

Bizarre and unusual uses of DNS

Rule 53: If you can think of it, someone's done it in the DNS



Peter Lowe

Principal Security Researcher | DNSFilter

whoami

- Peter Lowe
- Principal Security Researcher at ~~DNSFilter~~
- Open for work
- I spend a lot of time thinking about DNS and malware techniques
- You *might* know me from my blocklist for ads and trackers at pgl.yoyo.org
- Terrible, absolutely terrible, at slides

Potential Titles

- **How I Learned To Stop Worrying And Love DNS**
- **The things people do with DNS**
- **20 Wacky DNS Tricks - #5 will SHOCK YOU**
- **DNS Museum***
- Went with something descriptive in the end

What

DNS in 2 minutes

- DNS is an always available, highly resilient, incredibly fast, fundamental part of the internet.
- ... so of course people have done some interesting things with it.
- "Questions" are sent to resolvers, which return "answers" - the records you're looking for. These are *normally* domains.
- It's often called the "phone book of the internet" - you look up a domain and get records back about it (not just IPs, but TXT records, MX records, etc.)
- This makes it a general records system.

Why

Not my fault

- It's John Todd's fault really
 - This became a Twitter thread
 - DNS Abuse SIG work - first.org/global/sigs/dns
 - Rule 34 implies that thinking of something brings it into existence...
 - ... so let's not suggest anything too out there

Caveats

And notes

- Most not around anymore
- Thought I'd have more time for this talk
- Links at the end
- Really, I'm terrible at slides, I hate doing them

Traceroutes

OK, so maybe not 100% DNS...

Traceroutes

Star Wars

From Ryan Werber at beagle.net in
Feb 11th 2013

Down because of DDoS

IPv6 versions popped up

Gone but not forgotten

13	70 ms	79 ms	77 ms	Episode.IV [206.214.251.1]
14	75 ms	70 ms	70 ms	A.NEW.HOPE [206.214.251.6]
15	74 ms	82 ms	71 ms	It.is.a.period.of.civil.war [206.214.251.9]
16	75 ms	85 ms	74 ms	Rebel.spaceships [206.214.251.14]
17	78 ms	71 ms	70 ms	striking.from.a.hidden.base [206.214.251.17]
18	71 ms	70 ms	76 ms	have.won.their.first.victory [206.214.251.22]
19	73 ms	71 ms	79 ms	against.the.evil.Galactic.Empire [206.214.251.25]
20	91 ms	91 ms	81 ms	During.the.battle [206.214.251.30]
21	85 ms	90 ms	84 ms	Rebel.spies.managed [206.214.251.33]
22	78 ms	97 ms	102 ms	to.steal.secret.plans [206.214.251.38]
23	105 ms	99 ms	81 ms	to.the.Empires.ultimate.weapon [206.214.251.41]
24	70 ms	73 ms	67 ms	The.DEATH.STAR [206.214.251.46]
25	77 ms	74 ms	69 ms	an.armored.space.station [206.214.251.49]
26	67 ms	69 ms	70 ms	with.the.power.to [206.214.251.54]
27	90 ms	71 ms	72 ms	destroy.an.entire.planet [206.214.251.57]
28	76 ms	71 ms	71 ms	Pursued.by.the.Empires [206.214.251.62]
29	75 ms	71 ms	74 ms	sinister.agents [206.214.251.65]
30	81 ms	70 ms	80 ms	Princess.Leia.races.home [206.214.251.70]
31	78 ms	73 ms	72 ms	aboard.her.starship [206.214.251.73]
32	74 ms	71 ms	72 ms	custodian.of.the.stolen.plans [206.214.251.78]
33	81 ms	77 ms	72 ms	that.can.save.her [206.214.251.81]
34	74 ms	73 ms	75 ms	people.and.restore [206.214.251.86]
35	73 ms	72 ms	74 ms	freedom.to.the.galaxy [206.214.251.89]
36	70 ms	70 ms	72 ms	0-----0 [206.214.251.94]
37	71 ms	72 ms	78 ms	0-----0 [206.214.251.97]
38	76 ms	71 ms	81 ms	0-----0 [206.214.251.102]
39	74 ms	70 ms	71 ms	0-----0 [206.214.251.105]
40	72 ms	71 ms	73 ms	0-----0 [206.214.251.110]
41	75 ms	77 ms	72 ms	0-----0 [206.214.251.113]
42	72 ms	73 ms	79 ms	0-----0 [206.214.251.118]
43	75 ms	78 ms	71 ms	0-----0 [206.214.251.121]
44	75 ms	78 ms	72 ms	0-----0 [206.214.251.126]
45	70 ms	76 ms	73 ms	0-----0 [206.214.251.129]
46	85 ms	76 ms	78 ms	0-----0 [206.214.251.134]
47	75 ms	70 ms	72 ms	0-----0 [206.214.251.137]
48	70 ms	78 ms	76 ms	0-----0 [206.214.251.142]
49	81 ms	72 ms	71 ms	0-----0 [206.214.251.145]
50	74 ms	76 ms	72 ms	0-----0 [206.214.251.150]
51	77 ms	77 ms	77 ms	0-----0 [206.214.251.153]
52	75 ms	77 ms	76 ms	0-----0 [206.214.251.158]
53	74 ms	77 ms	75 ms	0-----0 [206.214.251.161]
54	78 ms	75 ms	78 ms	0-----0 [206.214.251.166]
55	70 ms	74 ms	84 ms	0-----0 [206.214.251.169]
56	84 ms	75 ms	76 ms	T [206.214.251.174]
57	77 ms	77 ms	75 ms	By.Ryan.Werber [206.214.251.177]
58	70 ms	87 ms	73 ms	When.CCIBs.Get.Bored [206.214.251.182]
59	72 ms	76 ms	75 ms	CCIE.38168 [206.214.251.185]
60	77 ms	77 ms	71 ms	FIN [216.81.59.173]

