

LAB



Compute the ratio of UDP packets and flows in the traffic

```
nfdump -r flows.nfcapd -s proto
```

Top 10 Protocol ordered by -:

Date first seen	Duration	Proto	Protocol	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2015-11-20 15:30:00.000	2100.999	UDP	17	6.2 M(77.7)	150.7 M(45.2)	96.9 G(37.7)	71731	369.1 M	643
2015-11-20 15:30:00.000	2100.998	TCP	6	1.6 M(20.4)	181.4 M(54.4)	159.0 G(61.9)	86338	605.4 M	876
2015-11-20 15:30:00.026	2100.934	ICMP	1	138972(1.7)	408257(0.1)	130.2 M(0.1)	194	495876	318
2015-11-20 15:30:00.168	2100.709	ICMP6	58	10591(0.1)	22164(0.0)	2.3 M(0.0)	10	8927	105
2015-11-20 15:30:00.341	2100.514	IPv6	41	3418(0.0)	347579(0.1)	181.8 M(0.1)	165	692367	523
2015-11-20 15:30:20.350	2077.562	ESP	50	303(0.0)	728412(0.2)	544.2 M(0.2)	350	2.1 M	747
2015-11-20 15:30:07.508	2091.023	Frag6	44	299(0.0)	1395(0.0)	1.4 M(0.0)	0	5267	987
2015-11-20 15:30:24.891	2048.222	SCTP	132	107(0.0)	25628(0.0)	1.6 M(0.0)	12	6438	64
2015-11-20 15:30:07.762	2075.365	IGMP	2	94(0.0)	199(0.0)	7520(0.0)	0	28	37
2015-11-20 15:30:47.831	2037.595	PIM	103	56(0.0)	977(0.0)	62409(0.0)	0	245	63

IP addresses anonymised

Summary: total flows: 7975525, total bytes: 256789591964, total packets: 333641465, avg bps: 977780920, avg pps: 158801, avg bpp: 769

Time window: 2015-11-20 15:30:00 - 2015-11-20 16:05:00

Total flows processed: 7975525, Blocks skipped: 0, Bytes read: 482516584

Count the hosts actively communicating from MU network

```
nfdump -r flows.nfcapd "src net  
83.187.0.0/16 " -A srcip -q | wc -l  
7781
```

Find most the web server most visited by users from MU network

```
nfdump -r flows.nfcapd "src net
83.187.0.0/16 and (dst port 443 or dst
port 80)" -s dstip/flows
```

Top 10 Dst IP Addr ordered by flows:

Date first seen	Duration	Proto	Dst IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2015-11-20 15:30:00.211	2100.492	any	183.13.67.26	12836(3.2)	313959(0.9)	97.5 M(2.1)	149	371157	310
2015-11-20 15:30:00.228	2100.683	any	183.13.67.31	9675(2.4)	577547(1.7)	52.0 M(1.1)	274	197857	89
2015-11-20 15:30:00.206	2100.448	any	83.187.49.10	8645(2.2)	209230(0.6)	35.2 M(0.8)	99	134109	168
2015-11-20 15:30:00.081	2100.602	any	183.13.67.25	5719(1.4)	87503(0.3)	8.4 M(0.2)	41	31892	95
2015-11-20 15:30:00.847	2099.964	any	183.13.67.36	5533(1.4)	428883(1.3)	159.9 M(3.5)	204	609047	372
2015-11-20 15:30:00.175	2100.516	any	47.197.47.167	4829(1.2)	61243(0.2)	11.8 M(0.3)	29	44781	191
2015-11-20 15:30:00.175	2100.360	any	47.197.47.163	3779(0.9)	175366(0.5)	28.7 M(0.6)	83	109336	163
2015-11-20 15:30:00.346	2099.816	any	183.13.67.37	3459(0.9)	16837(0.0)	3.0 M(0.1)	8	11339	176
2015-11-20 15:30:00.223	2099.901	any	135.141.94.209	2979(0.7)	141495(0.4)	13.4 M(0.3)	67	51227	95
2015-11-20 15:30:00.720	2088.200	any	206.132.167.53	2646(0.7)	42392(0.1)	6.0 M(0.1)	20	22817	140

IP addresses anonymised

Summary: total flows: 397904, total bytes: 4628663056, total packets: 33804233, avg bps: 17624634, avg pps: 16089, avg bpp: 136

