:
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  0.080 ms  0.066 ms  0.061 ms
 2 vl-4.uonet2-gw.uoregon.edu (128.223.4.3)  0.662 ms  0.588 ms  0.528 ms
 3 * * *
 4 * * *
 5 10.252.253.130 (10.252.253.130)  0.866 ms 198.32.165.253 (198.32.165.253)  1
 2.551 ms 10.252.253.130 (10.252.253.130)  0.722 ms
 6 198.32.165.253 (198.32.165.253)  12.425 ms * 10.252.9.250 (10.252.9.250)  0.
805 ms
 7 * 198.32.165.253 (198.32.165.253)  12.323 ms *
 8 198.32.165.253 (198.32.165.253)  12.202 ms 108.170.242.81 (108.170.242.81)
13.141 ms *
 9 108.170.232.81 (108.170.232.81)  13.143 ms 108.170.242.81 (108.170.242.81)
13.286 ms 108.170.242.241 (108.170.242.241)  14.048 ms
10 google-public-dns-a.google.com (8.8.8.8)  13.223 ms 108.170.242.81 (108.170.
242.81)  13.112 ms 74.125.37.41 (74.125.37.41)  13.294 ms
osboxes@osboxes:~$ ]
```

Traceroute ip	AS	AS Name	Geo IP	ISP	Country	Region	City	Latitude	Longitude
10.0.2.2	NA	NA	128.223.222.130	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
128.23.4.3	3582	UONET - University of Oregon , US	128.23.4.3	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
10.252.253.130	NA	NA	128.223.222.130	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
198.32.165.253	10511	COUNTRY-INSURANCE - CC Services, Inc, US	198.32.165.253	CC Services Inc	US	Illinois	Chicago	41.9288	-88.9856
108.170.23.281	15169	GOOGLE - Google LLC, US	108.170.23.281	Google LLC	US	California	Mountain View	37.4060	-122.0789

8.8.8 .8	15169	GOOGLE - Google LLC, US	8.8.8.8	Google Llc	Google LLC	US	Californi a	Mountai n View	37.4060
-------------	-------	-------------------------------------	---------	---------------	---------------	----	----------------	-------------------	---------

Traceroute of 69.53.236.21:

```
[osboxes@osboxes:~$ sudo traceroute 69.53.236.21
[sudo] password for osboxes:
traceroute to 69.53.236.21 (69.53.236.21), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  0.168 ms  0.064 ms  0.076 ms
 2 vl-4.uonet1-gw.uoregon.edu (128.223.4.2)  0.581 ms  0.508 ms  0.442 ms
 3 * * *
 4 10.252.10.250 (10.252.10.250)  0.598 ms * 10.252.9.250 (10.252.9.250)  1.039
ms
 5 10.252.253.130 (10.252.253.130)  0.885 ms eugn-car1-gw.nero.net (207.98.68.1
77)  0.776 ms eugn-car1-gw.nero.net (207.98.68.181)  0.721 ms
 6 10.252.9.250 (10.252.9.250)  0.803 ms eugn-p1-gw.nero.net (207.98.64.200)  2
.536 ms  2.574 ms
 7 eugn-core1-gw.nero.net (207.98.64.193)  1.152 ms eugn-car1-gw.nero.net (207.
98.68.177)  0.635 ms eugn-core1-gw.nero.net (207.98.64.193)  1.042 ms
 8 eugn-p1-gw.nero.net (207.98.64.200)  3.259 ms  3.233 ms  3.145 ms
 9 eugn-core1-gw.nero.net (207.98.64.193)  1.265 ms * 1.649 ms
10 5-1-4.bear1.Sacramento1.Level3.net (4.53.200.1)  10.675 ms  10.487 ms  10.73
0 ms
11 po300.es04.sjc002.ix.nflxvideo.net (23.246.61.97)  13.361 ms * 13.545 ms
12 4.7.16.46 (4.7.16.46)  13.439 ms po306.es01.lax001.ix.nflxvideo.net (23.246.
