Sniffer

这是一个基于python实现的仿wireshark的网络协议分析器

1.功能

基本功能

- 网卡选择
- 抓取数据包
- 保存数据
- 清除数据
- 读取数据
- 流量包基本信息显示
- 协议分析
- hexdump内容

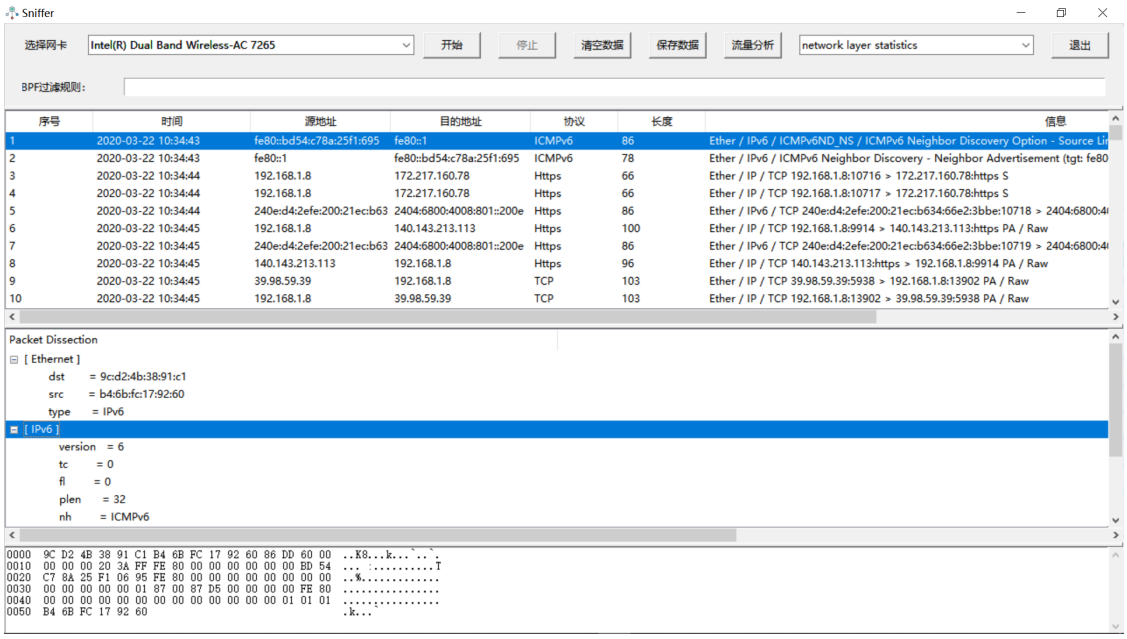
流量分析功能

- 流量协议统计（分层）
- 获取http/https请求（该功能存在问题）