Time window: 2015-11-20 15:30:00 - 2015-11-20 16:05:00

Total flows processed: 7975525, Blocks skipped: 0, Bytes read: 482516584

Find how many hosts from MU network has accessed the web on 60.182.41.219:80

```
nfdump -r flows.nfcapd "src net  
83.187.0.0/16 and dst ip 60.182.41.219  
and dst port 80" -A srcip -q | wc -l  
225
```

Find a horizontal scan

```
nfdump -r flows.nfcapd "dst port 22" -s
srcip/flows
```

Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2015-11-20 15:32:55.044	0.640	any	250.65.164.35	1911(14.9)	1911(0.4)	91728(0.1)	2985	1.1 M	48
2015-11-20 16:00:32.151	268.755	any	149.66.244.166	869(6.8)	13819(2.7)	1.9 M(1.3)	51	55763	135
2015-11-20 15:30:00.371	2100.202	any	254.192.34.177	807(6.3)	8877(1.7)	875595(0.6)	4	3335	98
2015-11-20 15:30:03.399	2091.705	any	172.59.185.229	624(4.9)	21562(4.2)	10.5 M(7.1)	10	39984	484
2015-11-20 15:30:00.932	2097.892	any	172.59.185.230	624(4.9)	21607(4.2)	10.5 M(7.1)	10	40071	486
2015-11-20 15:30:00.144	2097.328	any	172.59.185.226	623(4.9)	21566(4.2)	10.5 M(7.1)	10	40098	487
2015-11-20 15:30:05.238	2090.838	any	172.59.185.224	622(4.8)	21482(4.2)	10.5 M(7.1)	10	40137	488
2015-11-20 15:30:06.131	2089.995	any	172.59.185.225	622(4.8)	21501(4.2)	10.5 M(7.1)	10	40240	488
2015-11-20 15:30:04.890	2091.128	any	172.59.185.231	622(4.8)	21567(4.2)	10.6 M(7.2)	10	40490	490
2015-11-20 15:30:04.468	2090.862	any	172.59.185.232	622(4.8)	21479(4.2)	10.5 M(7.1)	10	40033	487

IP addresses anonymised

Summary: total flows: 12841, total bytes: 147070568, total packets: 511972, avg bps: 560065, avg pps: 243, avg bpp: 287

