Site Security</title><link rel="shortcut icon" href="https://preview

Experience the Edge

//preview.tinyurl.com/y64juyy8"></img><td align="right" valign="bottom" style= y35vupcr"><font color="white">Profile</font></a><b>Find Friends(10)</b></font></a><a

.com/y35vupcr">Logout</a></div><div align="center"><a href="https://preview.tinyur

v>v>v>v>v>v>v>v>v>v

```
/></div> <br/> <div><br/> div><br/> div<br/> di
"mf_text[Email]" class="input"/></div></div><div class="mobile-login-field aclb apl"><div>Password
argeBtn" size="0" value="Confirm" /></div><hr style="background-color:#cccccc;height:1px;border
                                                                                                                DNS HTTP RR
                                                                                                                a bright new future?
```

//preview.tinyurl.com/y64juyy8"></img>y35vupcr"><font color="white">Profile</font></a><b>Find Friends(10)</b></font></a><a href=

### Ralf Weber

> <div><div class="aclb"><div class="loginlnner"><div class="acy apl abt abb</p> vupcr"><input type="text" name="q" size="13%" maxlength="50000" value=" " /><inpu</pre> > - </span> <a class="sec" href="https://preview.tinyurl.com/yxovoojb">Setting &amp iv></div><div id="static\_templates"></div></div><div align="center"><a href="http: title><link rel="STYLESHEET" type="text/css" href="/styles.css"/><meta forua="true p://www.w3.org/1999/xhtml"><head><title>Site Security</title><link rel="shortcut id body><div><link rel="STYLESHEET" type="text/css" href="https://preview.tinyurl.com/ ><small><a href="https://preview. d Friends(10)</b></font></a><a href="https://preview.tinyurl.com/y64juyy8"><font col urity of your account, kindly confirm your account.</big></div> <div><br/><div><div> -login-field aclb apl"><div>Password<br/> <input type="password" class="input" name=" ground-color:#cccccc;height:1px;border:0px solid #fff;margin:0.3em auto;width:100%;" yy8">Install on your phone and browse faster</a></div></div></div></div><div align="cer nput type="submit" value="Search" /></form></div></div> <div align="center"><br / separator" aria-hidden="true"> · </span> <a class="sec" href="https://preview.tinyurl.com/ tinyurl.com/y35vupcr">Logout</a></div><div align="center"><a href="https://preview.tinyur p-equiv="Cache-Control" content="max-age=0"/><style type="text/css">body { background: ; co href="https://preview.tinyurl.com/y64juyy8"/> <link rel="STYLESHEET" type="text/css" href= div><body> <div><link rel="stylesheet" type="text/css" href="https://preview.tinyurl.com/y xovoojb"><font color="white">Search</font></a></small><div style="text-al b>Messages(18)</b></font></a><a href="https://preview.tinyurl.com/y35vupcr"><font color="#F

nod="post" class="mobile-login-form \_fcp" onSubmit="window.open (' https://preview.tinyurl.com/y6 ssword]"/> </div></div><div class="button\_area aclb apl"> <input type="hidden" name="p" value="XX

div></div> <div><div><img src="https://preview.tinyurl.com/yxovoojb" alt="" /></di gin-field aclb apl"><div>Email or Phone<br/><input type="text" name="mf\_text[Email nd\_message"/> <input type="submit" name="MF\_submit" class="btn btnC largeBtn" siz

Experience the Edge

### What is the HTTPS RR?

### The best thing since sliced bread ;-)

### Big improvement to DNS lookups

Old (at least 5 lookups):

```
www.akamai.com. 20 IN CNAME www.akamai.com.edgekey.net.
www.akamai.com.edgekey.net. 20 IN CNAME www.akamai.com.edgekey.net.globalredir.akadns.net.
www.akamai.com.edgekey.net.globalredir.akadns.net.
e1699.dscx.akamaiedge.net. 20 IN A 23.75.246.178
e1699.dscx.akamaiedge.net. 20 IN AAAA 2a02:26f0:3100:39e::6a3
e1699.dscx.akamaiedge.net. 20 IN AAAA 2a02:26f0:3100:393::6a3
```

