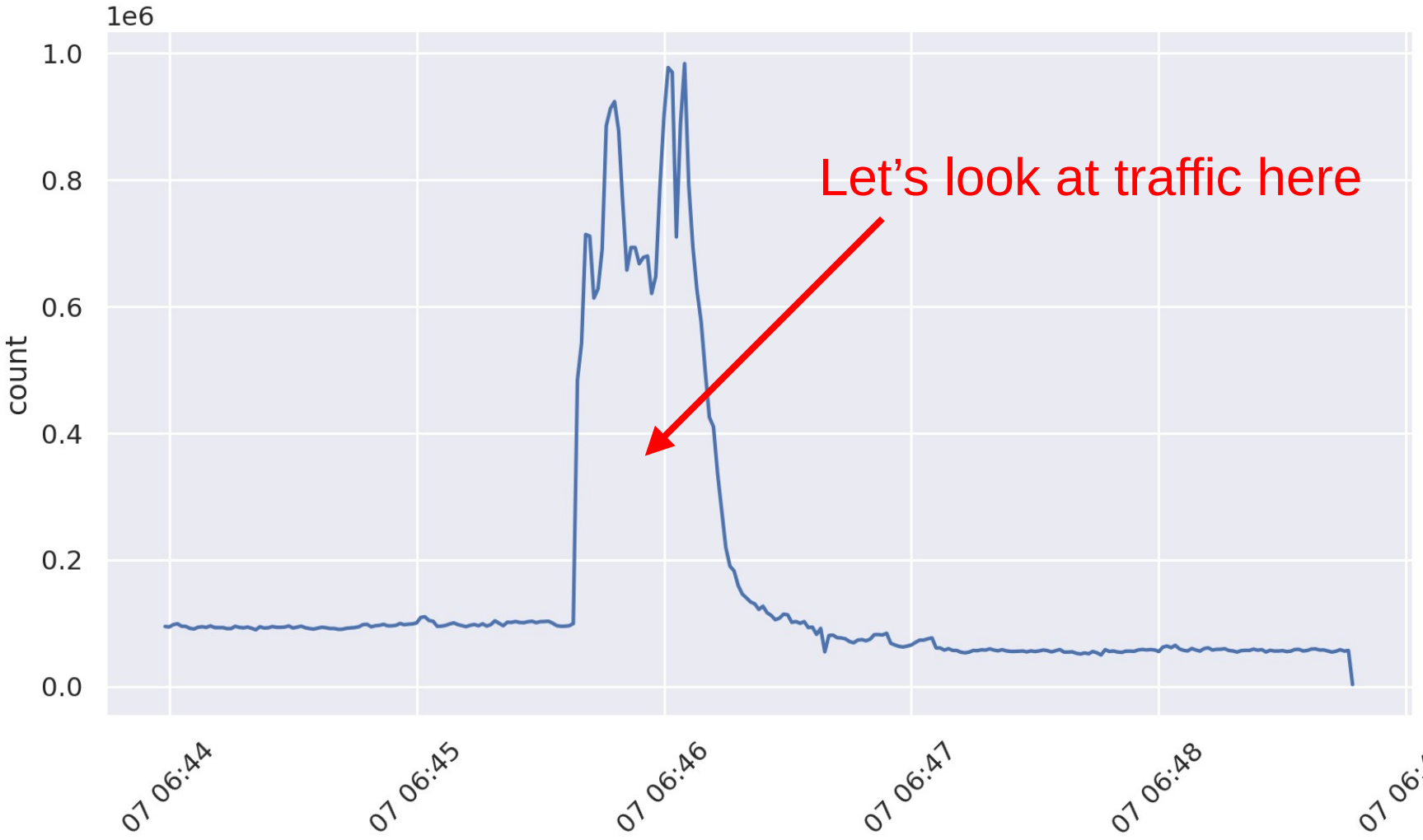
TO UNDERSTAND ANOMALIES..
...YOU MUST FIRST UNDERSTAND YOURSELF

2024-06 ICANN-80

Wes Hardaker <hardaker@isi.edu>
(wearing only my researcher hat)

Network operators are plagued with odd anomalies

An 10x increase in traffic to b.root-servers.net



What is this?

1) A DDoS attack?
2) Configuraton?
3) Software bug?

How did you know?