Time window: 2015-11-20 15:30:00 - 2015-11-20 16:05:00

Total flows processed: 7975525, Blocks skipped: 0, Bytes read: 482516584

2015-11-20 15:32:55.445	0.000	TCP	250.65.164.35:9312	->	83.187.159.50:22	1	48	1
2015-11-20 15:32:55.158	0.000	TCP	250.65.164.35:9312	->	83.187.73.59:22	1	48	1
2015-11-20 15:32:55.261	0.000	TCP	250.65.164.35:9312	->	83.187.63.114:22	1	48	1
2015-11-20 15:32:55.164	0.000	TCP	250.65.164.35:9312	->	83.187.64.150:22	1	48	1
2015-11-20 15:32:55.475	0.000	TCP	250.65.164.35:9312	->	83.187.144.225:22	1	48	1
2015-11-20 15:32:55.189	0.000	TCP	250.65.164.35:9312	->	83.187.64.253:22	1	48	1
2015-11-20 15:32:55.468	0.000	TCP	250.65.164.35:9312	->	83.187.154.244:22	1	48	1
2015-11-20 15:32:55.139	0.000	TCP	250.65.164.35:9312	->	83.187.63.2:22	1	48	1
2015-11-20 15:32:55.582	0.000	TCP	250.65.164.35:9312	->	83.187.148.9:22	1	48	1
2015-11-20 15:32:55.579	0.000	TCP	250.65.164.35:9312	->	83.187.148.123:22	1	48	1
2015-11-20 15:32:55.173	0.000	TCP	250.65.164.35:9312	->	83.187.67.215:22	1	48	1
2015-11-20 15:32:55.162	0.000	TCP	250.65.164.35:9312	->	83.187.9.167:22	1	48	1
2015-11-20 15:32:55.239	0.000	TCP	250.65.164.35:9312	->	83.187.104.12:22	1	48	1
2015-11-20 15:32:55.387	0.000	TCP	250.65.164.35:9312	->	83.187.67.131:22	1	48	1
2015-11-20 15:32:55.054	0.000	TCP	250.65.164.35:9312	->	83.187.9.192:22	1	48	1
2015-11-20 15:32:55.490	0.000	TCP	250.65.164.35:9312	->	83.187.148.70:22	1	48	1
2015-11-20 15:32:55.579	0.000	TCP	250.65.164.35:9312	->	83.187.148.35:22	1	48	1
2015-11-20 15:32:55.058	0.000	TCP	250.65.164.35:9312	->	83.187.9.253:22	1	48	1
2015-11-20 15:32:55.175	0.000	TCP	250.65.164.35:9312	->	83.187.67.168:22	1	48	1
2015-11-20 15:32:55.051	0.000	TCP	250.65.164.35:9312	->	83.187.9.159:22	1	48	1
2015-11-20 15:32:55.190	0.000	TCP	250.65.164.35:9312	->	83.187.67.244:22	1	48	1
2015-11-20 15:32:55.280	0.000	TCP	250.65.164.35:9312	->	83.187.69.4:22	1	48	1
2015-11-20 15:32:55.564	0.000	TCP	250.65.164.35:9312	->	83.187.158.210:22	1	48	1
2015-11-20 15:32:55.561	0.000	TCP	250.65.164.35:9312	->	83.187.158.137:22	1	48	1
2015-11-20 15:32:55.264	0.000	TCP	250.65.164.35:9312	->	83.187.67.87:22	1	48	1
2015-11-20 15:32:55.139	0.000	TCP	250.65.164.35:9312	->	83.187.62.34:22	1	48	1
2015-11-20 15:32:55.577	0.000	TCP	250.65.164.35:9312	->	83.187.152.4:22	1	48	1
2015-11-20 15:32:55.581	0.000	TCP	250.65.164.35:9312	->	83.187.148.185:22	1	48	1
2015-11-20 15:32:55.563	0.000	TCP	250.65.164.35:9312	->	83.187.158.178:22	1	48	1
2015-11-20 15:32:55.292	0.000	TCP	250.65.164.35:9312	->	83.187.69.33:22	1	48	1
2015-11-20 15:32:55.567	0.000	TCP	250.65.164.35:9312	->	83.187.158.233:22	1	48	1
2015-11-20 15:32:55.571	0.000	TCP	250.65.164.35:9312	->	83.187.152.39:22	1	48	1
2015-11-20 15:32:55.442	0.000	TCP	250.65.164.35:9312	->	83.187.158.245:22	1	48	1
2015-11-20 15:32:55.469	0.000	TCP	250.65.164.35:9312	->	83.187.148.160:22	1	48	1
2015-11-20 15:32:55.473	0.000	TCP	250.65.164.35:9312	->	83.187.148.147:22	1	48	1
2015-11-20 15:32:55.289	0.000	TCP	250.65.164.35:9312	->	83.187.69.24:22	1	48	1
2015-11-20 15:32:55.467	0.000	TCP	250.65.164.35:9312	->	83.187.158.207:22	1	48	1
2015-11-20 15:32:55.567	0.000	TCP	250.65.164.35:9312	->	83.187.152.26:22	1	48	1
2015-11-20 15:32:55.570	0.000	TCP	250.65.164.35:9312	->	83.187.152.78:22	1	48	1
2015-11-20 15:32:55.185	0.000	TCP	250.65.164.35:9312	->	83.187.67.76:22	1	48	1
2015-11-20 15:32:55.047	0.000	TCP	250.65.164.35:9312	->	83.187.9.70:22	1	48	1
2015-11-20 15:32:55.260	0.000	TCP	250.65.164.35:9312	->	83.187.62.59:22	1	48	1
2015-11-20 15:32:55.480	0.000	TCP	250.65.164.35:9312	->	83.187.145.114:22	1	48	1
2015-11-20 15:32:55.480	0.000	TCP	250.65.164.35:9312	->	83.187.148.48:22	1	48	1

Find vertical scan

```
nfdump -r flows.nfcapd "flags S and not
flags F" -A srcip,dstip -s record/flows
```

```
Aggregated flows 215811
Top 10 flows ordered by flows:
Date first seen      Duration      Dst IP Addr      Src IP Addr      Packets      Bytes      bps      Bpp Flows
2015-11-20 15:32:04.787  1959.656      83.187.11.217    83.187.168.221   328386      40.7 M     166042    123 57346
2015-11-20 15:30:02.805  2098.085      83.187.132.46    83.187.16.147    3168        160512     612       50 1056
2015-11-20 15:30:06.387  2090.561      111.232.34.230   83.187.18.248    3008        152404     583       50 1003
2015-11-20 15:30:04.202  2090.556      111.232.34.230   83.187.18.237    2989        151440     579       50 997
2015-11-20 15:30:02.983  2091.014      83.187.109.108   83.187.16.156    4190        1.4 M     5216     325 838
2015-11-20 15:30:05.703  2085.397      83.187.109.107   83.187.16.156    4140        1.3 M     5167     325 828
2015-11-20 15:30:00.371  2099.881      254.192.34.177   83.187.2.32      8888        2.0 M     7470     220 808
2015-11-20 15:30:00.371  2100.202      83.187.2.32      254.192.34.177   8877        875595     3335     98 807
2015-11-20 15:30:01.460  2097.526      232.145.107.108  83.187.153.148   1970        99812     380       50 659
2015-11-20 15:30:01.025  2095.765      63.71.241.25    83.187.153.125   599         31148     118       52 599
IP addresses anonymised
Summary: total flows: 486473, total bytes: 33187025024, total packets: 38178186, avg bps: 126366707, avg pps: 18171, avg bpp:
869
Time window: 2015-11-20 15:30:00 - 2015-11-20 16:05:00
Total flows processed: 7975525, Blocks skipped: 0, Bytes read: 482516584
```


