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

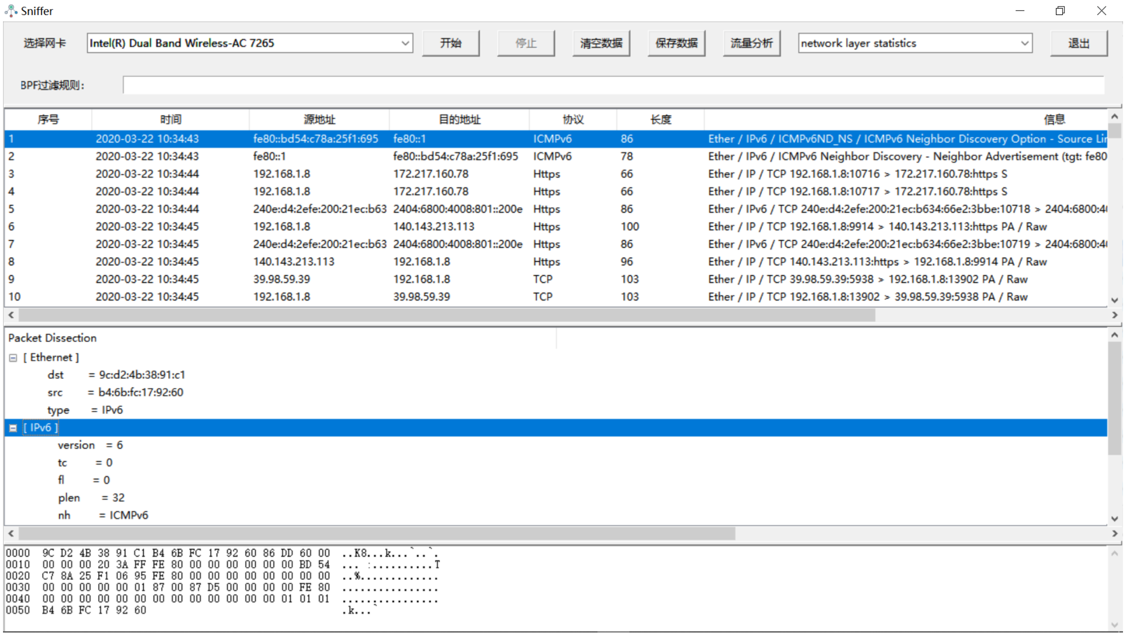
流量分析功能

- 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



选择网卡 Intel(R) Dual Band Wireless-AC 7265

network layer statistics

BPF过滤规则：

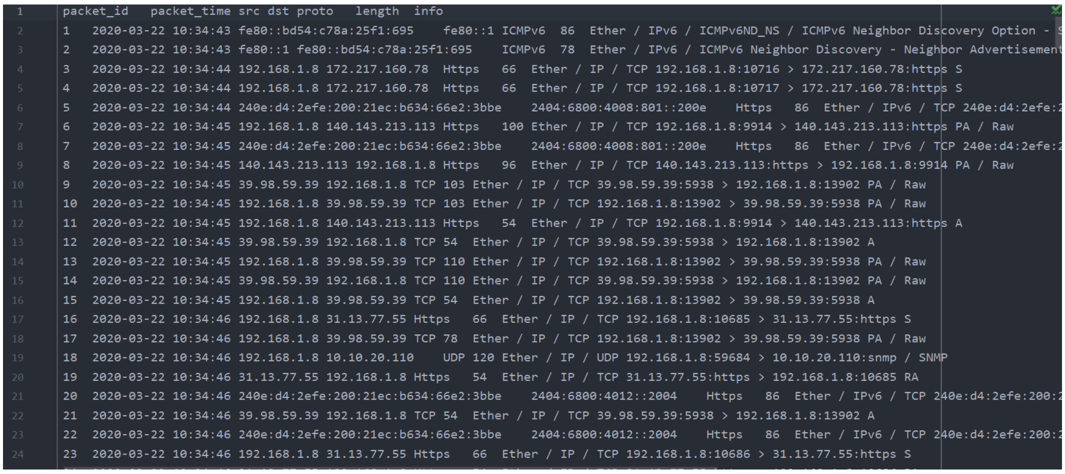
序号	时间	源地址	目的地址	协议	长度	信息
1	2020-03-22 10:34:43	fe80::bd54:c78a:25f1:695	fe80::1	ICMPv6	86	Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option - Source Lin
2	2020-03-22 10:34:43	fe80::1	fe80::bd54:c78a:25f1:695	ICMPv6	78	Ether / IPv6 / ICMPv6 Neighbor Discovery - Neighbor Advertisement (tgt: fe80
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	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	2020-03-22 10:34:44	240e:d4:2efe:200:21ec:b63	2404:6800:4008:801::200e	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:200:21ec:b634:66e2:3bbe:10718 > 2404:6800:4
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	2020-03-22 10:34:45	240e:d4:2efe:200:21ec:b63	2404:6800:4008:801::200e	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:200:21ec:b634:66e2:3bbe:10719 > 2404:6800:4
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	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	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

```
Packet Dissection
⊟ [ Ethernet ]
      dst     = 9c:d2:4b:38:91:c1
      src     = b4:6b:fc:17:92:60
      type    = IPv6
⊟ [ IPv6 ]
        version  = 6
        tc       = 0
        fl       = 0
        plen     = 32
        nh       = ICMPv6
```

```
0000  9C D2 4B 38 91 C1 B4 6B FC 17 92 60 86 DD 60 00   ..K8...k...`..`.
0010  00 00 00 20 3A FF FE 80 00 00 00 00 00 00 BD 54   ... :..........T
0020  C7 8A 25 F1 06 95 FE 80 00 00 00 00 00 00 00 00   ..%.............
0030  00 00 00 00 00 01 87 00 87 D5 00 00 00 00 FE 80   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 01 01 01   ................
0050  B4 6B FC 17 92 60                                 .k...`
```

- 流量分析部分
    - 对所有抓取到的数据包的日志

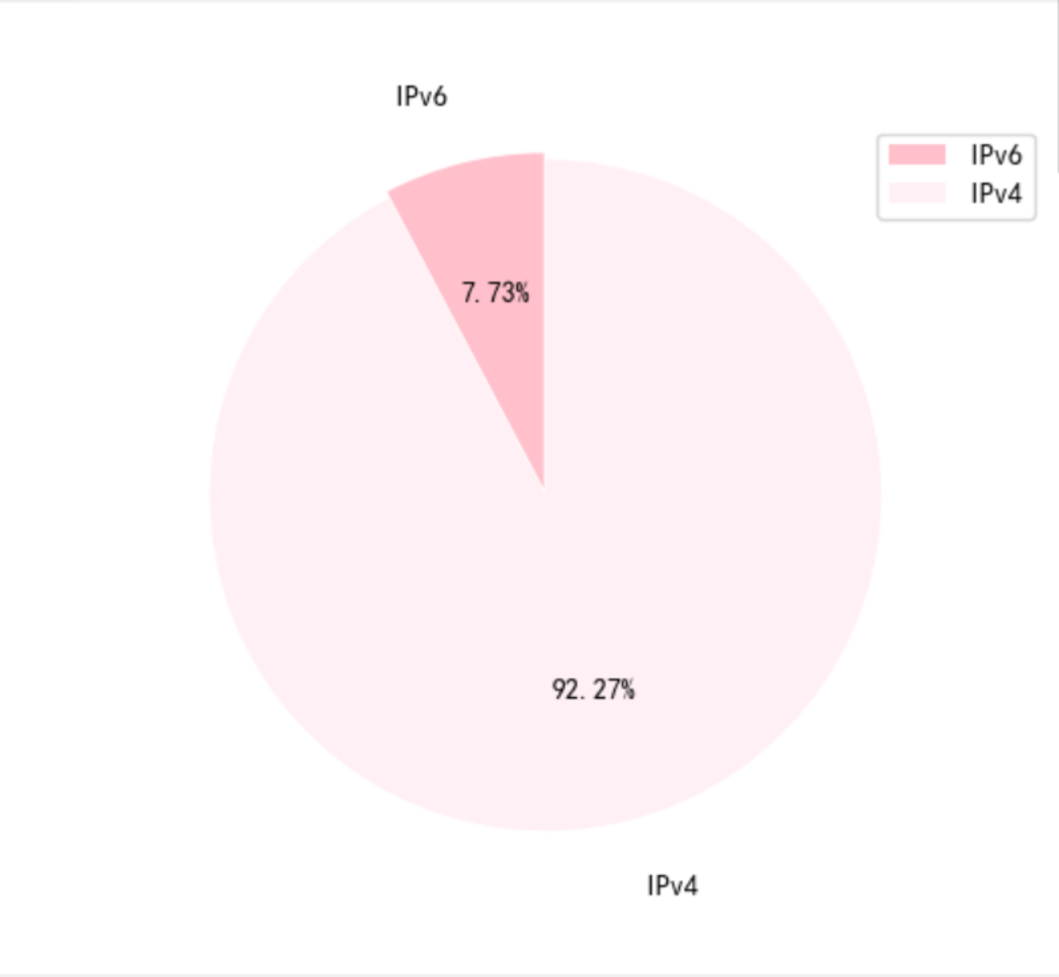
      相应结果保存在/log/packet_log_（2020_03_21_23_47_16）-时间戳

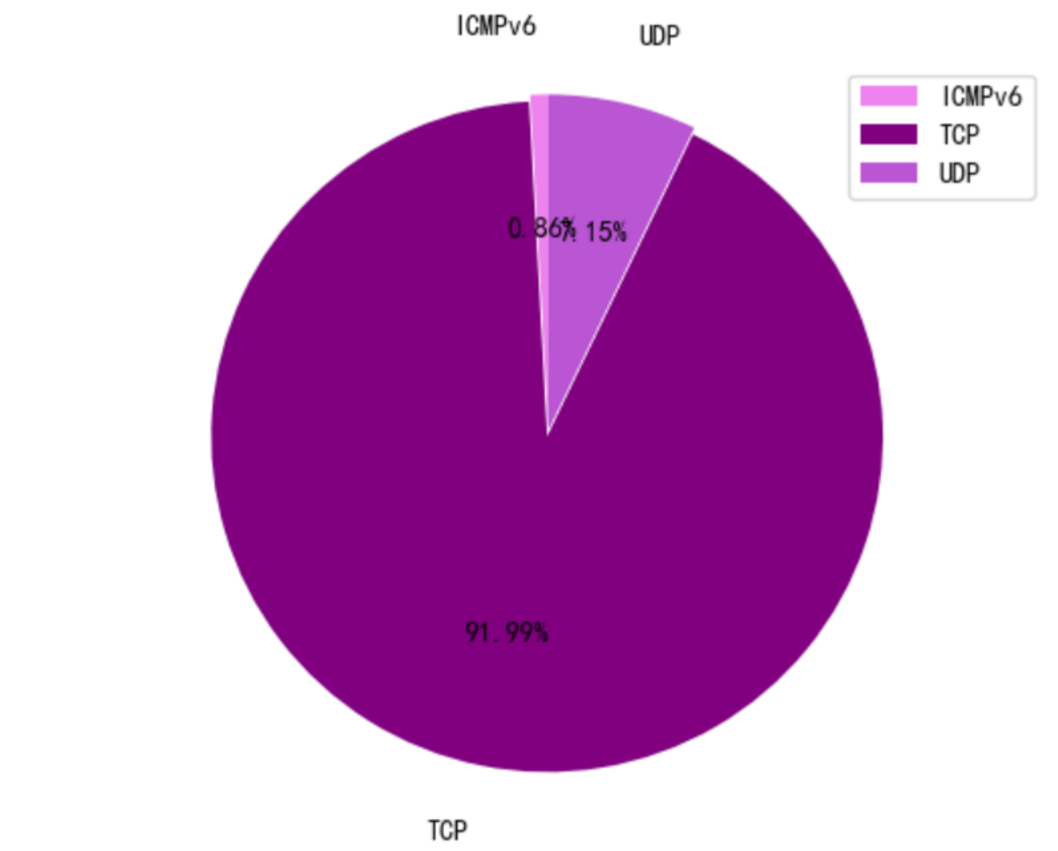


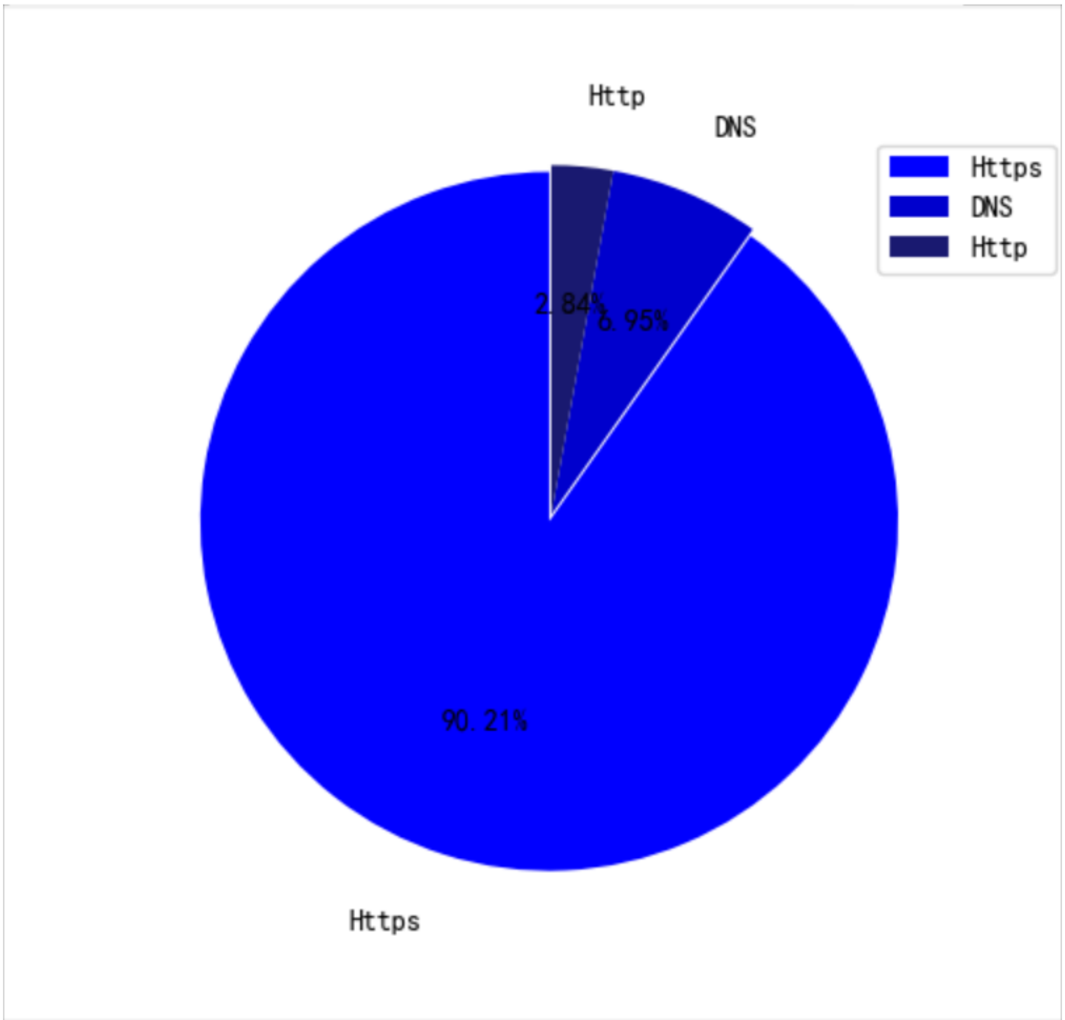
```
packet_id   packet_time src dst proto   length  info
1   2020-03-22 10:34:43 fe80::bd54:c78a:25f1:695    fe80::1 ICMPv6  86  Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option -
2   2020-03-22 10:34:43 fe80::1 fe80::bd54:c78a:25f1:695    ICMPv6  78  Ether / IPv6 / ICMPv6 Neighbor Discovery - Neighbor Advertisement
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   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   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:
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   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:
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   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  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  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  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  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  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  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  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  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  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  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  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:
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  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:
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

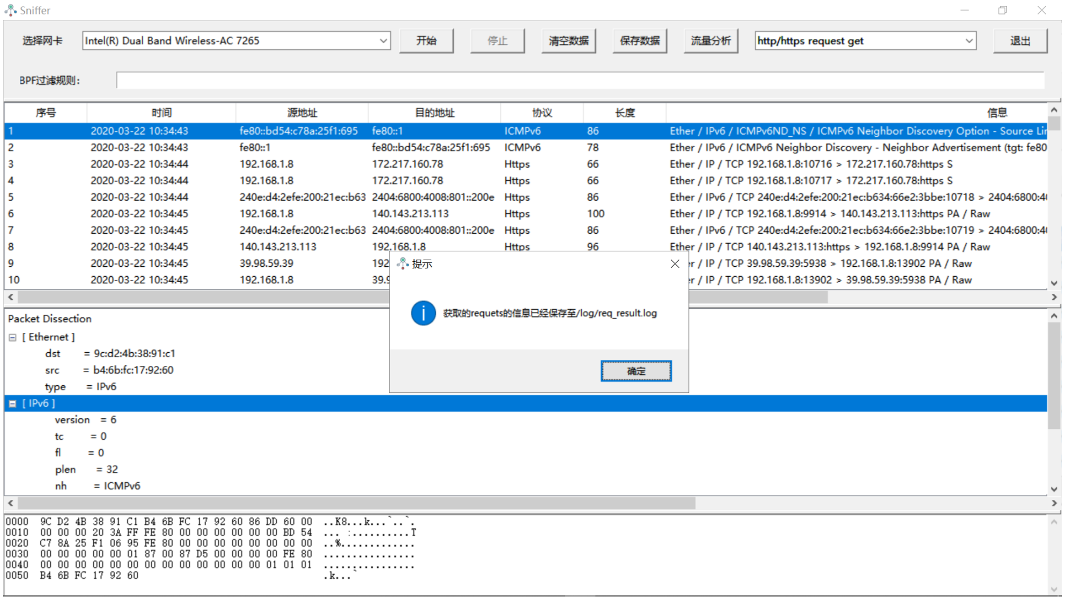
  相应的结果保存在/png




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


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

- 获取http/https请求（结果保存在日志中）



序号	时间	源地址	目的地址	协议	长度	信息
1	2020-03-22 10:34:43	fe80::bd54:c78a:25f1:695	fe80::1	ICMPv6	86	Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option - Source Lir
2	2020-03-22 10:34:43	fe80::1	fe80::bd54:c78a:25f1:695	ICMPv6	78	Ether / IPv6 / ICMPv6 Neighbor Discovery - Neighbor Advertisement (tgt: fe80
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	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	2020-03-22 10:34:44	240e:d4:2efe:200:21ec:b63	2404:6800:4008:801::200e	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:200:21ec:b634:66e2:3bbe:10718 > 2404:6800:4(
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	2020-03-22 10:34:45	240e:d4:2efe:200:21ec:b63	2404:6800:4008:801::200e	Https	86	Ether / IPv6 / TCP 240e:d4:2efe:200:21ec:b634:66e2:3bbe:10719 > 2404:6800:4(
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	2020-03-22 10:34:45	39.98.59.39	192			r / IP / TCP 39.98.59.39:5938 > 192.168.1.8:13902 PA / Raw
10	2020-03-22 10:34:45	192.168.1.8	39.9			r / IP / TCP 192.168.1.8:13902 > 39.98.59.39:5938 PA / Raw

提示

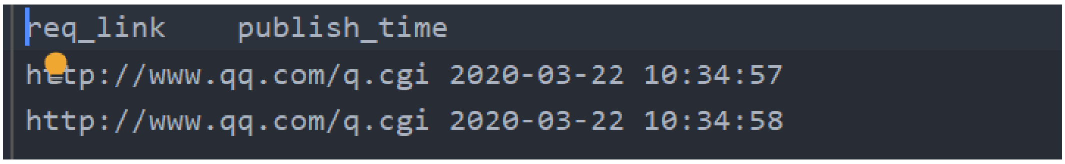
获取的requets的信息已经保存至/log/req_result.log

确定

```
Packet Dissection
⊟ [ Ethernet ]
      dst     = 9c:d2:4b:38:91:c1
      src     = b4:6b:fc:17:92:60
      type    = IPv6
⊟ [ IPv6 ]
        version   = 6
        tc       = 0
        fl       = 0
        plen     = 32
        nh       = ICMPv6
```

```
0000  9C D2 4B 38 91 C1 B4 6B FC 17 92 60 86 DD 60 00  ..K8...k...`..`.
0010  00 00 00 20 3A FF FE 80 00 00 00 00 00 00 BD 54  ... :..........T
0020  C7 8A 25 F1 06 95 FE 80 00 00 00 00 00 00 00 00  ..%.............
0030  00 00 00 00 00 01 87 00 87 D5 00 00 00 00 FE 80  ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 01 01 01  ................
0050  B4 6B FC 17 92 60                                .k...`
```

日志保存在/log/req_result.log

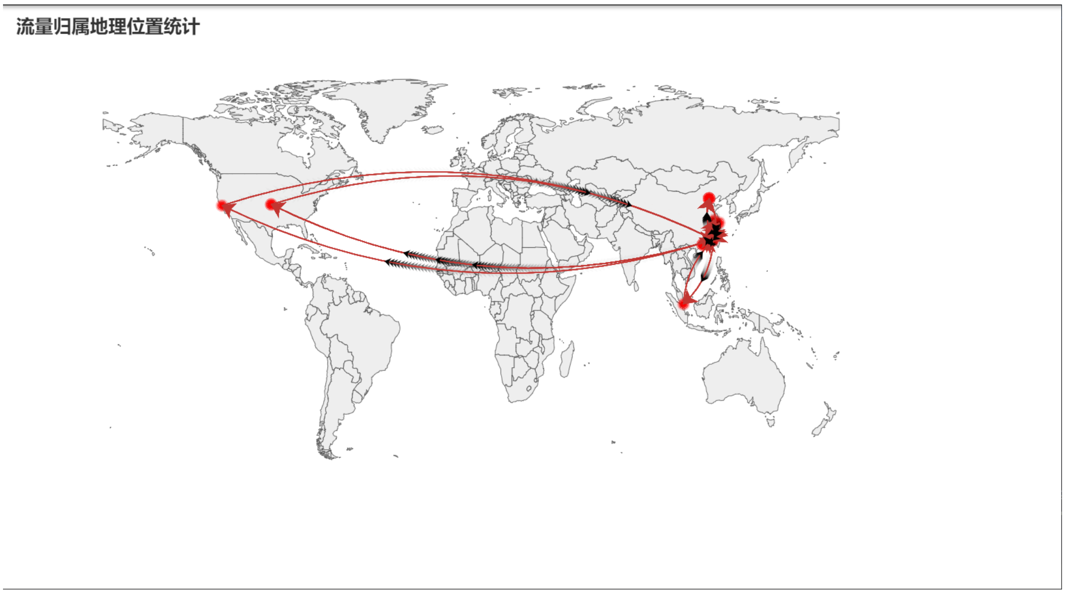


```
req_link     publish_time
http://www.qq.com/q.cgi 2020-03-22 10:34:57
http://www.qq.com/q.cgi 2020-03-22 10:34:58
```

- 流入/出流量IP归属地查询（包括可视化界面和日志）

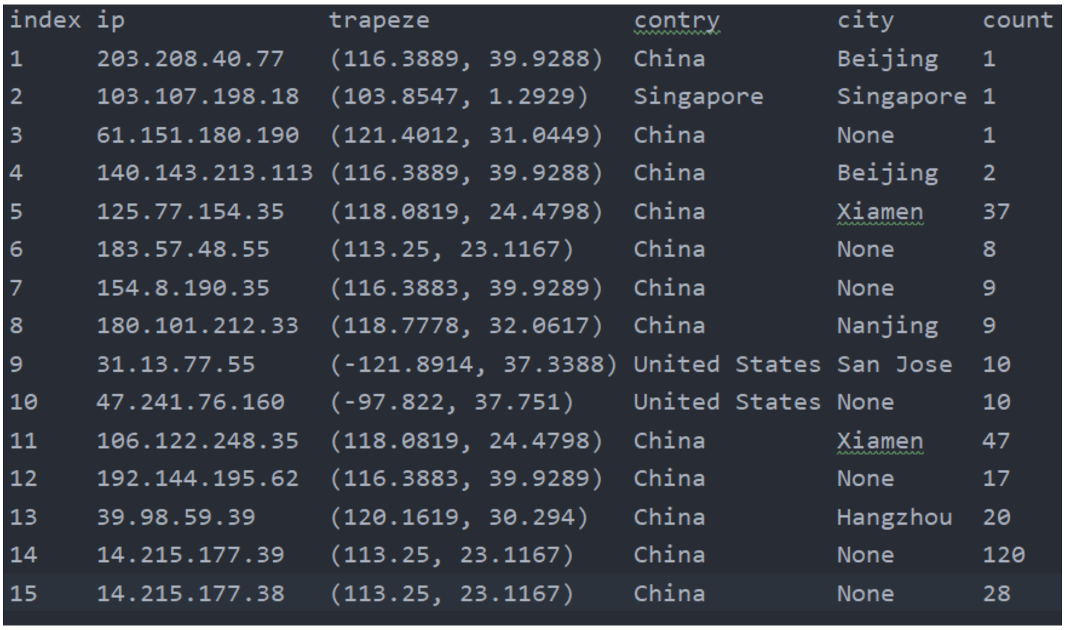
  可视化界面：

  相应结果保存在/html/query_address.html



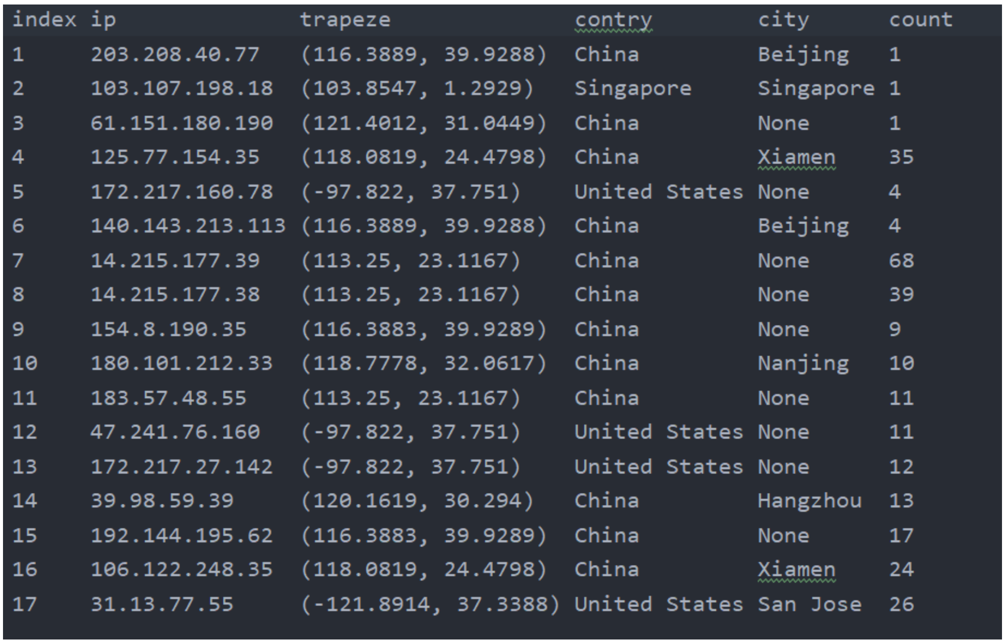
日志：（保存在/log/in_ip_addr.txt和/log/out_ip_addr.txt）

  - 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:

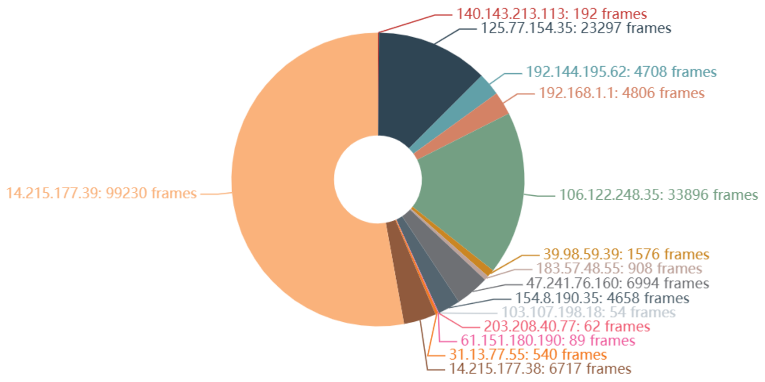


```
index ip              trapeze             contry        city      count
1     203.208.40.77   (116.3889, 39.9288) China         Beijing   1
2     103.107.198.18  (103.8547, 1.2929)  Singapore     Singapore 1
3     61.151.180.190  (121.4012, 31.0449) China         None      1
4     125.77.154.35   (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
```

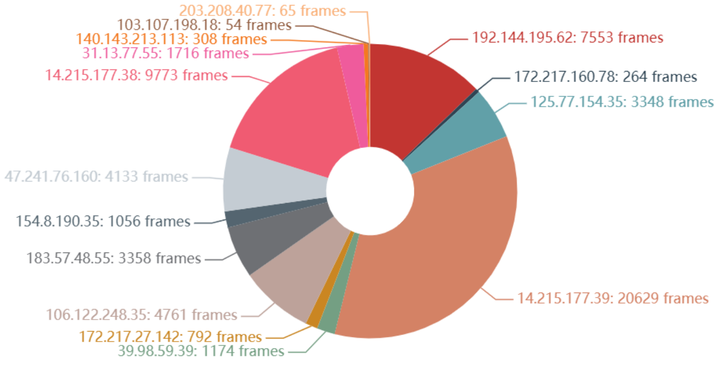
- 流出/流入流量数据包数量和时间统计

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

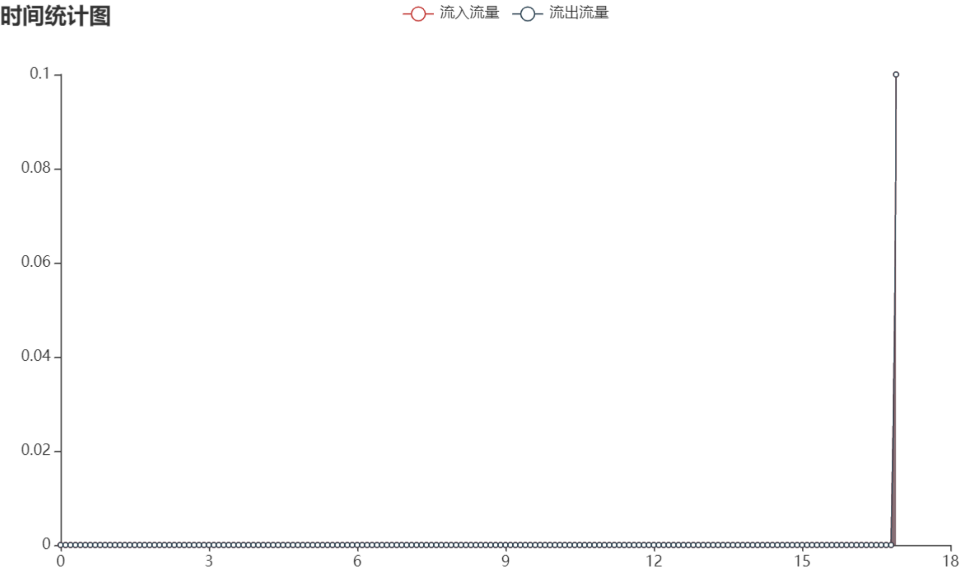
流入流量统计



流出流量统计



流量时间统计图



3.安装使用

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