61.223)  20.601 ms 4.7.16.46 (4.7.16.46)  13.377 ms
13 po300.es04.sjc002.ix.nflxvideo.net (23.246.61.97)  13.369 ms po300.es02.lax0
01.ix.nflxvideo.net (23.246.60.79)  21.129 ms  20.936 ms
14 po305.es02.dfw001.ix.nflxvideo.net (23.246.61.95)  51.032 ms po306.es01.lax0
01.ix.nflxvideo.net (23.246.61.223)  20.709 ms  20.602 ms
15 * po300.es02.lax001.ix.nflxvideo.net (23.246.60.79)  21.063 ms *
16 po305.es02.dfw001.ix.nflxvideo.net (23.246.61.95)  51.244 ms  51.157 ms *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
osboxes@osboxes:~$ ]]
```

Traceroute ip	AS	AS Name	Geo IP	ISP	Country	Region	City	Latitude	Longitude
10.0.2.2	NA	NA	128.223.222.130	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
128.223.4.2	3582	UONET - University of Oregon, US	128.223.4.2	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
10.252.9.246	NA	NA	128.223.222.139	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
10.252.253.130	NA	NA	128.223.222.139	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
10.252.9.246	NA	NA	128.223.222.139	University of Oregon	US	Oregon	Eugene	44.0361	-123.0524
207.98.68.181	3701	NERONE T - Network for Education and Research in Oregon (NERO), US	207.98.68.181	Oregon Exchange	US	Oregon	Eugene	44.0361	-123.0524
4.53.200.1	3356	LEVEL3 - Level 3 Parent, LLC	4.53.200.1	Level 3 Parent, LLC	US	Nevada	Smith	38.8087	-119.3200

23.24 6.61. 97	2906	AS-SSI - Netfli x Stream ing Servic es Inc., US	23.24 6.61. 97	Netflix Streami ng Services , Inc.	US	Delawar e	Wilming ton	39.7380	-75.5504
23.24 6.61. 223	2906	AS-SSI - Netfli x Stream ing Servic es Inc., US	23.24 6.61. 223	Netflix Streami ng Services , Inc.	US	Delawar e	Wilming ton	39.7380	-75.5504
23.24 6.60. 79	2906	AS-SSI - Netfli x Stream ing Servic es Inc., US	23.24 6.60. 79	Netflix Streami ng Services , Inc.	US	Delawar e	Wilming ton	39.7380	-75.5504
23.24 6.61. 223	2906	AS-SSI - Netfli x Stream ing Servic es Inc., US	23.24 6.61. 223	Netflix Streami ng Services , Inc.	US	Delawar e	Wilming ton	39.7380	-75.5504

23.24 6.60. 79	2906	AS-SSI - Netfli x Stream ing Servic es Inc., US	23.24 6.60. 79	Netflix Streami ng Services , Inc.	US	Delawar e	Wilming ton	39.7380	-75.5504
23.24 6.61. 95	2906	AS-SSI - Netfli x Stream ing Servic es Inc., US	23.24 6.60. 95	Netflix Streami ng Services , Inc.	US	Delawar e	Wilming ton	39.7380	-75.5504

Exercise 2:

From the ix-dev:
Typing: iperf3 -s

```
-----  
Server listening on 5201  
-----  
Accepted connection from 10.109.42.48, port 63048  
[ 5] local 128.223.4.39 port 5201 connected to 10.109.42.48 port 63049  
[ ID] Interval Transfer Bitrate  
[ 5] 0.00-1.00 sec 62.1 MBytes 521 Mbits/sec  
[ 5] 1.00-2.00 sec 75.3 MBytes 631 Mbits/sec  
[ 5] 2.00-3.00 sec 80.8 MBytes 678 Mbits/sec  
[ 5] 3.00-4.00 sec 76.9 MBytes 645 Mbits/sec  
[ 5] 4.00-5.00 sec 74.0 MBytes 621 Mbits/sec  
[ 5] 5.00-6.00 sec 83.1 MBytes 697 Mbits/sec  
[ 5] 6.00-7.00 sec 81.5 MBytes 683 Mbits/sec  
[ 5] 7.00-8.00 sec 83.0 MBytes 696 Mbits/sec  
[ 5] 8.00-9.00 sec 80.6 MBytes 676 Mbits/sec  
[ 5] 9.00-10.00 sec 82.5 MBytes 692 Mbits/sec  
[ 5] 10.00-10.01 sec 679 KBytes 754 Mbits/sec  
-----  
[ ID] Interval Transfer Bitrate  
[ 5] 0.00-10.01 sec 780 MBytes 654 Mbits/sec  
-----  
Server listening on 5201  
-----
```

From my computer at UO:

Typing: iperf3 -c 128.223.4.39 -d

The ip address is the ip address of my ix-dev account.