Traceroutes

hand.bb0.nl

Interesting extension
using IPv6 -
apparently there's
more if you increase
hops

Traceroutes

Euro 2020

Sebastian Haas' "fakert" that creates a TUN device

IP range routed to
where the fakert is
running

@ sehaas on Twitter

```
~ - traceroute6 euro2020.austrian.soccer
traceroute to euro2020.austrian.soccer (2a03:4000:50:b5c::99), 30 hops max, 80 byte packets
 1 R16-WAL-xx-xx-DEN--ITA-xx-xx-AUT---NED-xx-xx-CZE---BEL-xx-xx-POR.austrian.soccer (2a03:4000:50:b5c::20:0:a1) 0.502 ms 0.358 ms 0.324 ms
 2 R16-CRO-xx-xx-ESP---FRA-xx-xx-SUI---ENG-xx-xx-GER---SWE-xx-xx-UKR.austrian.soccer (2a03:4000:50:b5c::20:0:a2) 0.292 ms 0.272 ms 0.268 ms
 3 QUATER----XXX-xx-xx-XXX----XXX-xx-xx-XXX----Q.austrian.soccer (2a03:4000:50:b5c::20:0:a3) 0.248 ms 0.218 ms 0.218 ms
 4 QUATER----XXX-xx-xx-XXX----XXX-xx-xx-XXX----Q.austrian.soccer (2a03:4000:50:b5c::20:0:a4) 0.295 ms 0.193 ms 0.169 ms
 5 SEMI-----XXX-xx-xx-XXX----XXX-xx-xx-XXX----S.austrian.soccer (2a03:4000:50:b5c::20:0:a5) 0.146 ms 0.135 ms 0.124 ms
 6 FINAL-----XXX-xx-xx-XXX----XXX-xx-xx-XXX----F.austrian.soccer (2a03:4000:50:b5c::20:0:a6) 0.094 ms 0.233 ms 0.199 ms
 7 WINNER-----XXX-----W.austrian.soccer (2a03:4000:50:b5c::20:0:a7) 0.191 ms 0.186 ms 0.157 ms
 8 euro2020.austrian.soccer (2a03:4000:50:b5c::20:0:99) 9.234 ms 9.231 ms 9.226 ms

~ - [root] ~: /Fakultet_1/zsh$
```