Because it's obvious

Look at 2,000,000 packets and count values seen

Ethernet_IP_UDP_DNS_aa	0	1997067
Ethernet_IP_UDP_DNS_ad	0	1997143
Ethernet_IP_UDP_DNS_ancount	0	1997123
Ethernet_IP_UDP_DNS_arcount	0	1963689
Ethernet_IP_UDP_DNS_cd	0	1993688
Ethernet_IP_UDP_DNS_nscount	0	1969548
Ethernet_IP_UDP_DNS_opcode	0 (Query)	1997132
Ethernet_IP_UDP_DNS_qd_qclass	1 (Internet (IN))	1997130
Ethernet_IP_UDP_DNS_qd_qname	www.366901.com.	1988484
Ethernet_IP_UDP_DNS_qd_qname_domain	366901.com	1988484
Ethernet_IP_UDP_DNS_qd_qname_prefix	www	1988638
Ethernet_IP_UDP_DNS_qd_qname_psl	com	1990005
Ethernet_IP_UDP_DNS_qd_qtype	1 (A)	1994364
Ethernet_IP_UDP_DNS_qdcount	1	1997142
Ethernet_IP_UDP_DNS_qr	0	1969553
Ethernet_IP_UDP_DNS_ra	0	1997147
Ethernet_IP_UDP_DNS_rcode	0	1997074
Ethernet_IP_UDP_DNS_rd	1	1989304
Ethernet_IP_UDP_DNS_tc	0	1997144
Ethernet_IP_UDP_DNS_z	0	1997147
Ethernet_IP_UDP_dport	53 (domain)	1969554
Ethernet_IP_UDP_len	40	1961132
Ethernet_IP_dst	192.228.79.131	1971234
Ethernet_IP_dst_ASN	394353	1971234
Ethernet_IP_dst_country	US	1980903
Ethernet_IP_dst_owner	BROOT-AS	1971234
Ethernet_IP_frag	0	1998970
Ethernet_IP_ihl	5	1998970
Ethernet_IP_len	60	1961160
Ethernet_IP_proto	17 (UDP)	1997192
Ethernet_IP_tos	0	1583787
Ethernet_IP_version	4	1998970
Ethernet_dst	f4:79:99:bf:a2:04	1972070
Ethernet_src	98:fc:44:50:5c:94	1972070
Ethernet_type	2048	1998970
__TOTAL__	packet	2000000

Approach:

- Sample 2,000,000 packets
- Count values seen in every protocol field
- Only report counts > 1,000,000
- Which of these fields show the type of extra traffic seen?

Let's zoom in

Zoomed in to just UDP

Field Name	Field Value	Count
Ethernet_IP_UDP_DNS_cd	0	1993688
Ethernet_IP_UDP_DNS_nscount	0	1969548
Ethernet_IP_UDP_DNS_opcode	0 (Query)	1997132
Ethernet_IP_UDP_DNS_qd_qclass	1 (Internet (IN))	1997130
Ethernet_IP_UDP_DNS_qd_qname	www.366901.com.	1988484
Ethernet_IP_UDP_DNS_qd_qname_domain	366901.com	1988484
Ethernet_IP_UDP_DNS_qd_qname_prefix	www	1988638
Ethernet_IP_UDP_DNS_qd_qname_psl	com	1990005
Ethernet_IP_UDP_DNS_qd_qtype	1 (A)	1994364
Ethernet_IP_UDP_DNS_qdcount	1	1997142

Clearly, these
2M of the same name?

Unfortunately, it's not always that obvious

```
Ethernet_IP_UDP_DNS_qd_qname    www.366901.com.                1988484
Ethernet_IP_UDP_DNS_qd_qname_domain 366901.com                    1988484
Ethernet_IP_UDP_DNS_qd_qname_prefix www                           1988638
Ethernet_IP_UDP_DNS_qd_qname_psl com                               1990005
Ethernet_IP_UDP_DNS_qd_qtype    1 (A)                          1994364
Ethernet_IP_UDP_DNS_qdcount     1                              1997142
Ethernet_IP_UDP_DNS_qr          0                              1969553
Ethernet_IP_UDP_DNS_ra          0                              1997147
Ethernet_IP_UDP_DNS_rcode       0                              1997074
Ethernet_IP_UDP_DNS_rd          1                              1989304
```

What about these? Are these unusual?

What about recursion desired?

*** I *** don't even know!

- www could be the most common query prefix
- .com is the most popular TLD
- IPv4 (A) queries might be the most common?

