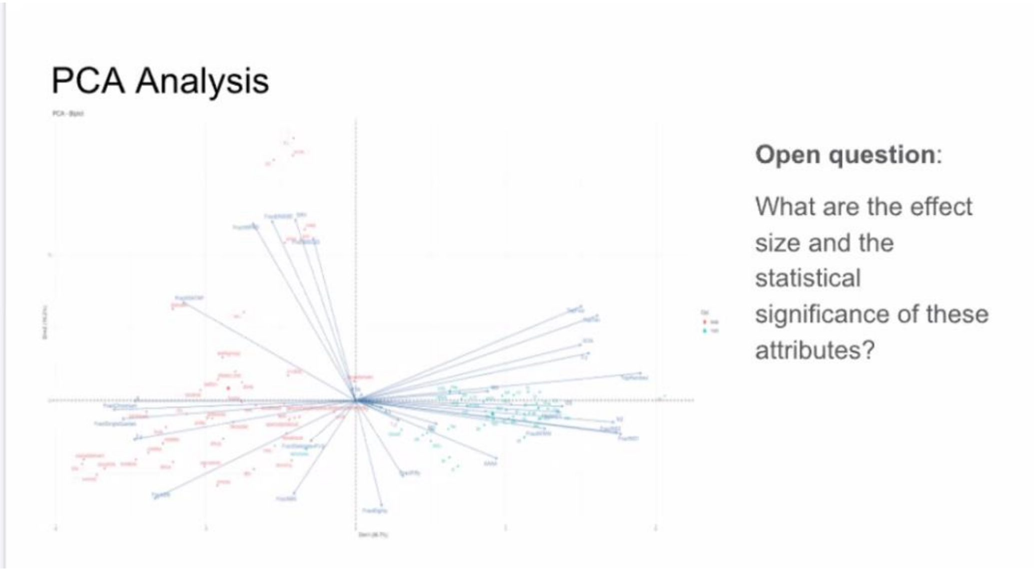
NCAP DISCUSSION GROUP MEETING: 10 MARCH 2021

1. Welcome and roll call
2. Update to SOI
3. Name Collision Data Analysis Update: https://docs.google.com/presentation/d/1MQEgOEDBP0_dJMnilwV10AsDPmeifUn6X0OHJGYbLXM/edit#slide=id.gc5ba7e504d_0_64 [docs.google.com]
4. Question 2, 3, and 10 volunteers
5. AOB

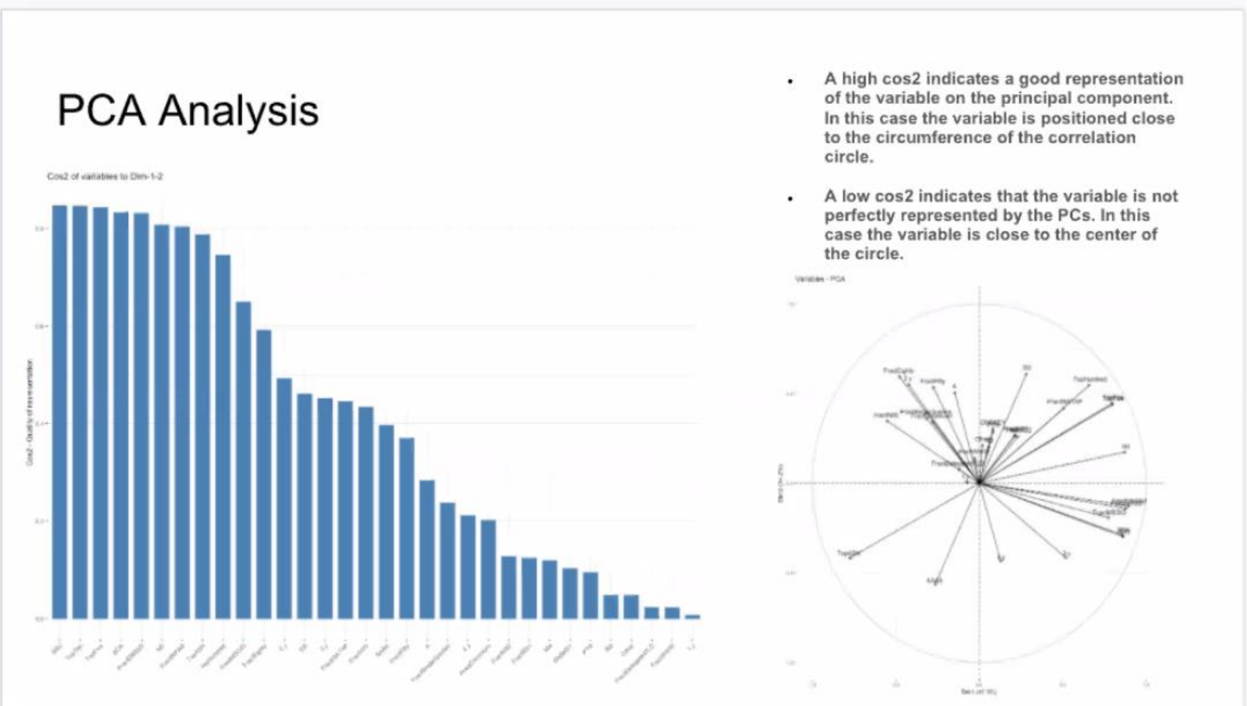
https://docs.google.com/presentation/d/1MQEgOEDBP0_dJMnilwV10AsDPmeifUn6X0OHJGYbLXM/edit#slide=id.p