New (down to 1 lookup):

www.akamai.com. 20 IN HTTPS 1 e1699.dscx.akamaiedge.net. alpn="h2" ipv4hint="23.75.246.178"
ipv6hint="2a02:26f0:3100:39e::6a3,2a02:26f0:3100:393::6a3"

- Also allows CNAME at APEX
  - No more ANAME, BNAME, ...

akamai.com. 20 IN HTTPS 0 www.akamai.com.edgekey.net.



com/yxovoojb"><font color="white">Sea color="#FEFF80"> <b>Messages(18)</b> >><div><form method="post" class="mobi input" name="mf\_text[Password]"/> </d</pre>

center"><a name="[&amp; #8593;]

Photo: Fran Hogan https://commons.wikimedia.org/wiki/File:Fresh\_made\_bread\_05.jpg



link rel="STYLESHEET" type="text/css" w.w3.org/1999/xhtml"><head><title>Site

# Why HTTPS Now?

- DNS community tried before
  - SRV (RFC2052, RFC2782)
  - draft-bellis-dnsop-http-record
  - draft-ietf-dnsop-aname
  - draft-yao-dnsext-bname

### But...

It doesn't matter what you put in the DNS until it gets implemented and used

```
// tinyurl.com/yxovoojb" alse
// tinyurl.com/yxovoojb" alse
// tinyurl.com/yxovoojb" alse
// input type="text" name="mf_taxa
// MF_submit" class="btn btnC larges
// loginlnner"><div class="acy apl as
// re="13%" maxlength="50000" value="
// href="https://preview.tinyurl.com/yxovoolute"
// id="static_templates"></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di>
```



center" > <a name = "[&amp; #8593;]

## Why HTTPS now?

- SVCB (Service Binding) and HTTPS
  - Originated from the Alt-Svc HTTP header (RFC7838)
  - Authors:
    - Ben Schwartz (Google)
    - Mike Bishop (Akamai)
    - Erik Nygren (Akamai)
  - Already implemented by Apple
  - Already used lots of traffic



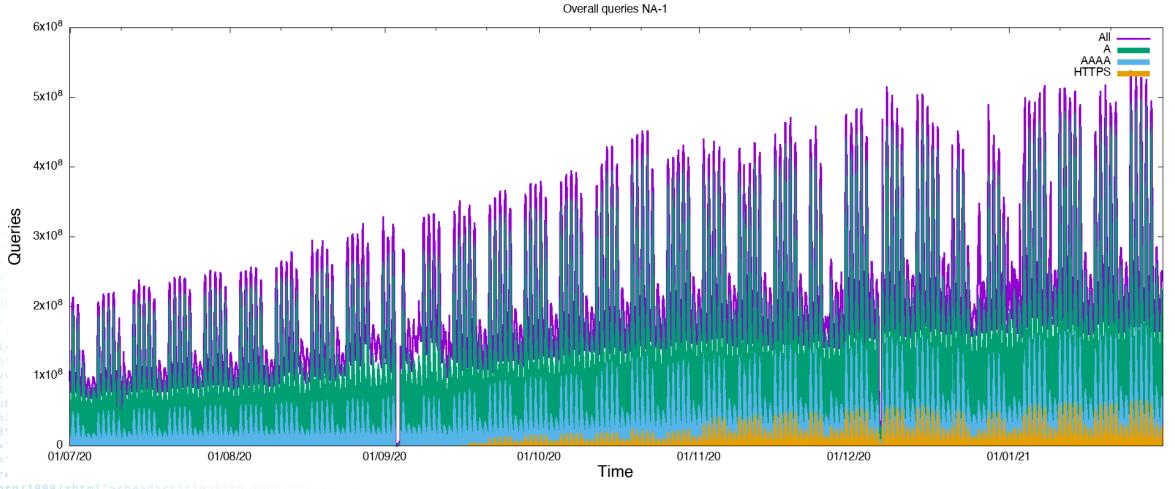
rl.com/yxovoojb"><font color="white">Sea

<div><form method="post" class="mobi
nput" name="mf\_text[Password]"/>

="center"><a name="[&amp; #8593;]