Let’s think about this

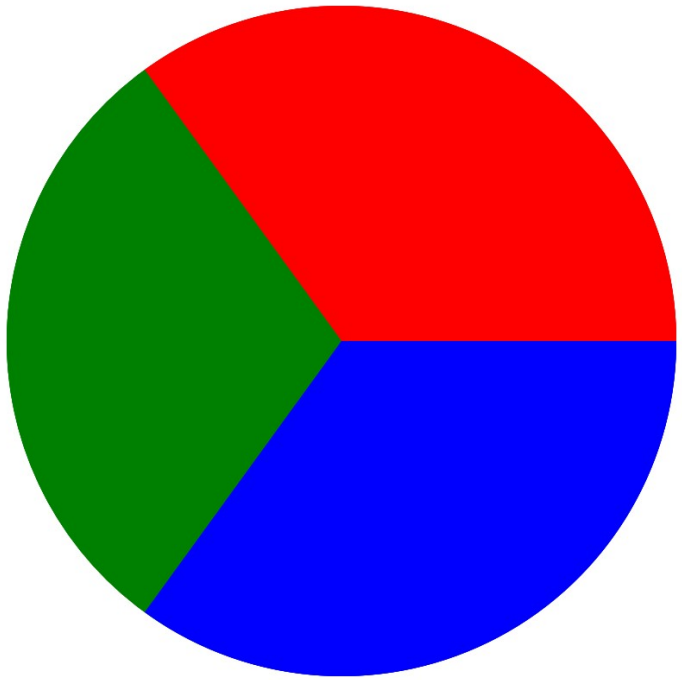
How can we do intelligent analysis?

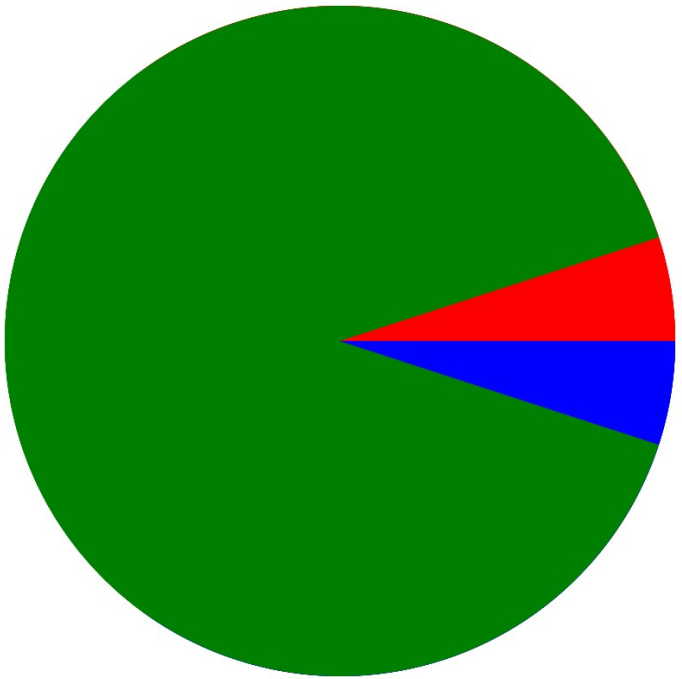
To find what is abnormal, you need to know what is normal

- Doctors use **bilateral comparison**
  - When your foot hurts… compare your left to your right
  - Is one more swollen than the other?
  - Is one larger?
  - Imagine if we didn't have a left and a right!
  - Your doctor would have to memorize what normal was

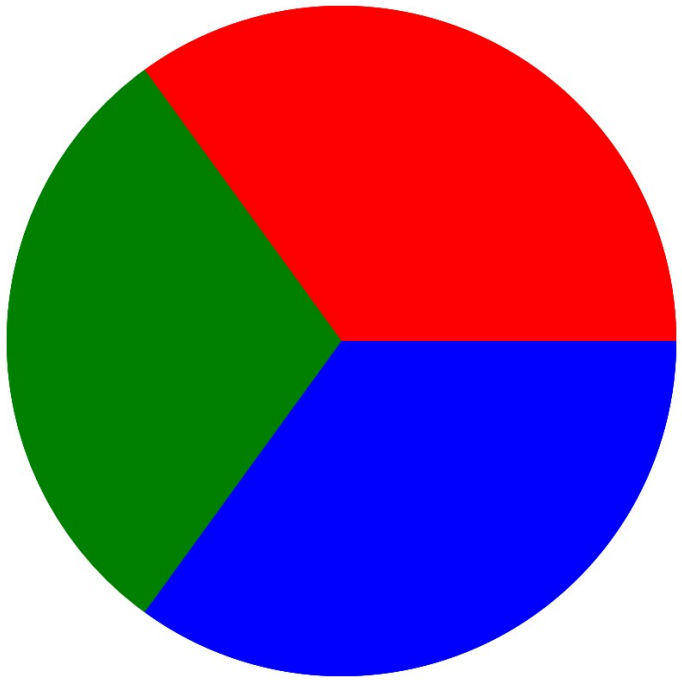
- Network anomalies should be treated with similar analysis