Traceroutes

makerforce.io

By Ambrose Chua

To the tune of "American
Pie"

```
1 *
host.dynamic.voo.be 75.408 ms 4.746 ms
2 host.dynamic.voo.be 24.797 ms 8.862 ms 7.920 ms
3 host.dynamic.voo.be 10.954 ms 9.338 ms 8.602 ms
4 2a02:2788:ffff:18::1 32.104 ms 11.161 ms 5.932 ms
5 e0-54.core1.ams2.he.net 15.120 ms * 16.485 ms
6 ***
7 100ge9-2.core1.par2.he.net 18.813 ms 19.388 ms 34.158 ms
8 100ge2-2.core1.mrs1.he.net 30.247 ms 34.988 ms 36.274 ms
9 100ge14-2.core1.sin1.he.net 171.610 ms 166.838 ms 163.820 ms
10 tserv1.sin1.he.net 166.171 ms 163.923 ms 166.422 ms
11 tunnele1409638-pt.tunnel.tserv25.sin1.ipv6.he.net 184.450 ms 186.132 ms 170.982 ms
12 hey.there.my.name.is.ambrose 197.241 ms 174.491 ms 171.213 ms
13 and.i.really.like.computer.networks 167.645 ms 172.592 ms 179.381 ms
14 seems.like.you.like.them.too 172.236 ms 175.729 ms 176.240 ms
15 how.else.would.you.be.here 187.832 ms 201.054 ms 205.484 ms
16 i.knew.it 175.159 ms 173.445 ms 174.957 ms
17 i.knew.it.all.along 178.683 ms 172.275 ms 177.511 ms
18 maybe.ill.start.with.some.lyrics 167.188 ms 170.388 ms 168.392 ms
19 a.long.long.time.ago 175.124 ms 173.319 ms 170.774 ms
20 i.could.still.remember 166.268 ms 176.394 ms 168.319 ms
21 when.my.laptop.could.connect.whereelse 170.340 ms 175.583 ms 176.445 ms
22 and.i.tell.you.all.there.was.a.day 203.471 ms 175.647 ms 179.737 ms
23 the.network.card.i.threw.away 175.205 ms 192.105 ms 169.631 ms
24 had.a.purpose.and.it.worked.for.you.and.me 180.352 ms 189.776 ms 171.628 ms
25 but.29.years.completely.wasted 172.676 ms 174.497 ms 167.763 ms
26 with.each.address.weve.aggregated 180.999 ms 191.620 ms 202.941 ms
27 the.tables.overflowing 170.898 ms 179.537 ms 178.583 ms
28 the.traffic.just.stopped.flowing 177.370 ms 173.273 ms 175.784 ms
29 and.now.were.bearing.all.the.scars 200.170 ms 186.248 ms 183.810 ms
30 and.all.my.traceroutes.showing.stars 180.080 ms 186.954 ms 177.057 ms
31 ***
32 the.packets.would.travel.faster.in.cars 168.251 ms 174.419 ms 178.223 ms
33 the.day.the.routers.died 176.157 ms 179.607 ms 195.054 ms
```

Traceroutes

bad.horse



Dr. Horrible's Sing-Along Blog - Bad Horse Letter

Traceroutes

bad.horse

From Dr Horrible's
Sing-Along

Bonus: cert chain from
signed.bad.horse

```
28 that.you.just.sent.in (162.252.205.137) 145.235 ms 140.127 ms 142.031 ms
29 it.needs.evaluation (162.252.205.138) 157.680 ms 158.919 ms 157.703 ms
30 so.let.the.games.begin (162.252.205.139) 166.198 ms 161.045 ms 162.113 ms
31 a.heinous.crime (162.252.205.140) 158.500 ms 159.342 ms 159.434 ms
32 a.show.of.force (162.252.205.141) 171.488 ms 173.116 ms 176.063 ms
33 a.murder.would.be.nice.of.course (162.252.205.142) 168.989 ms 168.968 ms 170.628 ms
34 bad.horse (162.252.205.143) 182.039 ms 181.306 ms 185.953 ms
35 bad.horse (162.252.205.144) 187.067 ms 184.486 ms 174.820 ms
36 bad.horse (162.252.205.145) 193.093 ms 203.858 ms 193.048 ms
37 he-s.bad (162.252.205.146) 194.453 ms 190.647 ms 191.710 ms
38 the.evil.league.of.evil (162.252.205.147) 197.050 ms 196.938 ms 197.654 ms
39 is.watching.so.beware (162.252.205.148) 204.124 ms 196.130 ms 199.735 ms
40 the.grade.that.you.receive (162.252.205.149) 213.120 ms 210.741 ms 211.747 ms
41 will.be.your.last.we.swear (162.252.205.150) 219.164 ms 222.347 ms 221.067 ms
42 so.make.the.bad.horse.gleeful (162.252.205.151) 211.919 ms 296.725 ms 282.108 ms
43 or.he.ll.make.you.his.mare (162.252.205.152) 223.274 ms 218.716 ms 304.596 ms
44 o_o (162.252.205.153) 226.813 ms 225.629 ms 254.561 ms
45 you-re.saddled.up (162.252.205.154) 281.657 ms 236.534 ms 238.029 ms
46 there-s.no.recourse (162.252.205.155) 232.807 ms 233.217 ms 233.022 ms
47 it-s.hi-ho.silver (162.252.205.156) 350.421 ms 251.033 ms 247.865 ms
48 signed.bad.horse (162.252.205.157) 237.987 ms 264.826 ms 239.413 ms
```