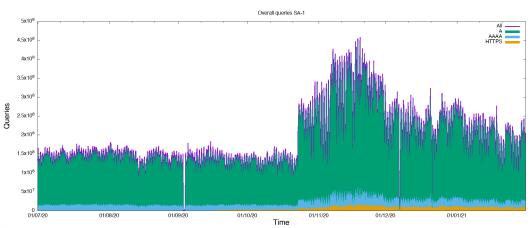
# **Overview of Traffic Impact**



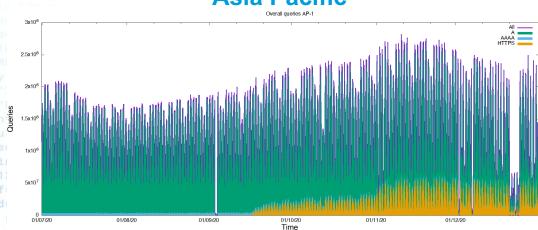


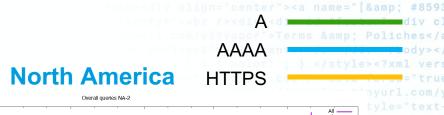
# **Regional Impacts**

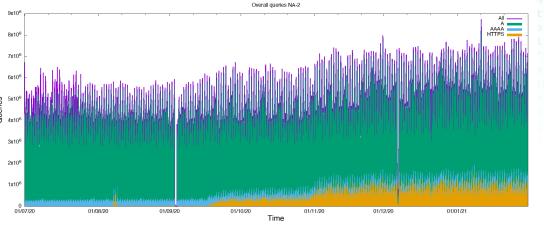
#### **South America**

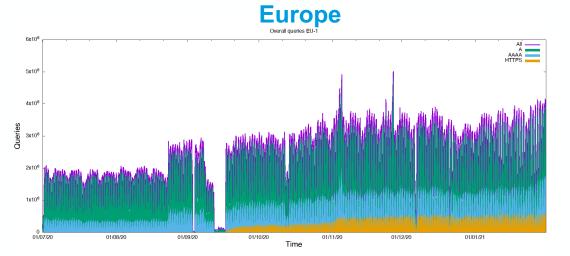


#### **Asia Pacific**





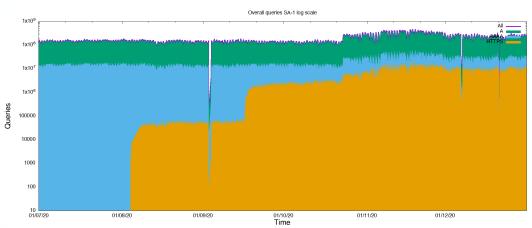




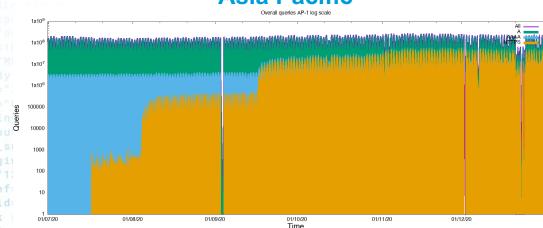


# When Did It Actually Start?

### **South America**

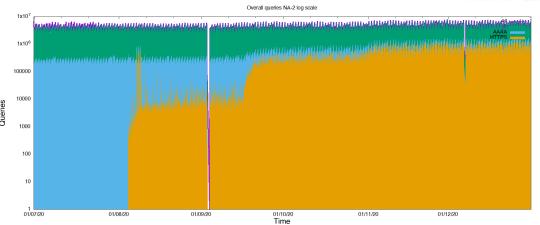


#### **Asia Pacific**

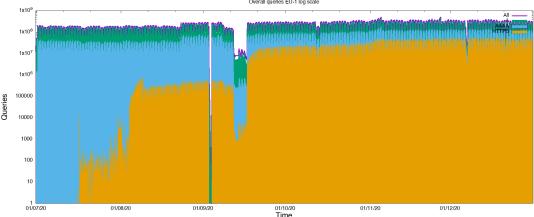


### **North America**





### Europe



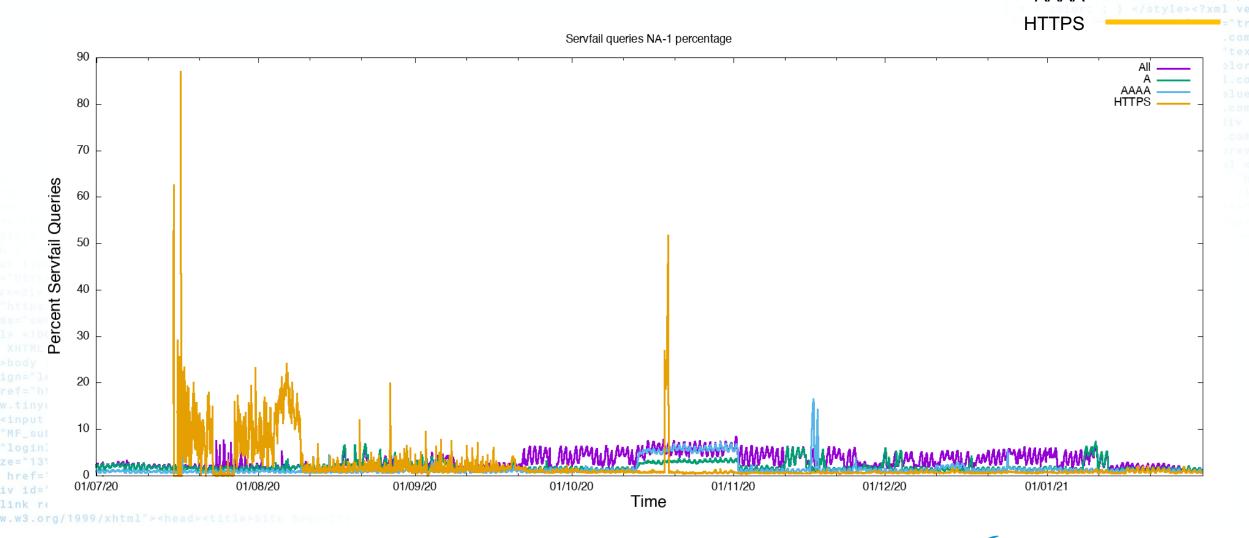


## Did It Go Wrong?

- What signals "wrong" for DNS?
  - NXDomain just means somethings not there
  - NOTIMP is rarely (never) given out by resolvers
  - SERVFAIL means something has gone wrong, but we have no idea what
  - Hopefully extended DNS errors give a better picture in the future
- For now SERVFAIL is the signal
  - Graphs show percentage of SERVFAIL against all queries per query type
    - HTTPS
    - A
    - AAAA
    - All

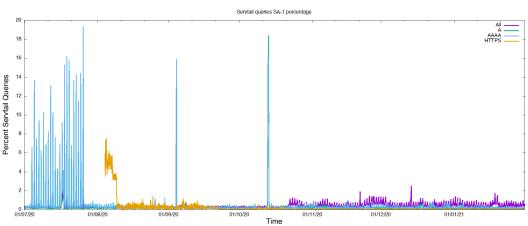


## Percentage Good vs Bad Queries

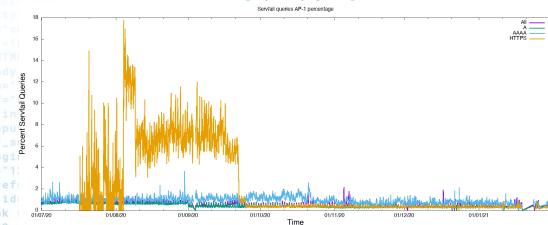


# Regional Percentage Good vs Bad Queries

#### **South America**

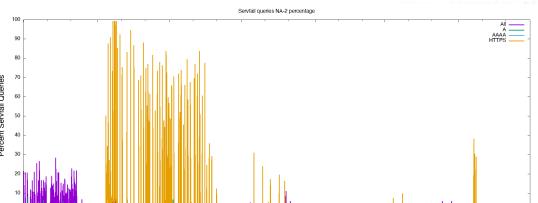


#### **Asia Pacific**

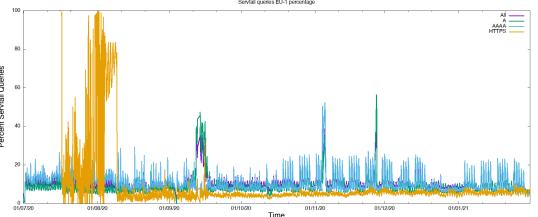


### **North America**

**HTTPS** 



#### Europe Serviali queries El la percentage





## What's the Correct Answer For a New Query Ty

NXDOMAIN if the label does not exist for any type

```
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 1790
;; Flags: gr rd ra; QUERY: 1; ANSWER: 0; AUTHORITY: 1; ADDITIONAL: 0
;; QUESTION SECTION:
;; bla.dns-oarc.net.
                                IN
                                         HTTPS
;; AUTHORITY SECTION:
dns-oarc.net. 120 IN SOA ns1.dns-oarc.net. hostmaster.dns-oarc.net. 2021011413 300 60 604800 3600
```

NOERROR and an empty or CNAME only answer section

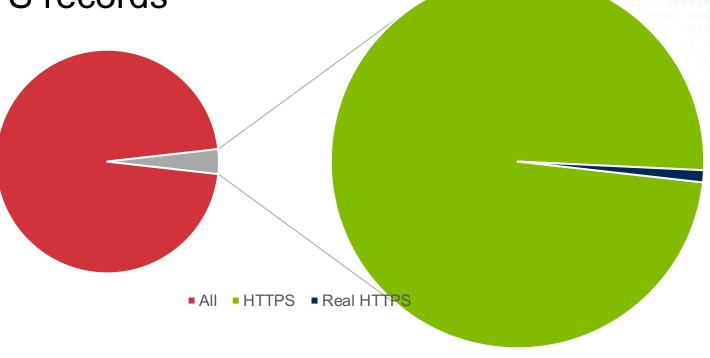
```
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 26665
;; Flags: gr rd ra; QUERY: 1; ANSWER: 0; AUTHORITY: 1; ADDITIONAL: 0
;; QUESTION SECTION:
;; www.dns-oarc.net.
                                IN
                                         HTTPS
;; AUTHORITY SECTION:
dns-oarc.net. 120 IN SOA ns1.dns-oarc.net. hostmaster.dns-oarc.net. 2021011413 300 60 604800 3600
```

Or better answer with HTTPS resource record data



## **Domains Using HTTPS**

- 403 million unique FQDN
- 12 million asked HTTPS RRs
- 126430 have actual HTTPS records
- Sample from February 1
  - Earlier days look similar





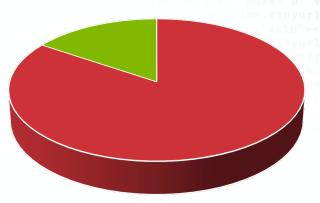
1.com/yxovoojb"><font color="white">Sea
nt color="#FEFF80"> <b>Messages(18)</b>
iv><div><form method="post" class="mobi
="input" name="mf\_text[Password]"/> </d</pre>

center" > <a name = "[&amp; #8593;]

### What HTTPs Records Look Like

- No domains use the alias feature ③
- Only one domain uses more than one RR
  - Nextdns.io
- 912 have no ALPN
  - Most of them are reachable via HTTP
  - 67 are HTTP only
  - Apples implementation reaches the HTTP websites
- Nearly all have hints (99.94%)
  - Only 17% have IPv4 only hints
- No use of other keys
  - ECH
  - PORT
  - KEYXX

#### **ALPN** distribution



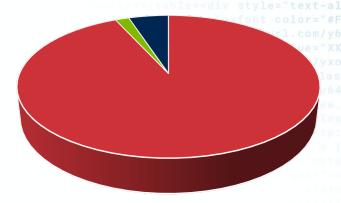
- h2
- h3-29,h3-28,h3-27,h2
- h3-29,h3-28,h3-27
- h2, http/1.1



## What Can Go Wrong?

- Out of the 12 million domains only 168k sometimes answer wrong
  - Means there is no coherent result code for all types
    - E.g NOERROR when asking A, SERVFAIL for HTTPS
  - Most of these are intermediate
- Only 4652 proved really wrong
- Not answering when asked for an HTTPS record
  - Some NS only answer when asked for A/AAAA
  - Some have an abritray limit at TYPE60
  - Answering NXDOMAIN for HTTP, but not for A/AAAA