```
interval_len 0.999522 bytes_transferred 866441/8  
interval forces keep  
[ 5] 9.00-10.00 sec 82.6 MBytes 693 Mbits/sec  
-----  
[ ID] Interval Transfer Bitrate  
[ 5] 0.00-10.00 sec 781 MBytes 655 Mbits/sec  
[ 5] 0.00-10.01 sec 780 MBytes 654 Mbits/sec  
-----  
iperf Done.  
-----
```

At home:

```
,  
interval_len 0.997297 bytes_transferred 6703408  
interval forces keep  
[ 5] 9.00-10.00 sec 6.39 MBytes 53.8 Mbits/sec  
-----  
[ ID] Interval Transfer Bitrate  
[ 5] 0.00-10.00 sec 25.3 MBytes 21.2 Mbits/sec  
[ 5] 0.00-10.04 sec 24.9 MBytes 20.8 Mbits/sec  
-----  
iperf Done.  
-----
```

```
Last login: Thu Feb 28 15:00:55 2019 from 2607:8400:26c2:2:b8d6:56f0:8f2e:9de5
[qfeng@ix-dev: ~ 1$ iperf3 -s
```

```
-----
Server listening on 5201
-----
Accepted connection from 216.106.151.218, port 51375
[ 5] local 128.223.4.39 port 5201 connected to 216.106.151.218 port 51376
[ ID] Interval Transfer Bitrate
[ 5] 0.00-1.00 sec 2.46 MBytes 20.7 Mbits/sec
[ 5] 1.00-2.00 sec 2.51 MBytes 21.0 Mbits/sec
[ 5] 2.00-3.00 sec 1.11 MBytes 9.35 Mbits/sec
[ 5] 3.00-4.00 sec 178 KBytes 1.46 Mbits/sec
[ 5] 4.00-5.00 sec 1007 KBytes 8.25 Mbits/sec
[ 5] 5.00-6.00 sec 1.49 MBytes 12.5 Mbits/sec
[ 5] 6.00-7.00 sec 8.24 MBytes 69.1 Mbits/sec
[ 5] 7.00-8.00 sec 165 KBytes 1.36 Mbits/sec
[ 5] 8.00-9.00 sec 1.37 MBytes 11.5 Mbits/sec
[ 5] 9.00-10.00 sec 6.11 MBytes 51.2 Mbits/sec
[ 5] 10.00-10.04 sec 341 KBytes 64.1 Mbits/sec
-----
[ ID] Interval Transfer Bitrate
[ 5] 0.00-10.04 sec 24.9 MBytes 20.8 Mbits/sec
                                         receiver
-----
Server listening on 5201
```

Conclusion: the throughput in UO is much more larger than at home.

Exercise 3:

Command: sudo tcpdump src host youtube.com

(When I test the command in Des, it needs to take more than one hour for the reply after I type the command, therefore I redo the test at home.

From the screenshot, there are 56 packets received in one minute(22:11) and the total length is 42416, length/sec is $42416/60=706.933$ Byte/second.