PCA Analysis

Open question:

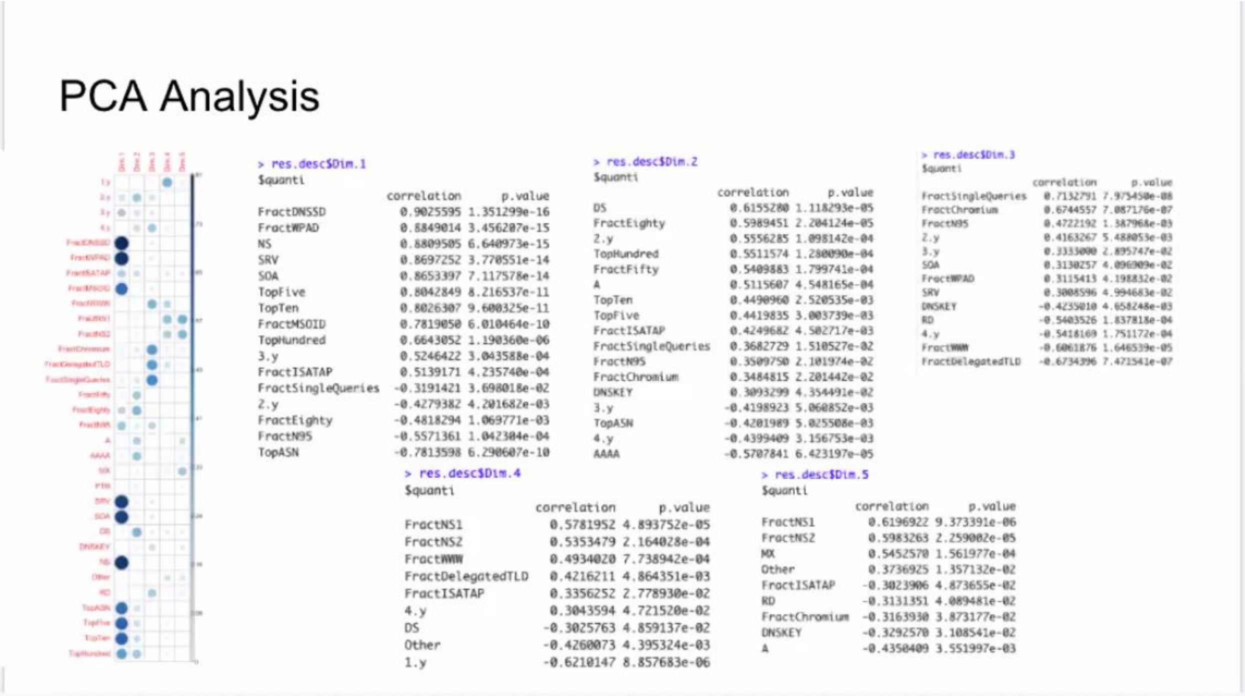
What are the effect size and the statistical significance of these attributes?



PCA Analysis

- A high cos2 indicates a good representation of the variable on the principal component. In this case the variable is positioned close to the circumference of the correlation circle.
- A low cos2 indicates that the variable is not perfectly represented by the PCs. In this case the variable is close to the center of the circle.

How much of a variance is that metric covering for the data points in that data set



PCA Analysis

```
> res.desc$Dim.1
$quanti
                   correlation      p.value
FractDNSSD           0.9025595 1.351299e-16
FractWPAD            0.8849014 3.456207e-15
NS                   0.8809505 6.640973e-15
SRV                  0.8697252 3.770551e-14
SOA                  0.8653397 7.117578e-14
TopFive              0.8042849 8.216537e-11
TopTen               0.8026307 9.600325e-11
FractMSOID           0.7819050 6.010464e-10
TopHundred           0.6643052 1.190360e-06
3.y                  0.5246422 3.043588e-04
FractISATAP          0.5139171 4.235740e-04
FractSingleQueries  -0.3191421 3.698018e-02
2.y                 -0.4279382 4.201682e-03
FractEighty         -0.4818294 1.069771e-03
FractN95            -0.5571361 1.042304e-04
TopASN              -0.7813598 6.290607e-10
```

```
> res.desc$Dim.2
$quanti
                   correlation      p.value
DS                   0.6155280 1.118293e-05
FractEighty          0.5989451 2.204124e-05
2.y                  0.5556285 1.098142e-04
TopHundred           0.5511574 1.280090e-04
FractFifty           0.5409883 1.799741e-04
A                    0.5115607 4.548165e-04
TopTen               0.4490960 2.520535e-03
TopFive              0.4419835 3.003739e-03
FractISATAP          0.4249682 4.502717e-03
FractSingleQueries   0.3682729 1.510527e-02
FractN95             0.3509750 2.101974e-02
FractChromium        0.3484815 2.201442e-02
DNSKEY               0.3093299 4.354491e-02
3.y                 -0.4198923 5.060852e-03
TopASN              -0.4201989 5.025508e-03
4.y                 -0.4399409 3.156753e-03
AAAA                -0.5707841 6.423197e-05
```

