FANTASTIC ATTACKS AND HOW KALIPSO CAN FIND THEM

Kamila Babayeva
babaykam@fel.cvut.cz, @_kamifai_

Sebastian Garcia
sebastian.garcia@agent.fel.cvut.cz, @eldracote

WHAT IF YOU NEED TO ANALYZE A VERY LARGE PCAP TO FIND IF THERE WAS AN INFECTION?

A REAL ANDROID INFECTION

KALIPSO DEMO

WHAT WAS HELPING THE DETECTION?

RED ALERTS

Slips can identify some weird situations and alert you about them

DST PORTS

In “dst ports as a client” we can see a lot of bytes and packets going to a dst port

BEHAVIORAL LETTERS

Tuples with a strong periodicity

HOW DOES SLIPS WORK?

IDEA

Machine Learning for Network Detection. Backend

TIMEWINDOWS

Profiles and detections happen in TW. Behaviors change.

HOME NET

Defines for which IPs it creates profiles

DIRECTIONALITY

Out: Only consider traffic going out of the profile
All: Consider traffic in and out of the profile

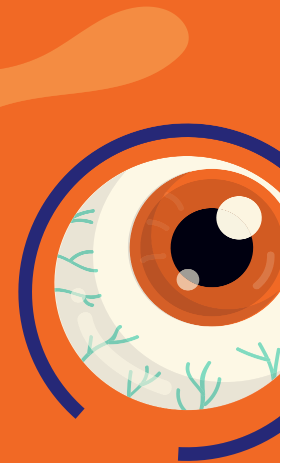
PROFILES

Profile per src IP. Computes all the features in the profile

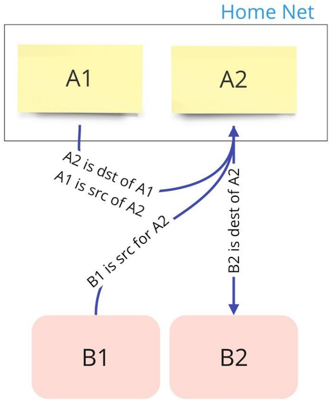
MODULES

Implement everything in modules as independent processes

DIRECTIONALITY

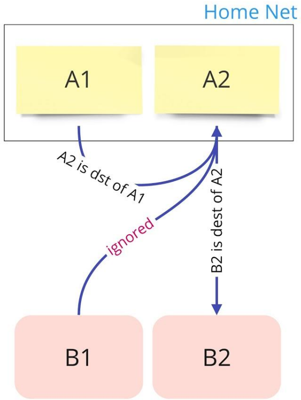


With home net and mode 'all'



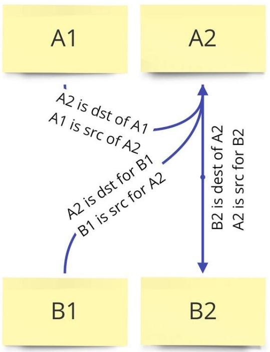
- Profiles only created for A's
- Both traffic going OUT of the profiles and IN to the profiles is accounted

With home net and mode 'out'



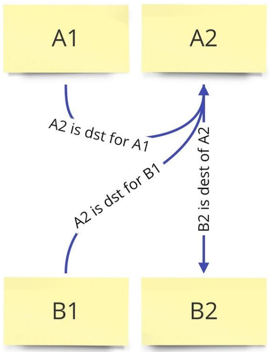
- Profiles only created for A's
- Only the traffic going OUT of the profiles is accounted

WithOUT home net and mode 'all'

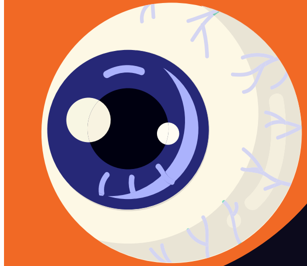


- Profiles created for A's and B's
- Both traffic going OUT of the profiles and IN to the profiles is accounted

WithOUT home net and mode 'out'



- Profiles created for A's and B's
- Only the traffic going OUT of the profiles is accounted



KALIPSO

KALIPSO'S MAGIC

NODEJS

Node.js is an open-source, cross-platform, JavaScript runtime environment that executes JavaScript code outside of a browser.

REDIS

Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache and message broker.

BLESSED LIBRARY

A high-level terminal interface library for node.js
https://pypi.org/project/blessed/

BLESSED-CONTRIB

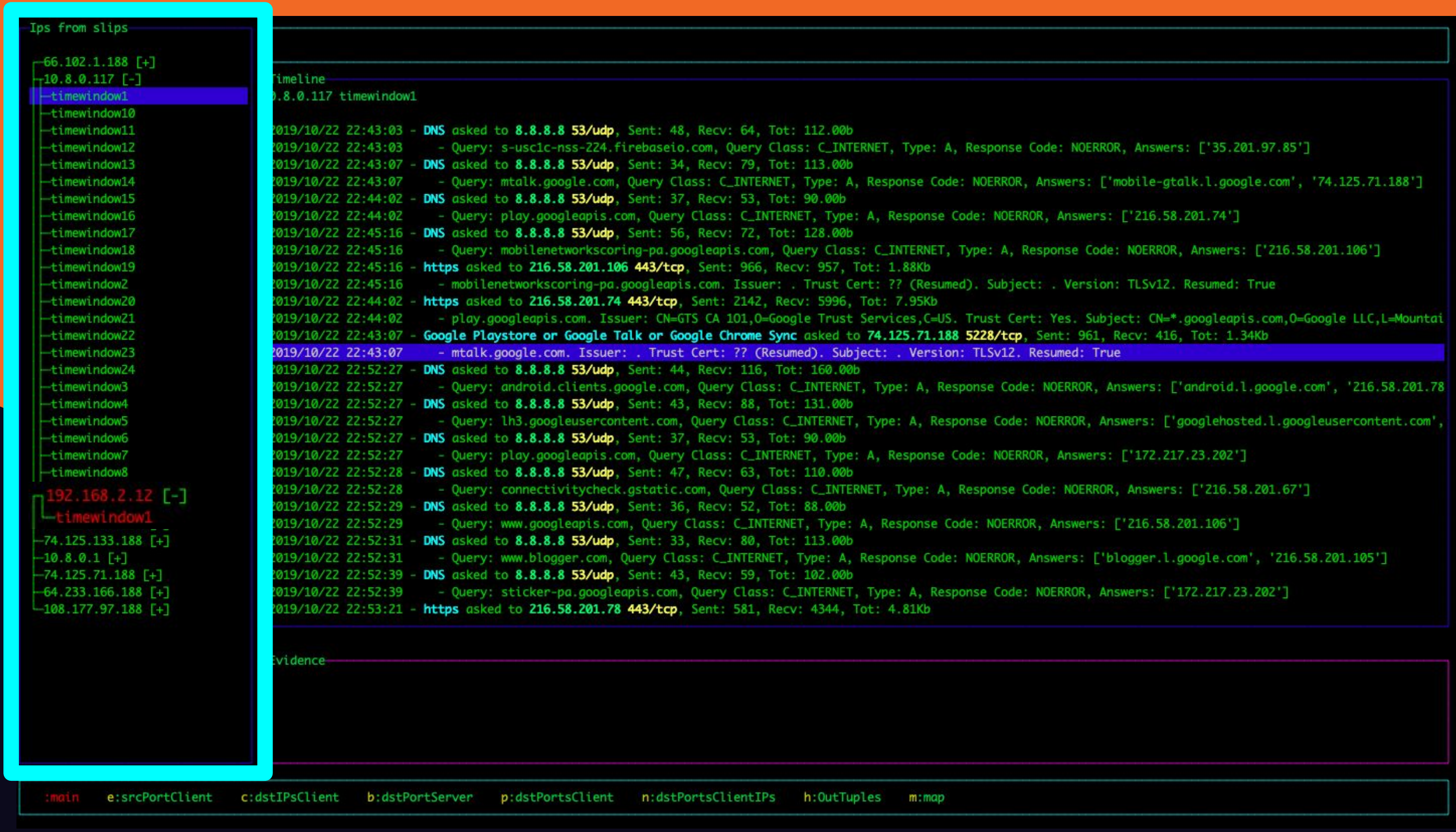
Build terminal dashboards using ascii/ansi art and javascript

https://github.com/yaronn/blessed-contrib

KALIPSO

PROFILES

All profiles and all the time windows when this profile communicated. Detected profiles and time windows are highlighted in red.



```
Ips from slips

┌66.102.1.188 [+]
├┬10.8.0.117 [-]
│├─timewindow1
│├─timewindow10
│├─timewindow11
│├─timewindow12
│├─timewindow13
│├─timewindow14
│├─timewindow15
│├─timewindow16
│├─timewindow17
│├─timewindow18
│├─timewindow19
│├─timewindow2
│├─timewindow20
│├─timewindow21
│├─timewindow22
│├─timewindow23
│├─timewindow24
│├─timewindow3
│├─timewindow4
│├─timewindow5
│├─timewindow6
│├─timewindow7
│└─timewindow8
├┬192.168.2.12 [-]
│└─timewindow1
├─74.125.133.188 [+]
├─10.8.0.1 [+]
├─74.125.71.188 [+]
├─64.233.166.188 [+]
└─108.177.97.188 [+]
```

```
Timeline
0.8.0.117 timewindow1

2019/10/22 22:43:03 - DNS asked to 8.8.8.8 53/udp, Sent: 48, Recv: 64, Tot: 112.00b
2019/10/22 22:43:03    - Query: s-usc1c-nss-224.firebaseio.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['35.201.97.85']
2019/10/22 22:43:07 - DNS asked to 8.8.8.8 53/udp, Sent: 34, Recv: 79, Tot: 113.00b
2019/10/22 22:43:07    - Query: mtalk.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['mobile-gtalk.l.google.com', '74.125.71.188']
2019/10/22 22:44:02 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
2019/10/22 22:44:02    - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.74']
2019/10/22 22:45:16 - DNS asked to 8.8.8.8 53/udp, Sent: 56, Recv: 72, Tot: 128.00b
2019/10/22 22:45:16    - Query: mobilenetworkscoring-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
2019/10/22 22:45:16 - https asked to 216.58.201.106 443/tcp, Sent: 966, Recv: 957, Tot: 1.88Kb
2019/10/22 22:45:16    - mobilenetworkscoring-pa.googleapis.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
2019/10/22 22:44:02 - https asked to 216.58.201.74 443/tcp, Sent: 2142, Recv: 5996, Tot: 7.95Kb
2019/10/22 22:44:02    - play.googleapis.com. Issuer: CN=GTS CA 101,O=Google Trust Services,C=US. Trust Cert: Yes. Subject: CN=*.googleapis.com,O=Google LLC,L=Mountai
2019/10/22 22:43:07 - Google Playstore or Google Talk or Google Chrome Sync asked to 74.125.71.188 5228/tcp, Sent: 961, Recv: 416, Tot: 1.34Kb
2019/10/22 22:43:07    - mtalk.google.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 44, Recv: 116, Tot: 160.00b
2019/10/22 22:52:27    - Query: android.clients.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['android.l.google.com', '216.58.201.78
2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 88, Tot: 131.00b
2019/10/22 22:52:27    - Query: lh3.googleusercontent.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['googlehosted.l.googleusercontent.com',
2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
2019/10/22 22:52:27    - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
2019/10/22 22:52:28 - DNS asked to 8.8.8.8 53/udp, Sent: 47, Recv: 63, Tot: 110.00b
2019/10/22 22:52:28    - Query: connectivitycheck.gstatic.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.67']
2019/10/22 22:52:29 - DNS asked to 8.8.8.8 53/udp, Sent: 36, Recv: 52, Tot: 88.00b
2019/10/22 22:52:29    - Query: www.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
2019/10/22 22:52:31 - DNS asked to 8.8.8.8 53/udp, Sent: 33, Recv: 80, Tot: 113.00b
2019/10/22 22:52:31    - Query: www.blogger.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['blogger.l.google.com', '216.58.201.105']
2019/10/22 22:52:39 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 59, Tot: 102.00b
2019/10/22 22:52:39    - Query: sticker-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
2019/10/22 22:53:21 - https asked to 216.58.201.78 443/tcp, Sent: 581, Recv: 4344, Tot: 4.81Kb
```

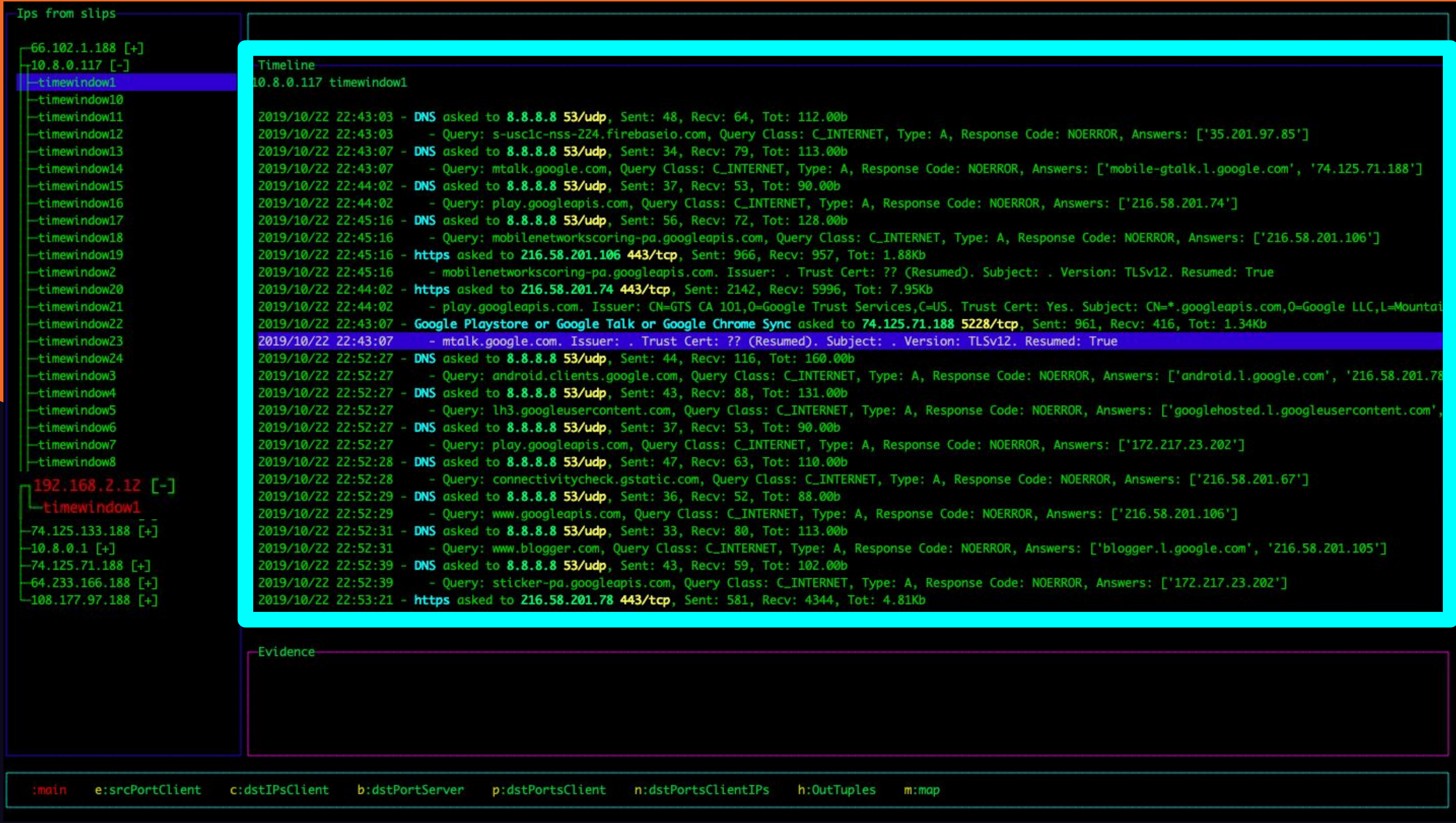
```
Evidence
```

```
:main    e:srcPortClient    c:dstIPsClient    b:dstPortServer    p:dstPortsClient    n:dstPortsClientIPs    h:OutTuples    m:map
```

KALIPSO

TIMELINE

A combined timeline of what happened and when. Based on Zeek files. Each main line (e.g DNS) has below its corresponding interpretation (Query:)



```
Ips from slips
┌66.102.1.188 [+]
├10.8.0.117 [-]
│ ├timewindow1
│ ├timewindow10
│ ├timewindow11
│ ├timewindow12
│ ├timewindow13
│ ├timewindow14
│ ├timewindow15
│ ├timewindow16
│ ├timewindow17
│ ├timewindow18
│ ├timewindow19
│ ├timewindow2
│ ├timewindow20
│ ├timewindow21
│ ├timewindow22
│ ├timewindow23
│ ├timewindow24
│ ├timewindow3
│ ├timewindow4
│ ├timewindow5
│ ├timewindow6
│ ├timewindow7
│ └timewindow8
├192.168.2.12 [-]
│ └timewindow1
├74.125.133.188 [+]
├10.8.0.1 [+]
├74.125.71.188 [+]
├64.233.166.188 [+]
└108.177.97.188 [+]
```

```
Timeline
10.8.0.117 timewindow1

2019/10/22 22:43:03 - DNS asked to 8.8.8.8 53/udp, Sent: 48, Recv: 64, Tot: 112.00b
2019/10/22 22:43:03     - Query: s-usc1c-nss-224.firebaseio.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['35.201.97.85']
2019/10/22 22:43:07 - DNS asked to 8.8.8.8 53/udp, Sent: 34, Recv: 79, Tot: 113.00b
2019/10/22 22:43:07     - Query: mtalk.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['mobile-gtalk.l.google.com', '74.125.71.188']
2019/10/22 22:44:02 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
2019/10/22 22:44:02     - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.74']
2019/10/22 22:45:16 - DNS asked to 8.8.8.8 53/udp, Sent: 56, Recv: 72, Tot: 128.00b
2019/10/22 22:45:16     - Query: mobilenetworkscoring-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
2019/10/22 22:45:16 - https asked to 216.58.201.106 443/tcp, Sent: 966, Recv: 957, Tot: 1.88Kb
2019/10/22 22:45:16     - mobilenetworkscoring-pa.googleapis.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
2019/10/22 22:44:02 - https asked to 216.58.201.74 443/tcp, Sent: 2142, Recv: 5996, Tot: 7.95Kb
2019/10/22 22:44:02     - play.googleapis.com. Issuer: CN=GTS CA 101,O=Google Trust Services,C=US. Trust Cert: Yes. Subject: CN=*.googleapis.com,O=Google LLC,L=Mountai
2019/10/22 22:43:07 - Google Playstore or Google Talk or Google Chrome Sync asked to 74.125.71.188 5228/tcp, Sent: 961, Recv: 416, Tot: 1.34Kb
2019/10/22 22:43:07     - mtalk.google.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 44, Recv: 116, Tot: 160.00b
2019/10/22 22:52:27     - Query: android.clients.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['android.l.google.com', '216.58.201.78
2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 88, Tot: 131.00b
2019/10/22 22:52:27     - Query: lh3.googleusercontent.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['googlehosted.l.googleusercontent.com',
2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
2019/10/22 22:52:27     - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
2019/10/22 22:52:28 - DNS asked to 8.8.8.8 53/udp, Sent: 47, Recv: 63, Tot: 110.00b
2019/10/22 22:52:28     - Query: connectivitycheck.gstatic.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.67']
2019/10/22 22:52:29 - DNS asked to 8.8.8.8 53/udp, Sent: 36, Recv: 52, Tot: 88.00b
2019/10/22 22:52:29     - Query: www.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
2019/10/22 22:52:31 - DNS asked to 8.8.8.8 53/udp, Sent: 33, Recv: 80, Tot: 113.00b
2019/10/22 22:52:31     - Query: www.blogger.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['blogger.l.google.com', '216.58.201.105']
2019/10/22 22:52:39 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 59, Tot: 102.00b
2019/10/22 22:52:39     - Query: sticker-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
2019/10/22 22:53:21 - https asked to 216.58.201.78 443/tcp, Sent: 581, Recv: 4344, Tot: 4.81Kb
```

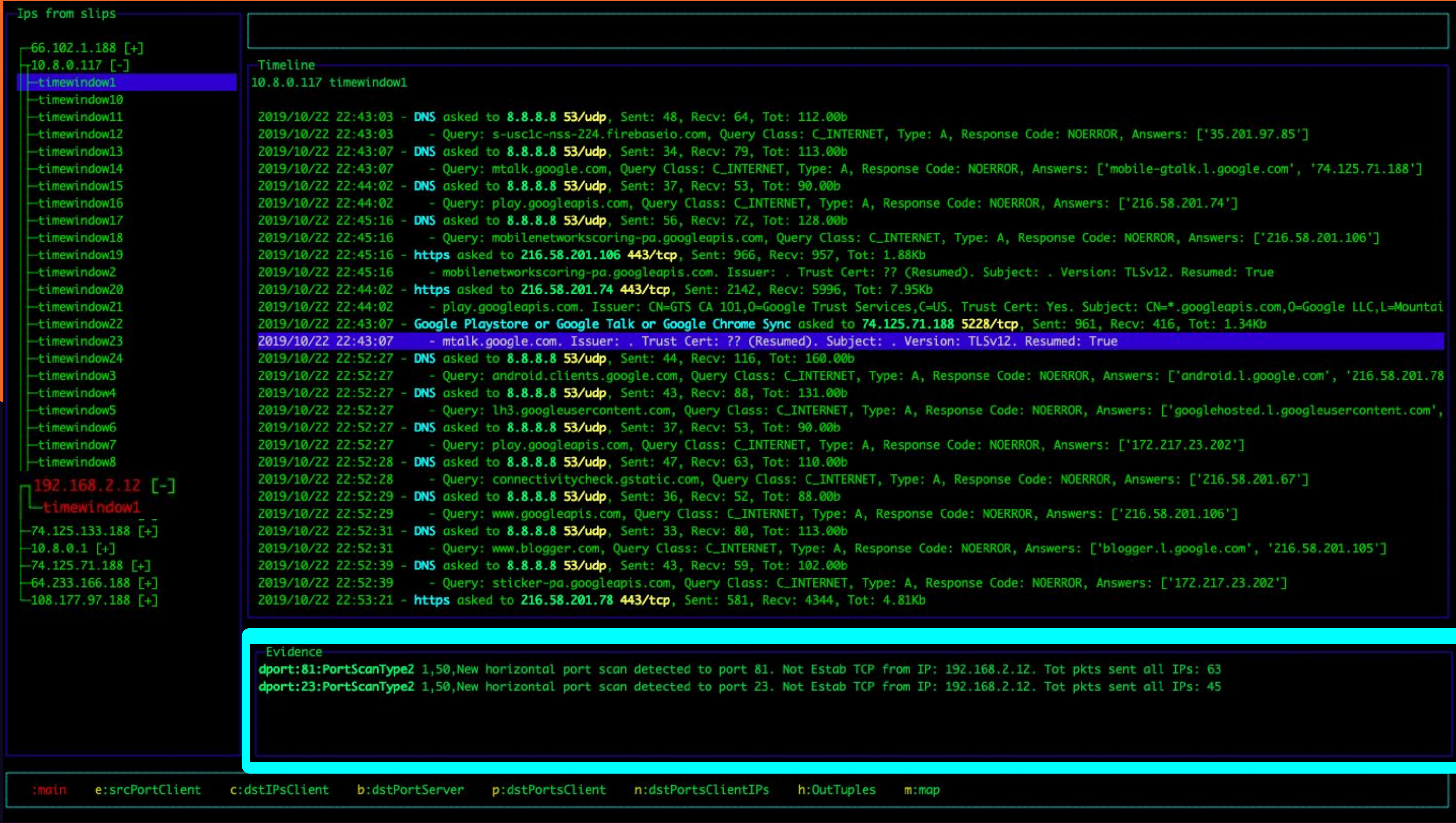
```
Evidence
```

```
:main   e:srcPortClient   c:dstIPsClient   b:dstPortServer   p:dstPortsClient   n:dstPortsClientIPs   h:OutTuples   m:map
```

KALIPSO

EVIDENCE

The evidence is generated by all detection modules. This is the supporting evidence for the detection.



```
Ips from slips

┌66.102.1.188 [+]
├10.8.0.117 [-]
│ ├timewindow1
│ ├timewindow10
│ ├timewindow11
│ ├timewindow12
│ ├timewindow13
│ ├timewindow14
│ ├timewindow15
│ ├timewindow16
│ ├timewindow17
│ ├timewindow18
│ ├timewindow19
│ ├timewindow2
│ ├timewindow20
│ ├timewindow21
│ ├timewindow22
│ ├timewindow23
│ ├timewindow24
│ ├timewindow3
│ ├timewindow4
│ ├timewindow5
│ ├timewindow6
│ ├timewindow7
│ └timewindow8
┌192.168.2.12 [-]
│ └timewindow1
├74.125.133.188 [+]
├10.8.0.1 [+]
├74.125.71.188 [+]
├64.233.166.188 [+]
└108.177.97.188 [+]
```

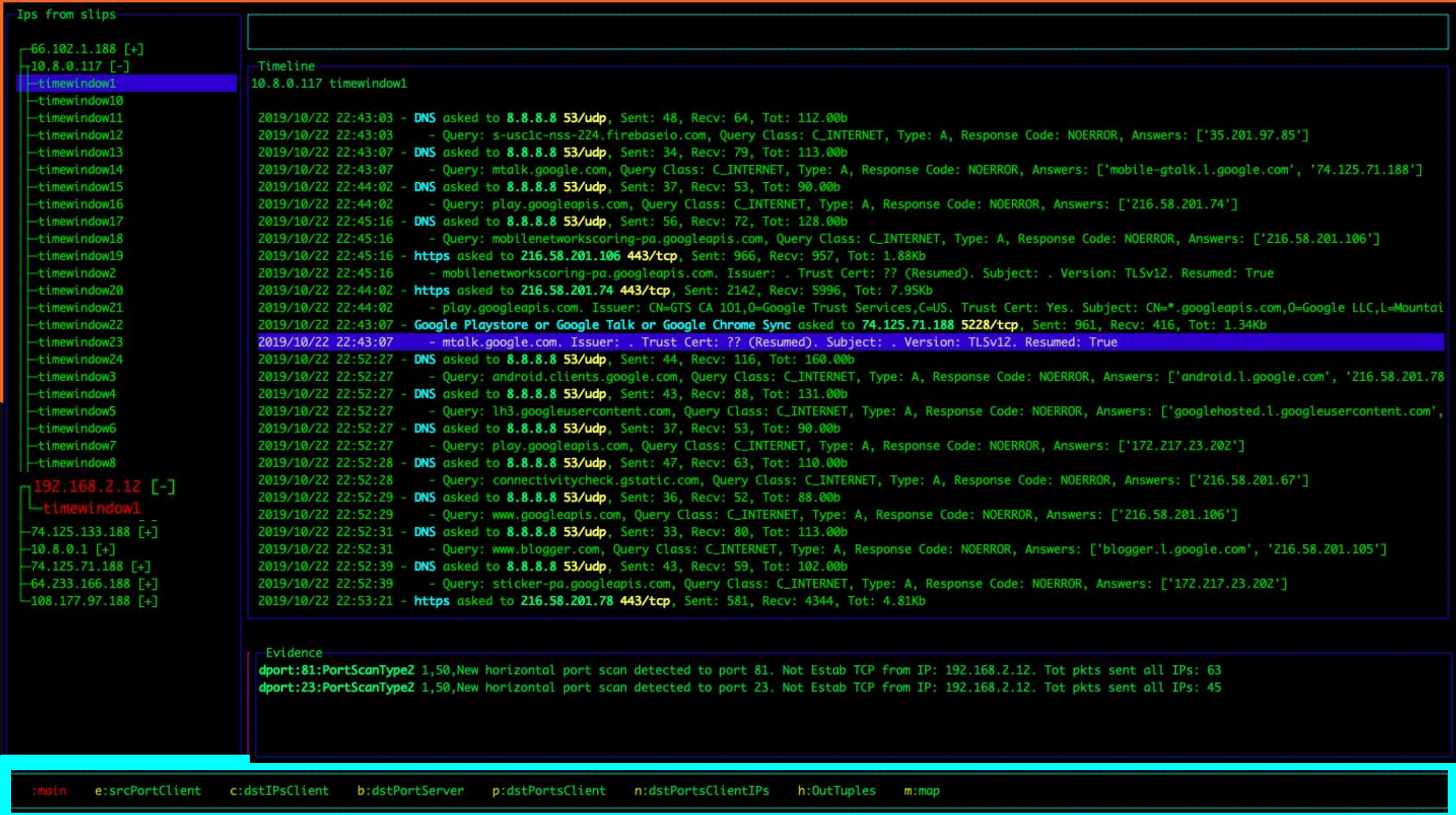
```
Timeline
10.8.0.117 timewindow1

 2019/10/22 22:43:03 - DNS asked to 8.8.8.8 53/udp, Sent: 48, Recv: 64, Tot: 112.00b
 2019/10/22 22:43:03     - Query: s-usc1c-nss-224.firebaseio.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['35.201.97.85']
 2019/10/22 22:43:07 - DNS asked to 8.8.8.8 53/udp, Sent: 34, Recv: 79, Tot: 113.00b
 2019/10/22 22:43:07     - Query: mtalk.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['mobile-gtalk.l.google.com', '74.125.71.188']
 2019/10/22 22:44:02 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
 2019/10/22 22:44:02     - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.74']
 2019/10/22 22:45:16 - DNS asked to 8.8.8.8 53/udp, Sent: 56, Recv: 72, Tot: 128.00b
 2019/10/22 22:45:16     - Query: mobilenetworkscoring-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
 2019/10/22 22:45:16 - https asked to 216.58.201.106 443/tcp, Sent: 966, Recv: 957, Tot: 1.88Kb
 2019/10/22 22:45:16     - mobilenetworkscoring-pa.googleapis.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
 2019/10/22 22:44:02 - https asked to 216.58.201.74 443/tcp, Sent: 2142, Recv: 5996, Tot: 7.95Kb
 2019/10/22 22:44:02     - play.googleapis.com. Issuer: CN=GTS CA 1O1,O=Google Trust Services,C=US. Trust Cert: Yes. Subject: CN=*.googleapis.com,O=Google LLC,L=Mountai
 2019/10/22 22:43:07 - Google Playstore or Google Talk or Google Chrome Sync asked to 74.125.71.188 5228/tcp, Sent: 961, Recv: 416, Tot: 1.34Kb
 2019/10/22 22:43:07     - mtalk.google.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
 2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 44, Recv: 116, Tot: 160.00b
 2019/10/22 22:52:27     - Query: android.clients.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['android.l.google.com', '216.58.201.78
 2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 88, Tot: 131.00b
 2019/10/22 22:52:27     - Query: lh3.googleusercontent.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['googlehosted.l.googleusercontent.com',
 2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
 2019/10/22 22:52:27     - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
 2019/10/22 22:52:28 - DNS asked to 8.8.8.8 53/udp, Sent: 47, Recv: 63, Tot: 110.00b
 2019/10/22 22:52:28     - Query: connectivitycheck.gstatic.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.67']
 2019/10/22 22:52:29 - DNS asked to 8.8.8.8 53/udp, Sent: 36, Recv: 52, Tot: 88.00b
 2019/10/22 22:52:29     - Query: www.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
 2019/10/22 22:52:31 - DNS asked to 8.8.8.8 53/udp, Sent: 33, Recv: 80, Tot: 113.00b
 2019/10/22 22:52:31     - Query: www.blogger.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['blogger.l.google.com', '216.58.201.105']
 2019/10/22 22:52:39 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 59, Tot: 102.00b
 2019/10/22 22:52:39     - Query: sticker-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
 2019/10/22 22:53:21 - https asked to 216.58.201.78 443/tcp, Sent: 581, Recv: 4344, Tot: 4.81Kb
```

```
Evidence
dport:81:PortScanType2 1,50,New horizontal port scan detected to port 81. Not Estab TCP from IP: 192.168.2.12. Tot pkts sent all IPs: 63
dport:23:PortScanType2 1,50,New horizontal port scan detected to port 23. Not Estab TCP from IP: 192.168.2.12. Tot pkts sent all IPs: 45
```

KALIPSO

HOTKEYS

Help on what you can do



```
Ips from slips
┌66.102.1.188 [+]
├10.8.0.117 [-]
│├timewindow1
│├timewindow10
│├timewindow11
│├timewindow12
│├timewindow13
│├timewindow14
│├timewindow15
│├timewindow16
│├timewindow17
│├timewindow18
│├timewindow19
│├timewindow2
│├timewindow20
│├timewindow21
│├timewindow22
│├timewindow23
│├timewindow24
│├timewindow3
│├timewindow4
│├timewindow5
│├timewindow6
│├timewindow7
│└timewindow8
├192.168.2.12 [-]
│└timewindow1
├74.125.133.188 [+]
├10.8.0.1 [+]
├74.125.71.188 [+]
├64.233.166.188 [+]
└108.177.97.188 [+]
```

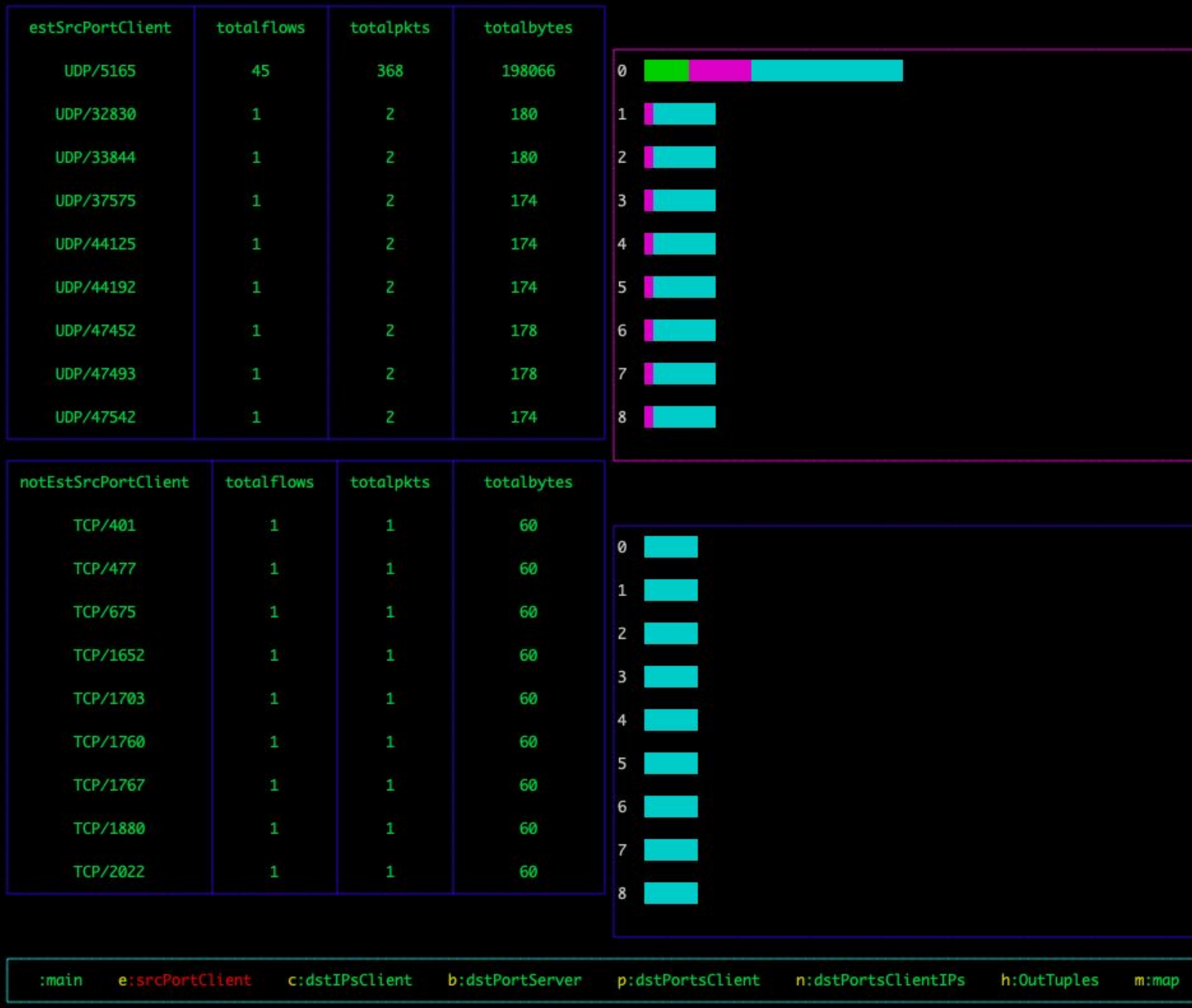
```
Timeline
10.8.0.117 timewindow1

 2019/10/22 22:43:03 - DNS asked to 8.8.8.8 53/udp, Sent: 48, Recv: 64, Tot: 112.00b
 2019/10/22 22:43:03     - Query: s-usc1c-nss-224.firebaseio.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['35.201.97.85']
 2019/10/22 22:43:07 - DNS asked to 8.8.8.8 53/udp, Sent: 34, Recv: 79, Tot: 113.00b
 2019/10/22 22:43:07     - Query: mtalk.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['mobile-gtalk.l.google.com', '74.125.71.188']
 2019/10/22 22:44:02 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
 2019/10/22 22:44:02     - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.74']
 2019/10/22 22:45:16 - DNS asked to 8.8.8.8 53/udp, Sent: 56, Recv: 72, Tot: 128.00b
 2019/10/22 22:45:16     - Query: mobilenetworkscoring-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
 2019/10/22 22:45:16 - https asked to 216.58.201.106 443/tcp, Sent: 966, Recv: 957, Tot: 1.88Kb
 2019/10/22 22:45:16     - mobilenetworkscoring-pa.googleapis.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
 2019/10/22 22:44:02 - https asked to 216.58.201.74 443/tcp, Sent: 2142, Recv: 5996, Tot: 7.95Kb
 2019/10/22 22:44:02     - play.googleapis.com. Issuer: CN=GTS CA 101,O=Google Trust Services,C=US. Trust Cert: Yes. Subject: CN=*.googleapis.com,O=Google LLC,L=Mountai
 2019/10/22 22:43:07 - Google Playstore or Google Talk or Google Chrome Sync asked to 74.125.71.188 5228/tcp, Sent: 961, Recv: 416, Tot: 1.34Kb
 2019/10/22 22:43:07     - mtalk.google.com. Issuer: . Trust Cert: ?? (Resumed). Subject: . Version: TLSv12. Resumed: True
 2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 44, Recv: 116, Tot: 160.00b
 2019/10/22 22:52:27     - Query: android.clients.google.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['android.l.google.com', '216.58.201.78
 2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 88, Tot: 131.00b
 2019/10/22 22:52:27     - Query: lh3.googleusercontent.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['googlehosted.l.googleusercontent.com',
 2019/10/22 22:52:27 - DNS asked to 8.8.8.8 53/udp, Sent: 37, Recv: 53, Tot: 90.00b
 2019/10/22 22:52:27     - Query: play.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
 2019/10/22 22:52:28 - DNS asked to 8.8.8.8 53/udp, Sent: 47, Recv: 63, Tot: 110.00b
 2019/10/22 22:52:28     - Query: connectivitycheck.gstatic.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.67']
 2019/10/22 22:52:29 - DNS asked to 8.8.8.8 53/udp, Sent: 36, Recv: 52, Tot: 88.00b
 2019/10/22 22:52:29     - Query: www.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['216.58.201.106']
 2019/10/22 22:52:31 - DNS asked to 8.8.8.8 53/udp, Sent: 33, Recv: 80, Tot: 113.00b
 2019/10/22 22:52:31     - Query: www.blogger.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['blogger.l.google.com', '216.58.201.105']
 2019/10/22 22:52:39 - DNS asked to 8.8.8.8 53/udp, Sent: 43, Recv: 59, Tot: 102.00b
 2019/10/22 22:52:39     - Query: sticker-pa.googleapis.com, Query Class: C_INTERNET, Type: A, Response Code: NOERROR, Answers: ['172.217.23.202']
 2019/10/22 22:53:21 - https asked to 216.58.201.78 443/tcp, Sent: 581, Recv: 4344, Tot: 4.81Kb
```

```
Evidence
dport:81:PortScanType2 1,50,New horizontal port scan detected to port 81. Not Estab TCP from IP: 192.168.2.12. Tot pkts sent all IPs: 63
dport:23:PortScanType2 1,50,New horizontal port scan detected to port 23. Not Estab TCP from IP: 192.168.2.12. Tot pkts sent all IPs: 45
```

KALIPSO

E HOTKEY

Src ports when the IP of the profile acted as **client.** Separated in Established and Not Established histograms. Shows the amount of total flows, total packets and total bytes going in a specific source port.



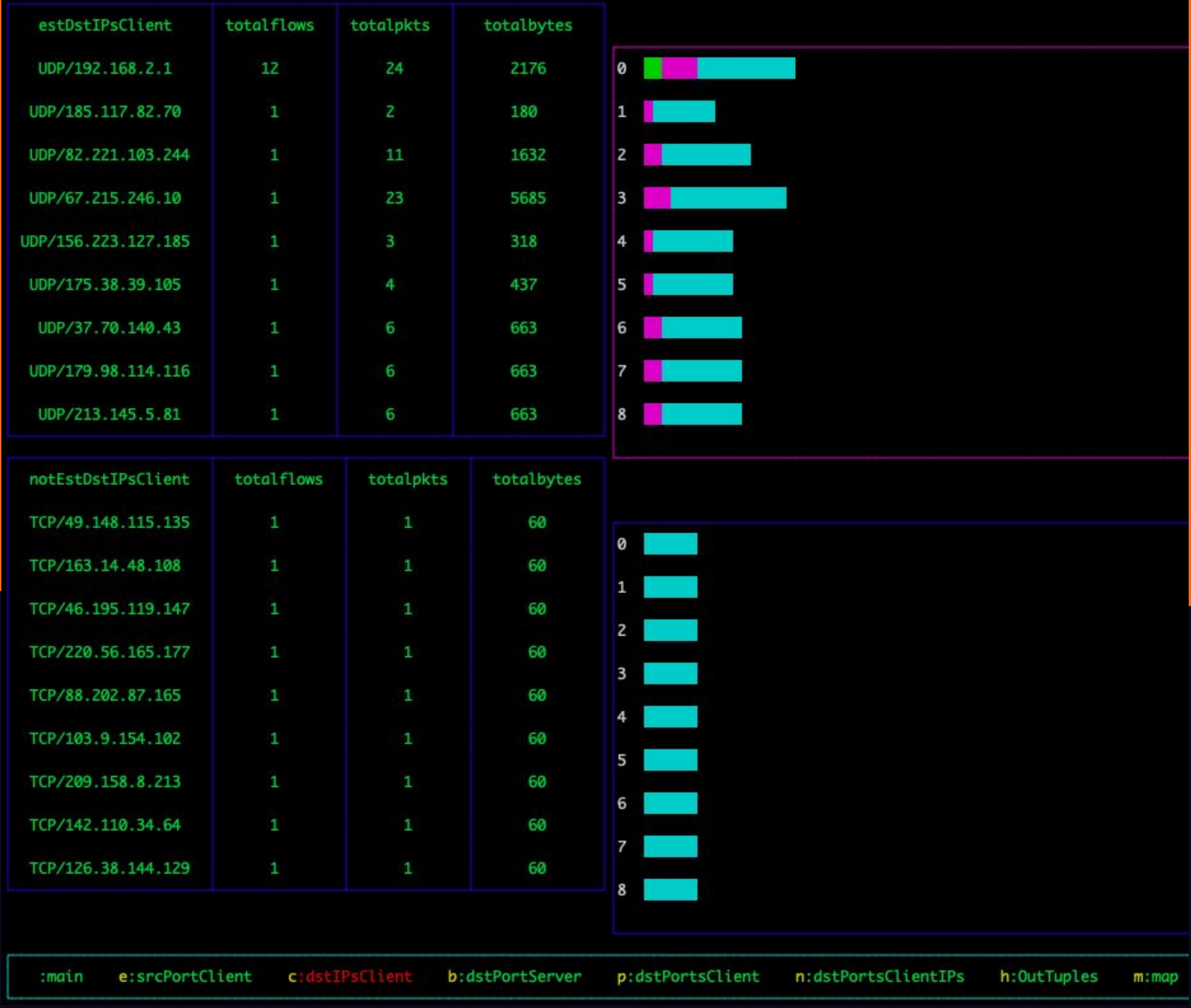
estSrcPortClient	totalflows	totalpkts	totalbytes
UDP/5165	45	368	198066
UDP/32830	1	2	180
UDP/33844	1	2	180
UDP/37575	1	2	174
UDP/44125	1	2	174
UDP/44192	1	2	174
UDP/47452	1	2	178
UDP/47493	1	2	178
UDP/47542	1	2	174

notEstSrcPortClient	totalflows	totalpkts	totalbytes
TCP/401	1	1	60
TCP/477	1	1	60
TCP/675	1	1	60
TCP/1652	1	1	60
TCP/1703	1	1	60
TCP/1760	1	1	60
TCP/1767	1	1	60
TCP/1880	1	1	60
TCP/2022	1	1	60

KALIPSO

C HOTKEY

Dst IPs when the IP of the profiles acted as **client**. Separated in Established and Not Established histograms. Shows the amount of total flows, total packets and total bytes going to a specific dst IP.



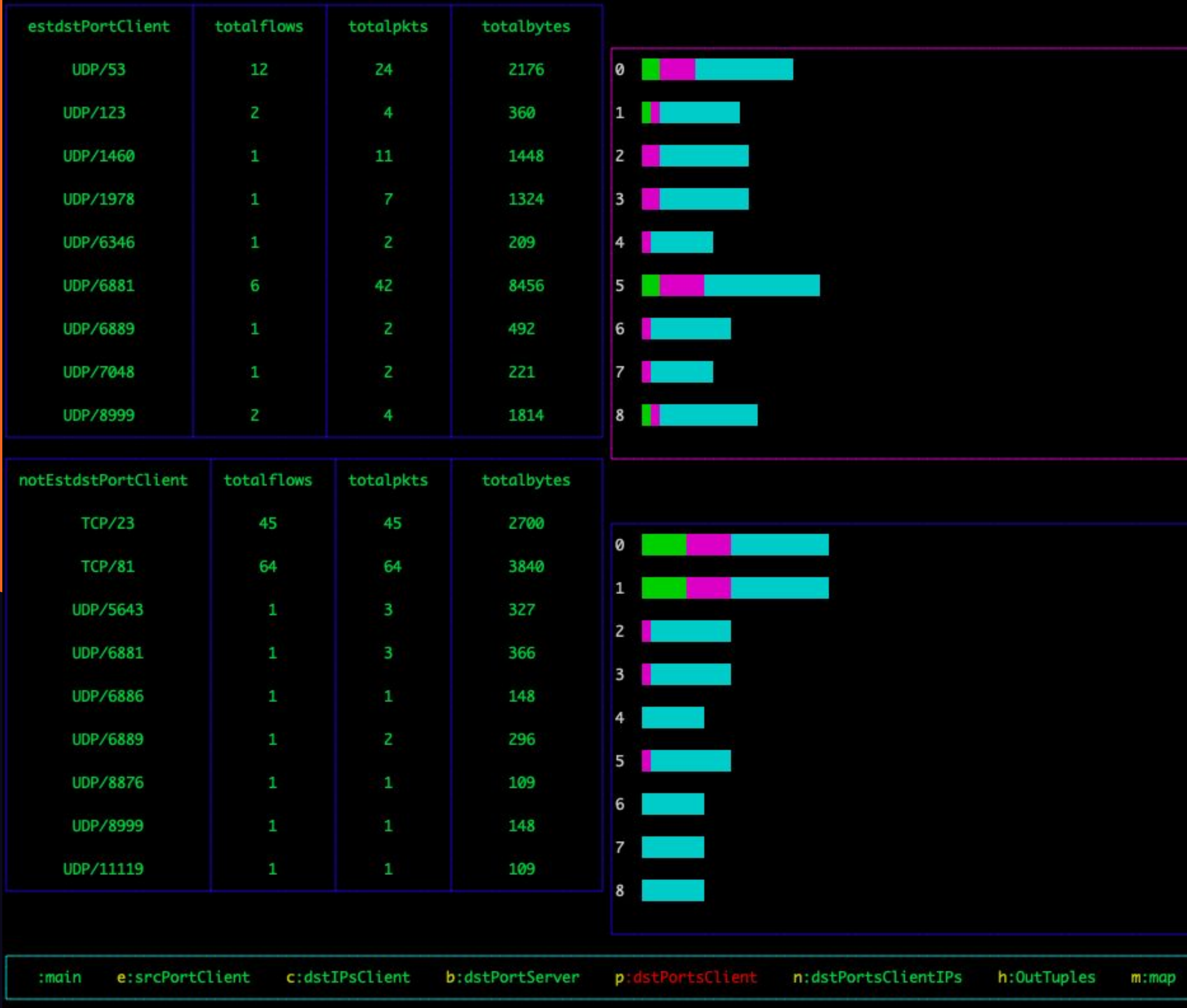
estDstIPsClient	totalflows	totalpkts	totalbytes
UDP/192.168.2.1	12	24	2176
UDP/185.117.82.70	1	2	180
UDP/82.221.103.244	1	11	1632
UDP/67.215.246.10	1	23	5685
UDP/156.223.127.185	1	3	318
UDP/175.38.39.105	1	4	437
UDP/37.70.140.43	1	6	663
UDP/179.98.114.116	1	6	663
UDP/213.145.5.81	1	6	663

notEstDstIPsClient	totalflows	totalpkts	totalbytes
TCP/49.148.115.135	1	1	60
TCP/163.14.48.108	1	1	60
TCP/46.195.119.147	1	1	60
TCP/220.56.165.177	1	1	60
TCP/88.202.87.165	1	1	60
TCP/103.9.154.102	1	1	60
TCP/209.158.8.213	1	1	60
TCP/142.110.34.64	1	1	60
TCP/126.38.144.129	1	1	60

KALIPSO

P HOTKEY

Dst ports when the IP of the profile acted as **client**. Separated in Established and Not Established histograms. Shows the amount of total flows, total bytes and total packets going to a specific dst port.



```
estdstPortClient   totalflows   totalpkts   totalbytes

     UDP/53            12           24         2176
     UDP/123            2            4          360
     UDP/1460           1           11         1448
     UDP/1978           1            7         1324
     UDP/6346           1            2          209
     UDP/6881           6           42         8456
     UDP/6889           1            2          492
     UDP/7048           1            2          221
     UDP/8999           2            4         1814
```

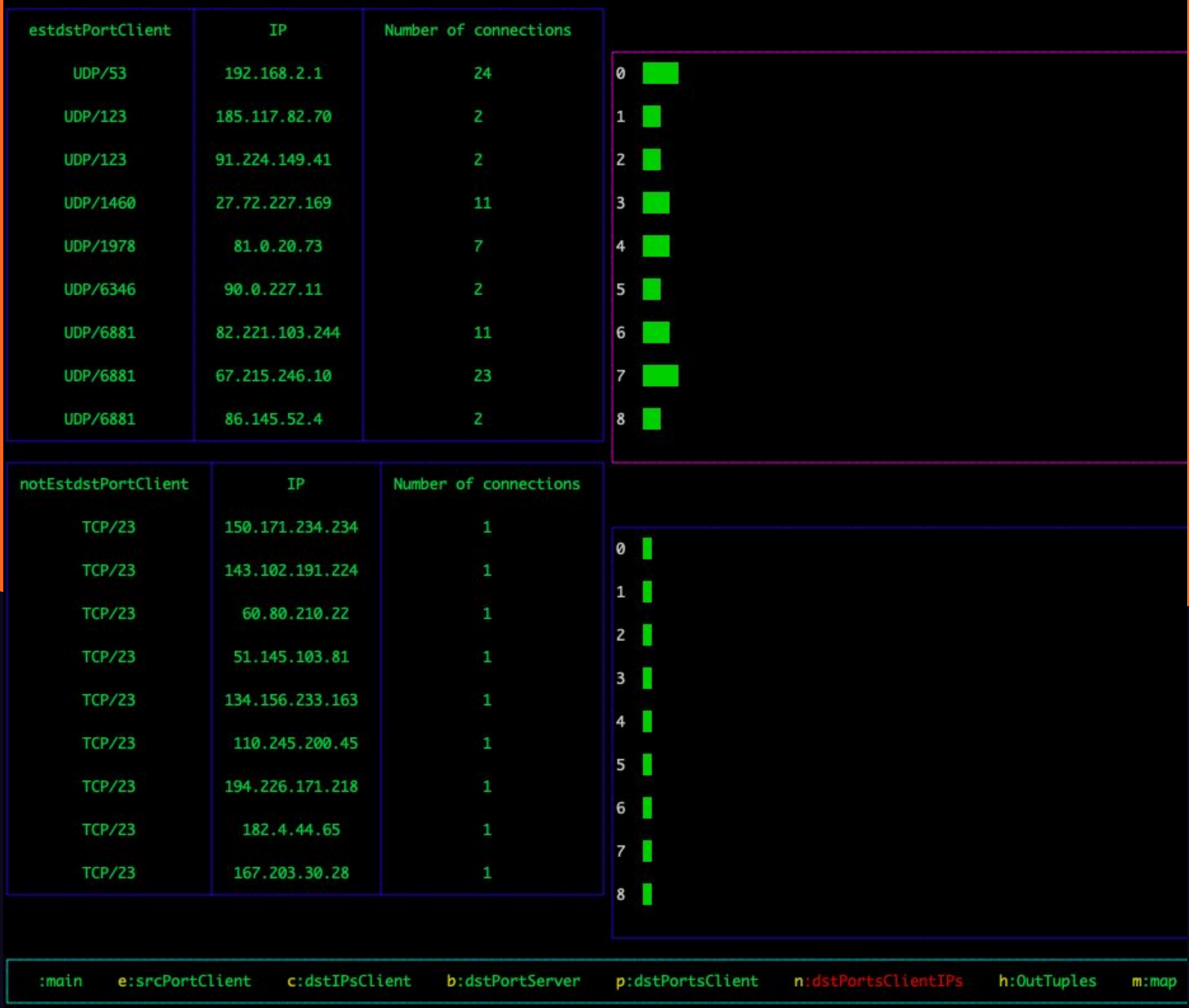
```
notEstdstPortClient   totalflows   totalpkts   totalbytes

       TCP/23             45           45         2700
       TCP/81             64           64         3840
       UDP/5643            1            3          327
       UDP/6881            1            3          366
       UDP/6886            1            1          148
       UDP/6889            1            2          296
       UDP/8876            1            1          109
       UDP/8999            1            1          148
       UDP/11119           1            1          109
```

```
:main   e:srcPortClient   c:dstIPsClient   b:dstPortServer   p:dstPortsClient   n:dstPortsClientIPs   h:OutTuples   m:map
```

KALIPSO

N HOTKEY

Dst Ports when the IP of the profile acted as **client**. Separated in Established and not Established histograms. Shows the amount of connections to a dst IP on a specific port .



estdstPortClient	IP	Number of connections
UDP/53	192.168.2.1	24
UDP/123	185.117.82.70	2
UDP/123	91.224.149.41	2
UDP/1460	27.72.227.169	11
UDP/1978	81.0.20.73	7
UDP/6346	90.0.227.11	2
UDP/6881	82.221.103.244	11
UDP/6881	67.215.246.10	23
UDP/6881	86.145.52.4	2

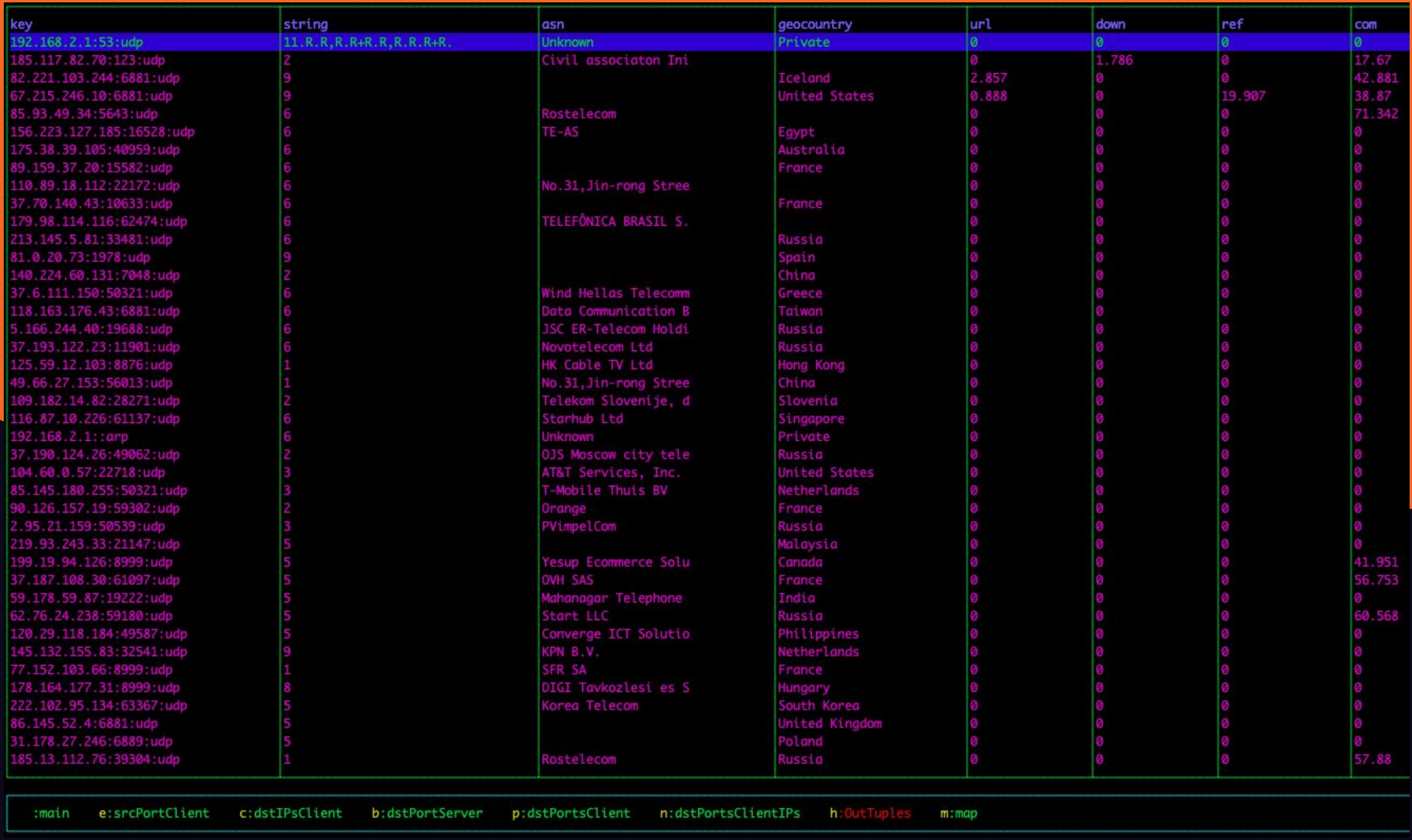
notEstdstPortClient	IP	Number of connections
TCP/23	150.171.234.234	1
TCP/23	143.102.191.224	1
TCP/23	60.80.210.22	1
TCP/23	51.145.103.81	1
TCP/23	134.156.233.163	1
TCP/23	110.245.200.45	1
TCP/23	194.226.171.218	1
TCP/23	182.4.44.65	1
TCP/23	167.203.30.28	1

```
:main    e:srcPortClient    c:dstIPsClient    b:dstPortServer    p:dstPortsClient    n:dstPortsClientIPs    h:OutTuples    m:map
```

KALIPSO

H HOTKEY

Out Tuples Behavioral letters about the out tuples ‘IP-port-protocol’ combined together with ASN, geo country and Virus Total summary

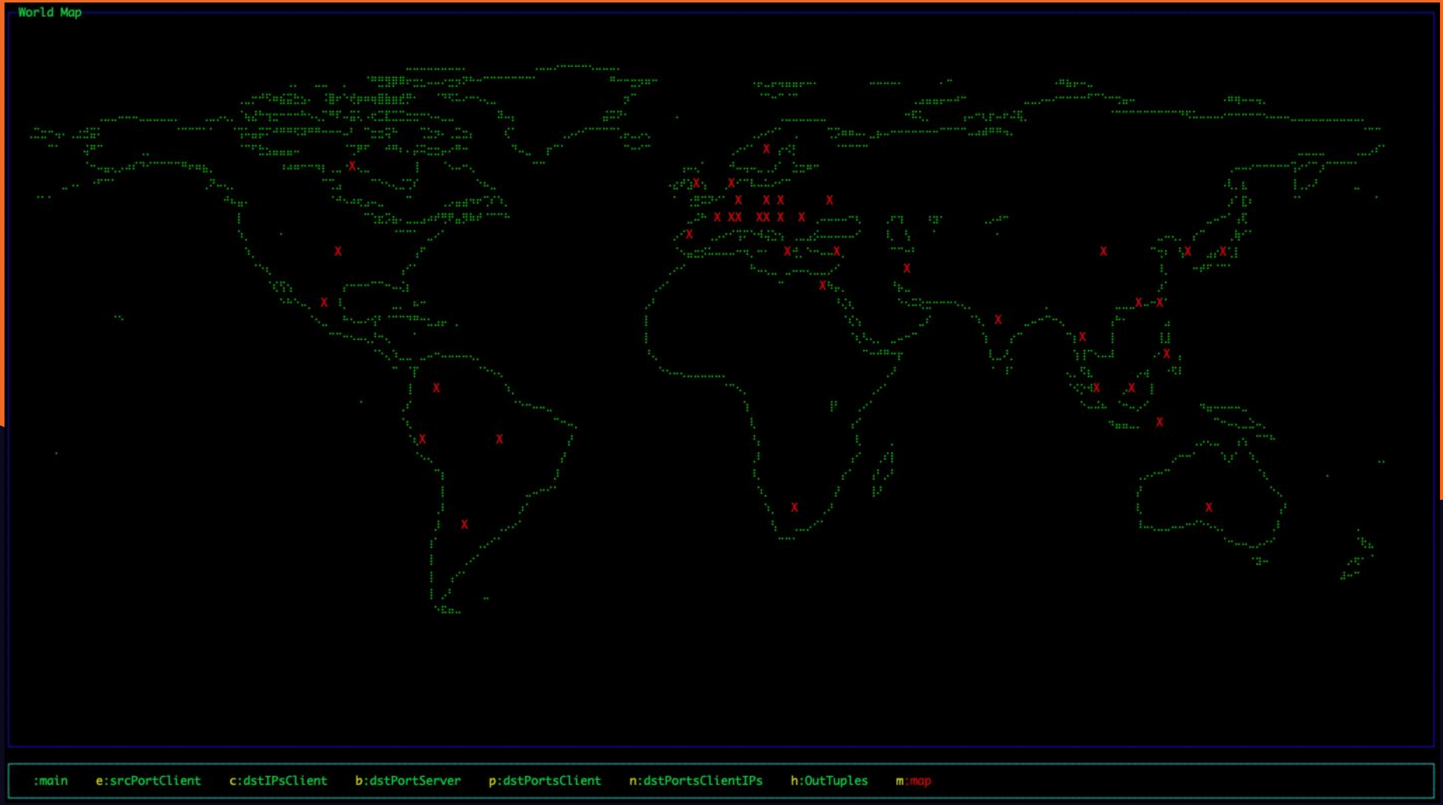


```
key                          string                  asn                    geocountry       url        down       ref         com
192.168.2.1:53:udp           11.R.R,R.R+R.R,R.R.R+R. Unknown                Private          0          0          0           0
185.117.82.70:123:udp        2                       Civil associaton Ini                    0          1.786      0           17.67
82.221.103.244:6881:udp      9                                              Iceland          2.857      0          0           42.881
67.215.246.10:6881:udp       9                                              United States    0.888      0          19.907      38.87
85.93.49.34:5643:udp         6                       Rostelecom                              0          0          0           71.342
156.223.127.185:16528:udp    6                       TE-AS                  Egypt            0          0          0           0
175.38.39.105:40959:udp      6                                              Australia        0          0          0           0
89.159.37.20:15582:udp       6                                              France           0          0          0           0
110.89.18.112:22172:udp      6                       No.31,Jin-rong Stree                    0          0          0           0
37.70.140.43:10633:udp       6                                              France           0          0          0           0
179.98.114.116:62474:udp     6                       TELEFÔNICA BRASIL S.                    0          0          0           0
213.145.5.81:33481:udp       6                                              Russia           0          0          0           0
81.0.20.73:1978:udp          9                                              Spain            0          0          0           0
140.224.60.131:7048:udp      2                                              China            0          0          0           0
37.6.111.150:50321:udp       6                       Wind Hellas Telecomm   Greece           0          0          0           0
118.163.176.43:6881:udp      6                       Data Communication B   Taiwan           0          0          0           0
5.166.244.40:19688:udp       6                       JSC ER-Telecom Holdi   Russia           0          0          0           0
37.193.122.23:11901:udp      6                       Novotelecom Ltd        Russia           0          0          0           0
125.59.12.103:8876:udp       1                       HK Cable TV Ltd        Hong Kong        0          0          0           0
49.66.27.153:56013:udp       1                       No.31,Jin-rong Stree   China            0          0          0           0
109.182.14.82:28271:udp      2                       Telekom Slovenije, d   Slovenia         0          0          0           0
116.87.10.226:61137:udp      6                       Starhub Ltd            Singapore        0          0          0           0
192.168.2.1::arp             6                       Unknown                Private          0          0          0           0
37.190.124.26:49062:udp      2                       OJS Moscow city tele   Russia           0          0          0           0
104.60.0.57:22718:udp        3                       AT&T Services, Inc.    United States    0          0          0           0
85.145.180.255:50321:udp     3                       T-Mobile Thuis BV      Netherlands      0          0          0           0
90.126.157.19:59302:udp      2                       Orange                 France           0          0          0           0
2.95.21.159:50539:udp        3                       PVimpelCom             Russia           0          0          0           0
219.93.243.33:21147:udp      5                                              Malaysia         0          0          0           0
199.19.94.126:8999:udp       5                       Yesup Ecommerce Solu   Canada           0          0          0           41.951
37.187.108.30:61097:udp      5                       OVH SAS                France           0          0          0           56.753
59.178.59.87:19222:udp       5                       Mahanagar Telephone    India            0          0          0           0
62.76.24.238:59180:udp       5                       Start LLC              Russia           0          0          0           60.568
120.29.118.184:49587:udp     5                       Converge ICT Solutio   Philippines      0          0          0           0
145.132.155.83:32541:udp     9                       KPN B.V.               Netherlands      0          0          0           0
77.152.103.66:8999:udp       1                       SFR SA                 France           0          0          0           0
178.164.177.31:8999:udp      8                       DIGI Tavkozlesi es S   Hungary          0          0          0           0
222.102.95.134:63367:udp     5                       Korea Telecom          South Korea      0          0          0           0
86.145.52.4:6881:udp         5                                              United Kingdom   0          0          0           0
31.178.27.246:6889:udp       5                                              Poland           0          0          0           0
185.13.112.76:39304:udp      1                       Rostelecom             Russia           0          0          0           57.88

   :main    e:srcPortClient    c:dstIPsClient    b:dstPortServer    p:dstPortsClient    n:dstPortsClientIPs    h:OutTuples    m:map
```

KALIPSO

M HOTKEY

Shows geolocations of all dst IPs to which the src IP of the profile connected to during the time window.



INSTALLATION

HTTPS://GITHUB.COM/STRATOSPHEREIPS/STRATOSPHERELINUXIPS

THANK YOU!

KAMILA BABAYEVA
BABAYKAM@FEL.CVUT.CZ,
@_KAMIFAI_

SEBASTIAN GARCIA
SEBASTIAN.GARCIA@AGENT.
FEL.CVUT.CZ, @ELDRACOTE

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.