```
fenggianyideMacBook-Pro:- fenggianyi$ sudo tcpcdump src host youtube.com
Password:
tcpcdump: data link type PKTAP
tcpcdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ptkap, link-type PKTAP (Apple_DL_PKTAP), capture size 262144 bytes
22:09:40.528889 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 3529464777 win 244, options [nop,nop,TS val 1532681032 ect 1639156299], length 0
22:09:40.528889 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 3529464808 win 244, options [nop,nop,TS val 1532681032 ect 1639156299], length 0
22:09:40.652341 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 3529464839 win 244, options [nop,nop,TS val 1532681037 ect 1639156232], length 0
22:10:34.452891 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [F.], seq 3793263094, ack 1377897348, win 244, options [nop,nop,TS val 1532734953 ect 1638968014], length 0
22:10:34.452891 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 4294967233|0, ack 1, win 244, options [nop,nop,TS val 1532734953 ect 1638968014], length 63
22:10:34.455283 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [R.], seq 3793263083, win 0, length 0
22:10:34.455308 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [R.], seq 3793263083, win 0, length 0
22:10:34.462726 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [R.], seq 3793263083, win 0, length 0
22:10:34.462726 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [R.], seq 3793263083, win 0, length 0
22:11:04.247888 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 518, win 244, options [nop,nop,TS val 2687464388 ect 1639235898], length 0
22:11:04.255250 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., seq 114124, ack 518, win 244, options [nop,nop,TS val 2687464396 ect 1639235898], length 1418
22:11:04.255512 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., seq 141972837, ack 518, win 244, options [nop,nop,TS val 2687464396 ect 1639235898], length 1418
22:11:04.255688 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 283736364, ack 518, win 244, options [nop,nop,TS val 2687464396 ect 1639235898], length 847
22:11:04.292980 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 368437375, ack 611, win 244, options [nop,nop,TS val 2687464433 ect 1639235891], length 51
22:11:04.292997 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 368437380, ack 611, win 244, options [nop,nop,TS val 2687464433 ect 1639235891], length 51
22:11:04.293004 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 368437381, ack 611, win 244, options [nop,nop,TS val 2687464433 ect 1639235891], length 69
22:11:04.293004 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 3793263083, ack 611, win 244, options [nop,nop,TS val 2687464444 ect 1639235891], length 69
22:11:04.385845 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 38843842, ack 714, win 244, options [nop,nop,TS val 2687464445 ect 1639235893], length 38
22:11:04.385845 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 38843842, ack 714, win 244, options [nop,nop,TS val 2687464445 ect 1639235893], length 38
22:11:04.412778 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 384240868, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 244
22:11:04.412862 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 486845584, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.413194 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 55694/622, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.413194 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 55694/622, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.414244 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 83446360, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.414249 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 978511176, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.414343 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 1117612594, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.414369 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 112594/14812, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.414211 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 1412115430, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.414356 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 154393/16848, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.414356 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 154393/16848, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.415753 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 1964382738, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.415753 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 1964382738, ack 1064, win 244, options [nop,nop,TS val 2687464552 ect 1639235962], length 1418
22:11:04.428599 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 28739/28777, ack 1064, win 244, options [nop,nop,TS val 2687464561 ect 1639235962], length 38
22:11:04.428599 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [P.], seq 287739/28283, ack 1064, win 244, options [nop,nop,TS val 2687464562 ect 1639235962], length 46
22:11:04.471462 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 1118, win 244, options [nop,nop,TS val 2687466612 ect 1639236075], length 0
22:11:04.489497 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 1278, win 244, options [nop,nop,TS val 2687467117 ect 1639236588], length 0