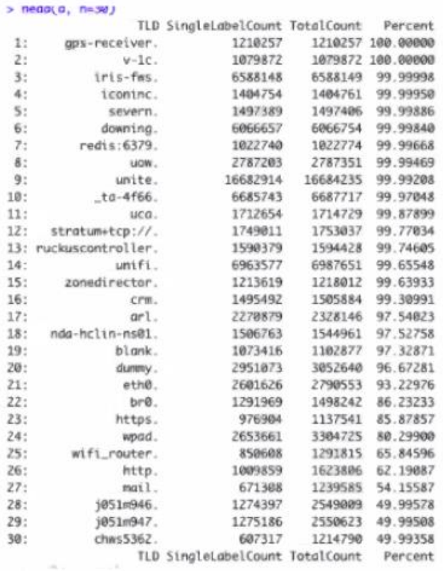
```
> res.desc$Dim.3
$quanti
                   correlation      p.value
FractSingleQueries   0.7132791 7.975450e-08
FractChromium        0.6744557 7.087176e-07
FractN95             0.4722192 1.387968e-03
2.y                  0.4163267 5.488053e-03
3.y                  0.3333000 2.895747e-02
SOA                  0.3130257 4.096909e-02
FractWPAD            0.3115413 4.198832e-02
SRV                  0.3008596 4.994683e-02
DNSKEY              -0.4235010 4.658248e-03
RD                  -0.5403526 1.837818e-04
4.y                 -0.5418169 1.751172e-04
FractWWW            -0.6061876 1.646539e-05
FractDelegatedTLD   -0.6734396 7.471541e-07
```

```
> res.desc$Dim.4
$quanti
                  correlation      p.value
FractNS1            0.5781952 4.893752e-05
FractNS2            0.5353479 2.164028e-04
FractWWW            0.4934020 7.738942e-04
FractDelegatedTLD   0.4216211 4.864351e-03
FractISATAP         0.3356252 2.778930e-02
4.y                 0.3043594 4.721520e-02
DS                 -0.3025763 4.859137e-02
Other              -0.4260073 4.395324e-03
1.y                -0.6210147 8.857683e-06
```

```
> res.desc$Dim.5
$quanti
              correlation      p.value
FractNS1        0.6196922 9.373391e-06
FractNS2        0.5983263 2.259002e-05
MX              0.5452570 1.561977e-04
Other           0.3736925 1.357132e-02
FractISATAP    -0.3023906 4.873655e-02
RD             -0.3131351 4.089481e-02
FractChromium  -0.3163930 3.873177e-02
DNSKEY         -0.3292570 3.108541e-02
A              -0.4350409 3.551997e-03
```

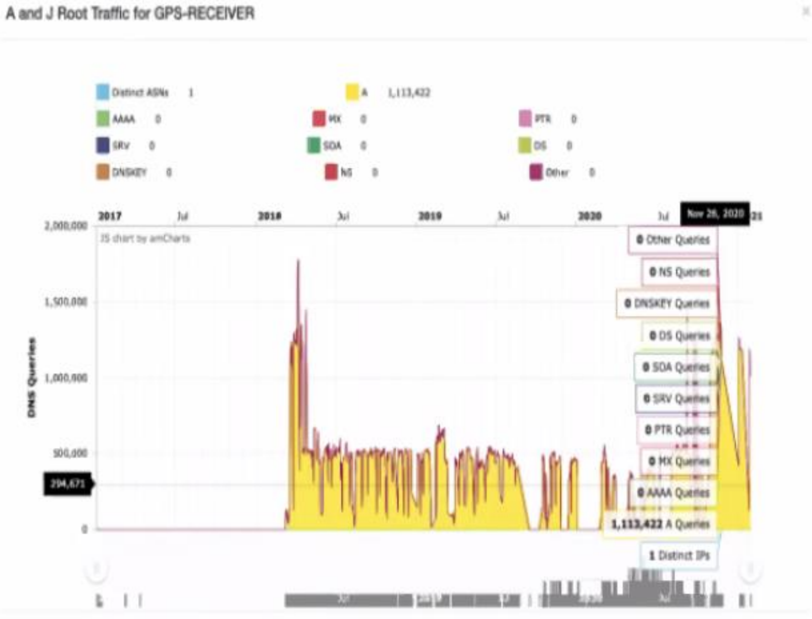
All p values are smaller than 0, so statistically significant