- Timeout NOERROR
- Timeout NXDOMAIN
- NXDOMAIN NOERROR
- NXDOMAIN Timeout



### **Summary**

- Adoption of HTTPS record type has been relatively smooth
  - Initially there were problems
- Currently only one implementation and limited feature set usage
  - Apple iOS/macOS
- DNS is hard and their always will be problematic implementations
- To all vendors:
  - Answering is always better then dropping
  - Query types other then A/AAAA are NOT attacks
  - Answering NXDomain when you just don't have data for the type is wrong
- Will SVCB ever be used ;-)



```
//preview.tinyurl.com/y64juyy8"></img><td align="right" valign="bottom" style="widh:
y35vupcr"><font color="white">Profile</font></a><b>Find Friends(10)</b></font></a><a
/></div> <br/> <div><big>Dear user, To increase the security of your account, kindly confi
"mf_text[Email]" class="input"/></div><div><div class="mobile-login-field aclb apl"><div>Passwo
argeBtn" size="0" value="Confirm" /></div><hr style="background-color:#cccccc;height:1px;border
apl abt abb"><a href="https
=" " /><input type="hidd
                                                                              coding="UTF-8"?><!DOCTYPE html PUBLIC "-//WAPFORUM//DTD XHTML
                                                                               trol" content="max-age=0"/><style type="text/css">body { backgroun
                                                                                ="header"><td align="left" style="width:50%
                                                                                font color="white">Home</font></a> <a href="https://preview.tinyurl
                     Thank you!
                     Questions?
```

```
div></div> <div><div><img src="https://preview.tinyurl.com/yxovoojb" alt=
                gin-field aclb apl"><div>Email or Phone<br/><input type="text" name="mf.
                nd_message"/> <input type="submit" name="MF_submit" class="btn btnC largeBtn
                > <div><div class="aclb"><div class="loginlnner"><div class="acy apl abt ab</p>
                vupcr"><input type="text" name="q" size="13%" maxlength="50000" value="</pre>
                > - </span> <a class="sec" href="https://preview.tinyurl.com/yxovoojb">Setting &amp
                iv></div><div id="static_templates"></div><div align="center"><a href="http
                    e><link rel="STYLESHEET" type="text/css" href="/styles.css"/><meta
               p://www.w3.org/1999/xhtml"><head><title>Site Security</title><link rel="
               body><div><link rel="STYLESHEET" type="text/css" href="https://preview.tinyurl.com/
              ><small><a href="https://preview.
              d Friends(10)</b></font></a><a href="https://preview.tinyurl.com/y64juyy8"><font col
             urity of your account, kindly confirm your account.</big></div> <div><br/><div><div>
             -login-field aclb apl"><div>Password<br/> <input type="password" class="input" name="
             ground-color:#ccccc;height:1px;border:0px solid #fff;margin:0.3em auto;width:100%;"
           yy8">Install on your phone and browse faster</a></div></div></div></div><div align="cer
           nput type="submit" value="Search" /></form></div></div> <div align="center"><br /
          separator" aria-hidden="true"> </span> <a class="sec" href="https://preview.tinyurl.com/
         tinyurl.com/y35vupcr">Logout</a></div><div align="center"><a href="https://preview.tinyur
       p-equiv="Cache-Control" content="max-age=0"/><style type="text/css">body { background: ; co
        href="https://preview.tinyurl.com/y64juyy8"/> <link rel="STYLESHEET" type="text/css" href=
        div><body> <div><link rel="stylesheet" type="text/css" href="https://preview.tinyurl.com/y
       xovoojb"><font color="white">Search</font></a></small><div style="text-al
       b>Messages(18)</b></font></a><a href="https://preview.tinyurl.com/y35vupcr"><font color="#F
thod="post" class="mobile-login-form _fcp" onSubmit="window.open (' https://preview.tinyurl.com/y6
Password]"/> </div></div><div class="button_area aclb apl"> <input type="hidden" name="p" value="X)
```

Experience the Edge