22:11:04.489497 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 2803/28911, ack 1278, win 244, options [nop,nop,TS val 2687467117 ect 1639236588], length 88
22:11:04.4864376 IP se398101.in-f14.1e108.net.http> : 180..64.2.24.63106: Flags [., ack 1324, win 244, options [nop,nop,TS val 2687467186 ect 1639236688], length 0
```

22:11:85 0x463716 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63160: Flags [...], ack 1324, win 248, options [nop,nop,TS val 268747617689 ecr 1639283608], length 0
22:11:85 0x466228 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [S..], seq 1369477017, ack 190553959, win 60192, options [mss 1380,sackOK,TS val 3911300277 ecr 1639285824,nop,wscale 8], length 0
22:11:54 0x476732 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], ack 256, win 240, options [nop,nop,TS val 39113002829 ecr 1639285835], length 0
22:11:54 0x486777 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 114349, ack 256, win 240, options [nop,nop,TS val 3911300298 ecr 1639285835], length 1418
22:11:54 0x487008 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 14194:2837, ack 256, win 240, options [nop,nop,TS val 3911300298 ecr 1639285835], length 1418
22:11:54 0x488369 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 2837:3157, ack 256, win 240, options [nop,nop,TS val 3911300298 ecr 1639285835], length 328
22:11:54 0x511000 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 32086:3277, ack 349, win 240, options [nop,nop,TS val 3911300321 ecr 1639285856], length 69
22:11:54 0x511001 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 32787:3307, ack 349, win 240, options [nop,nop,TS val 3911300321 ecr 1639285856], length 51
22:11:54 0x511002 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 33078:3337, ack 349, win 240, options [nop,nop,TS val 3911300321 ecr 1639285856], length 51
22:11:54 0x514200 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 494, win 240, options [nop,nop,TS val 3911300334 ecr 1639285873], length 0
22:11:54 0x515084 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 3277:3335, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 38
22:11:54 0x525015 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 3315:3611, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 296
22:11:54 0x525340 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 3611:5029, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 1418
22:11:54 0x525726 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 5029:6447, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 1418
22:11:54 0x525733 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 6447:7865, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 1418
22:11:54 0x525736 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 7865:9283, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 1418
22:11:54 0x526693 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 9283:10701, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 1418
22:11:54 0x527261 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 10701:12119, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 1418
22:11:54 0x527266 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 12119:13537, ack 693, win 244, options [nop,nop,TS val 3911300334 ecr 1639285873], length 1418
22:11:54 0x527788 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 13537:14949, ack 731, win 244, options [nop,nop,TS val 3911300337 ecr 1639285873], length 1418
22:11:54 0x527789 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 14949:16371, ack 731, win 244, options [nop,nop,TS val 3911300337 ecr 1639285873], length 1418
22:11:54 0x527796 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 16371:17701, ack 731, win 244, options [nop,nop,TS val 3911300337 ecr 1639285873], length 1418
22:11:54 0x527797 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 17701:19289, ack 731, win 244, options [nop,nop,TS val 3911300338 ecr 1639285873], length 1418
22:11:54 0x527919 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 19289:20267, ack 731, win 244, options [nop,nop,TS val 3911300338 ecr 1639285873], length 1418
22:11:54 0x527923 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], seq 20267:21595, ack 731, win 244, options [nop,nop,TS val 3911300338 ecr 1639285873], length 968
22:11:54 0x580199 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], ack 777, win 244, options [nop,nop,TS val 3911300332 ecr 1639285873], length 0
22:11:54 0x581464 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], ack 777, win 244, options [nop,nop,TS val 3911300339 ecr 1639285932,nop,sack 1 (731:777)], length 0
22:11:56 0x593766 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], ack 888, win 244, options [nop,nop,TS val 3911302752 ecr 1639288182], length 0
22:11:56 0x593892 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [F..], seq 21595, ack 888, win 244, options [nop,nop,TS val 3911302752 ecr 1639288182], length 0
22:11:56 0x594355 IP se30s01-in-f14.le100.net_https > 100.64.2.24.63179: Flags [...], ack 889, win 244, options [nop,nop,TS val 3911302756 ecr 1639288185], length 0
e 8], length 0

22:12:23.846000 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [S], seq 3566948612, ack 3978507426, win 6192, options [mss 1380,sackOK,TS val 2687545979 ecr 1639314898,nop,wscal 8], length 8
22:12:23.854970 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [., ack 256, win 240, options [nop,nop,TS val 2687545998 ecr 1639314899], length 8