- 流入/出流量IP归属地查询和统计
- 流量时间统计

2.效果展示

5.程序界面和运行效果

- 程序主界面



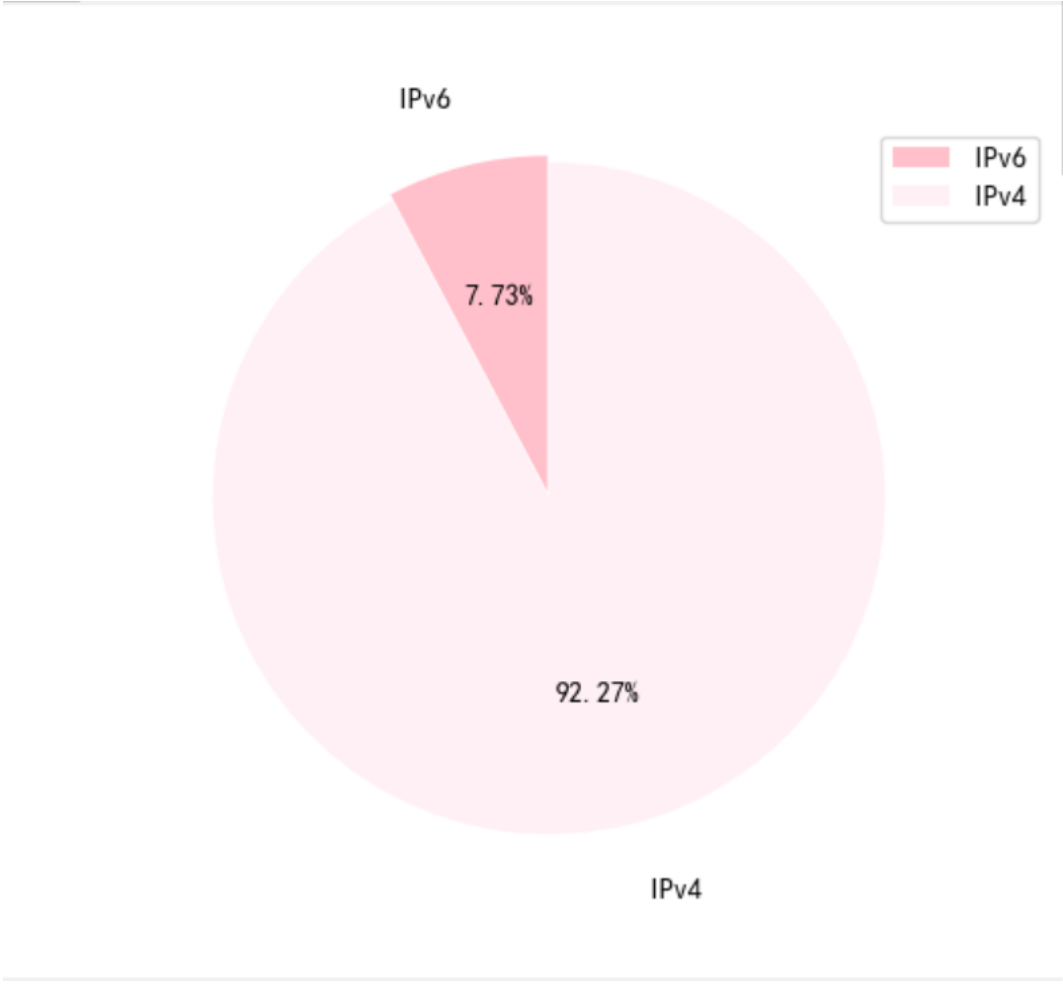
- 流量分析部分
  - 对所有抓取到的数据包的日志

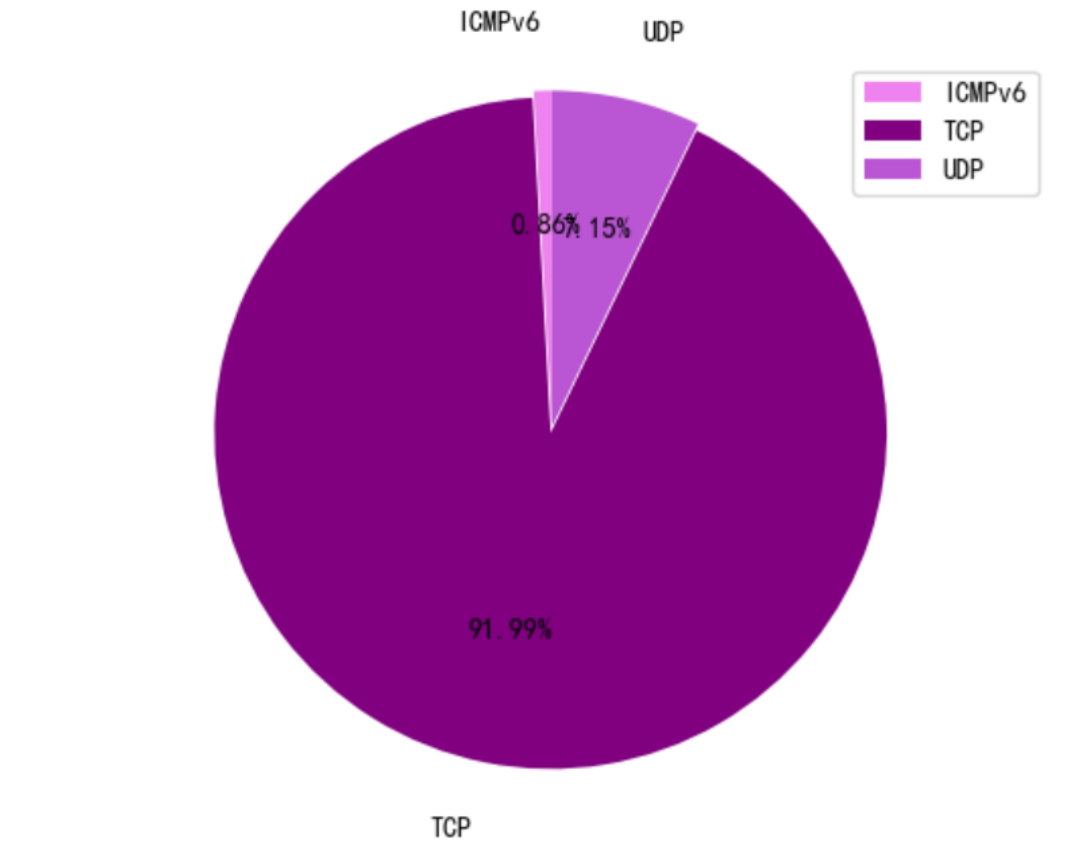
    相应结果保存在/log/packet_log_（2020_03_21_23_47_16）-时间戳