Most Qname Minimized TLDs



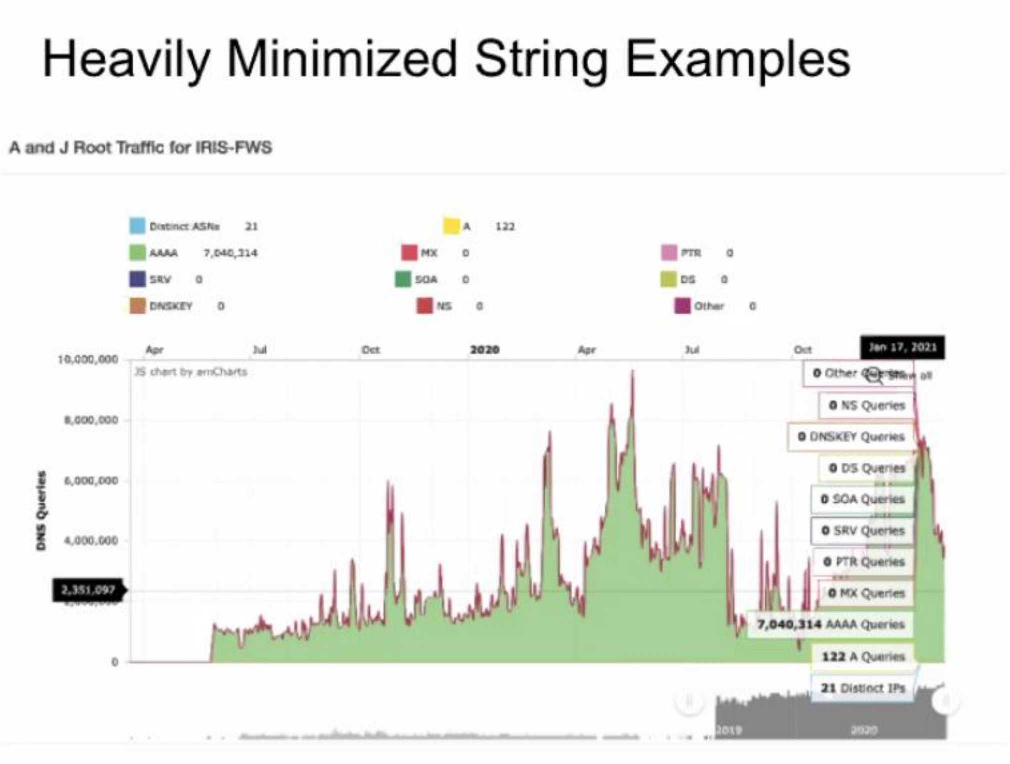
```
> head(a, n=30)
                    TLD SingleLabelCount TotalCount   Percent
 1:       gps-receiver.          1210257    1210257 100.00000
 2:                v-1c.          1079872    1079872 100.00000
 3:           iris-fms.          6588148    6588149  99.99998
 4:            iconinc.          1404754    1404761  99.99950
 5:             severn.          1497389    1497406  99.99886
 6:            downing.          6066657    6066754  99.99840
 7:         redis:6379.          1022740    1022774  99.99668
 8:                uow.          2787203    2787351  99.99469
 9:              unite.         16682914   16684235  99.99208
10:          _ta-4f66.          6685743    6687717  99.97048
11:                uca.          1712654    1714729  99.87899
12:    stratum+tcp://.          1749011    1753037  99.77034
13: ruckuscontroller.          1590379    1594428  99.74605
14:              unifi.          6963577    6987651  99.65548
15:       zonedirector.          1213619    1218012  99.63933
16:                crm.          1495492    1505884  99.30991
17:                arl.          2270879    2328146  97.54023
18:     nda-hclin-ns01.          1506763    1544961  97.52758
19:              blank.          1073416    1102877  97.32871
20:              dummy.          2951073    3052640  96.67281
21:               eth0.          2601626    2790553  93.22976
22:                br0.          1291969    1498242  86.23233
23:              https.           976904    1137541  85.87857
24:               wpad.          2653661    3304725  80.29900
25:        wifi_router.           850608    1291815  65.84596
26:               http.          1009859    1623806  62.19087
27:               mail.           671308    1239585  54.15587
28:          j051m946.          1274397    2549009  49.99578
29:          j051m947.          1275186    2550623  49.99508
30:          chws5362.           607317    1214790  49.99358
                    TLD SingleLabelCount TotalCount   Percent
```

Heavily Minimized String Examples



A and J Root Traffic for GPS-RECEIVER

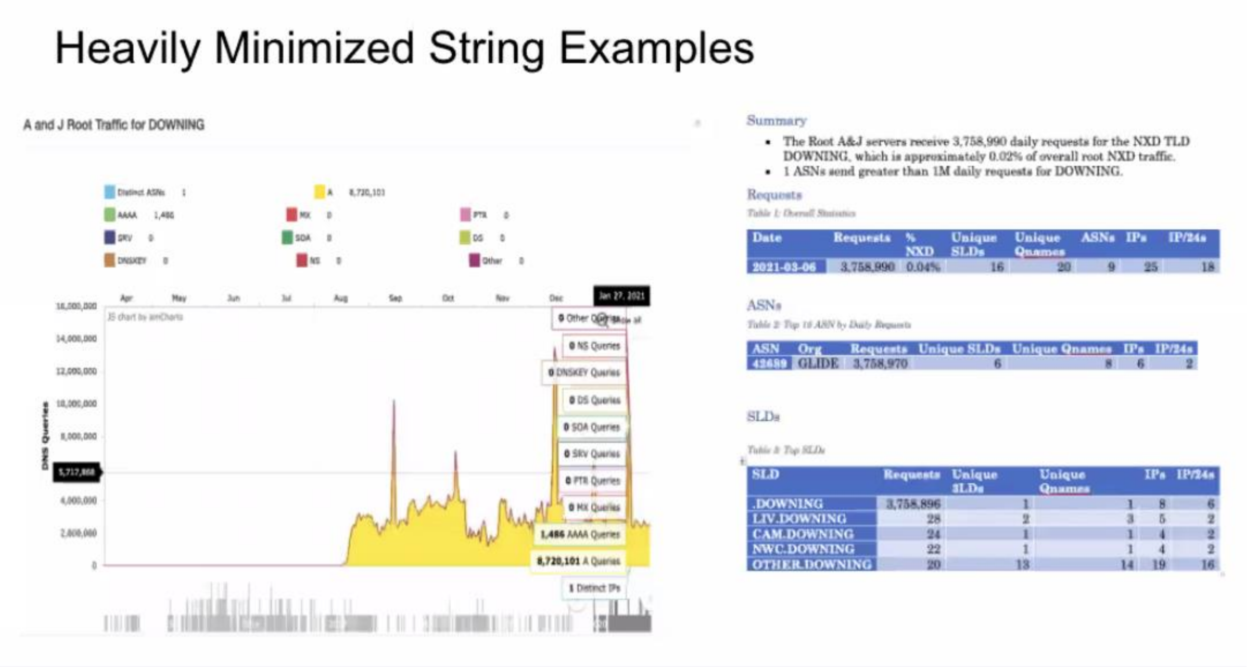
1 million queries a day since 2018. All A queries, only coming from 1 IP address.