2015-11-20 16:04:43.193	0.134	ICP	83.187.168.221:64198	->	83.187.11.217:5555	5	674	1
2015-11-20 16:04:44.279	10.503	TCP	83.187.168.221:64265	->	83.187.11.217:5555	4	172	1
2015-11-20 16:04:43.470	0.149	TCP	83.187.168.221:64230	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:42.938	0.126	TCP	83.187.168.221:64166	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:42.648	0.145	TCP	83.187.168.221:64134	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:42.678	0.136	TCP	83.187.168.221:64140	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:42.947	0.116	TCP	83.187.168.221:64172	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:43.493	0.138	TCP	83.187.168.221:64236	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:44.178	0.133	TCP	83.187.168.221:64259	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:43.203	0.125	TCP	83.187.168.221:64204	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:42.383	0.132	TCP	83.187.168.221:64105	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:42.438	0.124	TCP	83.187.168.221:64108	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:43.199	0.134	TCP	83.187.168.221:64201	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:44.180	0.125	TCP	83.187.168.221:64262	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:42.182	0.132	TCP	83.187.168.221:64076	->	83.187.11.217:5555	6	714	1
2015-11-20 16:04:43.491	0.133	TCP	83.187.168.221:64233	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:42.941	0.130	TCP	83.187.168.221:64169	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:42.653	0.141	TCP	83.187.168.221:64137	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:43.372	0.123	TCP	83.187.168.221:64224	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:44.441	10.340	TCP	83.187.168.221:64271	->	83.187.11.217:5555	4	172	1
2015-11-20 16:04:43.140	0.116	TCP	83.187.168.221:64192	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:42.377	0.142	TCP	83.187.168.221:64101	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:42.621	0.125	TCP	83.187.168.221:64128	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:42.868	0.109	TCP	83.187.168.221:64160	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:42.937	0.132	TCP	83.187.168.221:64165	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:42.646	0.132	TCP	83.187.168.221:64133	->	83.187.11.217:5555	5	674	1
2015-11-20 16:04:42.368	0.141	TCP	83.187.168.221:64096	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:43.192	0.131	TCP	83.187.168.221:64197	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:44.280	10.503	TCP	83.187.168.221:64266	->	83.187.11.217:5555	4	172	1
2015-11-20 16:04:43.433	0.138	TCP	83.187.168.221:64229	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:43.495	0.137	TCP	83.187.168.221:64239	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:44.176	0.266	TCP	83.187.168.221:64256	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:43.253	0.118	TCP	83.187.168.221:64207	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:42.384	0.135	TCP	83.187.168.221:64106	->	83.187.11.217:5555	6	726	1
2015-11-20 16:04:42.743	0.125	TCP	83.187.168.221:64143	->	83.187.11.217:5555	6	716	1
2015-11-20 16:04:43.011	0.110	TCP	83.187.168.221:64175	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:42.943	0.131	TCP	83.187.168.221:64170	->	83.187.11.217:5555	6	714	1
2015-11-20 16:04:42.671	0.134	TCP	83.187.168.221:64138	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:42.442	0.118	TCP	83.187.168.221:64111	->	83.187.11.217:5555	5	676	1
2015-11-20 16:04:43.200	0.131	TCP	83.187.168.221:64202	->	83.187.11.217:5555	6	714	1
2015-11-20 16:04:44.179	0.134	TCP	83.187.168.221:64261	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:42.189	0.130	TCP	83.187.168.221:64079	->	83.187.11.217:5555	6	728	1
2015-11-20 16:04:43.492	0.135	TCP	83.187.168.221:64234	->	83.187.11.217:5555	6	716	1