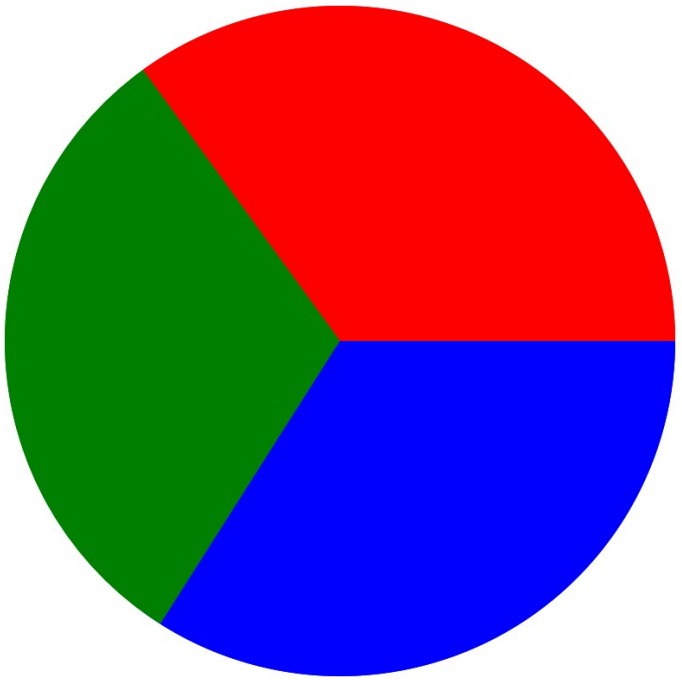
An example DDoS attack field values
Spot the difference!
What value is the problem?



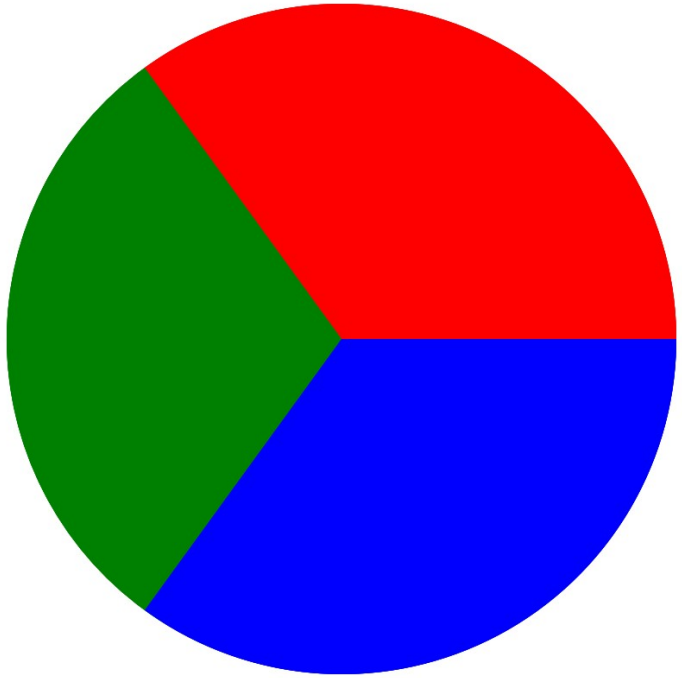


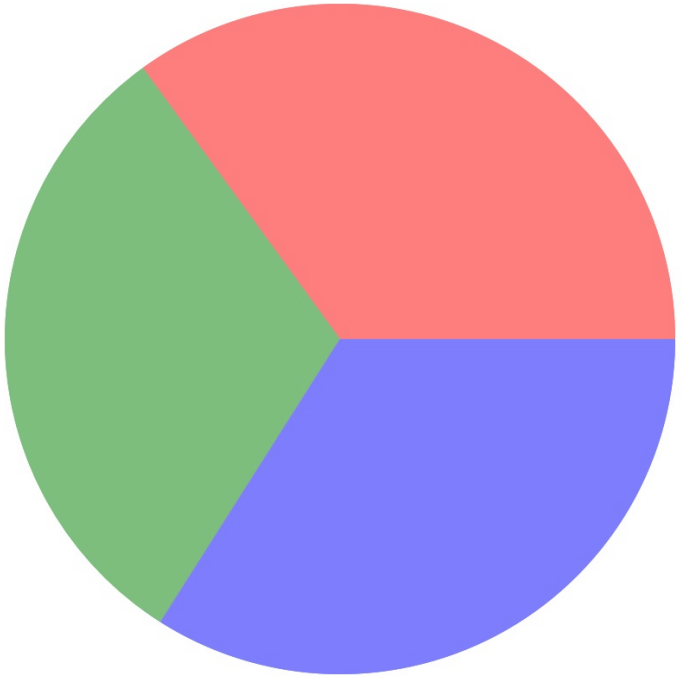
A smaller anomaly – spot the difference!



