



Use and Abuse at ns.icann.org

Roy Arends | ICANN | June 2016

Prologue

ns.icann.org

Traffic to NS.ICANN.ORG

What does NS.ICANN.ORG look like?

Two servers at two locations:

IAD and LAX

A few weeks of captured traffic, uploaded to Turing

What does ns.icann.org do?

Authoritative for:

```
dig @lax.xfr.dns.icann.org . axfr|grep "NS\tns.icann.org."
```

```
int.          172800 IN  NS  ns.icann.org.  
museum.      172800 IN  NS  ns.icann.org.  
ug.          172800 IN  NS  ns.icann.org.
```

What does ns.icann.org do?

Authoritative for:

```
dig @lax.xfr.dns.icann.org . axfr|grep "NS\tns.icann.org."
```

```
int.          172800 IN  NS  ns.icann.org.  
museum.      172800 IN  NS  ns.icann.org.  
ug.          172800 IN  NS  ns.icann.org.
```

and a whole bunch more

224.in-addr.arpa. – 239.in-addr.arpa.

ipv4only.arpa.

mcast.net.

icann.org.

etc

What does ns.icann.org do?

Authoritative for:

int.

ug.

Chapter One

The Telephone Company

Lets talk about INT

TPC.INT

RFC 1528-1529-1530

RFC 1569

RFC 1703

“Remote Printing”

The idea: send an email to a fax.

You'll need a phone number, reverse it, look it up in DNS (type MX)

Lets talk about INT

TPC.INT

“The Phone Company”

RFC 1528-1529-1530

RFC 1569

RFC 1703

“Remote Printing”

The idea: send an email to a fax.

You'll need a phone number, reverse it, look it up in DNS (type MX)

THE PRESIDENT'S ANALYST





Lets talk about TPC.INT

TPC.INT

You'll need a phone number, reverse it, look it up in DNS (type MX)

Example from the RFC:

+1 415 968 2510

```
0.1.5.2.8.6.9.5.1.4.1.tpc.int.      IN MX 10 dbc.mtview.ca.us.
```

Let's look at the delegation for TPC.INT:

Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.    NS  ns1.tpc.int.  
tpc.int.    NS  ns1.simkin.ca.  
tpc.int.    NS  ns1.covalent.net.  
tpc.int.    NS  ns2.simkin.ca.  
tpc.int.    NS  auth02.ns.uu.net.
```

Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.  NS  ns1.tpc.int.      A 216.152.192.130
tpc.int.  NS  ns1.simkin.ca.     A 10.255.255.251
tpc.int.  NS  ns1.covalent.net.
tpc.int.  NS  ns2.simkin.ca.     A 10.6.6.7
tpc.int.  NS  auth02.ns.uu.net.  A 198.6.1.82
```

Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.  NS  ns1.tpc.int.      A  216.152.192.130
tpc.int.  NS  ns1.simkin.ca.     A  10.255.255.251
tpc.int.  NS  ns1.covalent.net.  NXDOMAIN
tpc.int.  NS  ns2.simkin.ca.     A  10.6.6.7
tpc.int.  NS  auth02.ns.uu.net.  A  198.6.1.82
```

Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.  NS  ns1.tpc.int.      A  216.152.192.130
tpc.int.  NS  ns1.simkin.ca.     A  10.255.255.251
tpc.int.  NS  ns1.covalent.net.  NXDOMAIN
tpc.int.  NS  ns2.simkin.ca.     A  10.6.6.7
tpc.int.  NS  auth02.ns.uu.net.  A  198.6.1.82
```


Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.  NS  ns1.tpc.int.      A  216.152.192.130
```

```
tpc.int.  NS  auth02.ns.uu.net.  A  198.6.1.82
```

Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.  NS  ns1.tpc.int.      A 216.152.192.130
```

```
;; connection timed out; no servers could be reached
```

```
tpc.int.  NS  auth02.ns.uu.net.  A 198.6.1.82
```

Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.  NS  ns1.tpc.int.      A 216.152.192.130
```

```
;; connection timed out; no servers could be reached
```

```
tpc.int.  NS  auth02.ns.uu.net.  A 198.6.1.82
```

```
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL
```

Lets talk about TPC.INT

Let's look at the delegation for TPC.INT:

```
dig @ns.icann.org tpc.int ns
```

```
tpc.int.  NS  ns1.tpc.int.      A 216.152.192.130
```

```
;; connection timed out; no servers could be reached
```

```
tpc.int.  NS  auth02.ns.uu.net.  A 198.6.1.82
```

```
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL
```

```
tpc.int.  SOA ns1.tpc.int. dns.tpc.int. 2013103001 ...
```

Lets talk about TPC.INT

This stuff has stopped working YEARS AGO

Lets talk about TPC.INT

TOP 100 QNAMES: QNAME = TPC.INT, SUBDOMAIN = 1



VALUE	COUNT
ns1.tpc.int.	228
info.tpc.int.	33
www.tpc.int.	31
852 [REDACTED] 5178.iddd.tpc.int.	26
852 [REDACTED] 2525.iddd.tpc.int.	25
tpc.int.	11
9.9 [REDACTED] 7.6.2.1.2.1.tpc.int.	8
6.7 [REDACTED] 4.9.5.1.4.1.tpc.int.	6
2.3 [REDACTED] 0.5.2.1.2.1.tpc.int.	5
0.1 [REDACTED] 6.9.5.1.4.1.tpc.int.	5
020 [REDACTED] 6834.iddd.tpc.int.	5
861 [REDACTED] 45678.iddd.tpc.int.	3
161 [REDACTED] 932.iddd.tpc.int.	3
551 [REDACTED] 79413.iddd.tpc.int.	2
120 [REDACTED] 2883.iddd.tpc.int.	2
161 [REDACTED] 9123.iddd.tpc.int.	2
492 [REDACTED] 01059.iddd.tpc.int.	2
935 [REDACTED] 74.iddd.tpc.int.	2

Lets talk about TPC.INT

TOP 100 QNAMES: QNAME = TPC.INT, SUBDOMAIN = 1



VALUE	COUNT
ns1.tpc.int.	228
info.tpc.int.	33
www.tpc.int.	31
852 [REDACTED] 5178.iddd.tpc.int.	26
852 [REDACTED] 2525.iddd.tpc.int.	25
tpc.int.	11
9.9 [REDACTED] 7.6.2.1.2.1.tpc.int.	8
6.7 [REDACTED] 4.9.5.1.4.1.tpc.int.	6
2.3 [REDACTED] 0.5.2.1.2.1.tpc.int.	5
0.1 [REDACTED] 6.9.5.1.4.1.tpc.int.	5
020 [REDACTED] 834.iddd.tpc.int.	5
861 [REDACTED] 45678.iddd.tpc.int.	3
161 [REDACTED] 932.iddd.tpc.int.	3
551 [REDACTED] 79413.iddd.tpc.int.	2
120 [REDACTED] 2883.iddd.tpc.int.	2
161 [REDACTED] 9123.iddd.tpc.int.	2
492 [REDACTED] 01059.iddd.tpc.int.	2
935 [REDACTED] 74.iddd.tpc.int.	2

Normal stuff



Lets talk about TPC.INT

TOP 100 QNAMES: QNAME = TPC.INT, SUBDOMAIN = 1

VALUE	COUNT
ns1.tpc.int.	228
info.tpc.int.	33
www.tpc.int.	31
852 [REDACTED] 5178.iddd.tpc.int.	26
852 [REDACTED] 2525.iddd.tpc.int.	25
tpc.int.	11
9.9 [REDACTED] 7.6.2.1.2.1.tpc.int.	8
6.7 [REDACTED] 4.9.5.1.4.1.tpc.int.	6
2.3 [REDACTED] 0.5.2.1.2.1.tpc.int.	5
0.1 [REDACTED] 6.9.5.1.4.1.tpc.int.	5
020 [REDACTED] 6834.iddd.tpc.int.	5
861 [REDACTED] 45678.iddd.tpc.int.	3
161 [REDACTED] 0932.iddd.tpc.int.	3
551 [REDACTED] 79413.iddd.tpc.int.	2
120 [REDACTED] 2883.iddd.tpc.int.	2
161 [REDACTED] 0123.iddd.tpc.int.	2
492 [REDACTED] 01059.iddd.tpc.int.	2
935 [REDACTED] 74.iddd.tpc.int.	2

Normal stuff



Inter. Direct Distance Dialing



Lets talk about TPC.INT

TOP 100 QNAMES: QNAME = TPC.INT, SUBDOMAIN = 1

VALUE	COUNT
ns1.tpc.int.	228
info.tpc.int.	33
www.tpc.int.	31
852 [REDACTED] 5178.iddd.tpc.int.	26
852 [REDACTED] 2525.iddd.tpc.int.	25
tpc.int.	11
9.9 [REDACTED] 7.6.2.1.2.1.tpc.int.	8
6.7 [REDACTED] 4.9.5.1.4.1.tpc.int.	6
2.3 [REDACTED] 0.5.2.1.2.1.tpc.int.	5
0.1 [REDACTED] 6.9.5.1.4.1.tpc.int.	5
020 [REDACTED] 834.iddd.tpc.int.	5
861 [REDACTED] 45678.iddd.tpc.int.	3
161 [REDACTED] 932.iddd.tpc.int.	3
551 [REDACTED] 79413.iddd.tpc.int.	2
120 [REDACTED] 2883.iddd.tpc.int.	2
161 [REDACTED] 9123.iddd.tpc.int.	2
492 [REDACTED] 01059.iddd.tpc.int.	2
935 [REDACTED] 74.iddd.tpc.int.	2

Normal stuff



Inter. Direct Distance Dialing



+852 == Hong Kong

Lets talk about TPC.INT

TOP 100 QNAMES: QNAME = TPC.INT, SUBDOMAIN = 1

VALUE	COUNT
ns1.tpc.int.	228
info.tpc.int.	33
www.tpc.int.	31
852 [REDACTED] 5178.iddd.tpc.int.	26
852 [REDACTED] 2525.iddd.tpc.int.	25
tpc.int.	11
9.9 [REDACTED] 7.6.2.1.2.1.tpc.int.	8
6.7 [REDACTED] 4.9.5.1.4.1.tpc.int.	6
2.3 [REDACTED] 0.5.2.1.2.1.tpc.int.	5
0.1 [REDACTED] 6.9.5.1.4.1.tpc.int.	5
020 [REDACTED] 834.iddd.tpc.int.	5
861 [REDACTED] 45678.iddd.tpc.int.	3
161 [REDACTED] 932.iddd.tpc.int.	3
551 [REDACTED] 79413.iddd.tpc.int.	2
120 [REDACTED] 2883.iddd.tpc.int.	2
161 [REDACTED] 9123.iddd.tpc.int.	2
492 [REDACTED] 01059.iddd.tpc.int.	2
935 [REDACTED] 74.iddd.tpc.int.	2

Normal stuff



Inter. Direct Distance Dialing



+852 == Hong Kong

+1212 == New York



Chapter Two

The Ole' Forgotten ip6.int

Lets talk about IP6.INT

Network Working Group
Request for Comments: 4159
BCP: 109
Category: Best Current Practice

G. Huston
APNIC
August 2005

Deprecation of "ip6.int"

Status of This Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document advises of the deprecation of the use of "ip6.int" for Standards Conformant IPv6 implementations.

Lets talk about IP6.INT

Network Working Group
Request for Comments: 4159
BCP: 109
Category: Best Current Practice

G. Huston
APNIC
August 2005

Deprecation of "ip6.int"

Status of This Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document advises of the **deprecation of the use of "ip6.int"** for Standards Conformant IPv6 implementations.

Lets talk about IP6.INT

1. IPv6 Standards Action

In **August 2001** the IETF published [RFC3152], which advised that the use of "ip6.int" as the domain for reverse-mapping of IPv6 addresses to DNS names was deprecated. The document noted that the use of "ip6.int" would be phased out in an orderly fashion.

As of **1 September 2005**, the IETF advises the community that the DNS domain "ip6.int" should no longer be used to perform reverse mapping of IPv6 addresses to domain names, and that the domain "ip6.arpa" should be used henceforth, in accordance with the IANA Considerations described in [RFC3596]. The domain "ip6.int" is deprecated, and its use in IPv6 implementations that conform to the IPv6 Internet Standards is discontinued.

Lets talk about IP6.INT

August 2001

September 2005

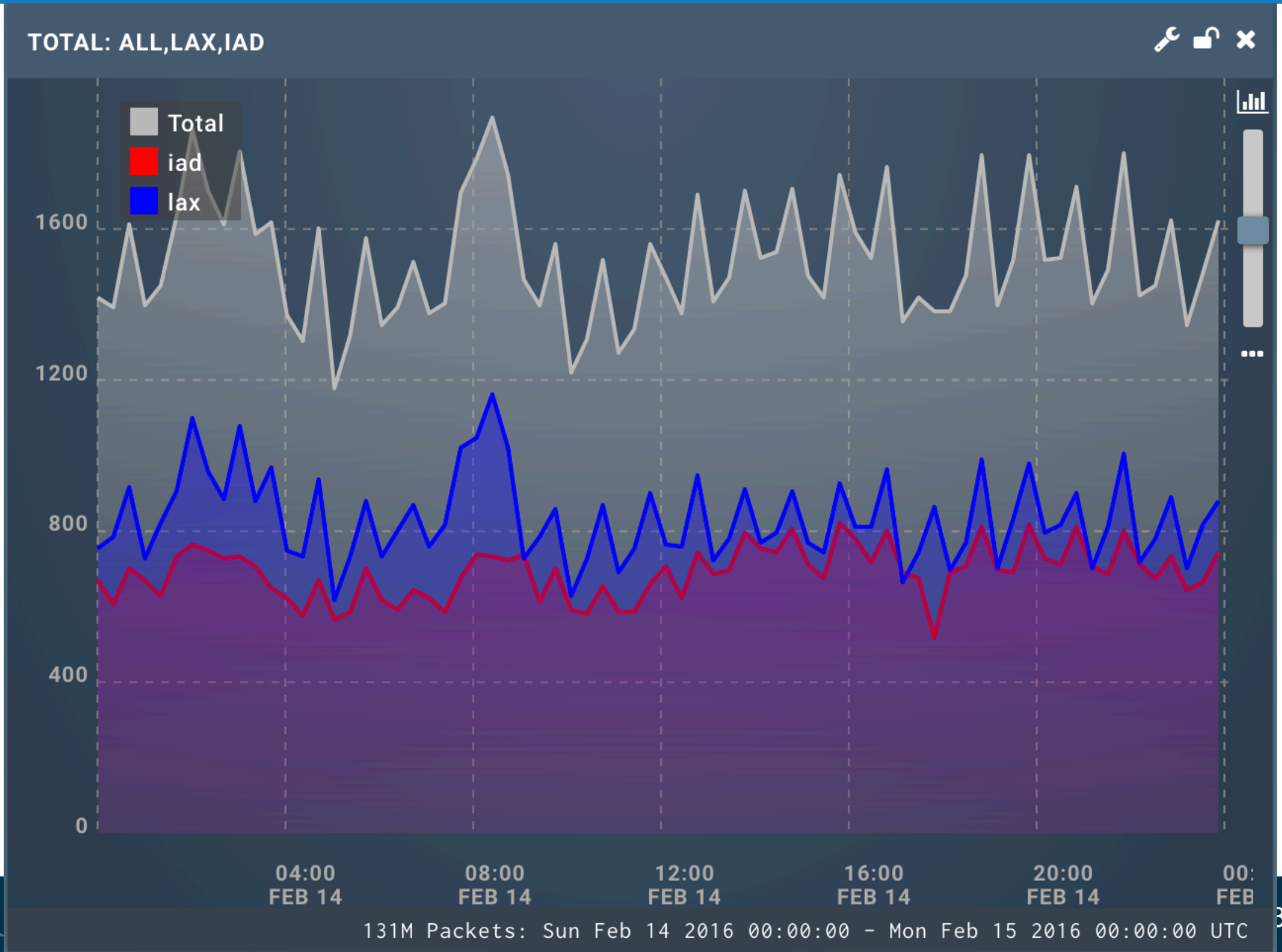
Lets talk about IP6.INT

IP6.INT was in use for 4 years

Then the TLD was “rolled” to ARPA

Over 10 years ago.

all traffic to ns.icann.org

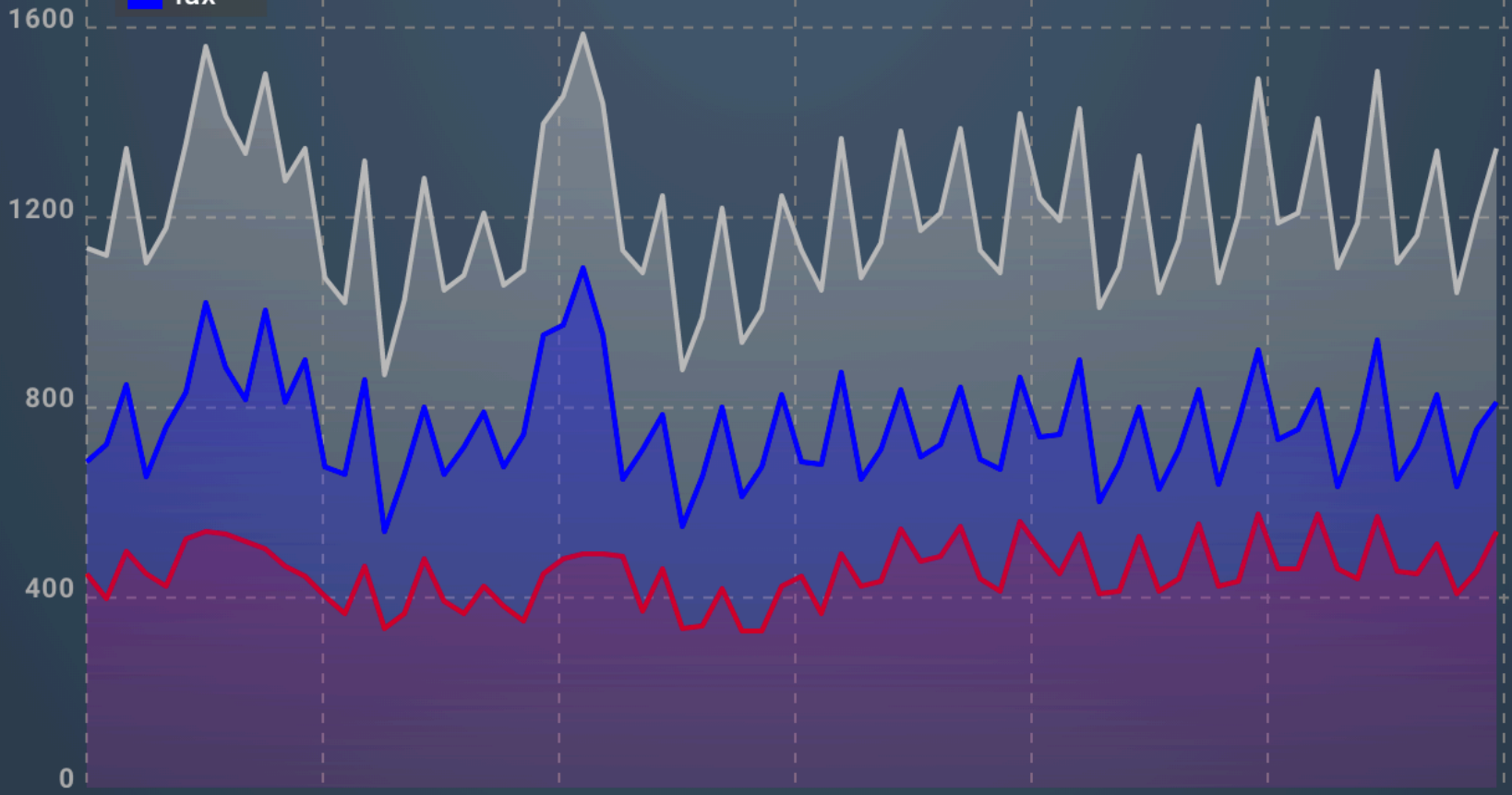


All traffic for INT

TOTAL: ALL,LAX,IAD, QNAME = INT, SUBDOMAIN = 1



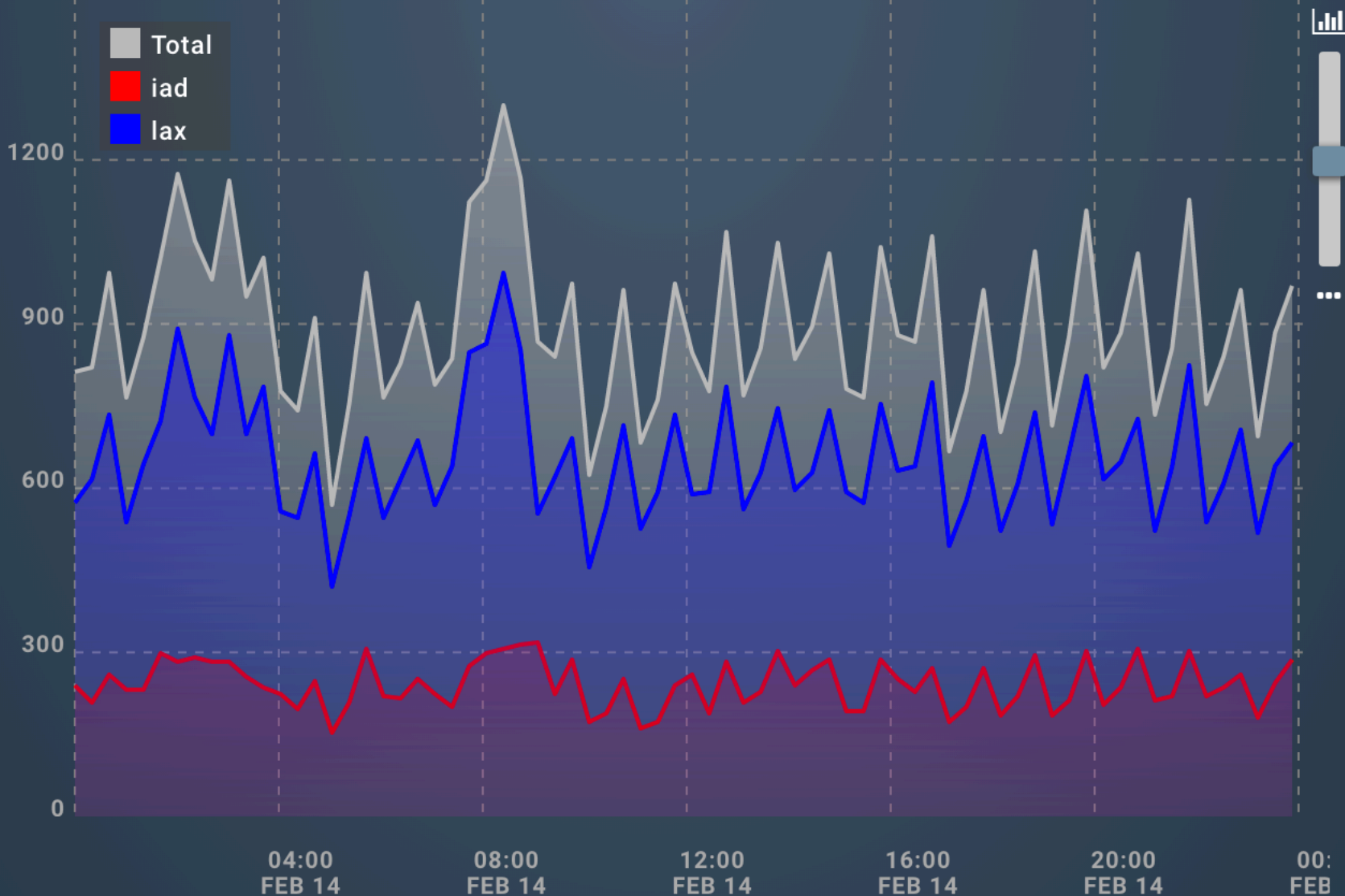
- Total
- iad
- lax



105M Packets: Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:00 UTC

All traffic for IP6.INT

TOTAL: ALL,LAX,IAD, QNAME = IP6.INT, SUBDOMAIN = 1



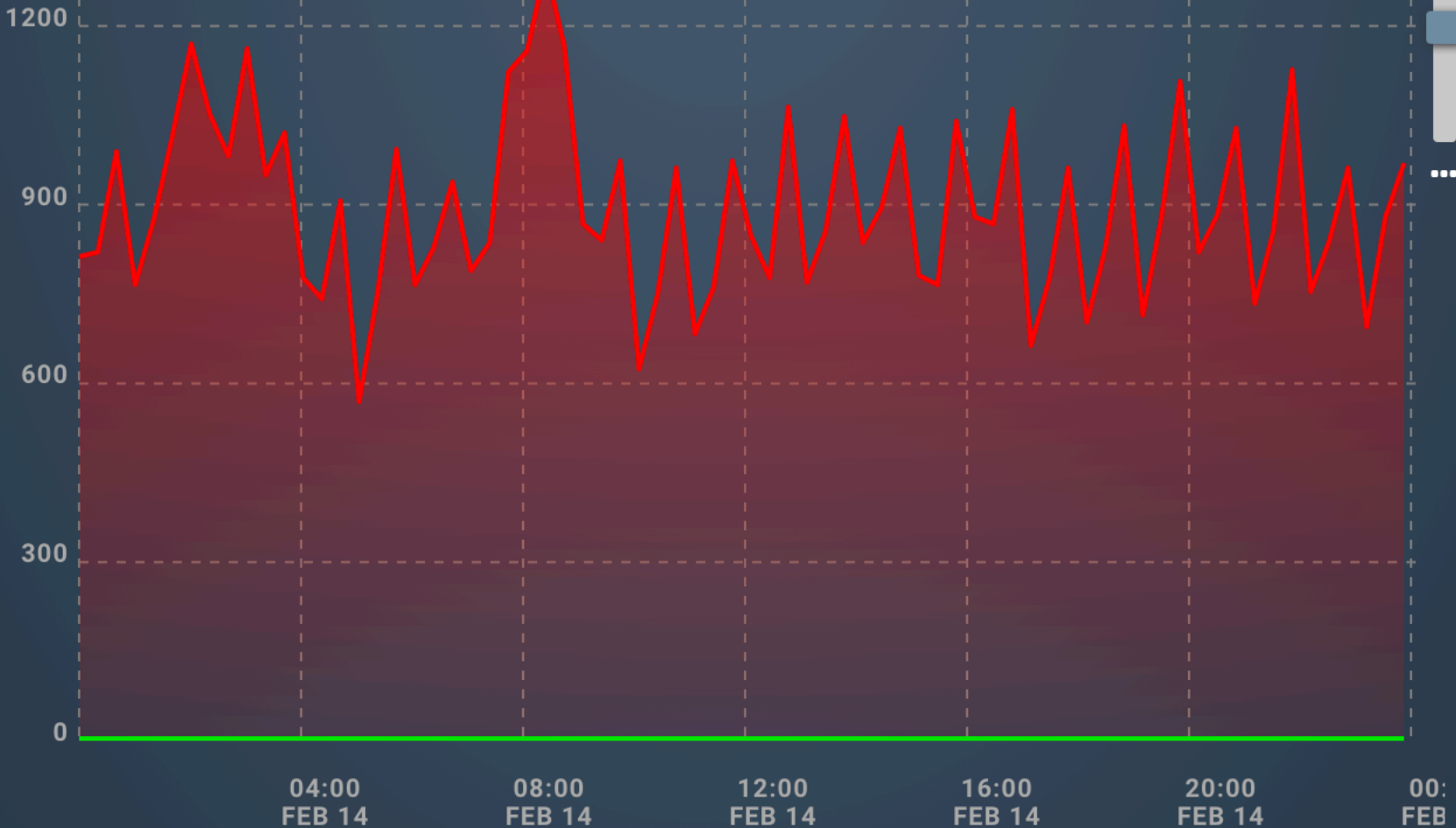
77M Packets: Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:00 UTC

All traffic for IP6.INT

RCODE: QNAME = IP6.INT, SUBDOMAIN = 1



- NoError
- NxDomain



77M Packets: Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:00 UTC

Lets talk about IP6.INT

Total traffic for ALL domains to NS.ICANN.ORG: 131M

Lets talk about IP6.INT

Total traffic for ALL domains to NS.ICANN.ORG: 131M

Total traffic for ALL int domains to NS.ICANN.ORG: 105M

Lets talk about IP6.INT

Total traffic for ALL domains to NS.ICANN.ORG:	131M
Total traffic for ALL int domains to NS.ICANN.ORG:	105M
Total traffic for IP6.INT domains to NS.ICANN.ORG:	77M

Lets talk about IP6.INT

59%

Of ALL queries to NS.ICANN.ORG is for IP6.INT

Lets talk about IP6.INT

73%

Of INT queries to NS.ICANN.ORG is for IP6.INT

Interlude

stale roots

.OM (Oman)

.OM (Oman)

March 21, 2012, ns.icann.org is de-listed from OM zone apex

.OM (Oman)

March 21, 2012, ns.icann.org is de-listed from OM zone apex

April 4 2012, OM domain is delegated away from ns.icann.org

.OM (Oman)

March 21, 2012, ns.icann.org is de-listed from OM zone apex

April 4 2012, OM domain is delegated away from ns.icann.org

April 5 2012, OM is not served from ns.icann.org anymore

OMAN

TOTAL: ALL,LAX,IAD, QNAME = OM, SUBDOMAIN = 1



- Total
- iad
- lax

TOP 100 IPS: QNAME = OM, SUBDOMAIN = 1



VALUE	COUNT	ASN	DESCRIPTION	CC
61.237.2.170	353	9394	CTTNET China Tie...	CN
183.136.160.231	18	58461	CT-HANGZHOU-ID...	CN
61.237.2.178	1	9394	CTTNET China Tie...	CN

372 packets, Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:00...



04:00
FEB 14

08:00
FEB 14

12:00
FEB 14

16:00
FEB 14

20:00
FEB 14

00:00
FEB 15

372 Packets: Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:00 UTC

Chapter Three

Wewe ni lulu ya taji la Afrika.

Chapter Three

Wewe ni lulu ya taji la Afrika.

(The Pearl of Africa's Crown.)



Lets talk about .UG

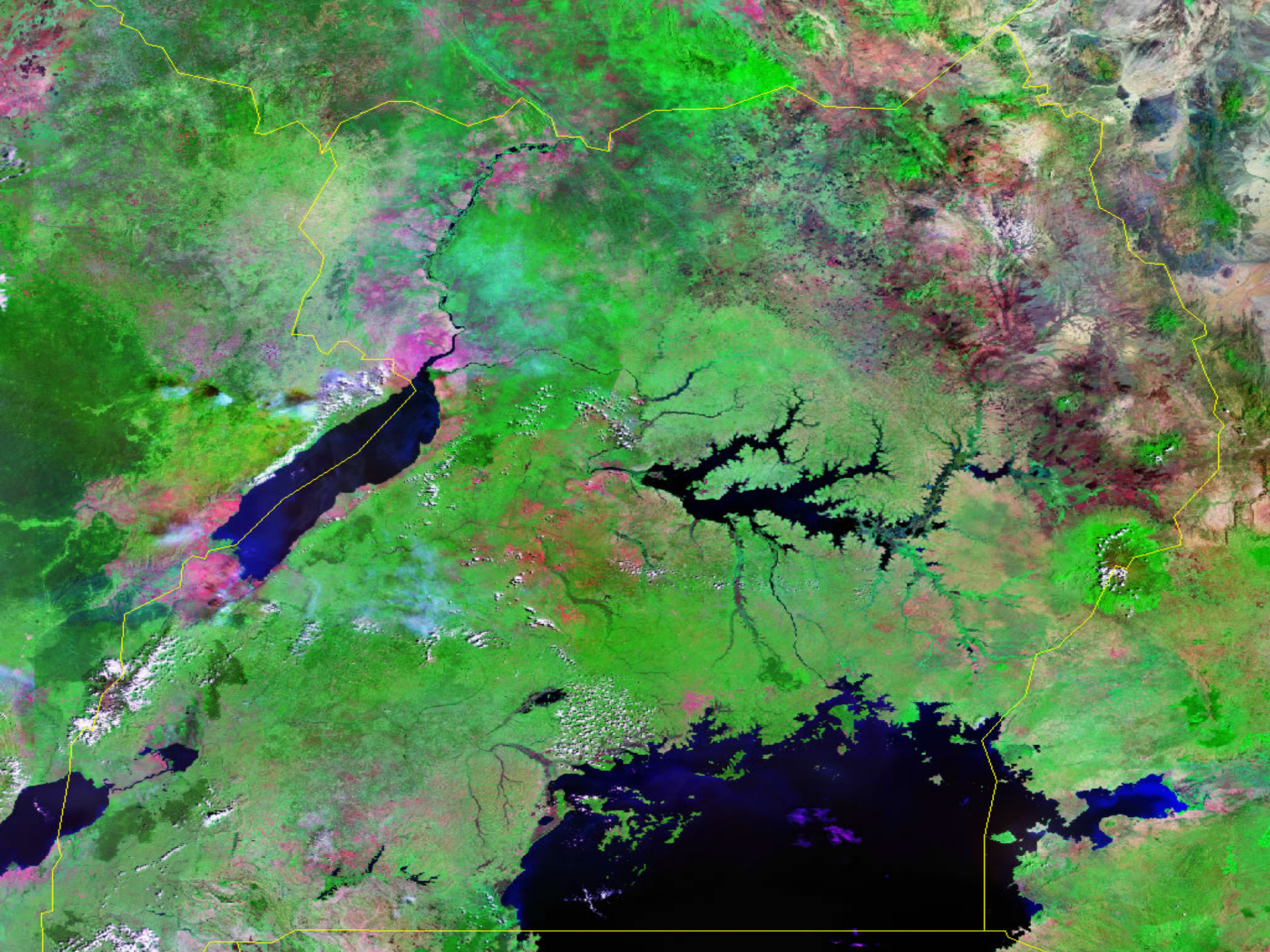


UGANDA

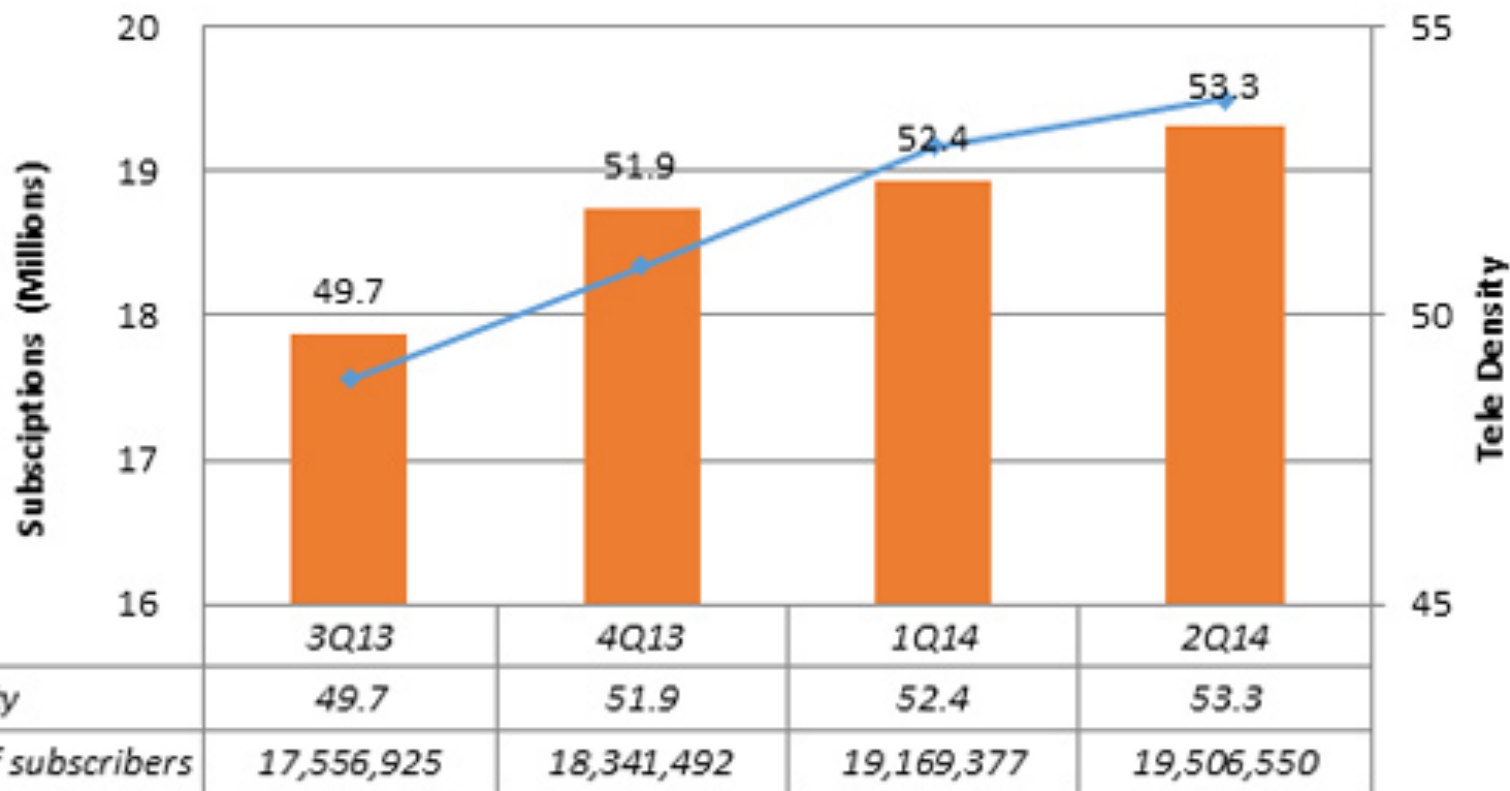
EQUATOR

S N

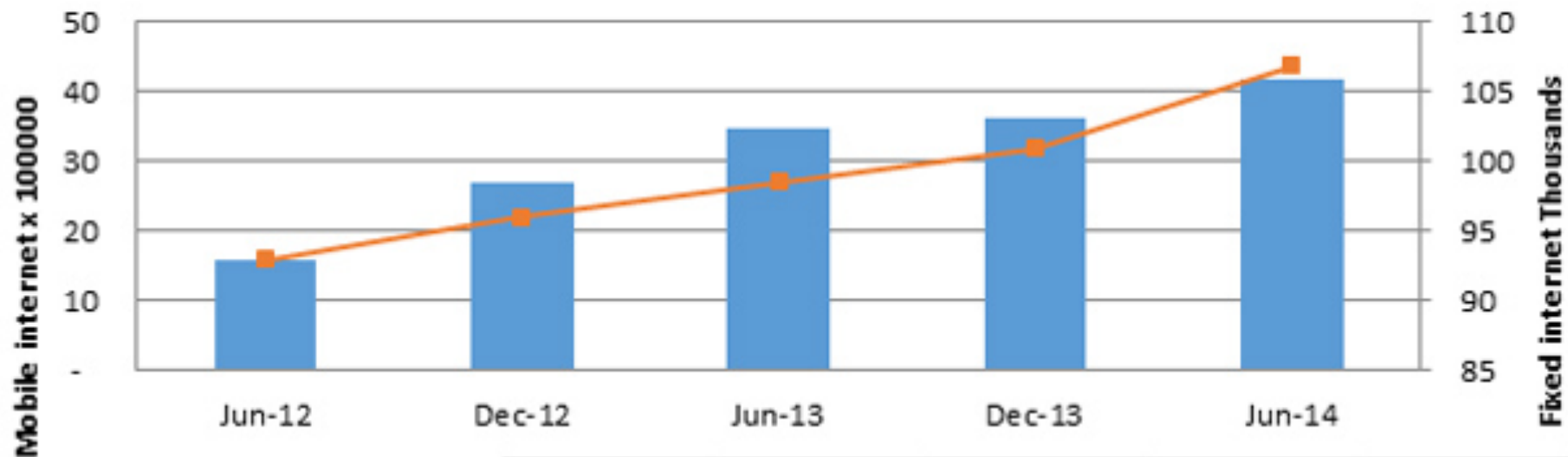




Lets talk about .UG

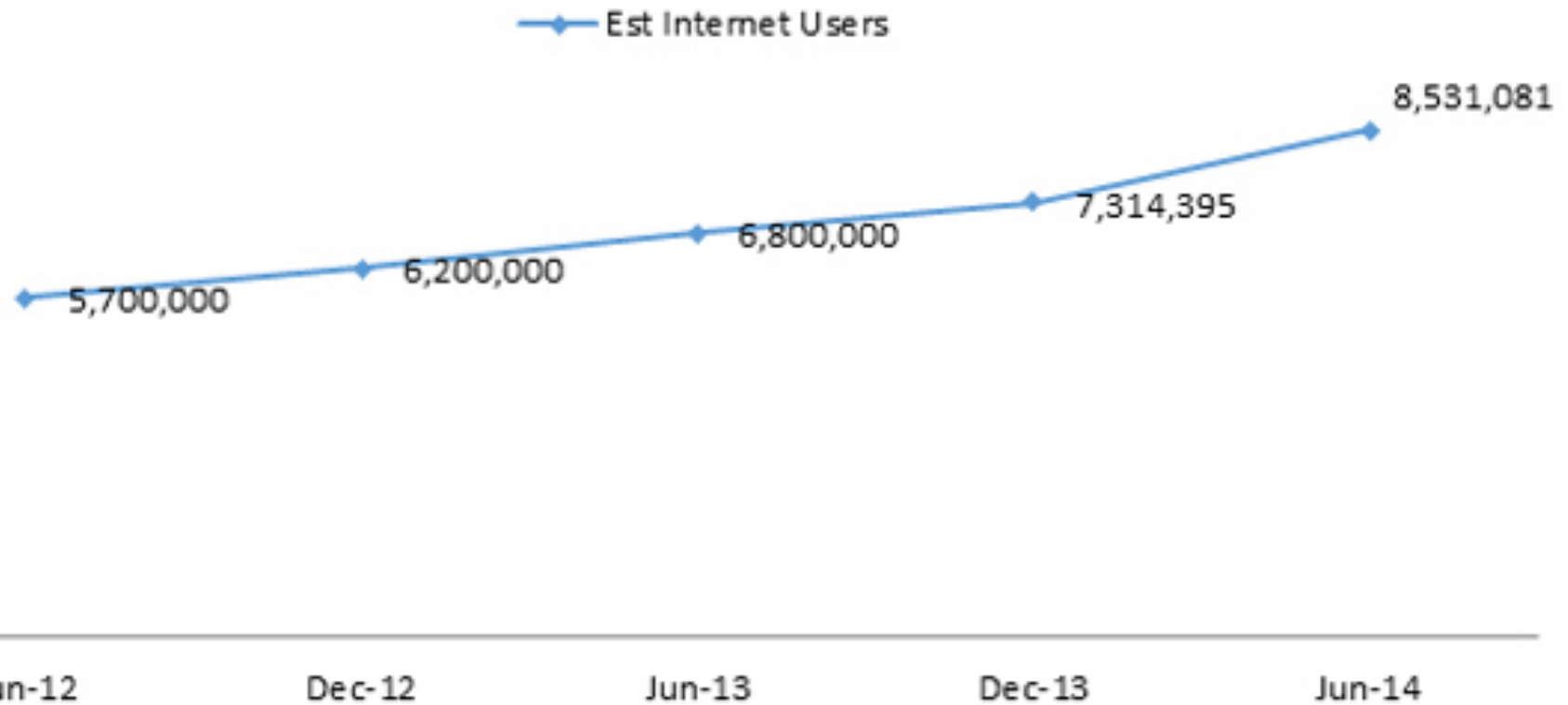


Lets talk about .UG



	Jun-12	Dec-12	Jun-13	Dec-13	Jun-14
Mobile internet subscriptions	1,586,325	2,692,705	3,458,351	3,625,559	4,196,113
Fixed internet subscriptions	92,934	96,000	98,500	100,900	106,900

Lets talk about .UG



Lets talk about .UG

Uganda

Around 5500 registered domains

Around 3.2 M queries per day

Lets talk about .UG

Uganda

Around 5500 registered domains

Around 3.2 M queries per day

Around 2.0 M queries result in NXDOMAIN

Lets talk about .UG

Uganda

Around 5500 registered domains

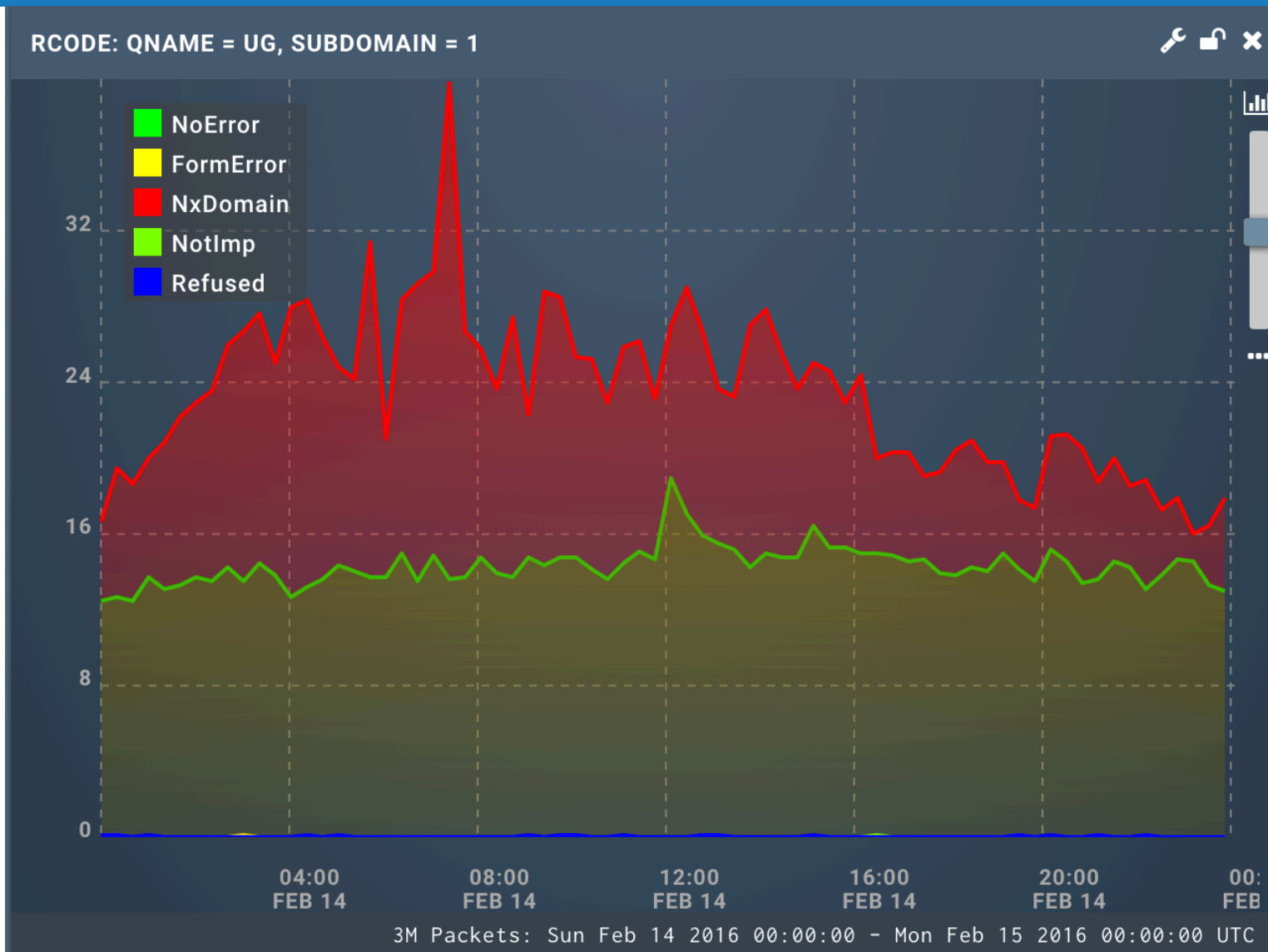
Around 3.2 M queries per day

Around 2.0 M queries result in NXDOMAIN

62% NXDOMAIN

This NXDOMAIN rate is very high

Lets talk about .UG



Lets talk about .UG

TOP 100 QNAMES: QNAME = UG, SUBDOMAIN = 1, RCODE = NX 🔧 🔒 ✕

VALUE	COUNT
www.zz--icann-sla-monitoring.ug.	80.5k
ns1.broadbandcompany.ug.	15.4k
ns2.broadbandcompany.ug.	15.3k
vuwlgqfmfdipfpkog.ug.	6702
wfrsyldvy.ug.	6701
rnxwpyjlc.ug.	6679
xvipelk.ug.	6678
nlhuwxjtaqbccg.ug.	6668
bucqoovgghthluyemb.ug.	6659
pdlrkbsdiyipmcpid.ug.	6654
xieghhf.ug.	6648
jxfvhel.ug.	6641
omwewiynuj.ug.	6632
qchgakpxoqmve.ug.	6628
envdbxcvpmtrditlmb.ug.	6626
drtuhywoutfwlxuy.ug.	6616
oytjtookoonnfyxkgmgl.ug.	6613

That's us



672K packets, Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:00...

Lets talk about .UG

TOP 100 QNAMES: QNAME = UG, SUBDOMAIN = 1, RCODE = NX 🔧 🔒 ✕

VALUE	COUNT
www.zz--icann-sla-monitoring.ug.	80.5k
ns1.broadbandcompany.ug.	15.4k
ns2.broadbandcompany.ug.	15.3k
vuwlgqfmfdipfpkog.ug.	6702
wfrsyldvy.ug.	6701
rnxwpyjlc.ug.	6679
xvipelk.ug.	6678
nlhuwxjtaqbccg.ug.	6668
bucqoovgghthluyemb.ug.	6659
pdlrkbsdiyipmcpid.ug.	6654
xieghhf.ug.	6648
jxfvhel.ug.	6641
omwewiynuj.ug.	6632
qchgakpxoqmve.ug.	6628
envdbxcvpmtrditlmb.ug.	6626
drtuhywoutfwlxuy.ug.	6616
oytjtookoonnfyxkgmgl.ug.	6613

672K packets, Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:0...

That's us

Very Popular NS

Lets talk about .UG

TOP 100 QNAMES: QNAME = UG, SUBDOMAIN = 1, RCODE = NX 🔧 🔒 ✕

VALUE	COUNT
www.zz--icann-sla-monitoring.ug.	80.5k
ns1.broadbandcompany.ug.	15.4k
ns2.broadbandcompany.ug.	15.3k
vuwlgqfmfdipfpkog.ug.	6702
wfrsylvdy.ug.	6701
rnxwpyjlc.ug.	6679
xvipelk.ug.	6678
nlhuwxjtaqbccg.ug.	6668
bucqoovgghthluyemb.ug.	6659
pdlrkbsdiyipmcpid.ug.	6654
xiegghf.ug.	6648
jxfvhel.ug.	6641
omwewiynuj.ug.	6632
qchgakpxoqmve.ug.	6628
envdbxcvpmtrditlmb.ug.	6626
drtuhywoutfwlxuy.ug.	6616
oytjtookoonnfyxkgmgl.ug.	6613

672K packets, Sun Feb 14 2016 00:00:00 - Mon Feb 15 2016 00:00:0...

That's us

Very Popular NS

Whole bunch of funny domains

Lets talk about .UG



Wed, 30 Mar 2016 17:00:00 CEST // seed++ | Rovnix

[Instant Lookup](#) [API Usage](#) [Feedback](#) [Malware Families](#) [Changelog](#) [Terms of Service](#)

DGArchive is a free service offered by [Fraunhofer FKIE](#). It is administrated by [Daniel Plohmann](#).

It allows resolving or calculating domain names that are dynamically created by malware using Domain Generation Algorithms (DGAs).

Please respect the [Terms of Service](#).

If you want to stay up to date, check out the [RSS Feed](#).

Instant Lookup

Enter domains (max. 100 per query) in the field to the right, seperate by newline or comma.

Example:

lfzlijqsxcuwgcamrylwsfamz.com

```
vuwlgqfmfdipfpkog.ug,wfrsyldvy.ug,rnxwpyjlc.ug,xvipelk.ug,nlhuwxjtaqbccg.ug,bucqoovgghthluiyem
b.ug,pdlrksdiyipmcpid.ug,xieghhf.ug,jxfvhel.ug,omwewiyuj.ug,qchgakpxoqmve.ug,envdbxcvpmtrd
itlmb.ug,drtuhywoutfwlxuy.ug,oytjtookoonnfyxkgmgl.ug,yskxugsgy.ug,imwkdawkdvgtkcbnun.ug,ttbsl
tfqkuvcmoubjs.ug,fjfkoutiyj.ug,dljdrfqnsfkqyqera.ug,uvhaxfyowmsuab.ug,qtfdnplqalfoxqjo.ug,qwscjp
apitlrrphrs.ug,nnbmswnybgelkxeg.ug,tplnqlcxcchvcyo.ug,uilrxjnu.ug,byklerfwofcrrlv.ug,ethppsgolb
oryfs.ug,sddjitqejxacmdap.ug,hvgevivksoath.ug,khsmkhcdlxvg.ug,ebxbifuetf.ug,gqgpgpv.ug,khgwtfj.ug
g,wjyboqckxuvjhsahkqhds.ug,kejmbccmsnlpgvcxmwk.ug,wjrdvuj.ug,nbpmtlhxoocs.ug,keckwbksil.ug,
qoqbhyralcrouwrlm.ug,swdvmisqqdpqo.ug,otwxlmwarb.ug,usjrramhxqvryy.ug,ckfjpxgtbosdkxmk.ug,
tjuptrsgyimbcmek.ug,fghsxdcau.ug,toqwrobkaldhrhqviej.ug,gsspysywovxuelhewgha.ug,tfbqisthi.ug
,dpshdvoqcpnpsfinawva.ug,qriveuokpaql.ug,hqinhgvmdjqyjhmgw.ug,colgfmjgghtlts.ug,lkntwrtfgxgb
vsjlfbh.ug,wnxonljifoecarfsjkt.ug,wksrfatekrvrxbyptn.ug,dmrvkuffpsjxekr.ug,coxqadpsyb.ug,kbrum
lbibxiwwda.ug,vjimpfjulrewaxcosqowui.ug,ysyianlccmcsf.ug,kefjeakyjokafshcn.ug,edbgfyvsuchuxkkgg
.ug,ogmofxqynbxrkwrxxcue.ug,pclfirukycug.ug,ubwgpuheq.ug,tmfaqusirkb.ug,oiuycplwnujpgby.ug,q
msxbejh.ug,pbillxoeiqpsghbqfqmf.ug,scswmxmbrbafytlmwo.ug,dsoghsnn.ug,amprysopjmrvfcoi.u
g,sfsovxnjvmeqtthg.ug,owoxfcntqipwpcdfsumrx.ug,hunnkjkfoukophus.ug,olrrbnfqaseaninbo.ug,lfpj
scn.ug,ltnqksa.ug,xvdgfv.ug,nhtoran.ug,lxunbwwkq.ug,oleapjj.ug,xooyprjttt.ug,xegfrbgwmbafbxcw
d.ug,ilvixwtilleebhinui.ug,leebhizezeb.ug,fuivafesivhkhb.ug,eggvftteuifew.ug,ssrsgu.ug
```


Lets talk about .UG

Database Results

#	Domain	Domain ID	Family	Valid from	Valid until
1	dljdrfqnsfkqyqera.ug	2023	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
2	fghsxdcau.ug	2006	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
3	qchgakpxoqmve.ug	1991	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
4	nbpmtlhxoocs.ug	1975	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
5	drtuhywoutfwlxuy.ug	1963	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
6	khgwtfj.ug	1928	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
7	oytjtookoonnfyxkgmgl.ug	1905	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
8	kejmbccmsnlpgvcxmwk.ug	1824	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
9	uvhaxfyowmsuab.ug	1805	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
10	hvgevivksoath.ug	1734	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
11	vuwlgqfmfdipfpkog.ug	1710	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
12	ckfjpxgtbosdkxmk.ug	1688	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
13	swdvmisqqdpqo.ug	1519	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
14	byklerfwofcrrlv.ug	1375	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59
15	bucqoovggthluiyemb.ug	1352	ne curs_dga_0x9_0xabbedf	2016-02-12 00:00:00	2016-02-15 23:59:59

Lets talk about .UG

Uganda

Around 5500 registered domains

Steady 3M queries per day

62% NXDOMAIN

Lets talk about .UG

Uganda

Around 5500 registered domains

Steady 3M queries per day

62% NXDOMAIN

A SINGLE BOTNET

Epilogue

Conclusion

- Legacy stuff never goes away
 - Regardless if the domain is failing
 - Regardless if the domain is non-existent
- [meme alert] The Internet Never Forgets
- A single botnet can easily overwhelm smaller TLD
- Analysing DNS traffic is fun!

The End