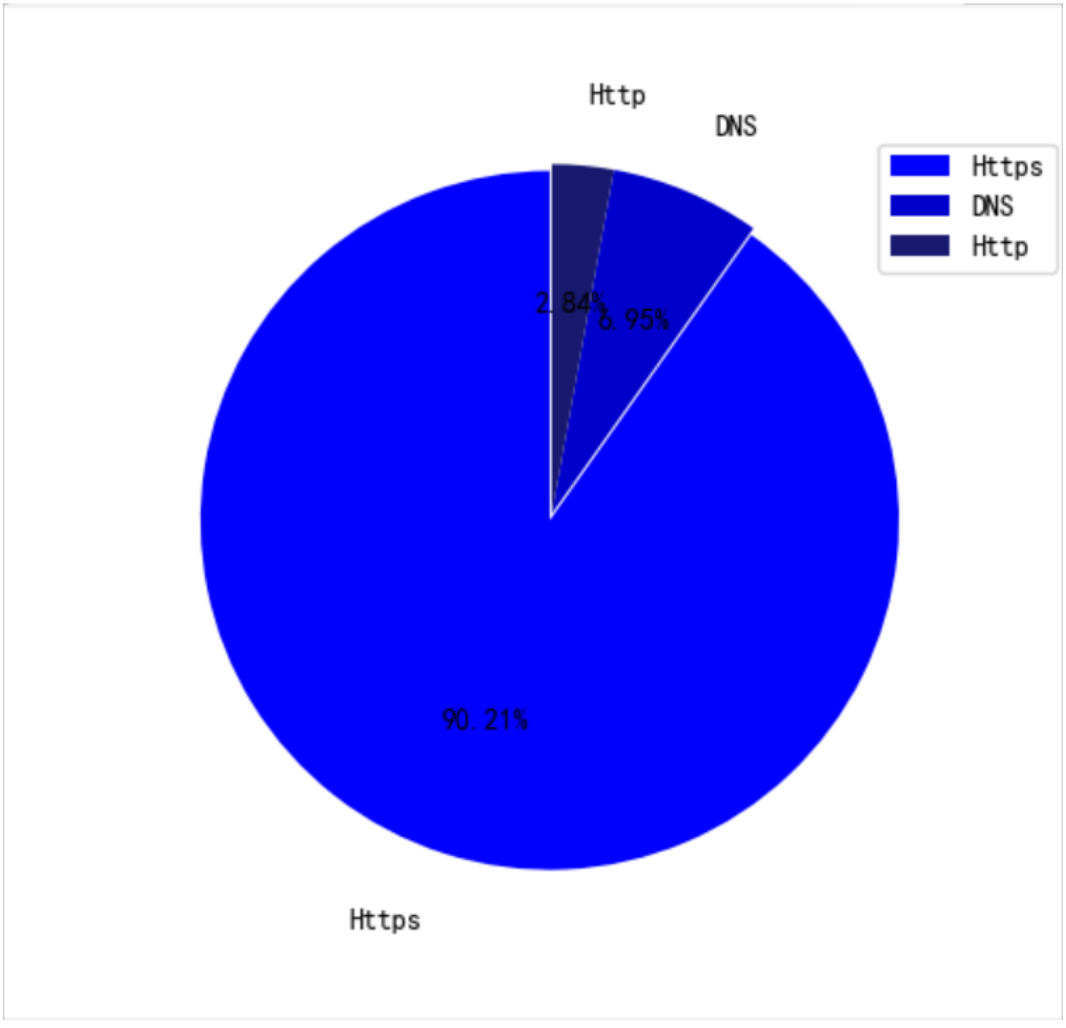
	packet_id	packet_time	src	dst	proto	length	info
1	1	2020-03-22 10:34:43	fe80::bd54:c78a:25f1:695	fe80::1	ICMPv6	86	Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option - S
2	2	2020-03-22 10:34:43	fe80::1	fe80::bd54:c78a:25f1:695	ICMPv6	78	Ether / IPv6 / ICMPv6 Neighbor Discovery - Neighbor Advertisement
3	3	2020-03-22 10:34:44	192.168.1.8	172.217.160.78	Https	66	Ether / IP / TCP 192.168.1.8:10716 > 172.217.160.78:https S
4	4	2020-03-22 10:34:44	192.168.1.8	172.217.160.78	Https	66	Ether / IP / TCP 192.168.1.8:10717 > 172.217.160.78:https S
5	5	2020-03-22 10:34:44	240e:d4:2efe:200:21ec:b634:66e2:3bbe	2404:6800:4008:801::200e	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:2
6	6	2020-03-22 10:34:45	192.168.1.8	140.143.213.113	Https	100	Ether / IP / TCP 192.168.1.8:9914 > 140.143.213.113:https PA / Raw
7	7	2020-03-22 10:34:45	240e:d4:2efe:200:21ec:b634:66e2:3bbe	2404:6800:4008:801::200e	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:2
8	8	2020-03-22 10:34:45	140.143.213.113	192.168.1.8	Https	96	Ether / IP / TCP 140.143.213.113:https > 192.168.1.8:9914 PA / Raw
9	9	2020-03-22 10:34:45	39.98.59.39	192.168.1.8	TCP	103	Ether / IP / TCP 39.98.59.39:5938 > 192.168.1.8:13902 PA / Raw
10	10	2020-03-22 10:34:45	192.168.1.8	39.98.59.39	TCP	103	Ether / IP / TCP 192.168.1.8:13902 > 39.98.59.39:5938 PA / Raw
11	11	2020-03-22 10:34:45	192.168.1.8	140.143.213.113	Https	54	Ether / IP / TCP 192.168.1.8:9914 > 140.143.213.113:https A
12	12	2020-03-22 10:34:45	39.98.59.39	192.168.1.8	TCP	54	Ether / IP / TCP 39.98.59.39:5938 > 192.168.1.8:13902 A
13	13	2020-03-22 10:34:45	192.168.1.8	39.98.59.39	TCP	110	Ether / IP / TCP 192.168.1.8:13902 > 39.98.59.39:5938 PA / Raw
14	14	2020-03-22 10:34:45	39.98.59.39	192.168.1.8	TCP	110	Ether / IP / TCP 39.98.59.39:5938 > 192.168.1.8:13902 PA / Raw
15	15	2020-03-22 10:34:45	192.168.1.8	39.98.59.39	TCP	54	Ether / IP / TCP 192.168.1.8:13902 > 39.98.59.39:5938 A
16	16	2020-03-22 10:34:46	192.168.1.8	31.13.77.55	Https	66	Ether / IP / TCP 192.168.1.8:10685 > 31.13.77.55:https S
17	17	2020-03-22 10:34:46	192.168.1.8	39.98.59.39	TCP	78	Ether / IP / TCP 192.168.1.8:13902 > 39.98.59.39:5938 PA / Raw
18	18	2020-03-22 10:34:46	192.168.1.8	10.10.20.110	UDP	120	Ether / IP / UDP 192.168.1.8:59684 > 10.10.20.110:snmp / SNMP
19	19	2020-03-22 10:34:46	31.13.77.55	192.168.1.8	Https	54	Ether / IP / TCP 31.13.77.55:https > 192.168.1.8:10685 RA
20	20	2020-03-22 10:34:46	240e:d4:2efe:200:21ec:b634:66e2:3bbe	2404:6800:4012::2004	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:200:2
21	21	2020-03-22 10:34:46	39.98.59.39	192.168.1.8	TCP	54	Ether / IP / TCP 39.98.59.39:5938 > 192.168.1.8:13902 A
22	22	2020-03-22 10:34:46	240e:d4:2efe:200:21ec:b634:66e2:3bbe	2404:6800:4012::2004	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:200:2
23	23	2020-03-22 10:34:46	192.168.1.8	31.13.77.55	Https	66	Ether / IP / TCP 192.168.1.8:10686 > 31.13.77.55:https S