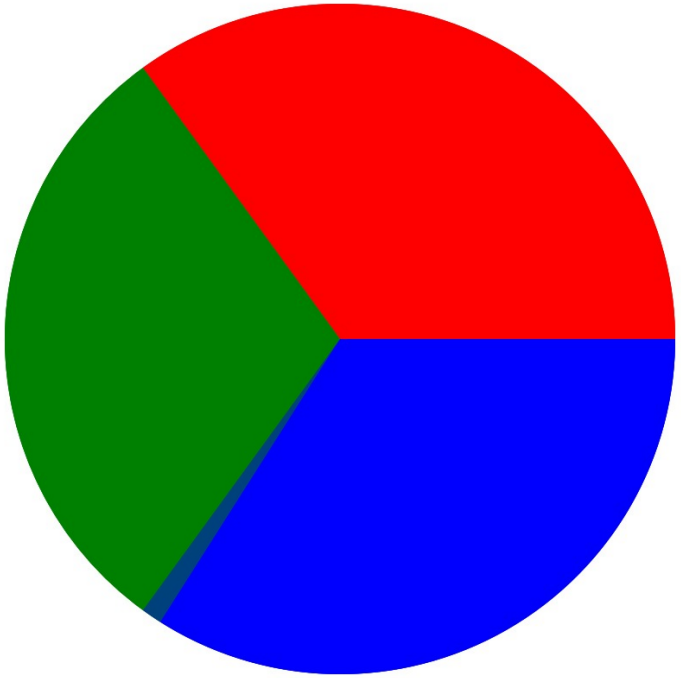


Let’s subtract – what is: *right* – *left*?