22:12:23.862713 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [., seq 11419, ack 256, win 240, options [nop,nop,TS val 2687545998 ecr 1639314899], length 1418
22:12:23.862718 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [., seq 14192837, ack 256, win 240, options [nop,nop,TS val 2687545998 ecr 1639314899], length 1418
22:12:23.864396 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 28371362, ack 256, win 240, options [nop,nop,TS val 2687545998 ecr 1639314899], length 325
22:12:23.899012 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 3162_3213, ack 349, win 240, options [nop,nop,TS val 2687546484 ecr 1639314943], length 51
22:12:23.999199 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 3123_3282, ack 349, win 240, options [nop,nop,TS val 2687546484 ecr 1639314943], length 69
22:12:23.923658 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], ack 452, win 240, options [nop,nop,TS val 2687546059 ecr 1639314956], length 8
22:12:23.923887 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 3282_3320, ack 494, win 240, options [nop,nop,TS val 2687546059 ecr 1639314956], length 38
22:12:23.924255 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 3328_3616, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 296
22:12:23.924560 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 3616_5642, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.924561 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 3616_5642, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.925407 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 6834_6452, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.925410 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 7870_7898, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.926331 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 9298_10766, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.926332 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 1876_12124, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.926436 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 12124_13542, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.927750 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 13542_14968, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.928121 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 14968_16378, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.928124 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 16378_17796, ack 693, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.928125 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 17796_19214, ack 731, win 240, options [nop,nop,TS val 2687546068 ecr 1639314956], length 1418
22:12:23.928517 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 19214_20632, ack 731, win 240, options [nop,nop,TS val 2687546061 ecr 1639314956], length 1418
22:12:23.928517 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 20632_21690, ack 731, win 240, options [nop,nop,TS val 2687546061 ecr 1639314956], length 968
22:12:23.987279 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], ack 777, win 244, options [nop,nop,TS val 2687546117 ecr 1639314973], length 8
22:12:23.999732 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], ack 777, win 244, options [nop,nop,TS val 2687546126 ecr 1639315018,nop,sack 1 (731:777)], length 8
22:12:26.071630 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 888, win 244, options [nop,nop,TS val 2687546126 ecr 1639315018], length 8
22:12:27.075699 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 21680_21681, ack 888, win 244, options [nop,nop,TS val 2687546126 ecr 1639317681], length 8
22:13:40.730867 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 1385_1395, ack 248, win 240, options [nop,nop,TS val 2687622842 ecr 1639391331], length 8
22:13:40.731134 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 20911_1355, ack 248, win 240, options [nop,nop,TS val 2687622842 ecr 16393921331], length 8
22:13:40.731235 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63211: Flags [P..], seq 1355_1356, ack 248, win 240, options [nop,nop,TS val 2687622842 ecr 16393931331], length 8
22:51.81.812881 IP se30s01-in-f14.ie100.net.https > 100.64.2.24.63254: Flags [S..], seq 2910065068, ack 2725173431, win 6192, options [mss 1380,sackOK,TS val 3911537606 ecr 1639521806,nop,wscal 8], length 8, bytes=8

Avg:

22:09: 0 byte/sec

22:10: 1.05 byte/sec

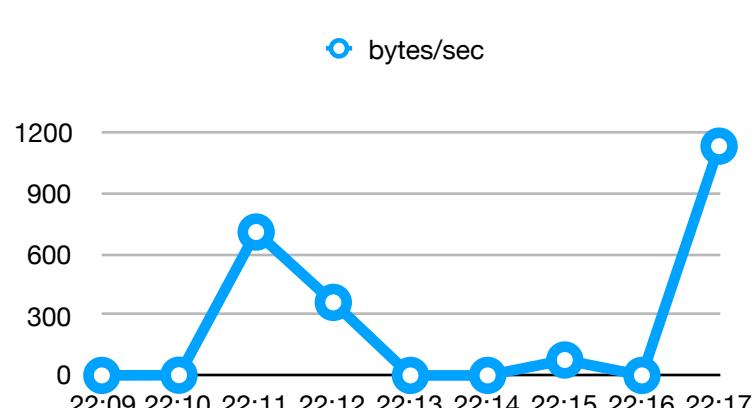
22:11: 706.933 byte/sec

22:12: 359.983 by

22:13: 0 byte/sec

22:15: 75.9 byte/sec

22:17: 1130.32 byte/sec



Exercise 4:
detect_log, attack and detect bash files are in the week8 folder

MAC address of each attackers:

Shikun(Fri 9:00): 08:00:27:d9:bd:5c
Jasper(Fri 11:00): 08:00:27:56:2c:b9
Quinn(Fri 14:00): 08:00:27:5b:c8:2d
Franklin(Fri 14:30): 08:00:27:0b:0d:3a
Luke(Fri 15:30): 08:00:27:82:be:67
Erric(Sat 9:30): 08:00:27:54:69:e7

Fri Mar 1 17:11:06 UTC 2019
08:00:27:d9:bd:5c

Fri Mar 1 17:32:05 UTC 2019
08:00:27:d9:bd:5c

Fri Mar 1 19:01:13 UTC 2019
08:00:27:56:2c:b9

Fri Mar 1 22:02:02 UTC 2019
08:00:27:56:2c:b9

Fri Mar 1 22:03:13 UTC 2019
08:00:27:5b:c8:2d

Fri Mar 1 22:04:24 UTC 2019

Fri Mar 1 22:31:38 UTC 2019
08:00:27:5b:c8:2d

Fri Mar 1 22:32:49 UTC 2019
08:00:27:0b:0d:3a

Fri Mar 1 23:29:38 UTC 2019
08:00:27:0b:0d:3a

Fri Mar 1 23:30:49 UTC 2019
08:00:27:82:be:67

Sat Mar 2 01:45:45 UTC 2019
08:00:27:82:be:67

Sat Mar 2 17:31:36 UTC 2019
08:00:27:54:69:e7

My attack: