pktvisor.

summarizing traffic for observability and DDoS mitigation

Shannon Weyrick ◦ VP Research @ NS1 ◦ Office of CTO
sweyrick@ns1.com

pktvisor.com · IDS 2021

NS1.

1. pktvisor in 15 mins

2. Deeper Dive

3. The Future: Orb

pktvisor in 15 mins

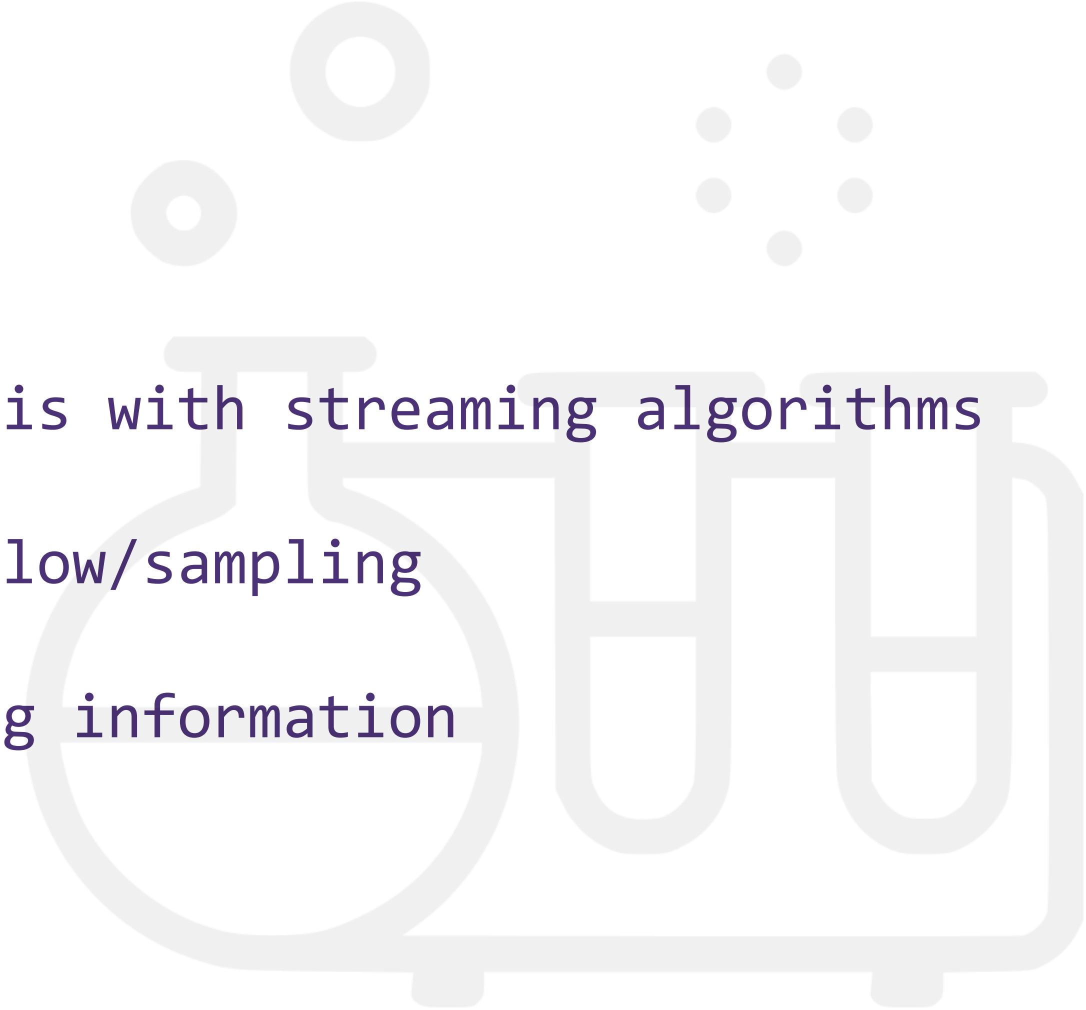
What is pktvisor?

- Open Source observability *Agent*
- *Taps into* pcap and (soon) DNSTAP streams
- *Summarizes* critical data from streams
- Provides both *Local* and *Global* visibility

What is pktvisor *not*?

- A full packet capture system
- A query audit log system
- A database
- Resource heavy

Why pktvisor?

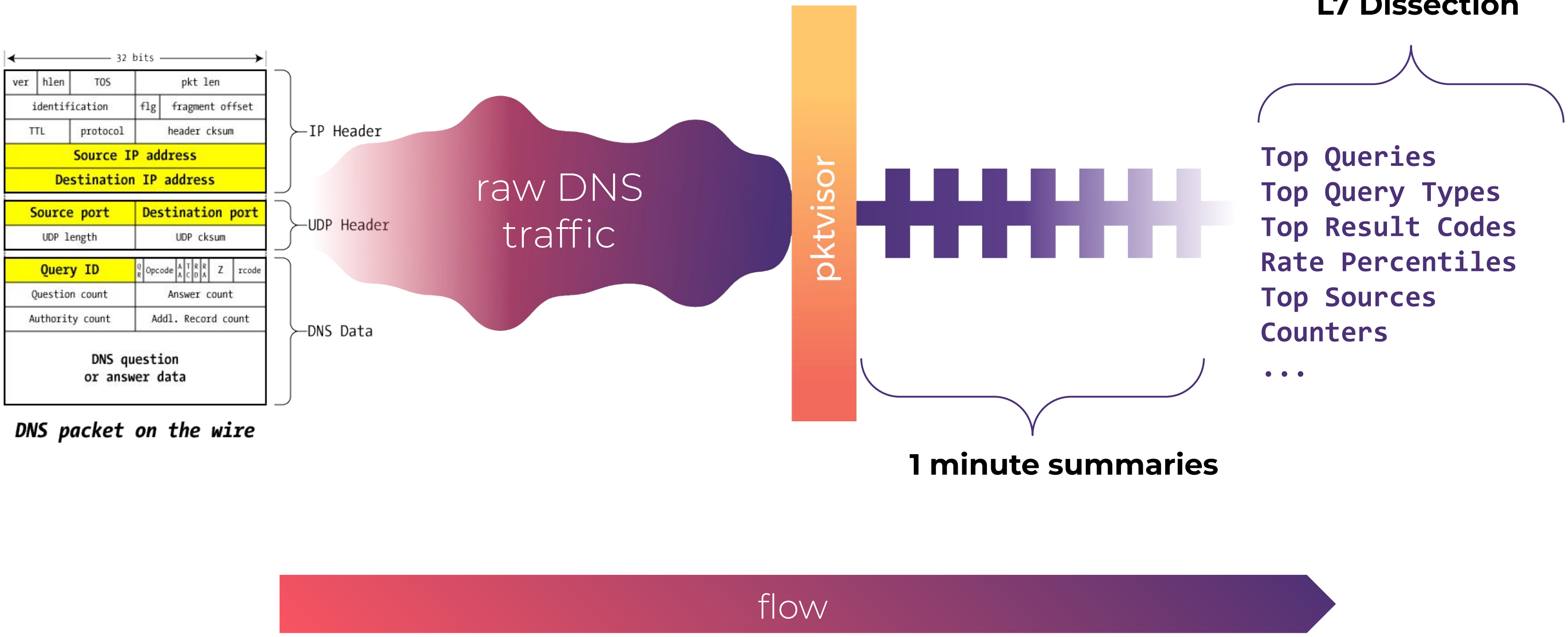


- Deep L7 analysis with streaming algorithms
- Not based on flow/sampling
- Small data, big information

pktvisor extracts signal and produces summaries

- “Signal” is critical Net and DNS info
- Summarizes into live + 1 minute buckets
- JSON output is ~4kb *per bucket*
- ...regardless of input throughput!

DNS signal extraction



ver	hlen	TOS	pkt len
identification		flg	fragment offset
TTL	protocol	header cksum	
Source IP address			
Destination IP address			
Source port		Destination port	
UDP length		UDP cksum	
Query ID		QR Opcode AA TC RD RA Z rcode	
Question count		Answer count	
Authority count		Addl. Record count	
DNS question or answer data			

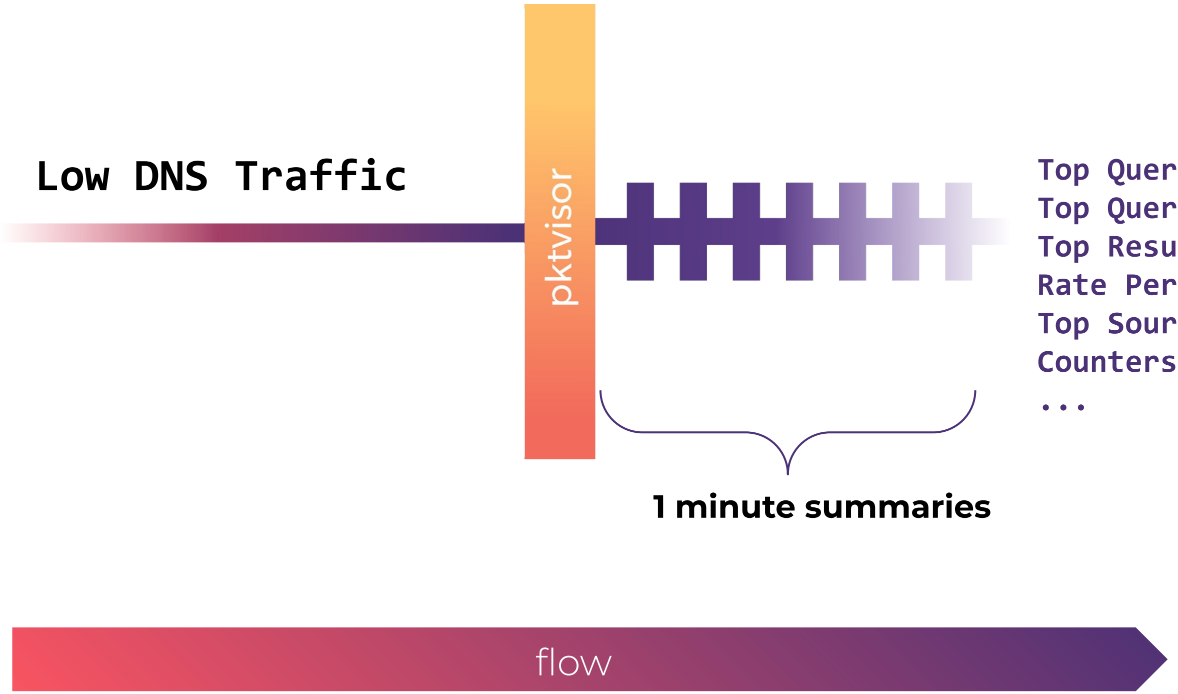
DNS packet on the wire

L7 Dissection

Top Queries
Top Query Types
Top Result Codes
Rate Percentiles
Top Sources
Counters
...

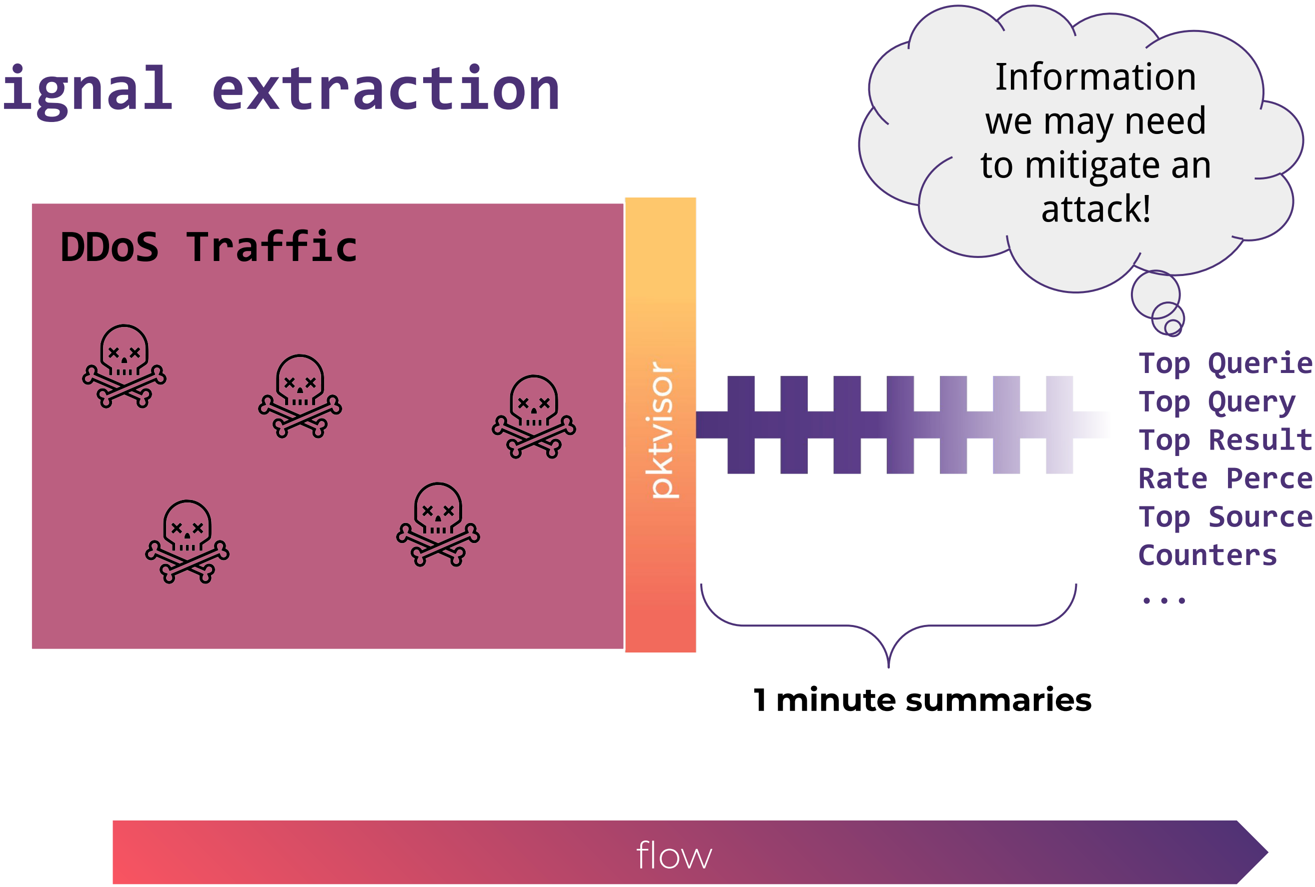
1 minute summaries

DNS signal extraction



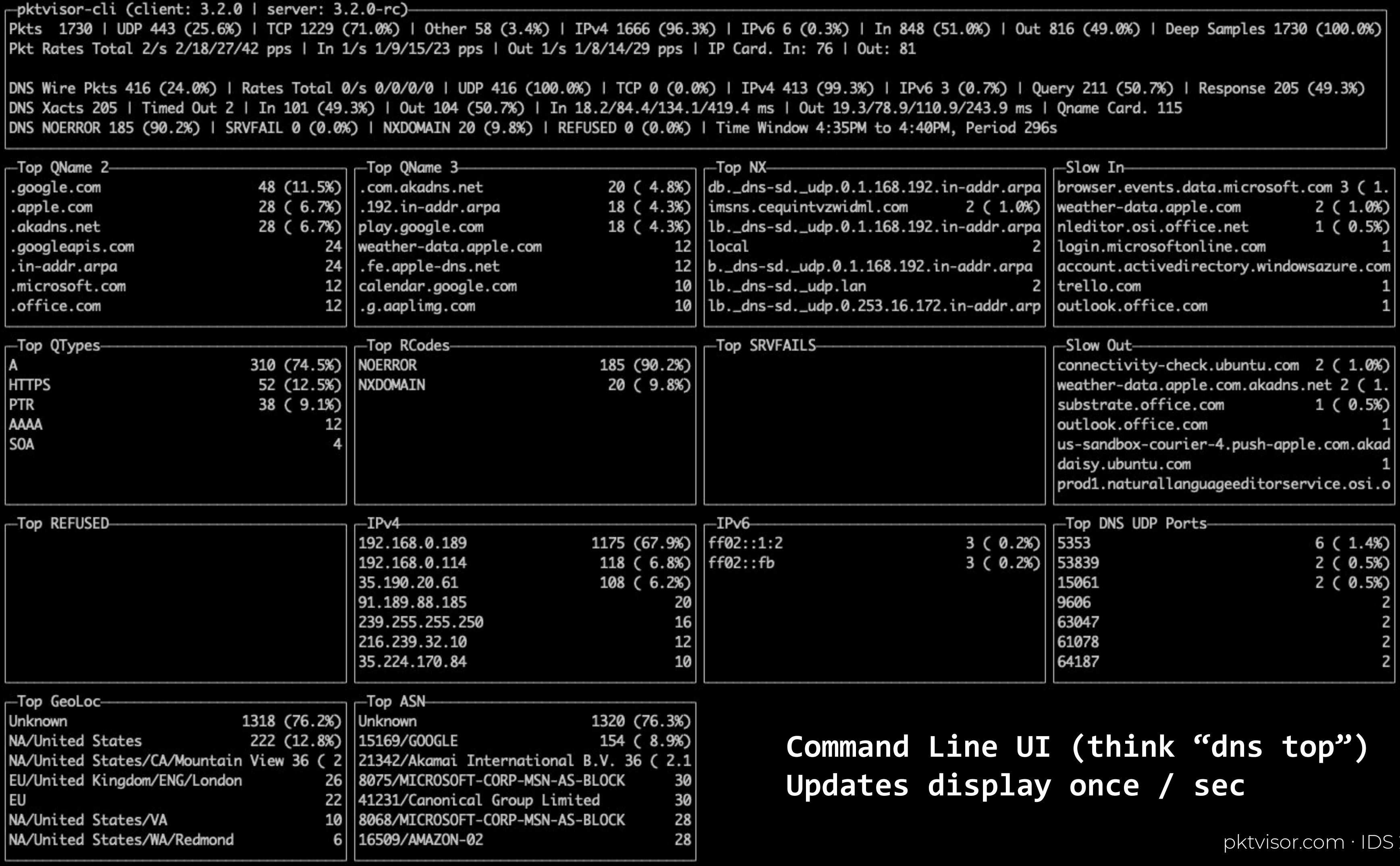
Top Queries
Top Query Types
Top Result Codes
Rate Percentiles
Top Sources
Counters
...

DNS signal extraction



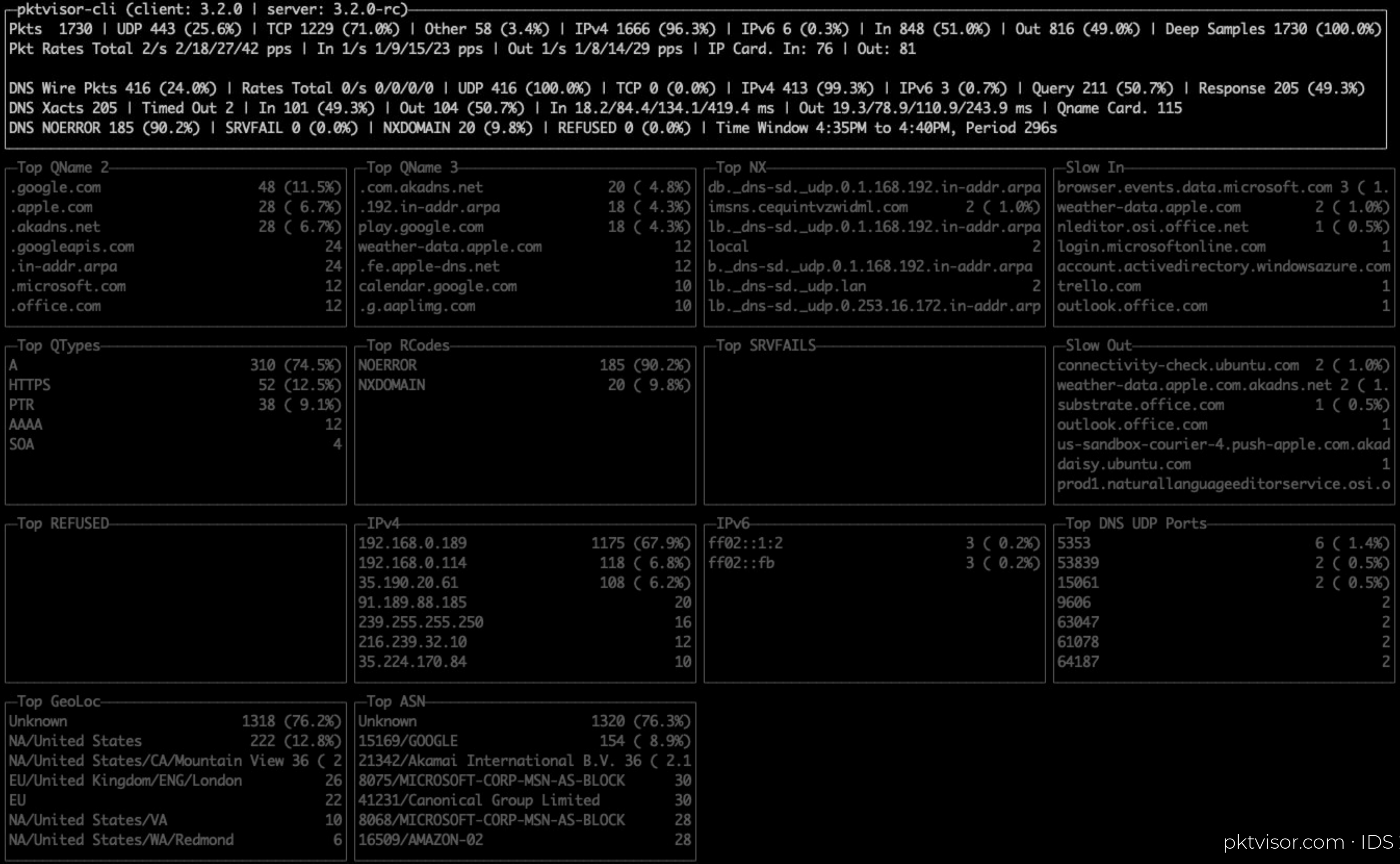
Top Queries
Top Query Types
Top Result Codes
Rate Percentiles
Top Sources
Counters
...

Shannon Weyrick · sweyrick@ns1.com

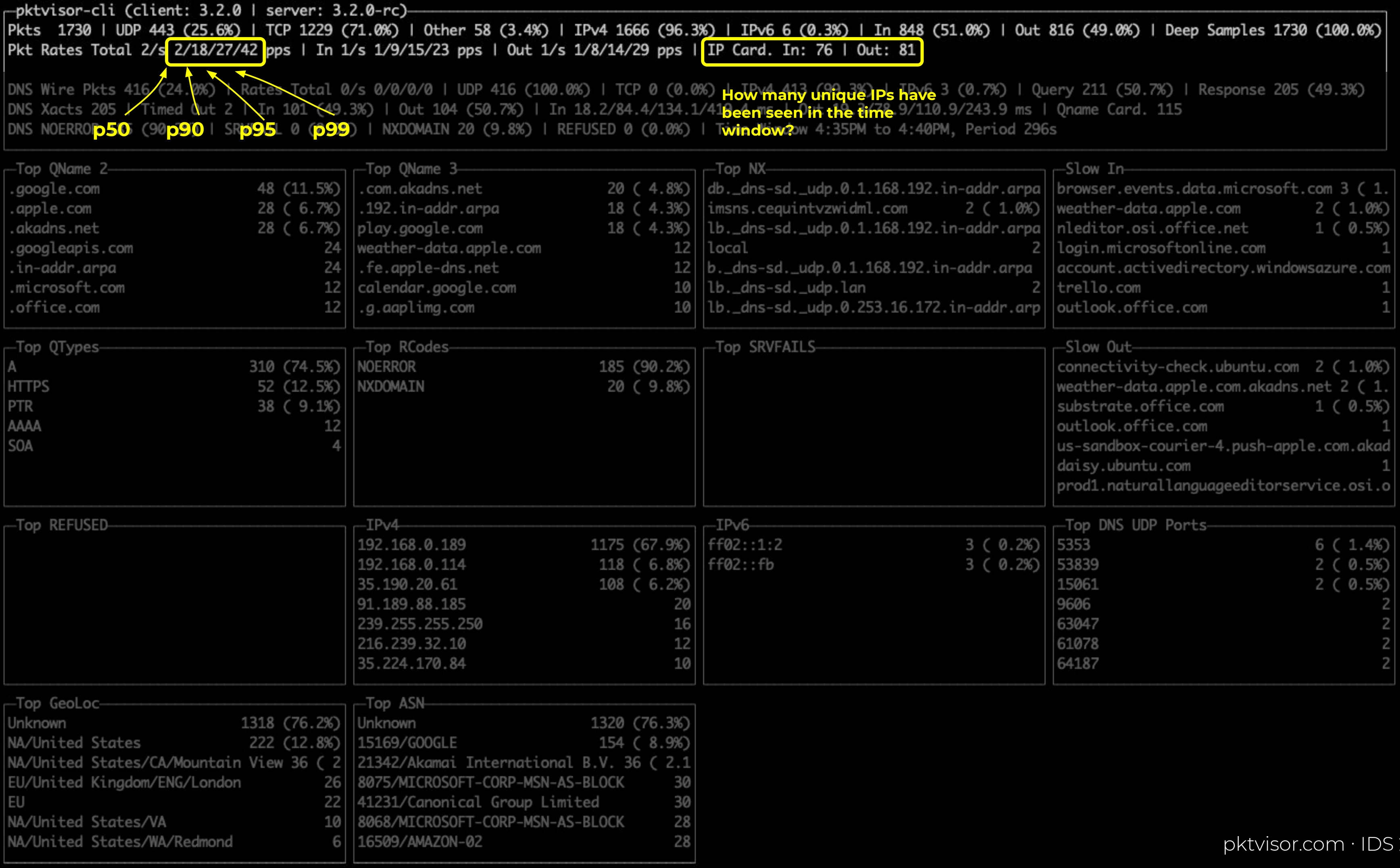


```
pktvisor-cli (client: 3.2.0 | server: 3.2.0-rc)
Pkts  1730 | UDP 443 (25.6%) | TCP 1229 (71.0%) | Other 58 (3.4%) | IPv4 1666 (96.3%) | IPv6 6 (0.3%) | In 848 (51.0%) | Out 816 (49.0%) | Deep Samples 1730 (100.0%)
Pkt Rates Total 2/s 2/18/27/42 pps | In 1/s 1/9/15/23 pps | Out 1/s 1/8/14/29 pps | IP Card. In: 76 | Out: 81

DNS Wire Pkts 416 (24.0%) | Rates Total 0/s 0/0/0/0 | UDP 416 (100.0%) | TCP 0 (0.0%) | IPv4 413 (99.3%) | IPv6 3 (0.7%) | Query 211 (50.7%) | Response 205 (49.3%)
DNS Xacts 205 | Timed Out 2 | In 101 (49.3%) | Out 104 (50.7%) | In 18.2/84.4/134.1/419.4 ms | Out 19.3/78.9/110.9/243.9 ms | Qname Card. 115
DNS NOERROR 185 (90.2%) | SRVFAIL 0 (0.0%) | NXDOMAIN 20 (9.8%) | REFUSED 0 (0.0%) | Time Window 4:35PM to 4:40PM, Period 296s

Top QName 2                            Top QName 3                            Top NX                                     Slow In
.google.com               48 (11.5%)   .com.akadns.net           20 ( 4.8%)   db._dns-sd._udp.0.1.168.192.in-addr.arpa   browser.events.data.microsoft.com 3 ( 1.
.apple.com                28 ( 6.7%)   .192.in-addr.arpa         18 ( 4.3%)   imsns.cequintvzwidml.com        2 ( 1.0%)  weather-data.apple.com           2 ( 1.0%)
.akadns.net               28 ( 6.7%)   play.google.com           18 ( 4.3%)   lb._dns-sd._udp.0.1.168.192.in-addr.arpa   nleditor.osi.office.net          1 ( 0.5%)
.googleapis.com                   24   weather-data.apple.com            12   local                                   2  login.microsoftonline.com                1
.in-addr.arpa                     24   .fe.apple-dns.net                 12   b._dns-sd._udp.0.1.168.192.in-addr.arpa    account.activedirectory.windowsazure.com
.microsoft.com                    12   calendar.google.com               10   lb._dns-sd._udp.lan                     2  trello.com                               1
.office.com                       12   .g.aaplimg.com                    10   lb._dns-sd._udp.0.253.16.172.in-addr.arp   outlook.office.com                       1

Top QTypes                             Top RCodes                             Top SRVFAILS                               Slow Out
A                        310 (74.5%)   NOERROR                  185 (90.2%)                                              connectivity-check.ubuntu.com  2 ( 1.0%)
HTTPS                     52 (12.5%)   NXDOMAIN                  20 ( 9.8%)                                              weather-data.apple.com.akadns.net 2 ( 1.
PTR                       38 ( 9.1%)                                                                                     substrate.office.com           1 ( 0.5%)
AAAA                              12                                                                                     outlook.office.com                      1
SOA                                4                                                                                     us-sandbox-courier-4.push-apple.com.akad
                                                                                                                         daisy.ubuntu.com                        1
                                                                                                                         prod1.naturallanguageeditorservice.osi.o

Top REFUSED                            IPv4                                   IPv6                                       Top DNS UDP Ports
                                       192.168.0.189           1175 (67.9%)   ff02::1:2                        3 ( 0.2%) 5353                            6 ( 1.4%)
                                       192.168.0.114            118 ( 6.8%)   ff02::fb                         3 ( 0.2%) 53839                           2 ( 0.5%)
                                       35.190.20.61             108 ( 6.2%)                                              15061                           2 ( 0.5%)
                                       91.189.88.185                     20                                              9606                                   2
                                       239.255.255.250                   16                                              63047                                  2
                                       216.239.32.10                     12                                              61078                                  2
                                       35.224.170.84                     10                                              64187                                  2

Top GeoLoc                             Top ASN
Unknown                 1318 (76.2%)   Unknown                 1320 (76.3%)
NA/United States         222 (12.8%)   15169/GOOGLE             154 ( 8.9%)
NA/United States/CA/Mountain View 36 ( 2   21342/Akamai International B.V. 36 ( 2.1
EU/United Kingdom/ENG/London      26   8075/MICROSOFT-CORP-MSN-AS-BLOCK  30
EU                                22   41231/Canonical Group Limited     30
NA/United States/VA               10   8068/MICROSOFT-CORP-MSN-AS-BLOCK  28
NA/United States/WA/Redmond        6   16509/AMAZON-02                   28
```

Command Line UI (think “dns top”)
Updates display once / sec



```
┌pktvisor-cli (client: 3.2.0 | server: 3.2.0-rc)──────────────────────────────────────────────────────────────────────────────────────────────────────────────────┐
│Pkts  1730 | UDP 443 (25.6%) | TCP 1229 (71.0%) | Other 58 (3.4%) | IPv4 1666 (96.3%) | IPv6 6 (0.3%) | In 848 (51.0%) | Out 816 (49.0%) | Deep Samples 1730 (100.0%)│
│Pkt Rates Total 2/s 2/18/27/42 pps | In 1/s 1/9/15/23 pps | Out 1/s 1/8/14/29 pps | IP Card. In: 76 | Out: 81                                                      │
│                                                                                                                                                                    │
│DNS Wire Pkts 416 (24.0%) | Rates Total 0/s 0/0/0/0 | UDP 416 (100.0%) | TCP 0 (0.0%) | IPv4 413 (99.3%) | IPv6 3 (0.7%) | Query 211 (50.7%) | Response 205 (49.3%) │
│DNS Xacts 205 | Timed Out 2 | In 101 (49.3%) | Out 104 (50.7%) | In 18.2/84.4/134.1/419.4 ms | Out 19.3/78.9/110.9/243.9 ms | Qname Card. 115                      │
│DNS NOERROR 185 (90.2%) | SRVFAIL 0 (0.0%) | NXDOMAIN 20 (9.8%) | REFUSED 0 (0.0%) | Time Window 4:35PM to 4:40PM, Period 296s                                      │
└────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────┘

┌Top QName 2─────────────────────────┐┌Top QName 3─────────────────────────┐┌Top NX──────────────────────────────┐┌Slow In─────────────────────────────┐
│.google.com              48 (11.5%)││.com.akadns.net          20 ( 4.8%)││db._dns-sd._udp.0.1.168.192.in-addr.arpa││browser.events.data.microsoft.com 3 ( 1.│
│.apple.com               28 ( 6.7%)││.192.in-addr.arpa        18 ( 4.3%)││imsns.cequintvzwidml.com   2 ( 1.0%)││weather-data.apple.com       2 ( 1.0%)│
│.akadns.net              28 ( 6.7%)││play.google.com          18 ( 4.3%)││lb._dns-sd._udp.0.1.168.192.in-addr.arpa││nleditor.osi.office.net      1 ( 0.5%)│
│.googleapis.com                  24││weather-data.apple.com           12││local                              2││login.microsoftonline.com            1│
│.in-addr.arpa                    24││.fe.apple-dns.net                12││b._dns-sd._udp.0.1.168.192.in-addr.arpa ││account.activedirectory.windowsazure.com│
│.microsoft.com                   12││calendar.google.com              10││lb._dns-sd._udp.lan                2││trello.com                           1│
│.office.com                      12││.g.aaplimg.com                   10││lb._dns-sd._udp.0.253.16.172.in-addr.arp││outlook.office.com                   1│
└────────────────────────────────────┘└────────────────────────────────────┘└────────────────────────────────────┘└────────────────────────────────────┘

┌Top QTypes──────────────────────────┐┌Top RCodes──────────────────────────┐┌Top SRVFAILS────────────────────────┐┌Slow Out────────────────────────────┐
│A                       310 (74.5%)││NOERROR                 185 (90.2%)││                                    ││connectivity-check.ubuntu.com  2 ( 1.0%)│
│HTTPS                    52 (12.5%)││NXDOMAIN                 20 ( 9.8%)││                                    ││weather-data.apple.com.akadns.net 2 ( 1.│
│PTR                      38 ( 9.1%)││                                    ││                                    ││substrate.office.com          1 ( 0.5%)│
│AAAA                             12││                                    ││                                    ││outlook.office.com                   1│
│SOA                               4││                                    ││                                    ││us-sandbox-courier-4.push-apple.com.akad│
│                                    ││                                    ││                                    ││daisy.ubuntu.com                     1│
│                                    ││                                    ││                                    ││prod1.naturallanguageeditorservice.osi.o│
└────────────────────────────────────┘└────────────────────────────────────┘└────────────────────────────────────┘└────────────────────────────────────┘

┌Top REFUSED─────────────────────────┐┌IPv4────────────────────────────────┐┌IPv6────────────────────────────────┐┌Top DNS UDP Ports───────────────────┐
│                                    ││192.168.0.189          1175 (67.9%)││ff02::1:2                 3 ( 0.2%)││5353                      6 ( 1.4%)│
│                                    ││192.168.0.114           118 ( 6.8%)││ff02::fb                  3 ( 0.2%)││53839                     2 ( 0.5%)│
│                                    ││35.190.20.61            108 ( 6.2%)││                                    ││15061                     2 ( 0.5%)│
│                                    ││91.189.88.185                    20││                                    ││9606                              2│
│                                    ││239.255.255.250                  16││                                    ││63047                             2│
│                                    ││216.239.32.10                    12││                                    ││61078                             2│
│                                    ││35.224.170.84                    10││                                    ││64187                             2│
└────────────────────────────────────┘└────────────────────────────────────┘└────────────────────────────────────┘└────────────────────────────────────┘

┌Top GeoLoc──────────────────────────┐┌Top ASN─────────────────────────────┐
│Unknown                1318 (76.2%)││Unknown                1320 (76.3%)│
│NA/United States        222 (12.8%)││15169/GOOGLE            154 ( 8.9%)│
│NA/United States/CA/Mountain View 36 ( 2││21342/Akamai International B.V. 36 ( 2.1│
│EU/United Kingdom/ENG/London     26││8075/MICROSOFT-CORP-MSN-AS-BLOCK   30│
│EU                               22││41231/Canonical Group Limited      30│
│NA/United States/VA              10││8068/MICROSOFT-CORP-MSN-AS-BLOCK   28│
│NA/United States/WA/Redmond       6││16509/AMAZON-02                    28│
└────────────────────────────────────┘└────────────────────────────────────┘
```



```
pktvisor-cli (client: 3.2.0 | server: 3.2.0-rc)
Pkts 1730 | UDP 443 (25.6%) | TCP 1229 (71.0%) | Other 58 (3.4%) | IPv4 1666 (96.3%) | IPv6 6 (0.3%) | In 848 (51.0%) | Out 816 (49.0%) | Deep Samples 1730 (100.0%)
Pkt Rates Total 2/s 2/18/27/42 pps | In 1/s 1/9/15/23 pps | Out 1/s 1/8/14/29 pps | IP Card. In: 76 | Out: 81

DNS Wire Pkts 416 (24.0%) | Rates Total 0/s 0/0/0/0 | UDP 416 (100.0%) | TCP 0 (0.0%) | IPv4 413 (99.3%) | IPv6 3 (0.7%) | Query 211 (50.7%) | Response 205 (49.3%)
DNS Xacts 205 | Timed Out 2 | In 101 (49.3%) | Out 104 (50.7%) | In 18.2/84.4/134.1/419.4 ms | Out 19.3/78.9/110.9/243.9 ms | Qname Card. 115
DNS NOERROR 185 (90.2%) | SRVFAIL 0 (0.0%) | NXDOMAIN 20 (9.8%) | REFUSED 0 (0.0%) | Time Window 4:35PM to 4:40PM, Period 296s

Top QName 2
.google.com                      48 (11.5%)
.apple.com                       28 ( 6.7%)
.akadns.net                      28 ( 6.7%)
.googleapis.com                          24
.in-addr.arpa                            24
.microsoft.com                           12
.office.com                              12

Top QName 3
.com.akadns.net                  20 ( 4.8%)
.192.in-addr.arpa                18 ( 4.3%)
play.google.com                  18 ( 4.3%)
weather-data.apple.com                   12
.fe.apple-dns.net                        12
calendar.google.com                      10
.g.aaplimg.com                           10

Top NX
db._dns-sd._udp.0.1.168.192.in-addr.arpa
imsns.cequintvzwidml.com          2 ( 1.0%)
lb._dns-sd._udp.0.1.168.192.in-addr.arpa
local                                     2
b._dns-sd._udp.0.1.168.192.in-addr.arpa
lb._dns-sd._udp.lan                       2
lb._dns-sd._udp.0.253.16.172.in-addr.arp

Slow In
browser.events.data.microsoft.com 3 ( 1.
weather-data.apple.com            2 ( 1.0%)
nleditor.osi.office.net           1 ( 0.5%)
login.microsoftonline.com                 1
account.activedirectory.windowsazure.com
trello.com                                1
outlook.office.com                        1

Top QTypes
A                               310 (74.5%)
HTTPS                            52 (12.5%)
PTR                              38 ( 9.1%)
AAAA                                     12
SOA                                       4

Top RCodes
NOERROR                         185 (90.2%)
NXDOMAIN                         20 ( 9.8%)

Top SRVFAILS

Slow Out
connectivity-check.ubuntu.com   2 ( 1.0%)
weather-data.apple.com.akadns.net 2 ( 1.
substrate.office.com            1 ( 0.5%)
outlook.office.com                      1
us-sandbox-courier-4.push-apple.com.akad
daisy.ubuntu.com                        1
prod1.naturallanguageeditorservice.osi.o

Top REFUSED

IPv4
192.168.0.189                  1175 (67.9%)
192.168.0.114                   118 ( 6.8%)
35.190.20.61                    108 ( 6.2%)
91.189.88.185                            20
239.255.255.250                          16
216.239.32.10                            12
35.224.170.84                            10

IPv6
ff02::1:2                         3 ( 0.2%)
ff02::fb                          3 ( 0.2%)

Top DNS UDP Ports
5353                              6 ( 1.4%)
53839                             2 ( 0.5%)
15061                             2 ( 0.5%)
9606                                      2
63047                                     2
61078                                     2
64187                                     2

Top GeoLoc
Unknown                        1318 (76.2%)
NA/United States                222 (12.8%)
NA/United States/CA/Mountain View 36 ( 2
EU/United Kingdom/ENG/London             26
EU                                       22
NA/United States/VA                      10
NA/United States/WA/Redmond               6

Top ASN
Unknown                        1320 (76.3%)
15169/GOOGLE                    154 ( 8.9%)
21342/Akamai International B.V. 36 ( 2.1
8075/MICROSOFT-CORP-MSN-AS-BLOCK         30
41231/Canonical Group Limited            30
8068/MICROSOFT-CORP-MSN-AS-BLOCK         28
16509/AMAZON-02                          28
```

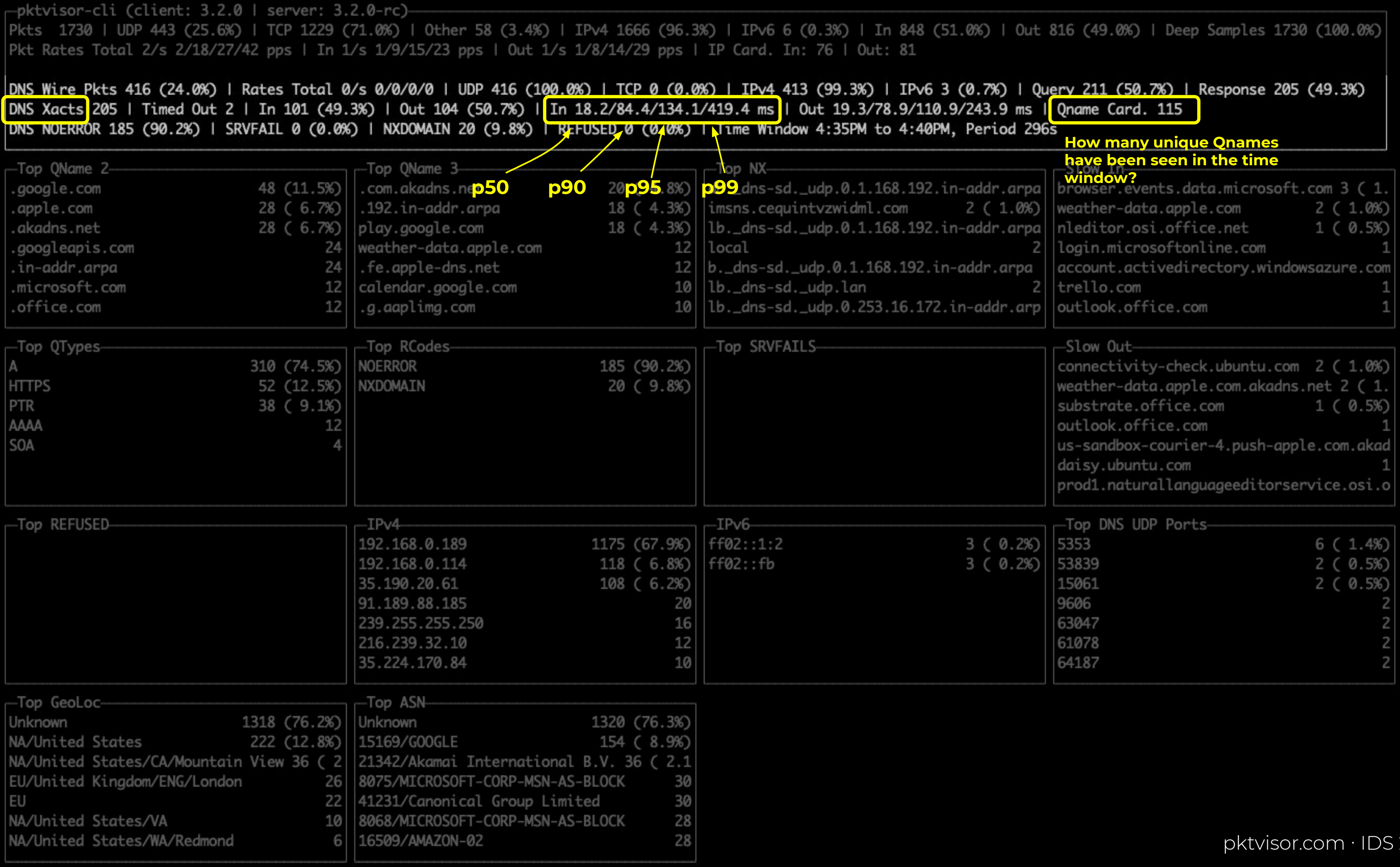
p50

p90

p95

p99

How many unique IPs have been seen in the time window?



```
pktvisor-cli (client: 3.2.0 | server: 3.2.0-rc)
Pkts  1730 | UDP 443 (25.6%) | TCP 1229 (71.0%) | Other 58 (3.4%) | IPv4 1666 (96.3%) | IPv6 6 (0.3%) | In 848 (51.0%) | Out 816 (49.0%) | Deep Samples 1730 (100.0%)
Pkt Rates Total 2/s 2/18/27/42 pps | In 1/s 1/9/15/23 pps | Out 1/s 1/8/14/29 pps | IP Card. In: 76 | Out: 81

DNS Wire Pkts 416 (24.0%) | Rates Total 0/s 0/0/0/0 | UDP 416 (100.0%) | TCP 0 (0.0%) | IPv4 413 (99.3%) | IPv6 3 (0.7%) | Query 211 (50.7%) | Response 205 (49.3%)
DNS Xacts 205 | Timed Out 2 | In 101 (49.3%) | Out 104 (50.7%) | In 18.2/84.4/134.1/419.4 ms | Out 19.3/78.9/110.9/243.9 ms | Qname Card. 115
DNS NOERROR 185 (90.2%) | SRVFAIL 0 (0.0%) | NXDOMAIN 20 (9.8%) | REFUSED 0 (0.0%) | Time Window 4:35PM to 4:40PM, Period 296s

Top QName 2
.google.com                       48 (11.5%)
.apple.com                        28 ( 6.7%)
.akadns.net                       28 ( 6.7%)
.googleapis.com                           24
.in-addr.arpa                             24
.microsoft.com                            12
.office.com                               12

Top QName 3
.com.akadns.ne                    20  .8%)
.192.in-addr.arpa                 18 ( 4.3%)
play.google.com                   18 ( 4.3%)
weather-data.apple.com                    12
.fe.apple-dns.net                         12
calendar.google.com                       10
.g.aaplimg.com                            10

Top NX
dns-sd._udp.0.1.168.192.in-addr.arpa
imsns.cequintvzwidml.com          2 ( 1.0%)
lb._dns-sd._udp.0.1.168.192.in-addr.arpa
local                                     2
b._dns-sd._udp.0.1.168.192.in-addr.arpa
lb._dns-sd._udp.lan                       2
lb._dns-sd._udp.0.253.16.172.in-addr.arp

Slow In
browser.events.data.microsoft.com 3 ( 1.
weather-data.apple.com            2 ( 1.0%)
nleditor.osi.office.net           1 ( 0.5%)
login.microsoftonline.com                 1
account.activedirectory.windowsazure.com
trello.com                                1
outlook.office.com                        1

Top QTypes
A                                310 (74.5%)
HTTPS                             52 (12.5%)
PTR                               38 ( 9.1%)
AAAA                                      12
SOA                                        4

Top RCodes
NOERROR                          185 (90.2%)
NXDOMAIN                          20 ( 9.8%)

Top SRVFAILS

Slow Out
connectivity-check.ubuntu.com     2 ( 1.0%)
weather-data.apple.com.akadns.net 2 ( 1.
substrate.office.com              1 ( 0.5%)
outlook.office.com                        1
us-sandbox-courier-4.push-apple.com.akad
daisy.ubuntu.com                          1
prod1.naturallanguageeditorservice.osi.o

Top REFUSED

IPv4
192.168.0.189                   1175 (67.9%)
192.168.0.114                    118 ( 6.8%)
35.190.20.61                     108 ( 6.2%)
91.189.88.185                             20
239.255.255.250                           16
216.239.32.10                             12
35.224.170.84                             10

IPv6
ff02::1:2                          3 ( 0.2%)
ff02::fb                           3 ( 0.2%)

Top DNS UDP Ports
5353                               6 ( 1.4%)
53839                              2 ( 0.5%)
15061                              2 ( 0.5%)
9606                                       2
63047                                      2
61078                                      2
64187                                      2

Top GeoLoc
Unknown                         1318 (76.2%)
NA/United States                 222 (12.8%)
NA/United States/CA/Mountain View 36 ( 2
EU/United Kingdom/ENG/London              26
EU                                        22
NA/United States/VA                       10
NA/United States/WA/Redmond                6

Top ASN
Unknown                         1320 (76.3%)
15169/GOOGLE                     154 ( 8.9%)
21342/Akamai International B.V. 36 ( 2.1
8075/MICROSOFT-CORP-MSN-AS-BLOCK          30
41231/Canonical Group Limited             30
8068/MICROSOFT-CORP-MSN-AS-BLOCK          28
16509/AMAZON-02                           28
```

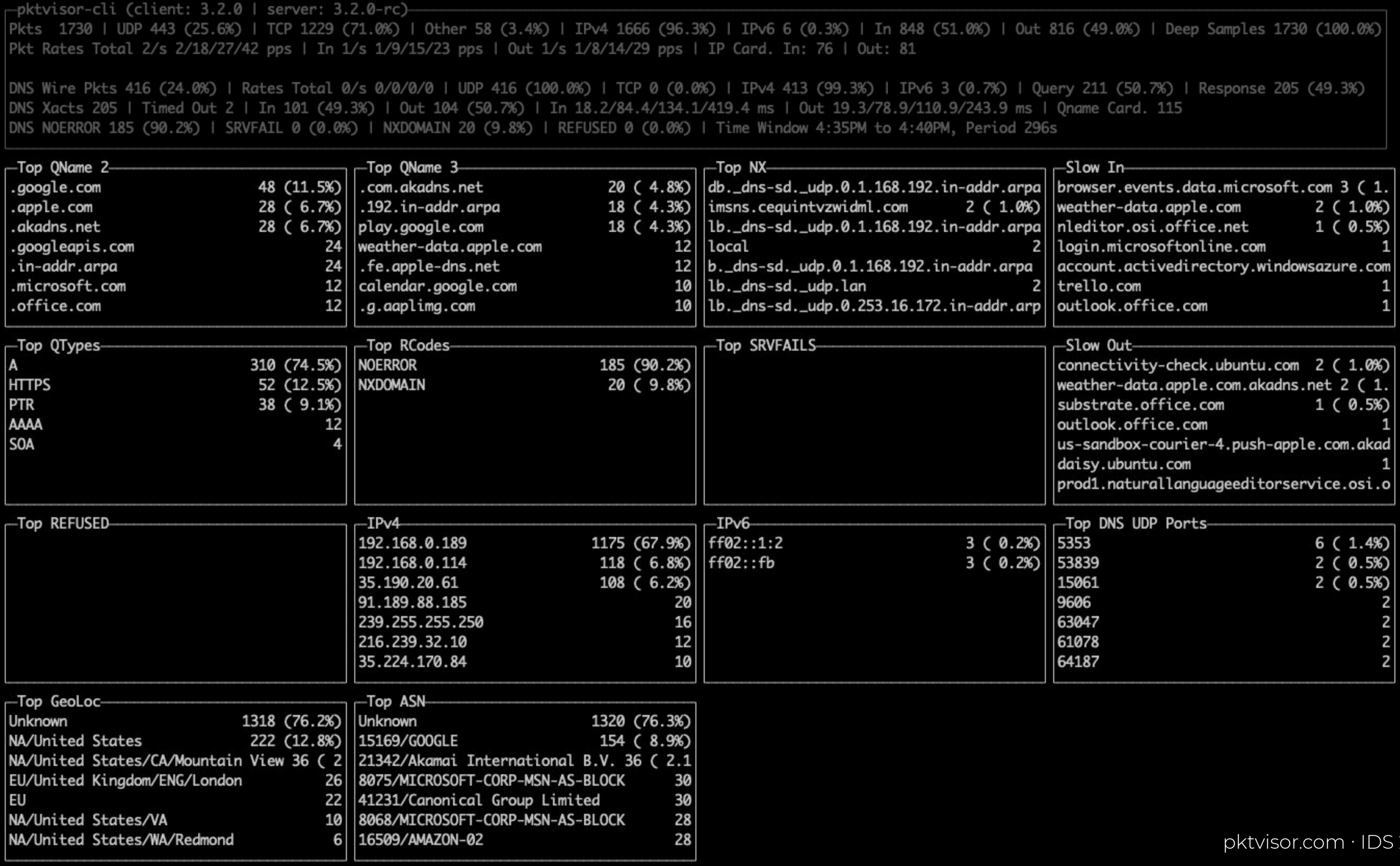
p50

p90

p95

p99

How many unique Qnames have been seen in the time window?



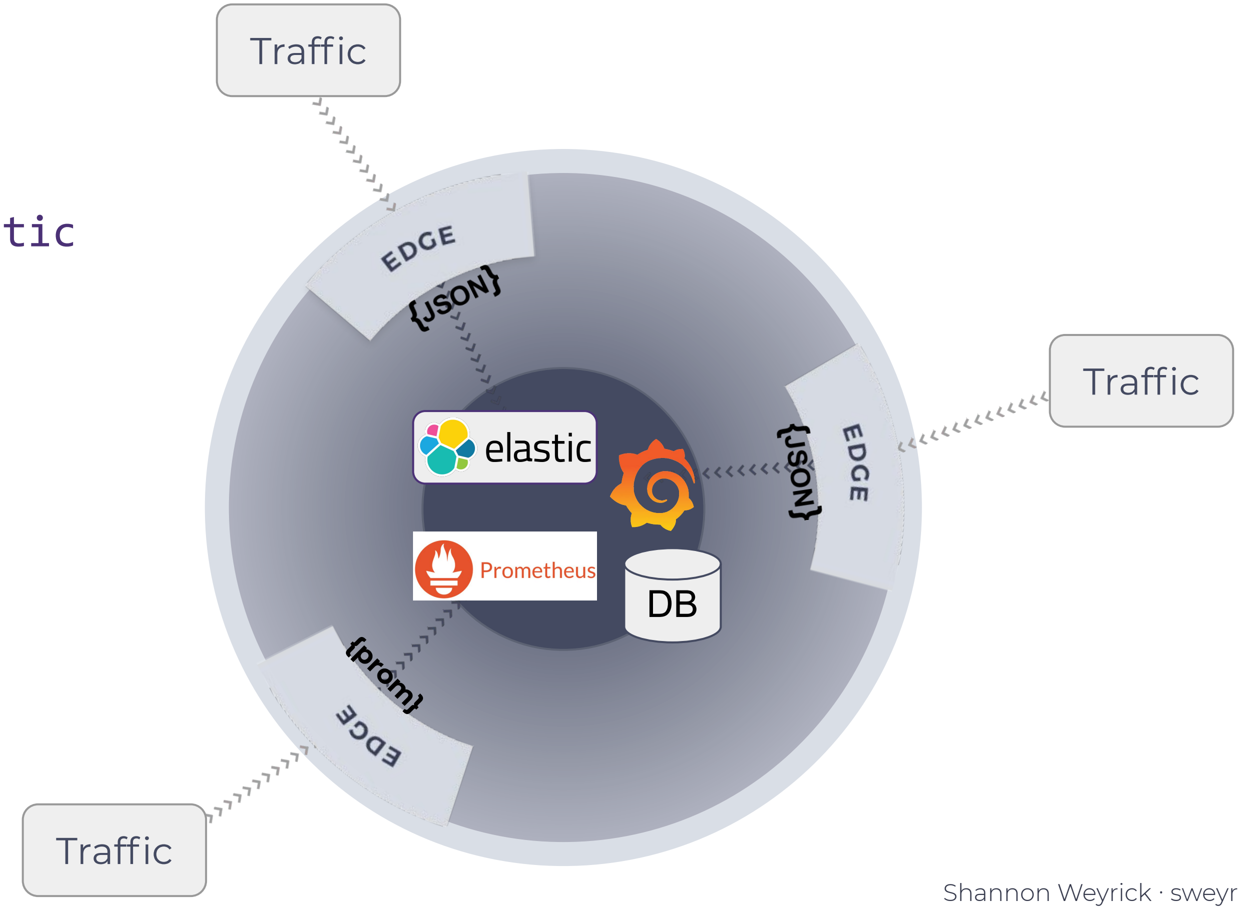
```
pktvisor-cli (client: 3.2.0 | server: 3.2.0-rc)
Pkts  1730 | UDP 443 (25.6%) | TCP 1229 (71.0%) | Other 58 (3.4%) | IPv4 1666 (96.3%) | IPv6 6 (0.3%) | In 848 (51.0%) | Out 816 (49.0%) | Deep Samples 1730 (100.0%)
Pkt Rates Total 2/s 2/18/27/42 pps | In 1/s 1/9/15/23 pps | Out 1/s 1/8/14/29 pps | IP Card. In: 76 | Out: 81

DNS Wire Pkts 416 (24.0%) | Rates Total 0/s 0/0/0/0 | UDP 416 (100.0%) | TCP 0 (0.0%) | IPv4 413 (99.3%) | IPv6 3 (0.7%) | Query 211 (50.7%) | Response 205 (49.3%)
DNS Xacts 205 | Timed Out 2 | In 101 (49.3%) | Out 104 (50.7%) | In 18.2/84.4/134.1/419.4 ms | Out 19.3/78.9/110.9/243.9 ms | Qname Card. 115
DNS NOERROR 185 (90.2%) | SRVFAIL 0 (0.0%) | NXDOMAIN 20 (9.8%) | REFUSED 0 (0.0%) | Time Window 4:35PM to 4:40PM, Period 296s

Top QName 2                          Top QName 3                          Top NX                               Slow In
.google.com                48 (11.5%)  .com.akadns.net            20 ( 4.8%)  db._dns-sd._udp.0.1.168.192.in-addr.arpa  browser.events.data.microsoft.com 3 ( 1.
.apple.com                 28 ( 6.7%)  .192.in-addr.arpa          18 ( 4.3%)  imsns.cequintvzwidml.com       2 ( 1.0%)  weather-data.apple.com           2 ( 1.0%)
.akadns.net                28 ( 6.7%)  play.google.com            18 ( 4.3%)  lb._dns-sd._udp.0.1.168.192.in-addr.arpa  nleditor.osi.office.net          1 ( 0.5%)
.googleapis.com                    24  weather-data.apple.com             12  local                                   2  login.microsoftonline.com                1
.in-addr.arpa                      24  .fe.apple-dns.net                  12  b._dns-sd._udp.0.1.168.192.in-addr.arpa   account.activedirectory.windowsazure.com
.microsoft.com                     12  calendar.google.com                10  lb._dns-sd._udp.lan                     2  trello.com                               1
.office.com                        12  .g.aaplimg.com                     10  lb._dns-sd._udp.0.253.16.172.in-addr.arp  outlook.office.com                       1

Top QTypes                           Top RCodes                           Top SRVFAILS                         Slow Out
A                         310 (74.5%)  NOERROR                   185 (90.2%)                                           connectivity-check.ubuntu.com  2 ( 1.0%)
HTTPS                      52 (12.5%)  NXDOMAIN                   20 ( 9.8%)                                           weather-data.apple.com.akadns.net 2 ( 1.
PTR                        38 ( 9.1%)                                                                                  substrate.office.com           1 ( 0.5%)
AAAA                               12                                                                                  outlook.office.com                     1
SOA                                 4                                                                                  us-sandbox-courier-4.push-apple.com.akad
                                                                                                                       daisy.ubuntu.com                       1
                                                                                                                       prod1.naturallanguageeditorservice.osi.o

Top REFUSED                          IPv4                                 IPv6                                 Top DNS UDP Ports
                                       192.168.0.189           1175 (67.9%)  ff02::1:2                   3 ( 0.2%)  5353                       6 ( 1.4%)
                                       192.168.0.114            118 ( 6.8%)  ff02::fb                    3 ( 0.2%)  53839                      2 ( 0.5%)
                                       35.190.20.61             108 ( 6.2%)                                           15061                      2 ( 0.5%)
                                       91.189.88.185                     20                                           9606                               2
                                       239.255.255.250                   16                                           63047                              2
                                       216.239.32.10                     12                                           61078                              2
                                       35.224.170.84                     10                                           64187                              2

Top GeoLoc                           Top ASN
Unknown                  1318 (76.2%)  Unknown                  1320 (76.3%)
NA/United States          222 (12.8%)  15169/GOOGLE              154 ( 8.9%)
NA/United States/CA/Mountain View 36 ( 2  21342/Akamai International B.V. 36 ( 2.1
EU/United Kingdom/ENG/London       26  8075/MICROSOFT-CORP-MSN-AS-BLOCK     30
EU                                 22  41231/Canonical Group Limited        30
NA/United States/VA                10  8068/MICROSOFT-CORP-MSN-AS-BLOCK     28
NA/United States/WA/Redmond         6  16509/AMAZON-02                      28
```

Central Collection

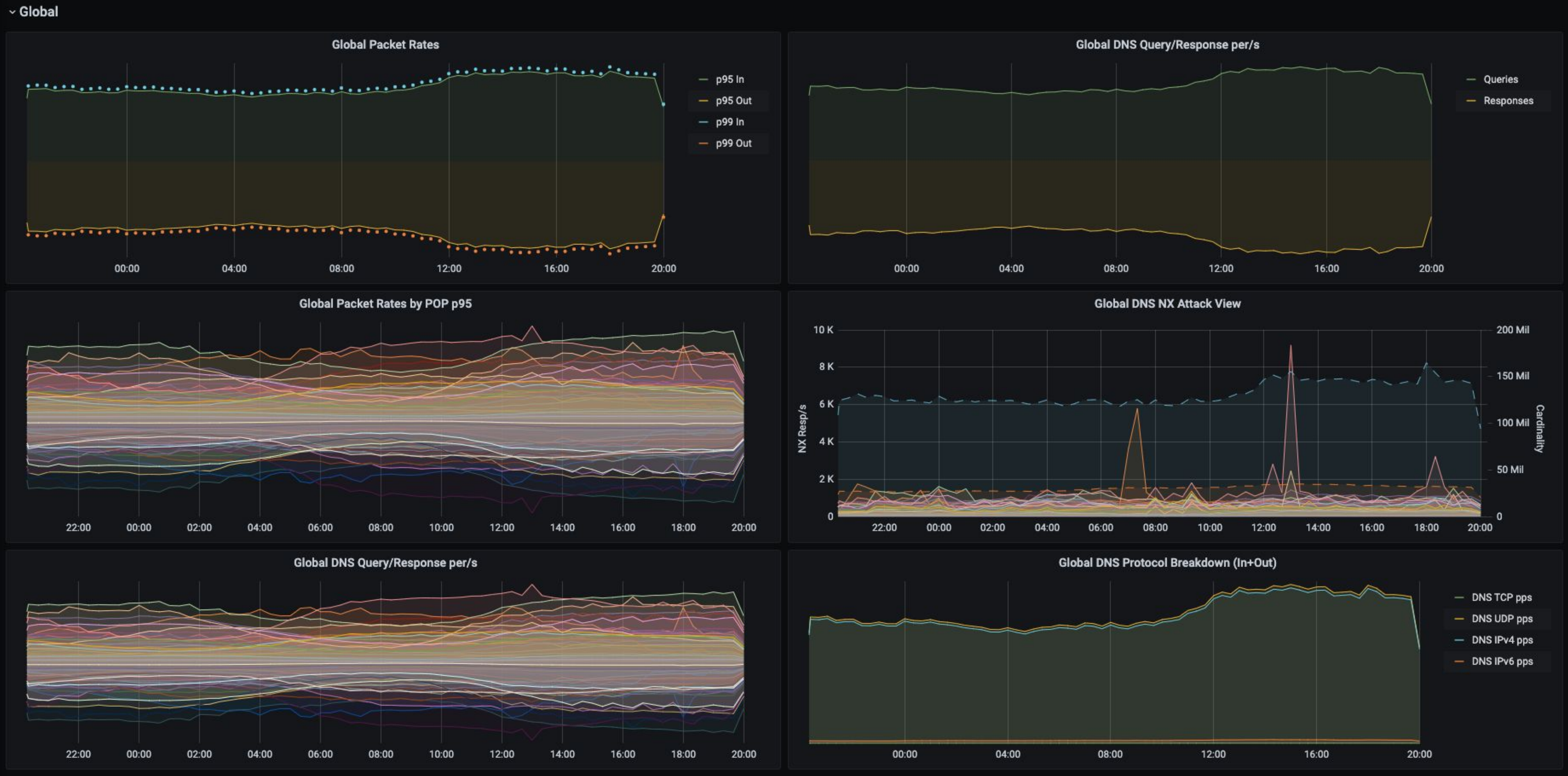
- Provides a *Global* view of distributed Agents
- Metric database agnostic
- Tools for Prometheus and Elasticsearch
- Grafana Dashboard

Central Collection

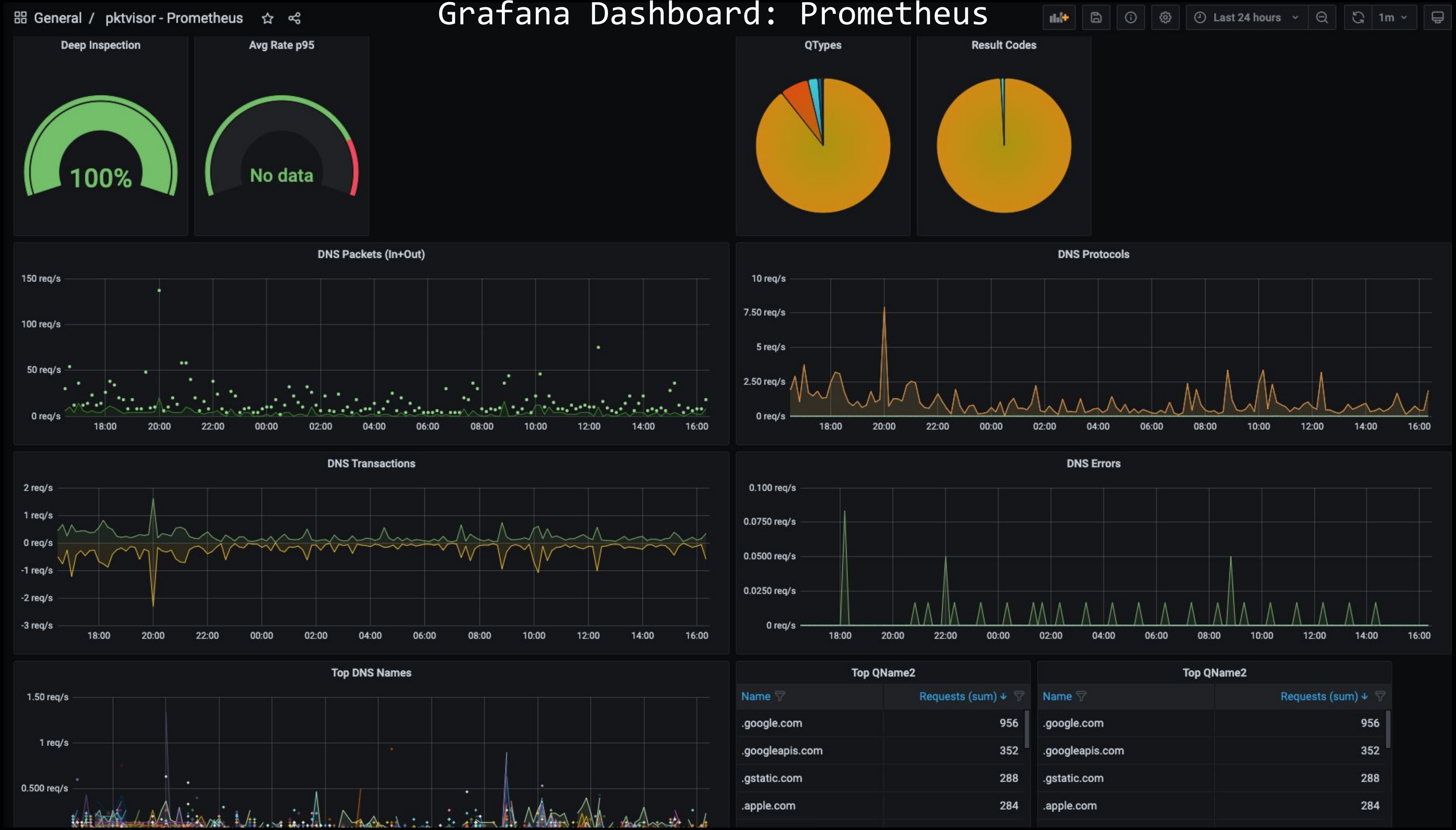
- Database agnostic
- Scrape or Push
- Small Data



Grafana Dashboard: Elasticsearch



Grafana Dashboard: Prometheus



Top QName2

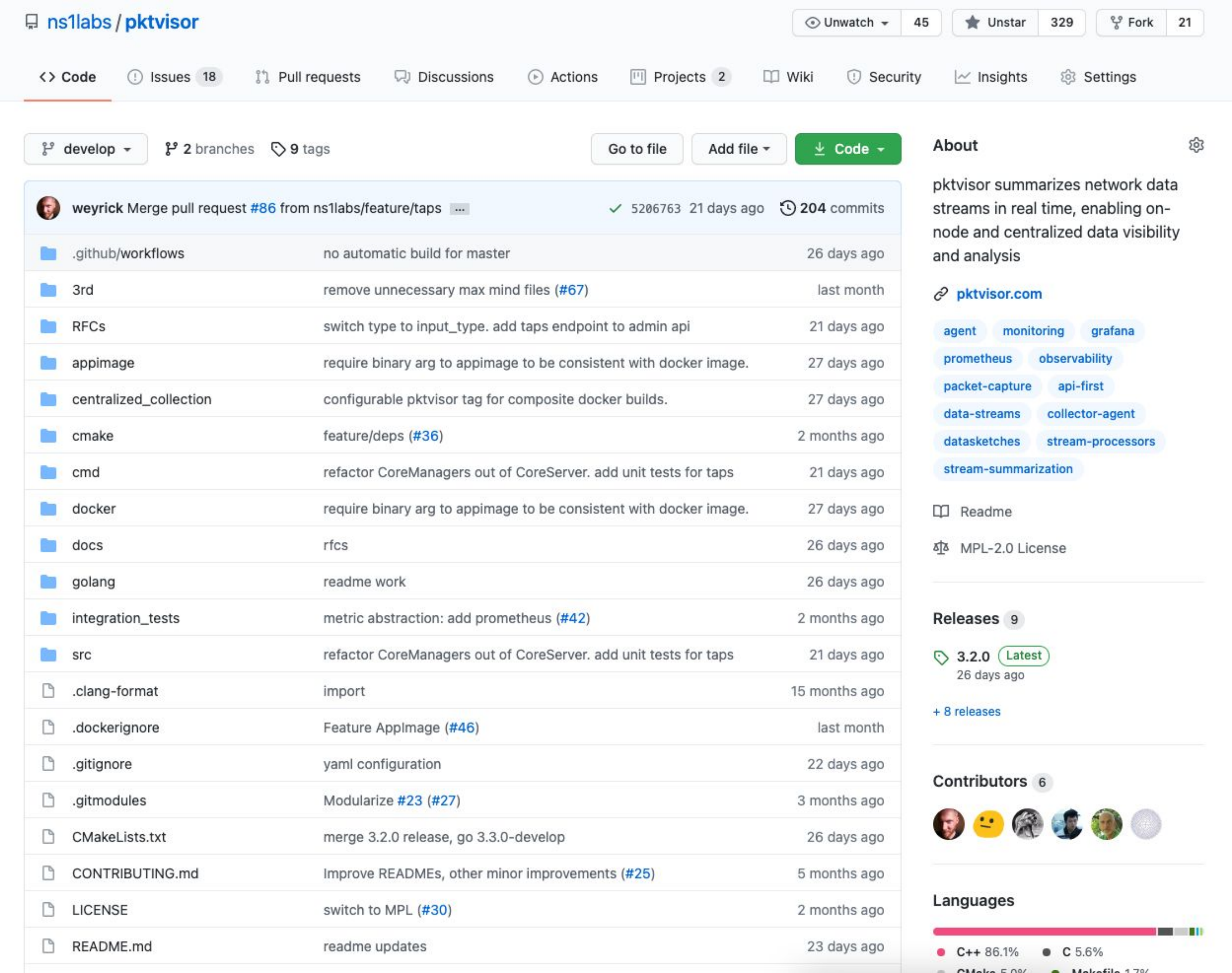
Name	Requests (sum) ↓
.google.com	956
.googleapis.com	352
.gstatic.com	288
.apple.com	284

Top QName2

Name	Requests (sum) ↓
.google.com	956
.googleapis.com	352
.gstatic.com	288
.apple.com	284

GitHub

http://pktvisor.com



ns1labs / pktvisor

Unwatch 45 | Unstar 329 | Fork 21

Code | Issues 18 | Pull requests | Discussions | Actions | Projects 2 | Wiki | Security | Insights | Settings

develop | 2 branches | 9 tags | Go to file | Add file | Code

weyrick Merge pull request #86 from ns1labs/feature/taps ... ✓ 5206763 21 days ago 204 commits

.github/workflows	no automatic build for master	26 days ago
3rd	remove unnecessary max mind files (#67)	last month
RFCs	switch type to input_type. add taps endpoint to admin api	21 days ago
appimage	require binary arg to appimage to be consistent with docker image.	27 days ago
centralized_collection	configurable pktvisor tag for composite docker builds.	27 days ago
cmake	feature/deps (#36)	2 months ago
cmd	refactor CoreManagers out of CoreServer. add unit tests for taps	21 days ago
docker	require binary arg to appimage to be consistent with docker image.	27 days ago
docs	rfcs	26 days ago
golang	readme work	26 days ago
integration_tests	metric abstraction: add prometheus (#42)	2 months ago
src	refactor CoreManagers out of CoreServer. add unit tests for taps	21 days ago
.clang-format	import	15 months ago
.dockerignore	Feature AppImage (#46)	last month
.gitignore	yaml configuration	22 days ago
.gitmodules	Modularize #23 (#27)	3 months ago
CMakeLists.txt	merge 3.2.0 release, go 3.3.0-develop	26 days ago
CONTRIBUTING.md	Improve READMEs, other minor improvements (#25)	5 months ago
LICENSE	switch to MPL (#30)	2 months ago
README.md	readme updates	23 days ago

About

pktvisor summarizes network data streams in real time, enabling on-node and centralized data visibility and analysis

pktvisor.com

agent, monitoring, grafana, prometheus, observability, packet-capture, api-first, data-streams, collector-agent, datasketches, stream-processors, stream-summarization

Readme

MPL-2.0 License

Releases 9

3.2.0 Latest
26 days ago

+ 8 releases

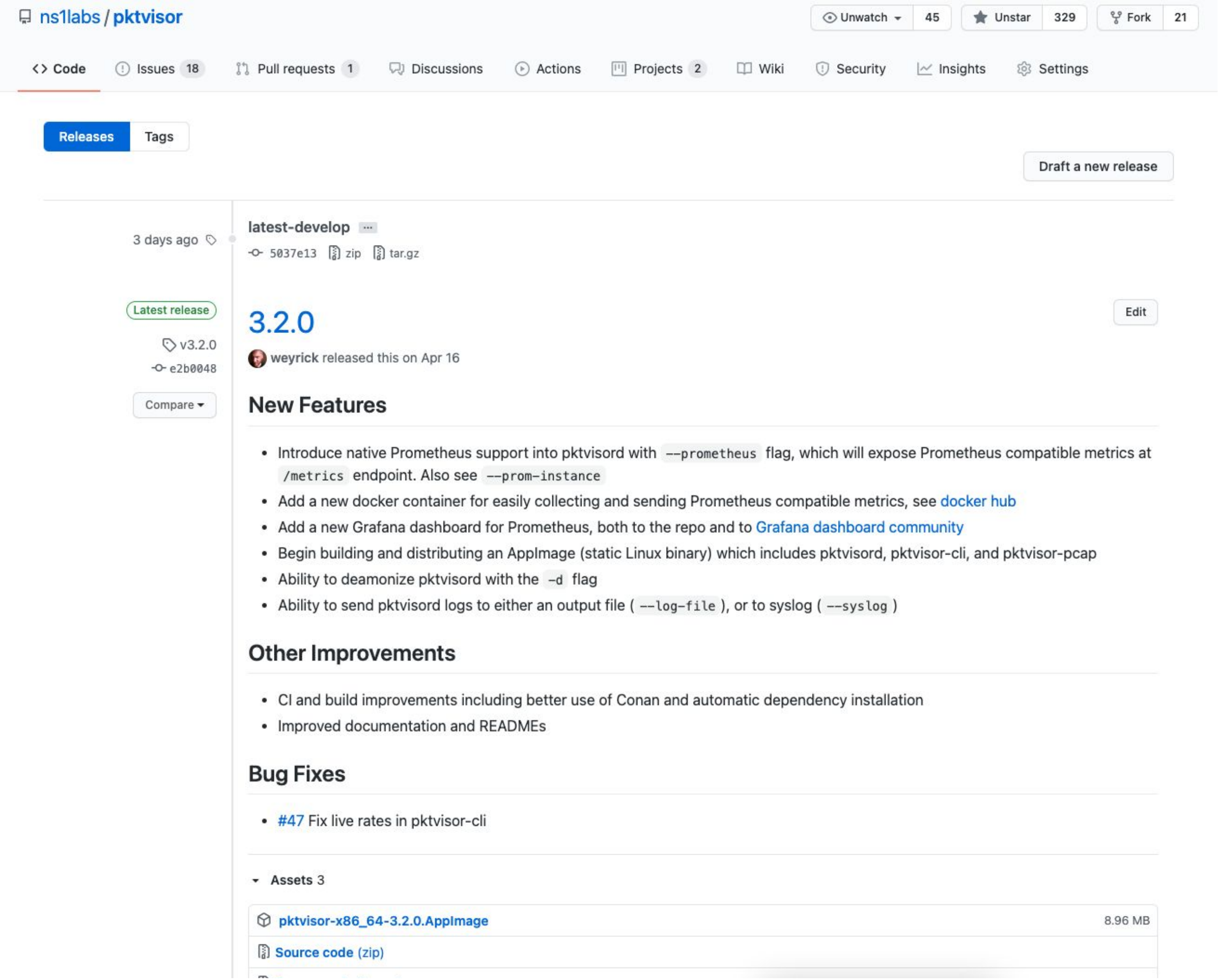
Contributors 6

Languages

● C++ 86.1% ● C 5.6%
● CMake 5.0% ● Makefile 1.7%

GitHub

http://pktvisor.com



latest-develop

5037e13 zip tar.gz

3.2.0

weyrick released this on Apr 16

New Features

- Introduce native Prometheus support into pktvisord with `--prometheus` flag, which will expose Prometheus compatible metrics at `/metrics` endpoint. Also see `--prom-instance`
- Add a new docker container for easily collecting and sending Prometheus compatible metrics, see docker hub
- Add a new Grafana dashboard for Prometheus, both to the repo and to Grafana dashboard community
- Begin building and distributing an AppImage (static Linux binary) which includes pktvisord, pktvisor-cli, and pktvisor-pcap
- Ability to deamonize pktvisord with the `-d` flag
- Ability to send pktvisord logs to either an output file (`--log-file`), or to syslog (`--syslog`)

Other Improvements

- CI and build improvements including better use of Conan and automatic dependency installation
- Improved documentation and READMEs

Bug Fixes

- #47 Fix live rates in pktvisor-cli

Assets 3

pktvisor-x86_64-3.2.0.AppImage	8.96 MB
Source code (zip)	

Easy Install

pull the image

```
root@dnshost:~$ docker pull ns1labs/pktvisor
```

start the agent

```
root@dnshost:~$ docker run --net=host -d ns1labs/pktvisor pktvisord eth0
```

run the command line UI

```
root@dnshost:~$ docker run -it --rm --net=host ns1labs/pktvisor pktvisor-cli
```

Easy Install Static Linux Binary

download the binary, make executable

```
root@dnshost:~$ curl -L http://pktvisor.com/download -o pktvisor-x86_64.AppImage
root@dnshost:~$ chmod +x pktvisor-x86_64.AppImage
```

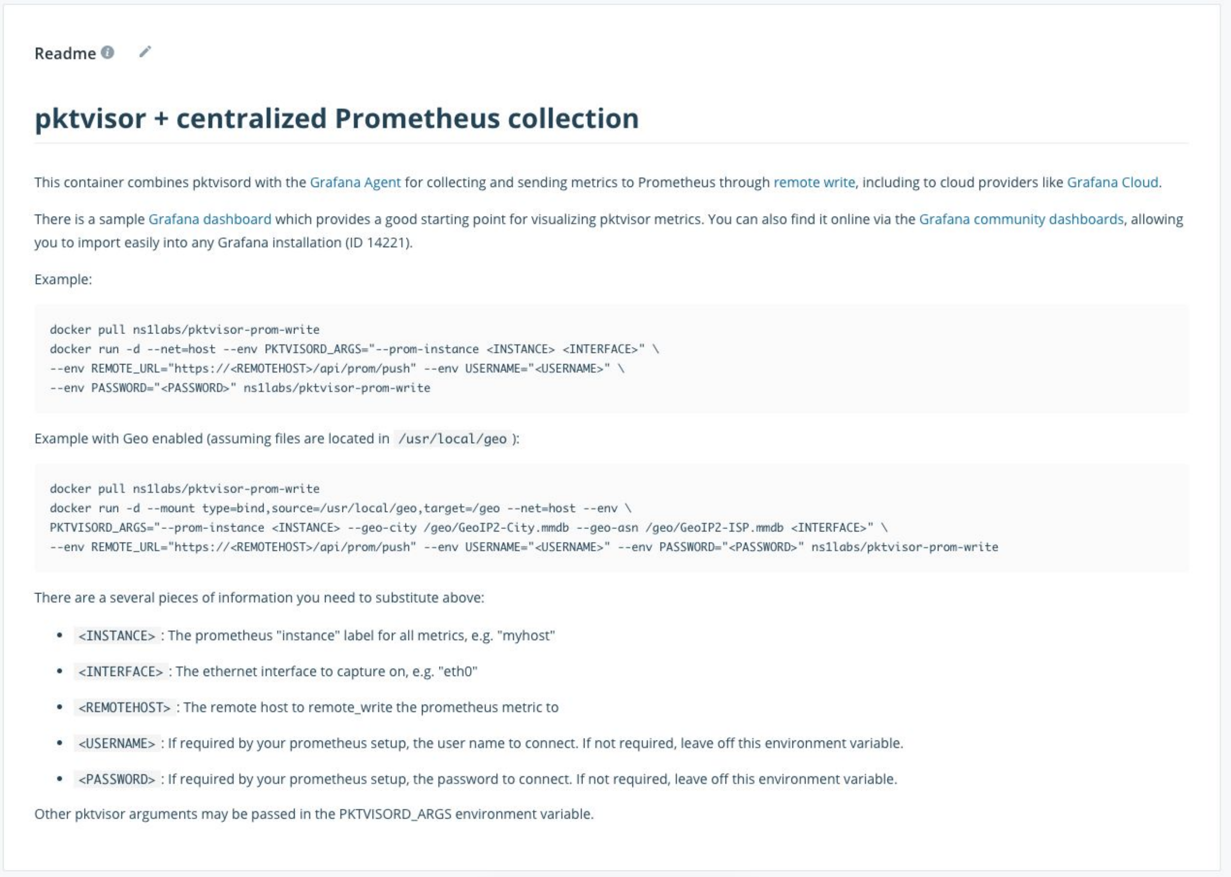
start the agent

```
root@dnshost:~$ sudo ./pktvisor-x86_64.AppImage pktvisord eth0
```

run the command line UI

```
root@dnshost:~$ ./pktvisor-x86_64.AppImage pktvisor-cli
```

Easily Plugin To Prometheus



Readme

pktvisor + centralized Prometheus collection

This container combines pktvisord with the Grafana Agent for collecting and sending metrics to Prometheus through remote write, including to cloud providers like Grafana Cloud.

There is a sample Grafana dashboard which provides a good starting point for visualizing pktvisor metrics. You can also find it online via the Grafana community dashboards, allowing you to import easily into any Grafana installation (ID 14221).

Example:

```
docker pull ns1labs/pktvisor-prom-write
docker run -d --net=host --env PKTVISORD_ARGS="--prom-instance <INSTANCE> <INTERFACE>" \
--env REMOTE_URL="https://<REMOTEHOST>/api/prom/push" --env USERNAME="<USERNAME>" \
--env PASSWORD="<PASSWORD>" ns1labs/pktvisor-prom-write
```

Example with Geo enabled (assuming files are located in `/usr/local/geo`):

```
docker pull ns1labs/pktvisor-prom-write
docker run -d --mount type=bind,source=/usr/local/geo,target=/geo --net=host --env \
PKTVISORD_ARGS="--prom-instance <INSTANCE> --geo-city /geo/GeoIP2-City.mmdb --geo-asn /geo/GeoIP2-ISP.mmdb <INTERFACE>" \
--env REMOTE_URL="https://<REMOTEHOST>/api/prom/push" --env USERNAME="<USERNAME>" --env PASSWORD="<PASSWORD>" ns1labs/pktvisor-prom-write
```

There are a several pieces of information you need to substitute above:

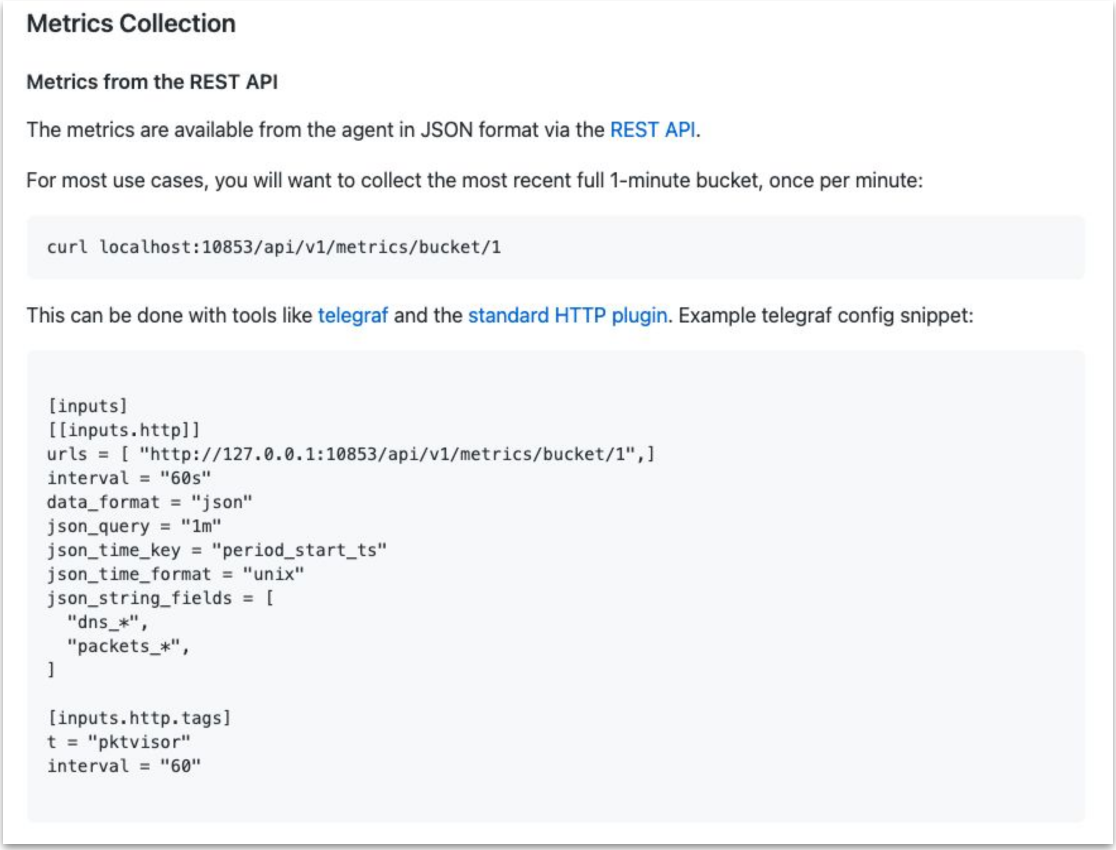
- `<INSTANCE>` : The prometheus "instance" label for all metrics, e.g. "myhost"
- `<INTERFACE>` : The ethernet interface to capture on, e.g. "eth0"
- `<REMOTEHOST>` : The remote host to remote_write the prometheus metric to
- `<USERNAME>` : If required by your prometheus setup, the user name to connect. If not required, leave off this environment variable.
- `<PASSWORD>` : If required by your prometheus setup, the password to connect. If not required, leave off this environment variable.

Other pktvisor arguments may be passed in the PKTVISORD_ARGS environment variable.

Easily Plugin To Elasticsearch

telegraf™

elastic



Metrics Collection

Metrics from the REST API

The metrics are available from the agent in JSON format via the REST API.

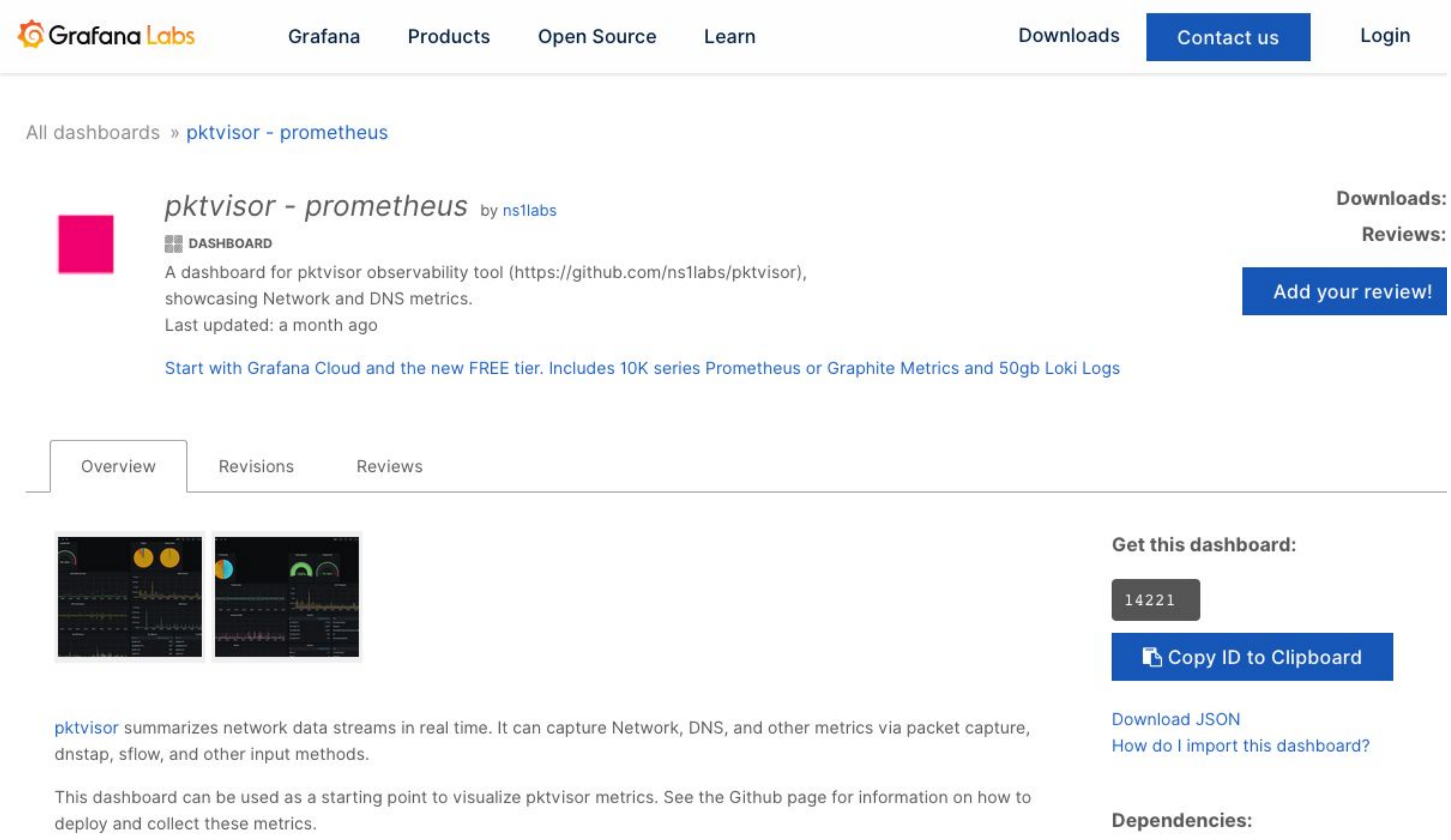
For most use cases, you will want to collect the most recent full 1-minute bucket, once per minute:

```
curl localhost:10853/api/v1/metrics/bucket/1
```

This can be done with tools like telegraf and the standard HTTP plugin. Example telegraf config snippet:

```
[inputs]
[[inputs.http]]
urls = [ "http://127.0.0.1:10853/api/v1/metrics/bucket/1",]
interval = "60s"
data_format = "json"
json_query = "1m"
json_time_key = "period_start_ts"
json_time_format = "unix"
json_string_fields = [
  "dns_*",
  "packets_*",
]

[inputs.http.tags]
t = "pktvisor"
interval = "60"
```

Install Grafana Dashboard



All dashboards » pktvisor - prometheus

pktvisor - prometheus by ns1labs

DASHBOARD

A dashboard for pktvisor observability tool (https://github.com/ns1labs/pktvisor), showcasing Network and DNS metrics.

Last updated: a month ago

Start with Grafana Cloud and the new FREE tier. Includes 10K series Prometheus or Graphite Metrics and 50gb Loki Logs

Downloads:

Reviews:

pktvisor summarizes network data streams in real time. It can capture Network, DNS, and other metrics via packet capture, dnstap, sflow, and other input methods.

This dashboard can be used as a starting point to visualize pktvisor metrics. See the Github page for information on how to deploy and collect these metrics.

Get this dashboard:

14221

Dependencies:

Deeper Dive

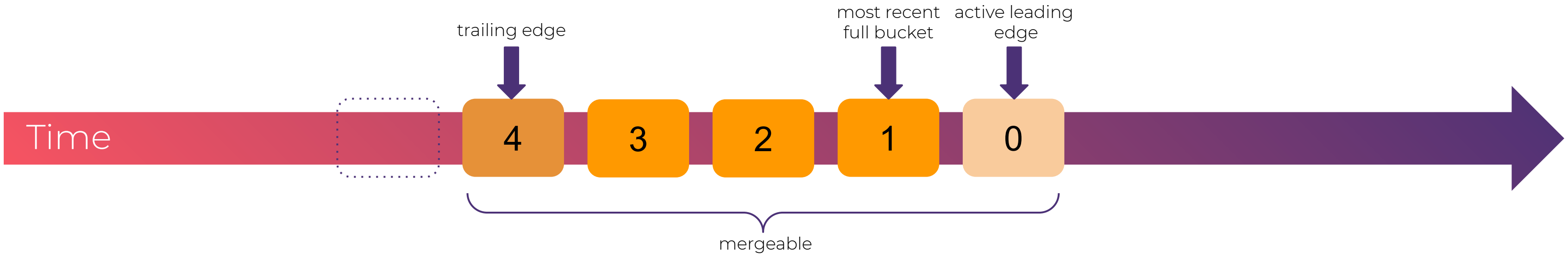
History

- pktvisor v1 2014 (forked netsniff-ng, remains open source)
- operations, debugging, DDoS visibility
- essentially simple DNS “top”
- deficiencies
  - central collection was a hack
  - resource usage
  - missing IPv6 and TCP support
  - did not track transactions (query/reply pair)

Rewrite

- move to Agent paradigm
- fix deficiencies
- modularize: inputs, dissectors, analyzers, sinks
- parallelize
- summarize with stream processing techniques (DataSketches)
- API first: built-in HTTP control plane

Sliding time window, JSON interface



- maintain mergeable 1m buckets of metrics to provide summary across full window
- always-on Agent supplies information to CLI UI and central collection via HTTP
- both merged and individual buckets are available for collection in REST API
  - CLI UI uses the merged window
  - Central collector gathers a single minute, once a minute

Under The Hood

- agent written in modern C++
- CLI UI is written in Go
- PcapPlusPlus abstraction for pcap input + custom AF_PACKET
- Apache Data Sketches
- optional MaxMind support for GeoIP and ASN
- HTTP(S) API, JSON + native Prometheus output
- Linux, OSX. Windows?

Data Sketches

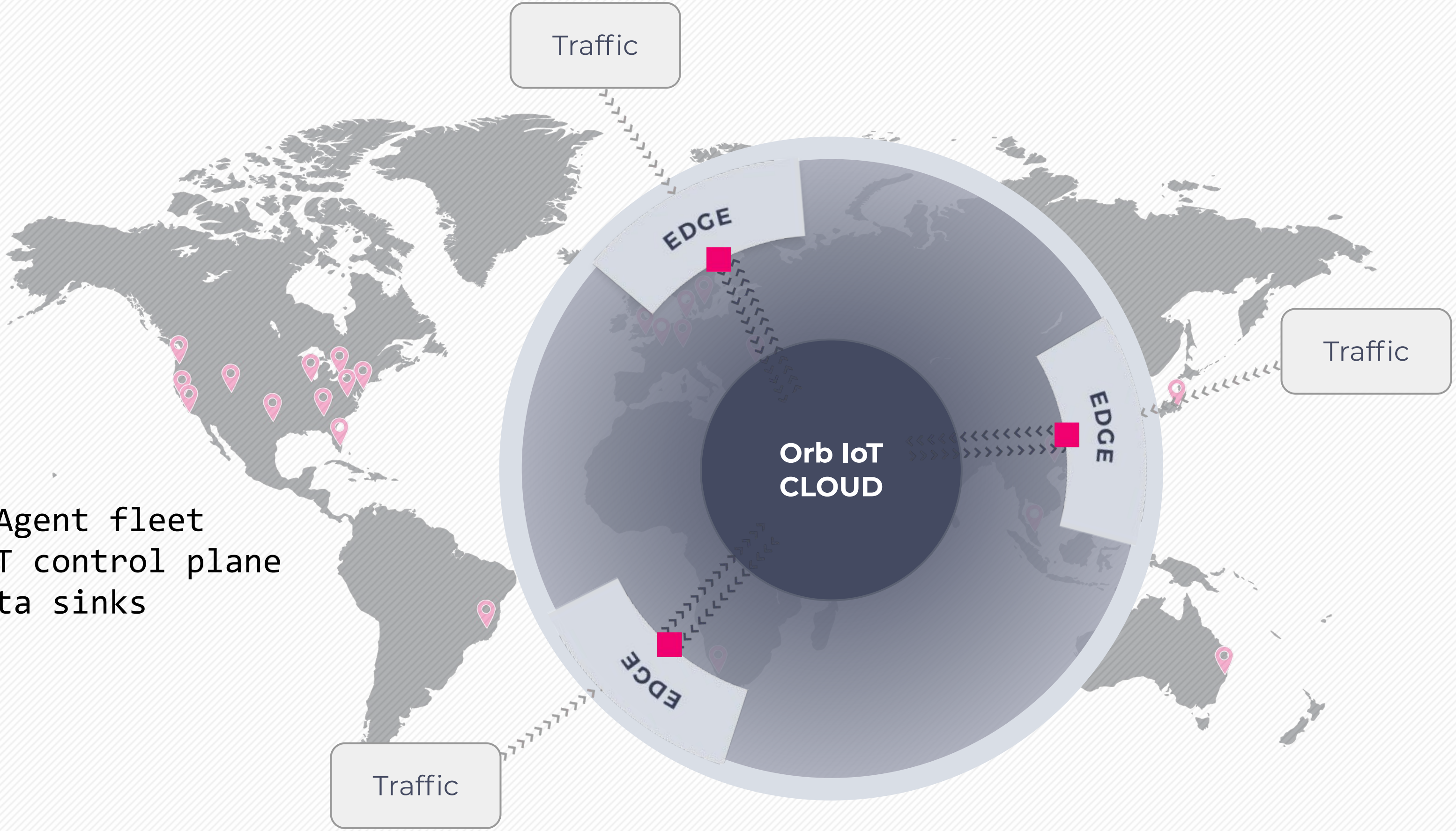
- fast, probabilistic data structures designed for streaming
- results are approximate but within well defined error bounds
- provide cardinality, heavy hitters (frequent items), quantiles
- designed to be merged, which is how we support time window
- possible to expose raw binary sketch data via API so that it can be merged across hosts and data centers

The Future: Orb

IoT Inspired Cloud Control Plane
for Fleet of pktvisor Agents

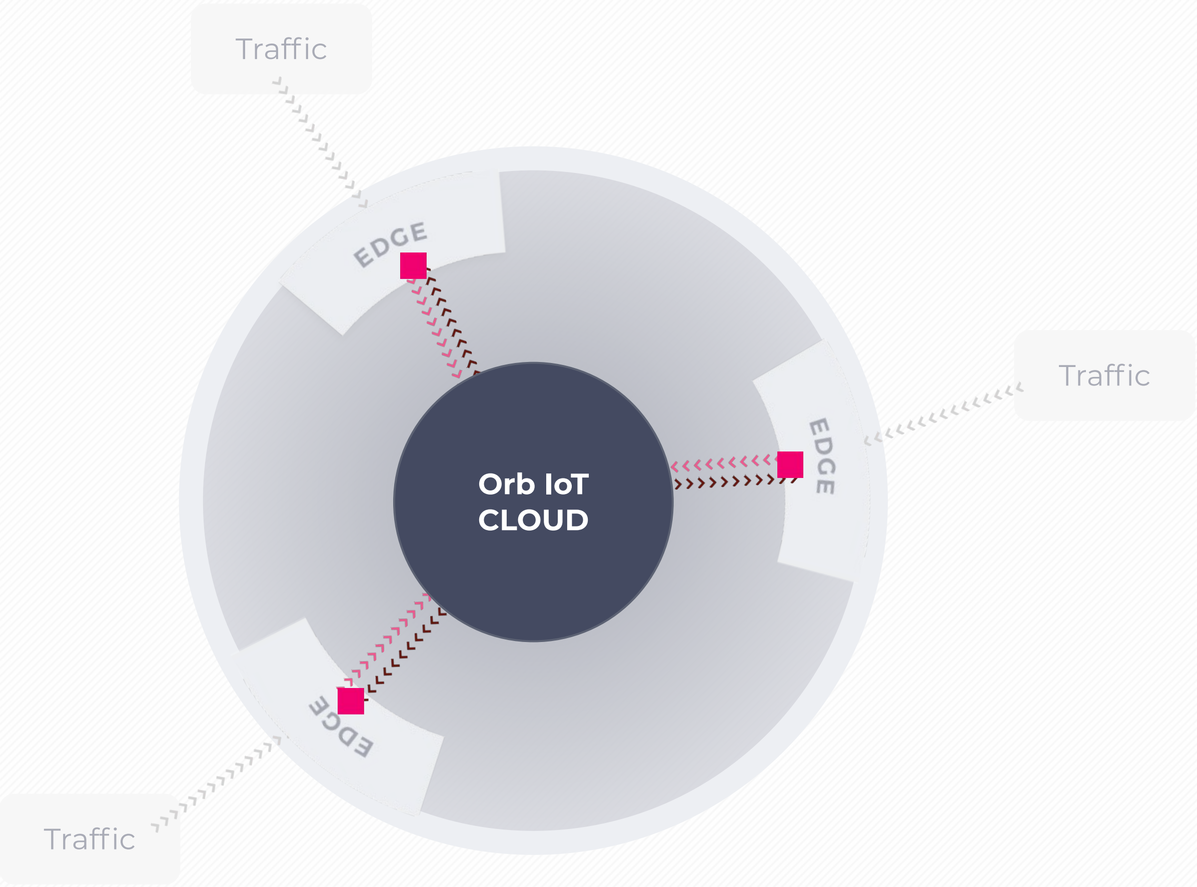
Orb

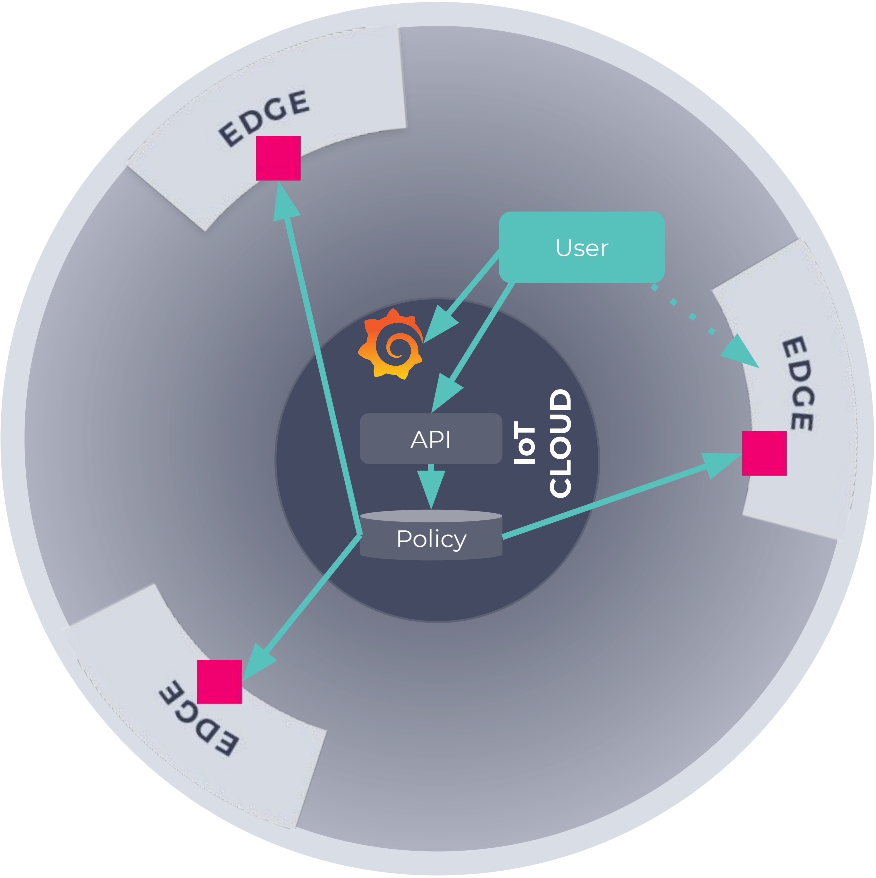
1. 🟥 Agent fleet
2. IoT control plane
3. Data sinks



Orb

1. 🟥 Agent fleet
2. IoT control plane
3. Data sinks



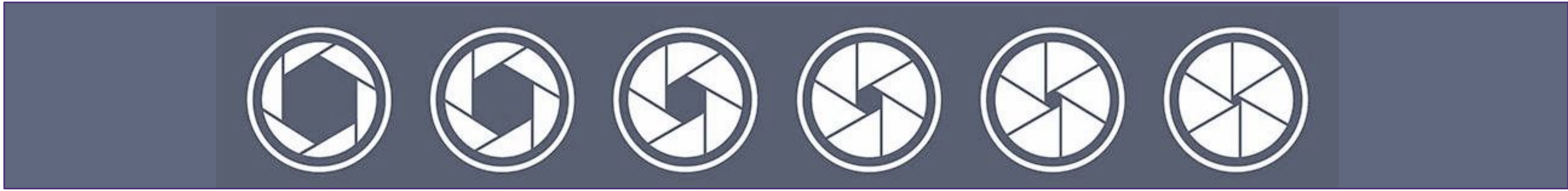


IoT Control Plane

API based configuration management

Agents connect via MQTT

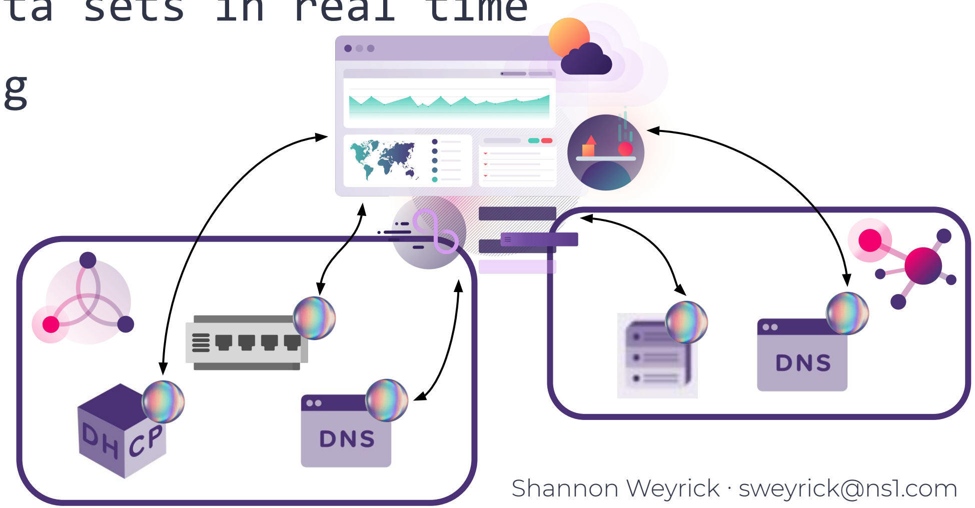
Exploring Edge Data with Dynamic Datasets



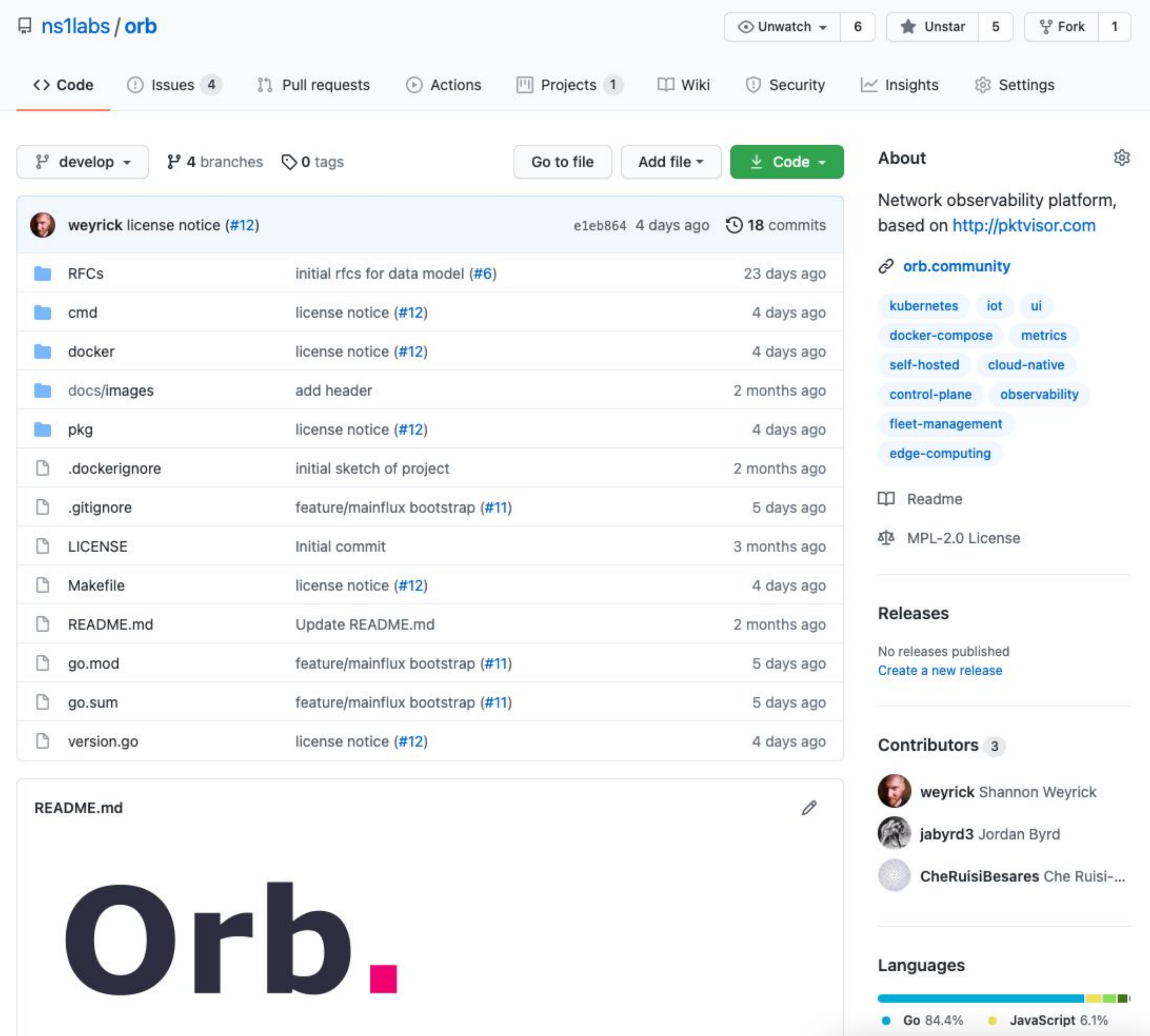
- apply multiple layered policies per Agent to extract different dimensions of Signal
- separate datasets for each policy
- filter out unwanted upstream data
- choose which summary data to collect
- choose where to send the data (built-in TSDB, S3 bucket, etc)

Orb Project Goals

- open source, vendor neutral, cloud native (microservices, k8s)
- orchestrate fleet of pktvisor Agents
- single pane of glass dashboarding
- create and explore Signal data sets in real time
- central analysis and alerting



http://orb.community



weyrick license notice (#12) e1eb864 4 days ago 18 commits

RFCs	initial rfcs for data model (#6)	23 days ago
cmd	license notice (#12)	4 days ago
docker	license notice (#12)	4 days ago
docs/images	add header	2 months ago
pkg	license notice (#12)	4 days ago
.dockerignore	initial sketch of project	2 months ago
.gitignore	feature/mainflux bootstrap (#11)	5 days ago
LICENSE	Initial commit	3 months ago
Makefile	license notice (#12)	4 days ago
README.md	Update README.md	2 months ago
go.mod	feature/mainflux bootstrap (#11)	5 days ago
go.sum	feature/mainflux bootstrap (#11)	5 days ago
version.go	license notice (#12)	4 days ago

README.md

Orb.

About

Network observability platform, based on http://pktvisor.com

orb.community

kubernetes iot ui docker-compose metrics self-hosted cloud-native control-plane observability fleet-management edge-computing

Readme

MPL-2.0 License

Releases

No releases published
Create a new release

Contributors 3

weyrick Shannon Weyrick
jabyrd3 Jordan Byrd
CheRuisiBesares Che Ruisi-...

Languages

Go 84.4% JavaScript 6.1%

Thank You!

Questions?

Shannon Weyrick ◦ VP Research @ NS1 ◦ Office of CTO

sweyrick@ns1.com