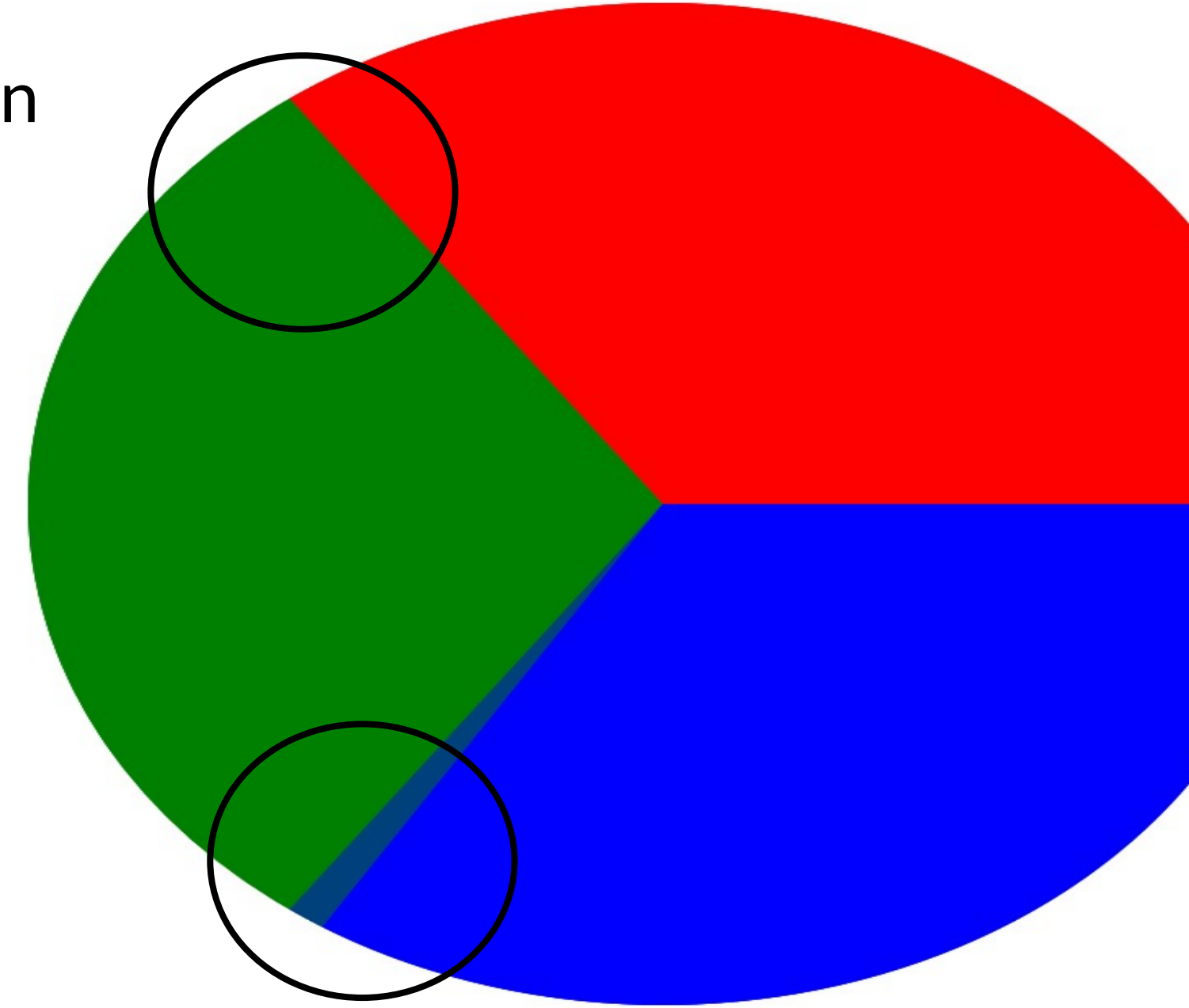




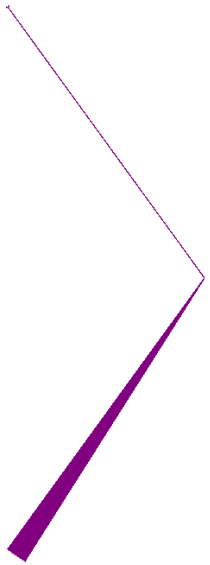
This is right overlapped with left – spot the difference!