- 针对各层协议数据包的统计分析

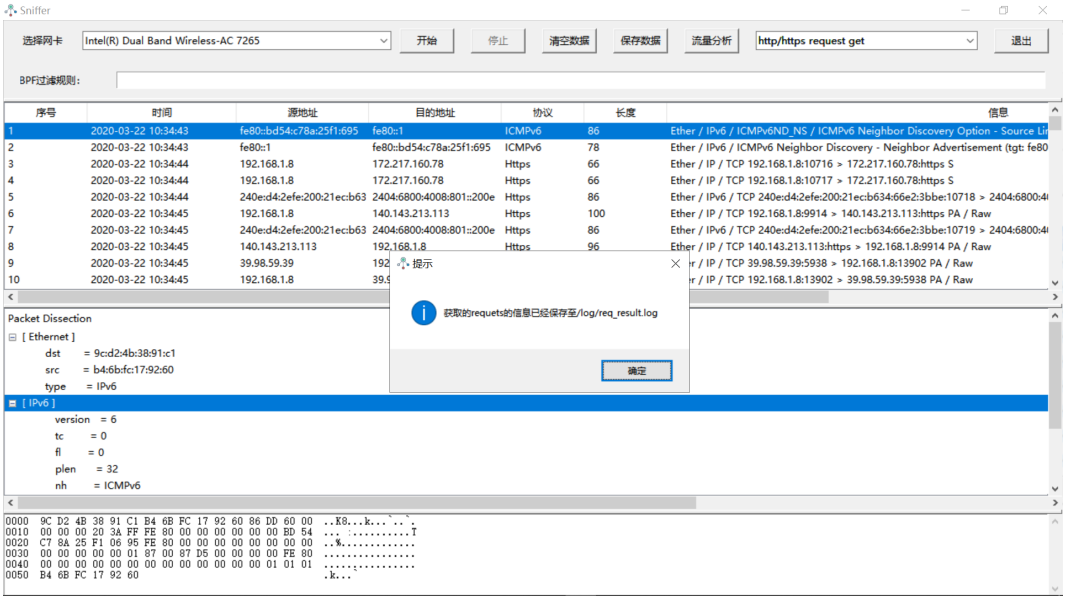
  相应的结果保存在/png



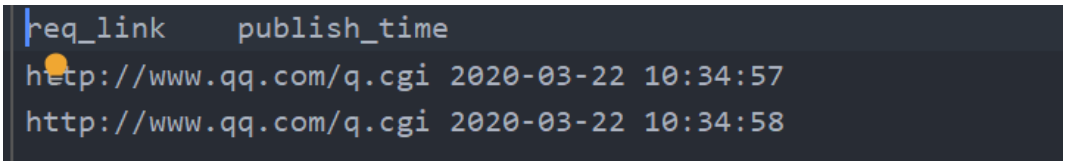

ICMPv6
UDP
ICMPv6
TCP
UDP
0.86%
7.15%
91.99%
TCP


Http
DNS
Https
DNS
Http
2.84%
6.95%
90.21%
Https