Heavily Minimized String Examples

A and J Root Traffic for IRIS-FWS

8 mil queries a day mid 2019 to A&J. consistent



Heavily Minimized String Examples

A and J Root Traffic for DOWNING

Summary

- The Root A&J servers receive 3,758,990 daily requests for the NXD TLD DOWNING, which is approximately 0.02% of overall root NXD traffic.
- 1 ASNs send greater than 1M daily requests for DOWNING.

Requests

Table 1: Overall Statistics

Date	Requests	% NXD	Unique SLDs	Unique Qnames	ASNs	IPs	IP/24s
2021-03-06	3,758,990	0.04%	16	20	9	25	18

ASNs

Table 2: Top 10 ASN by Daily Requests

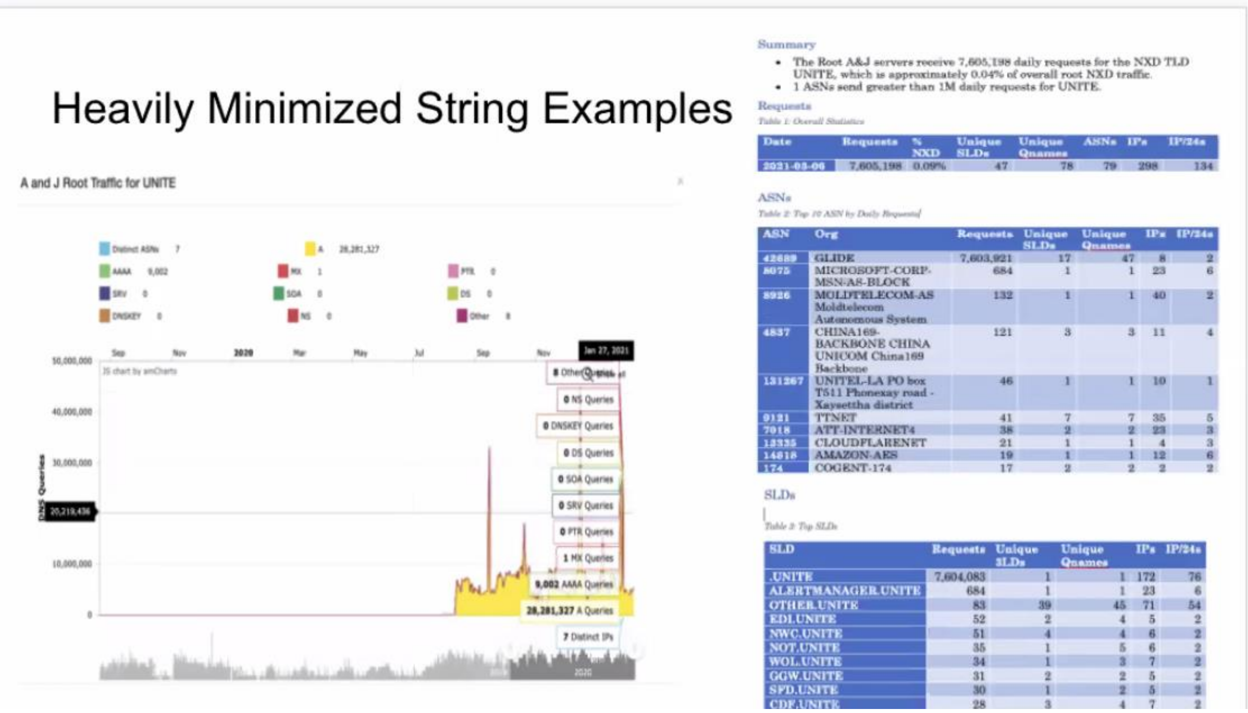
ASN	Org	Requests	Unique SLDs	Unique Qnames	IPs	IP/24s
42689	GLIDE	3,758,970	6	8	6	2

SLDs

Table 3: Top SLDs

SLD	Requests	Unique 3LDs	Unique Qnames	IPs	IP/24s
.DOWNING	3,758,896	1	1	8	6
LIV.DOWNING	28	2	3	5	2
CAM.DOWNING	24	1	1	4	2
NWC.DOWNING	22	1	1	4	2
OTHER.DOWNING	20	13	14	19	16

Vast majority of traffic is 1 single label, sending 3.75 mil queries daily from 1 ASN in UK, company Glide https://glide.co.uk/about-us/#:~:text=The%20Glide%20group%20is%20the,%2C%20broadband%2C%20connectivity%20and%20communications



Heavily Minimized String Examples

Summary

- The Root A&J servers receive 7,605,198 daily requests for the NXD TLD UNITE, which is approximately 0.04% of overall root NXD traffic.
- 1 ASNs send greater than 1M daily requests for UNITE.

Requests

Table 1: Overall Statistics

Date	Requests	% NXD	Unique SLDs	Unique Qnames	ASNs	IPs	IP/24s
2021-03-06	7,605,198	0.09%	47	78	79	298	134

ASNs

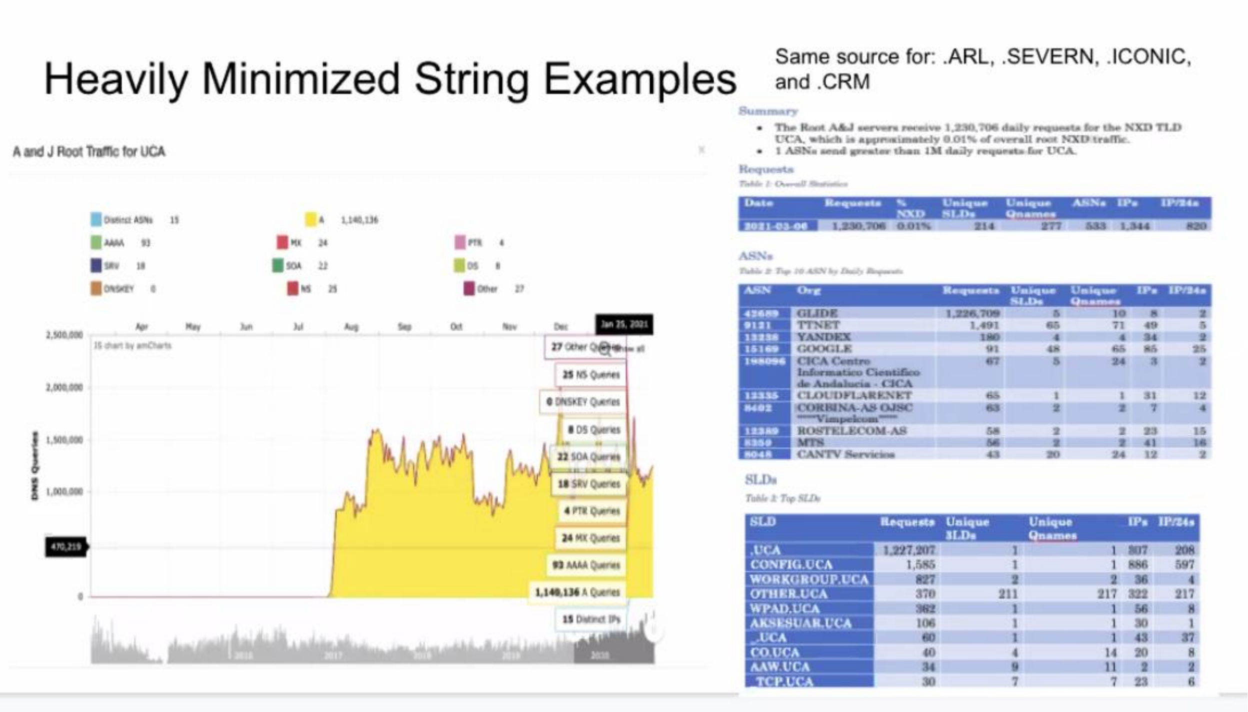
Table 2: Top 10 ASN by Daily Requests

ASN	Org	Requests	Unique SLDs	Unique Qnames	IPs	IP/24s
42689	GLIDE	7,603,921	17	47	8	2
8075	MICROSOFT-CORP-MSN-AS-BLOCK	684	1	1	23	6
8926	MOLDTELECOM-AS Moldtelecom Autonomous System	132	1	1	40	2
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	121	3	3	11	4
131267	UNITEL-LA PO box T511 Phonexay road - Xaysettha district	46	1	1	10	1
9121	TTNET	41	7	7	35	5
7018	ATT-INTERNET4	38	2	2	23	3
13335	CLOUDFLARENET	21	1	1	4	3
14618	AMAZON-AES	19	1	1	12	6
174	COGENT-174	17	2	2	2	2

SLDs

Table 3: Top SLDs

SLD	Requests	Unique SLDs	Unique Qnames	IPs	IP/24s
.UNITE	7,604,083	1	1	172	76
ALERTMANAGER.UNITE	684	1	1	23	6
OTHER.UNITE	83	39	45	71	54
EDI.UNITE	52	2	4	5	2
NWC.UNITE	51	4	4	6	2
NOT.UNITE	35	1	5	6	2
WOL.UNITE	34	1	3	7	2
GGW.UNITE	31	2	2	5	2
SFD.UNITE	30	1	2	5	2
CDF.UNITE	28	3	4	7	2



Heavily Minimized String Examples

Same source for: .ARL, .SEVERN, .ICONIC, and .CRM

Summary

- The Root A&J servers receive 1,230,706 daily requests for the NXD TLD UCA, which is approximately 0.01% of overall root NXD traffic.
- 1 ASNs send greater than 1M daily requests for UCA.

Requests

Table 1: Overall Statistics

Date	Requests	% NXD	Unique SLDs	Unique Qnames	ASNs	IPs	IP/24s
2021-03-06	1,230,706	0.01%	214	277	533	1,344	820

ASNs

Table 2: Top 10 ASN by Daily Requests

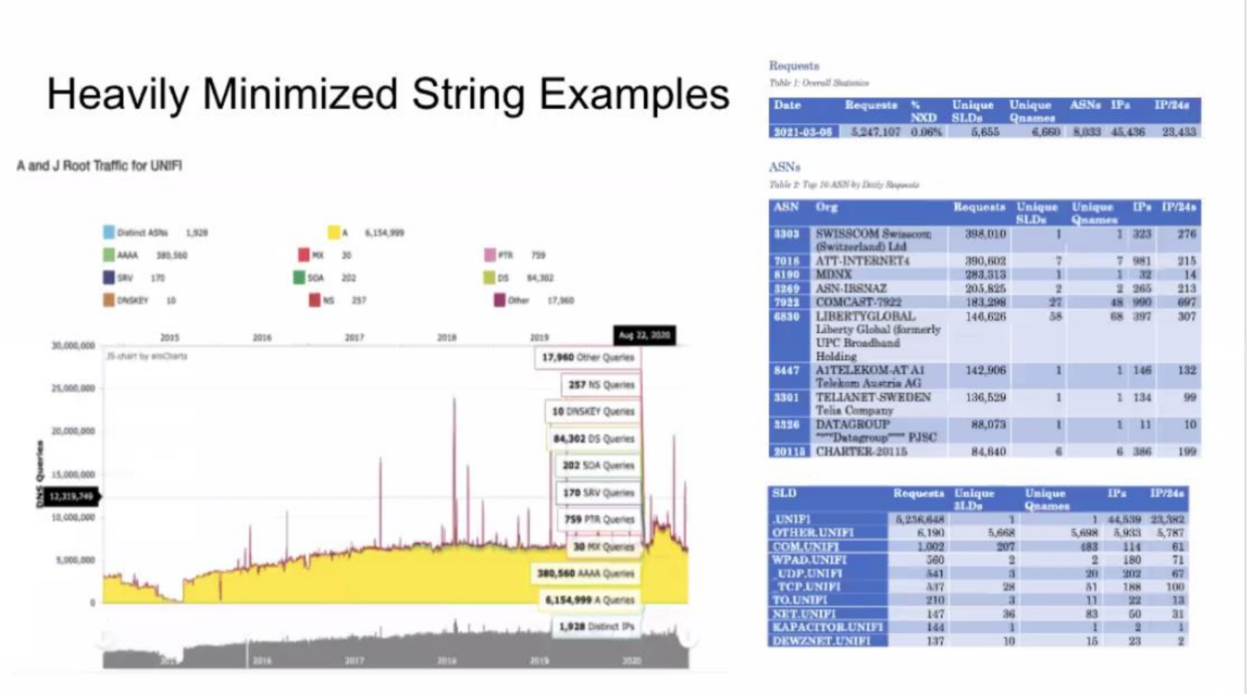
ASN	Org	Requests	Unique SLDs	Unique Qnames	IPs	IP/24s
42689	GLIDE	1,226,709	5	10	8	2
9121	TTNET	1,491	65	71	49	5
13238	YANDEX	180	4	4	34	2
15169	GOOGLE	91	48	65	85	25
198096	CICA Centro Informatico Cientifico de Andalucia - CICA	67	5	24	3	2
13335	CLOUDFLARENET	65	1	1	31	12
8402	CORBINA-AS OJSC """"Vimpelcom""""	63	2	2	7	4
12389	ROSTELECOM-AS	58	2	2	23	15
8359	MTS	56	2	2	41	16
8048	CANTV Servicios	43	20	24	12	2

SLDs

Table 3: Top SLDs

SLD	Requests	Unique SLDs	Unique Qnames	IPs	IP/24s
.UCA	1,227,207	1	1	807	208
CONFIG.UCA	1,585	1	1	886	597
WORKGROUP.UCA	827	2	2	36	4
OTHER.UCA	370	211	217	322	217
WPAD.UCA	362	1	1	56	8
AKSESUAR.UCA	106	1	1	30	1
_.UCA	60	1	1	43	37
CO.UCA	40	4	14	20	8
AAW.UCA	34	9	11	2	2
_TCP.UCA	30	7	7	23	6

Same company behind this as last slide



Heavily Minimized String Examples

A and J Root Traffic for UNIFI

Requests

Table 1: Overall Statistics

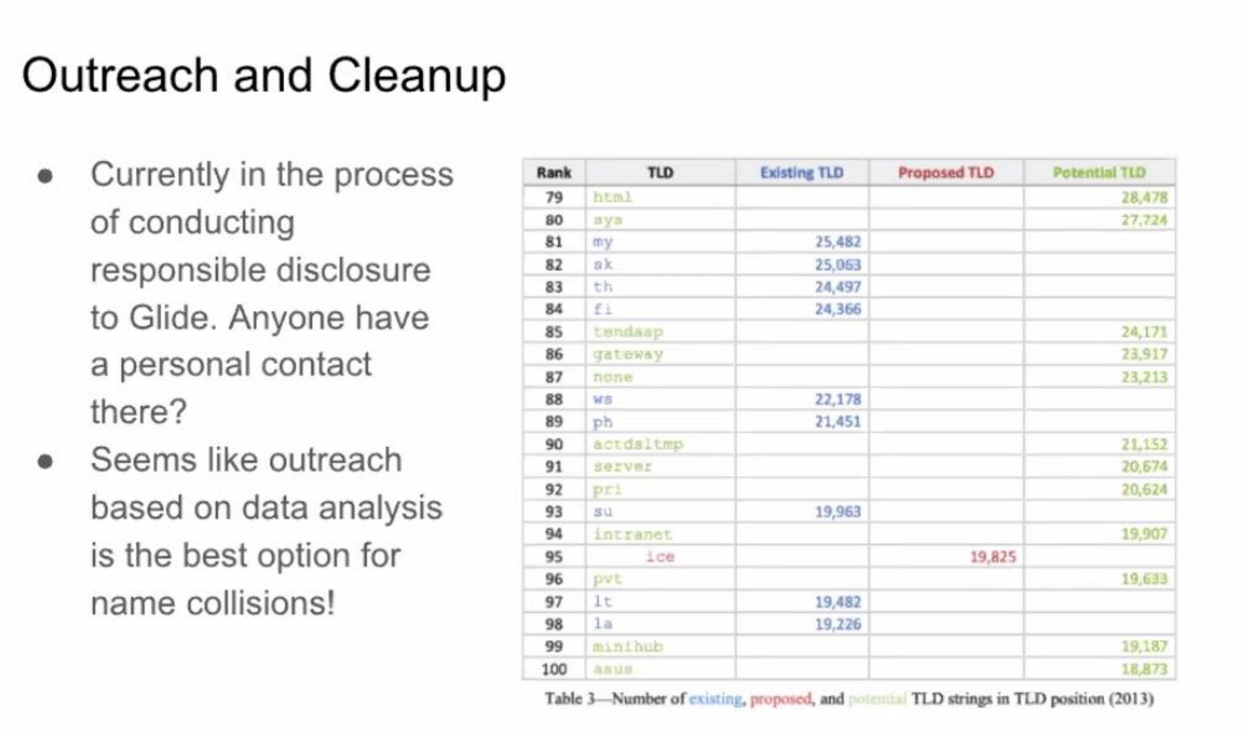
Date	Requests	% NXD	Unique SLDs	Unique Qnames	ASNs	IPs	IP/24s
2021-03-05	5,247,107	0.06%	5,655	6,660	8,033	45,436	23,433

ASNs

Table 2: Top 10 ASN by Daily Requests

ASN	Org	Requests	Unique SLDs	Unique Qnames	IPs	IP/24s
3303	SWISSCOM Swisscom (Switzerland) Ltd	398,010	1	1	323	276
7018	ATT-INTERNET4	390,602	7	7	981	215
8190	MDNX	283,313	1	1	32	14
3269	ASN-IBSNAZ	205,825	2	2	265	213
7922	COMCAST-7922	183,298	27	48	990	697
6830	LIBERTYGLOBAL Liberty Global (formerly UPC Broadband Holding	146,626	58	68	397	307
8447	A1TELEKOM-AT A1 Telekom Austria AG	142,906	1	1	146	132
3301	TELIANET-SWEDEN Telia Company	136,529	1	1	134	99
3326	DATAGROUP """"Datagroup"""" PJSC	88,073	1	1	11	10
20115	CHARTER-20115	84,640	6	6	386	199

SLD	Requests	Unique SLDs	Unique Qnames	IPs	IP/24s
.UNIFI	5,236,648	1	1	44,539	23,382
OTHER.UNIFI	6,190	5,668	5,698	5,933	5,787
COM.UNIFI	1,002	207	483	114	61
WPAD.UNIFI	560	2	2	180	71
_UDP.UNIFI	541	3	20	202	67
_TCP.UNIFI	537	28	51	188	100
TO.UNIFI	210	3	11	22	13
NET.UNIFI	147	36	83	50	31
KAPACITOR.UNIFI	144	1	1	2	1
DEWZNET.UNIFI	137	10	15	23	2



Outreach and Cleanup

- Currently in the process of conducting responsible disclosure to Glide. Anyone have a personal contact there?
- Seems like outreach based on data analysis is the best option for name collisions!

Rank	TLD	Existing TLD	Proposed TLD	Potential TLD
79	html			28,478
80	sys			27,724
81	my	25,482		
82	sk	25,063		
83	th	24,497		
84	fi	24,366		
85	tendaap			24,171
86	gateway			23,917
87	none			23,213
88	ws	22,178		
89	ph	21,451		
90	actdsltmp			21,152
91	server			20,674
92	pri			20,624
93	su	19,963		
94	intranet			19,907
95	ice		19,825	
96	pvt			19,633
97	lt	19,482		
98	la	19,226		
99	minihub			19,187
100	asus			18,873

Table 3—Number of existing, proposed, and potential TLD strings in TLD position (2013)

Capture analsyis – continue doing this type of analysis in event that hyprlocal root service becomes abundant and what is desireable to enable this anslysis with hyperlocal root service? Bring to DNSOARK

JOHN KRISTOFF