If you look carefully…
you can see discoloration



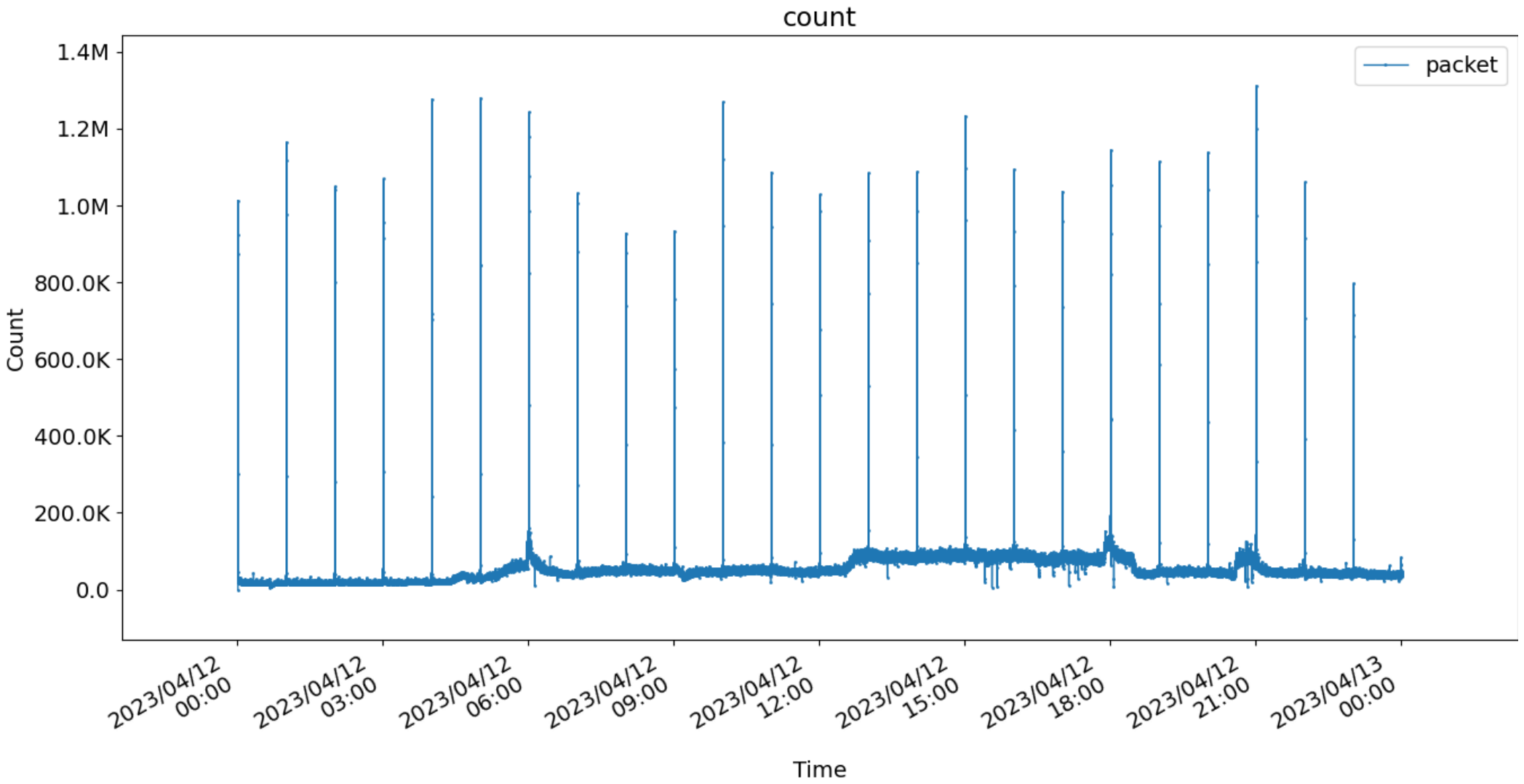
This is the real *right - left*



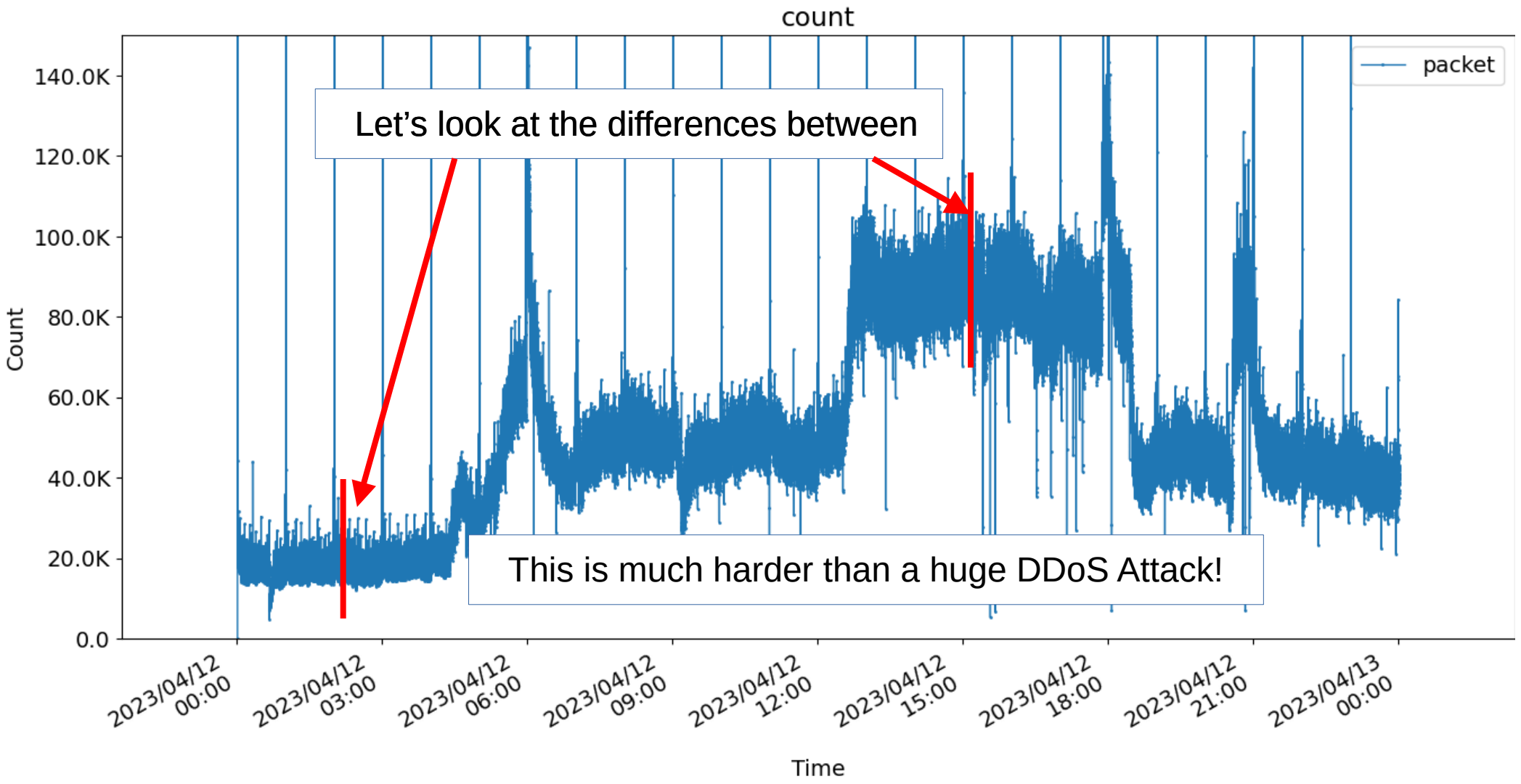
When we
remove “normal”
we are left with just the abnormal

Let’s go back to internet traffic

The b.root-server.net 2023 DITL at its MIA instance

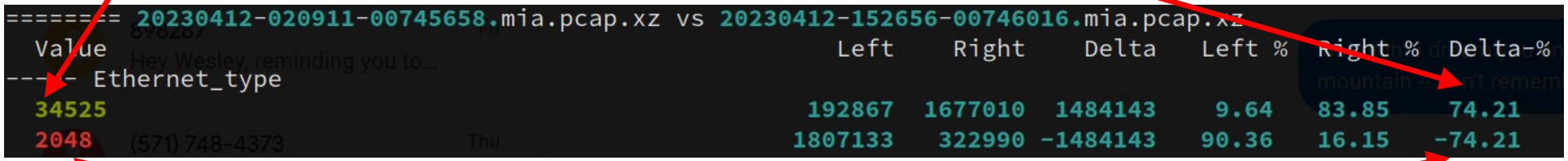


The b.root-server.net 2023 DITL at its MIA instance



In 2M packets: shift in Ethernet type identifiers

IPv6 went up (a lot)



```
======== 20230412-020911-00745658.mia.pcap.xz vs 20230412-152656-00746016.mia.pcap.xz
  Value                                    Left    Right    Delta   Left %  Right %  Delta-%
----- Ethernet_type
  34525                                  192867  1677010  1484143    9.64    83.85    74.21
  2048                                  1807133   322990 -1484143   90.36    16.15   -74.21
```

IPv4 went down (a lot)

In 2M packets: increase in traffic from AWS (over IPv6)

```
======== 20230412-020911-00745658.mia.pcap.xz vs 20230412-152656-00746016.mia.pcap.xz
  Value                                  Left     Right     Delta    Left %   Right %  Delta-%
----- Ethernet_IPv6_src_ASN
 16509                                   2380    937909    935529      1.23     55.92    54.69
----- Ethernet_IPv6_src_country
 US                                    134251   1661773   1527522     69.58     99.09    29.50
----- Ethernet_IPv6_src_owner
 AMAZON-02                               2380    937909    935529      1.23     55.92    54.69
```

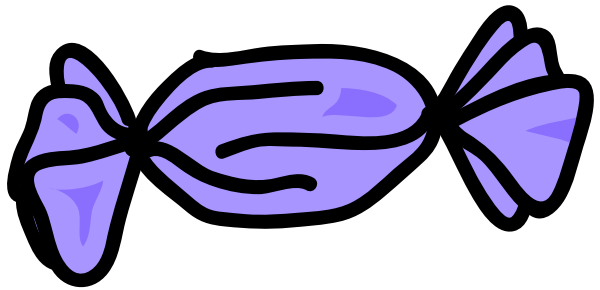
In 2M packets: increase in truncation bit seen

```
========= 20230412-020911-00745658.mia.pcap.xz vs 20230412-152656-00746016.mia.pcap.xz
  Value                                    Left    Right    Delta   Left %  Right %  Delta-%
----- Ethernet_IPv6_UDP_DNS_tc
  1                                        5922   161682   155760    4.31    42.84    38.53
  0                                      131619   215756    84137   95.69    57.16   -38.53
```

One word of caution: other things may change as well!

```
======== 20230412-020911-00745658.mia.pcap.xz vs 20230412-152656-00746016.mia.pcap.xz
  Value                                    Left    Right    Delta    Left %  Right %  Delta-%
------ Ethernet_IP_UDP_DNS_ns_serial
  2023041200                                  0    52105    52105     0.00    99.79   100.00
```

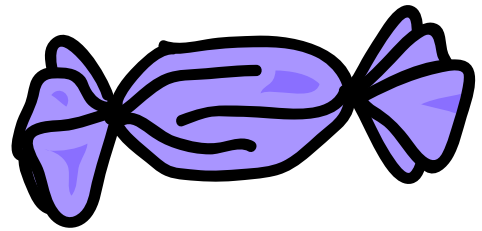
Between the “normal” traffic and the anomaly,
the zone’s serial number changed



INTRODUCING “TRAFFIC-TAFFY”

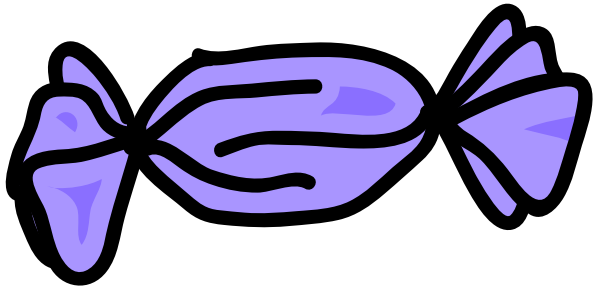
The toolset that helps automate bilateral traffic analysis

Introducing traffic-taffy



- Approach:
  - Perform deep packet inspection of a **base-line**
  - Perform deep packet inspection of an **anomaly**
  - Compare levels for ***each value*** of ***each protocol field***
  - **Sort, Filter and Report** based on findings
- Some of the tools:
  - taffy-dissect: enumerates field counts in a pcap file
  - taffy-compare: compares one file/time-range against another
  - taffy-graph: graphs enumerated fields in pcap files
- Easy to install: ***pip install traffic-taffy***

Try it!



- Please test it!
  - https://traffic-taffy.readthedocs.io/
    - The video from dns-oarc goes into greater usage detail
  - **pip install traffic-taffy**

- Thank you to the **Comcast innovation fund** for sponsoring this work!

Wes Hardaker <hardaker@isi.edu>