- 获取http/https请求（结果保存在日志中）



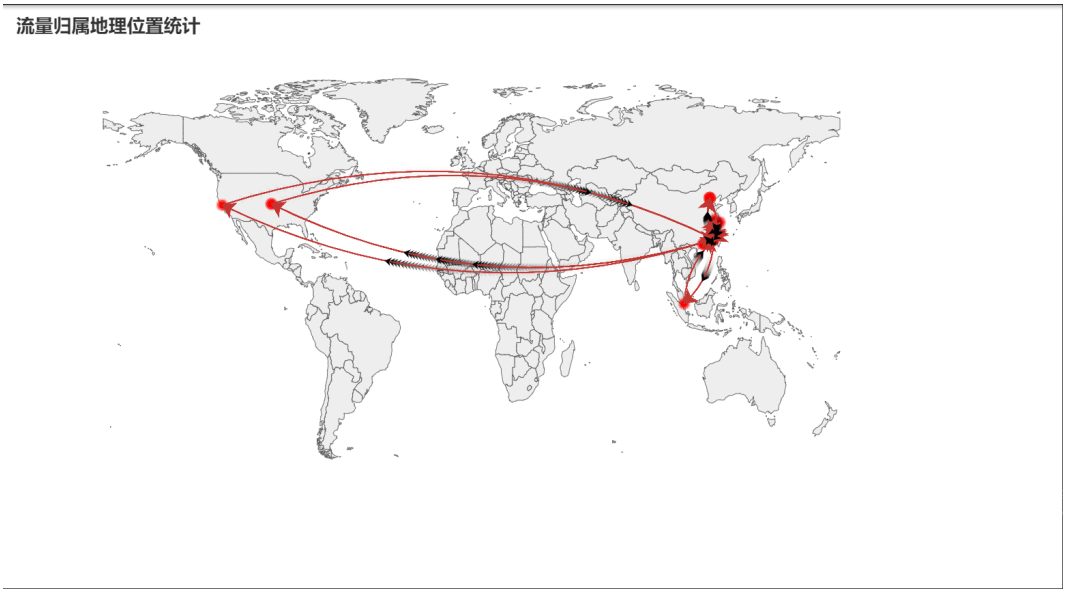
日志保存在/log/req_result.log



- 流入/出流量IP归属地查询（包括可视化界面和日志）

  可视化界面：

  相应结果保存在/html/query_address.html



日志：（保存在/log/in_ip_addr.txt和/log/out_ip_addr.txt)

  - in_ip_addr.txt:

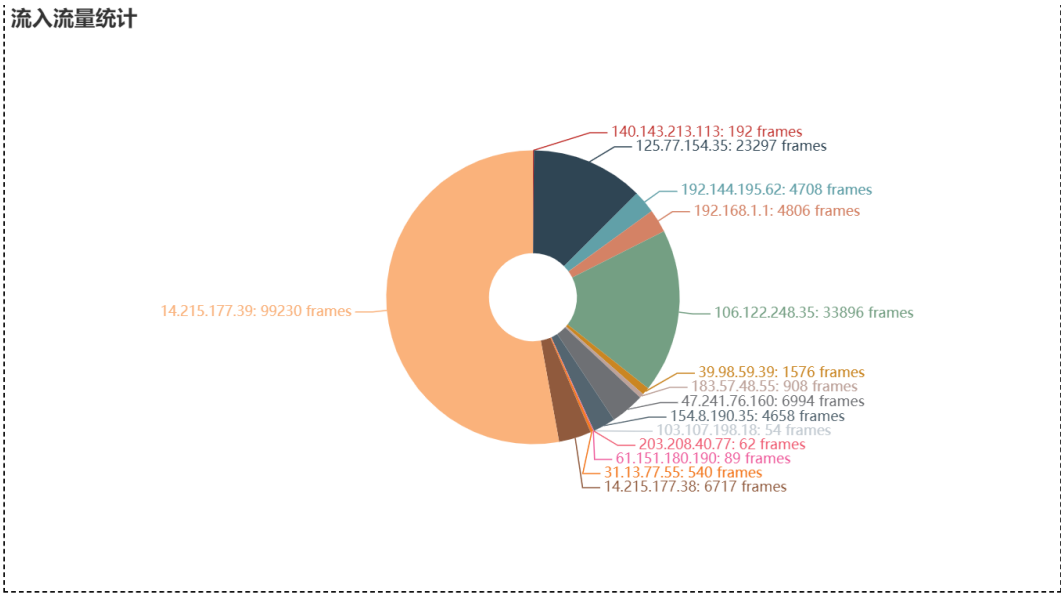
index	ip	trapeze	contry	city	count
1	203.208.40.77	(116.3889, 39.9288)	China	Beijing	1
2	103.107.198.18	(103.8547, 1.2929)	Singapore	Singapore	1
3	61.151.180.190	(121.4012, 31.0449)	China	None	1
4	140.143.213.113	(116.3889, 39.9288)	China	Beijing	2
5	125.77.154.35	(118.0819, 24.4798)	China	Xiamen	37
6	183.57.48.55	(113.25, 23.1167)	China	None	8
7	154.8.190.35	(116.3883, 39.9289)	China	None	9
8	180.101.212.33	(118.7778, 32.0617)	China	Nanjing	9
9	31.13.77.55	(-121.8914, 37.3388)	United States	San Jose	10
10	47.241.76.160	(-97.822, 37.751)	United States	None	10
11	106.122.248.35	(118.0819, 24.4798)	China	Xiamen	47
12	192.144.195.62	(116.3883, 39.9289)	China	None	17
13	39.98.59.39	(120.1619, 30.294)	China	Hangzhou	20
14	14.215.177.39	(113.25, 23.1167)	China	None	120
15	14.215.177.38	(113.25, 23.1167)	China	None	28

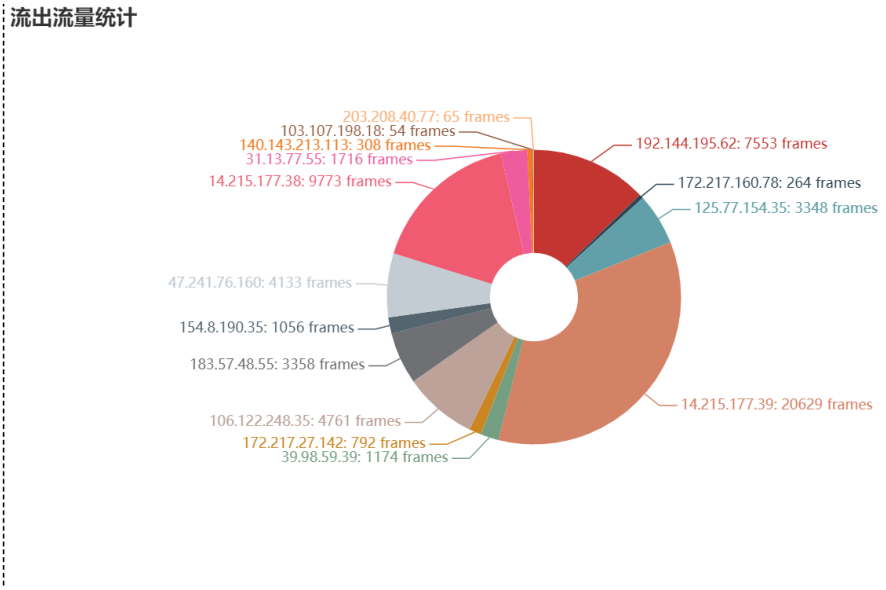
- out_ip_addr.txt:

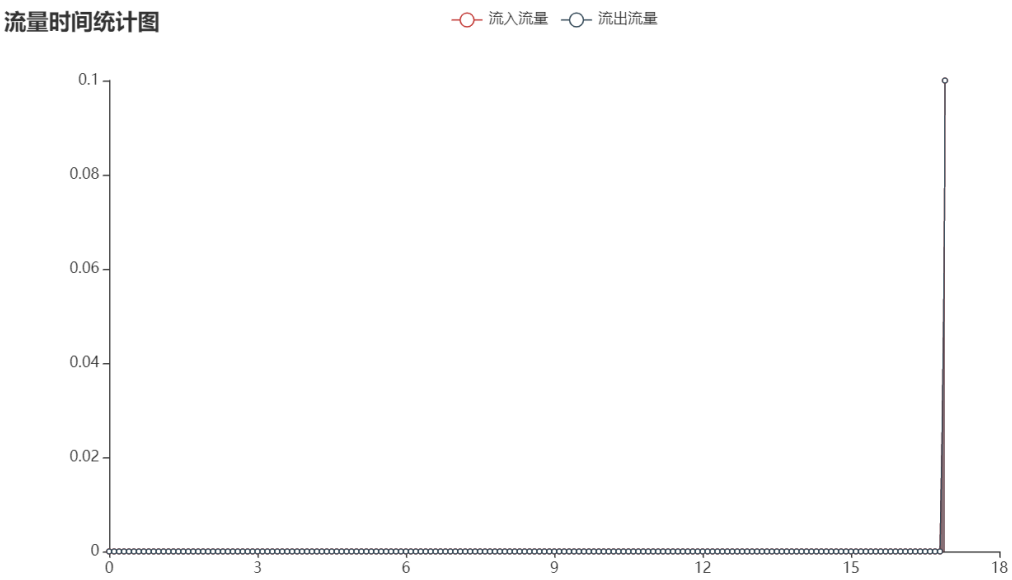
index	ip	trapeze	contry	city	count
1	203.208.40.77	(116.3889, 39.9288)	China	Beijing	1
2	103.107.198.18	(103.8547, 1.2929)	Singapore	Singapore	1
3	61.151.180.190	(121.4012, 31.0449)	China	None	1
4	125.77.154.35	(118.0819, 24.4798)	China	Xiamen	35
5	172.217.160.78	(-97.822, 37.751)	United States	None	4
6	140.143.213.113	(116.3889, 39.9288)	China	Beijing	4
7	14.215.177.39	(113.25, 23.1167)	China	None	68
8	14.215.177.38	(113.25, 23.1167)	China	None	39
9	154.8.190.35	(116.3883, 39.9289)	China	None	9
10	180.101.212.33	(118.7778, 32.0617)	China	Nanjing	10
11	183.57.48.55	(113.25, 23.1167)	China	None	11
12	47.241.76.160	(-97.822, 37.751)	United States	None	11
13	172.217.27.142	(-97.822, 37.751)	United States	None	12
14	39.98.59.39	(120.1619, 30.294)	China	Hangzhou	13
15	192.144.195.62	(116.3883, 39.9289)	China	None	17
16	106.122.248.35	(118.0819, 24.4798)	China	Xiamen	24
17	31.13.77.55	(-121.8914, 37.3388)	United States	San Jose	26

- 流出/流入流量数据包数量和时间统计

  相应结果保存在/html/ip_packet_statistic.html







3.安装使用

```
git clone https://github.com/Estherbdf/sniffer.git
cd ./sniffer
pip3 install requirements.txt
python3 capture_packet.py
```

4.参考

https://blog.csdn.net/wmrem/article/details/80465104?depth_1-utm_source=distribute.pc_relevant.none-task&utm_source=distribute.pc_relevant.none-task