Traceroutes

Christmas

Ho

Ho

Ho

12	oooooxoooooooooooo.v.oooooooooooooooooooo	(82.133.91.37)	32.520 ms	85.029 ms	84.417 ms
13	oooooooxxxoooo.mmm.mooooooooooooxoo	(82.133.91.18)	28.508 ms	29.413 ms	159.747 ms
14	ooooxooooooxoooo.eeeee.oxxxooooooxoooo	(82.133.91.63)	30.813 ms	27.738 ms	28.727 ms
15	ooooooxooooox.rrrrrrrr.ooooooooooooox	(82.133.91.56)	98.966 ms	26.433 ms	26.304 ms
16	oooooooxxooo.rrrrrrrrr.ooooxooooooo	(82.133.91.55)	25.990 ms	25.856 ms	175.046 ms
17	xoooooooy.yyyyyyyyyy.ooooxooooo	(82.133.91.58)	35.091 ms	28.833 ms	27.252 ms
18	oooooooxxooooo.ccc.ooooooooooooxooo	(82.133.91.96)	33.924 ms	27.624 ms	28.044 ms
19	ooooooxooo.hhhhhhhhhhhh.oxooooxoooo	(82.133.91.23)	26.037 ms	27.727 ms	27.233 ms
20	oooooxoo.rrrrrrrrrrrrrr.oooooooxxoo	(82.133.91.49)	27.114 ms	26.809 ms	27.727 ms
21	oooooxo.iiiiiiiiiiiiii.ooooxoo	(82.133.91.68)	27.393 ms	79.425 ms	35.691 ms
22	ooooxo.sssssssssssssssssssssssoooo	(82.133.91.42)	38.394 ms	26.477 ms	27.073 ms
23	ooooooxooooooo.ttt.ooooooooooooooxoo	(82.133.91.61)	26.567 ms	27.164 ms	27.260 ms
24	ooxoo.mmmmmmmmmmmmmmmmmmmmmmmmm.oooox	(82.133.91.34)	26.268 ms	26.292 ms	27.335 ms
25	xxoo.aaaaaaaaaaaaaaaaaaaaaaa.oxooo	(82.133.91.80)	27.087 ms	26.545 ms	25.758 ms
26	oxo.ssssssssssssssssssssssssss.ooo	(82.133.91.48)	28.201 ms	26.604 ms	31.071 ms
27	ooooooooooooooooo.xxx.oooooooooooooxo	(82.133.91.35)	27.685 ms	34.823 ms	27.358 ms
28	oxooooooooooooo.xxx.oooooooooooooxo	(82.133.91.10)	26.663 ms	30.052 ms	28.420 ms
29	oh.the.weather.outside.is.frightful	(82.133.91.41)	28.655 ms	27.795 ms	28.863 ms
30	but.the.fire.is.so.delightful	(82.133.91.19)	26.172 ms	26.577 ms	26.777 ms
31	and.since.weve.no.place.to.go	(82.133.91.77)	26.537 ms	28.931 ms	35.163 ms
32	let.it.snow.let.it.snow.let.it.snow	(82.133.91.43)	28.258 ms	30.653 ms	43.191 ms
33	xxx (82.133.91.24)	30.019 ms	30.663 ms	31.834 ms	
34	it.doesnt.show.signs.of.stopping	(82.133.91.36)	26.373 ms	29.913 ms	25.671 ms
35	and.ive.bought.some.corn.for.popping	(82.133.91.73)	27.470 ms	26.959 ms	26.904 ms
36	the.lights.are.turned.way.down.low	(82.133.91.76)	26.997 ms	28.610 ms	32.095 ms

Tools and Toys

Tools and Toys

Calculator

Sadly not around
anymore

There's a reverse
Polish calculator out
there as well

```
dig @dns.postel.org 2.8.add.calc.postel.org +short  
0.10.0.0
```

```
dig @dns.postel.org 8.2.sub.calc.postel.org +short  
0.6.0.0
```

```
dig @dns.postel.org 2.8.mul.calc.postel.org +short  
0.16.0.0
```

```
dig @dns.postel.org 8.2.div.calc.postel.org +short  
0.4.0.0
```

Tools and Toys

"My IP"

Google

```
[pgl-macbook-pro:pgl]:~ $ host -t txt o-o.myaddr.l.google.com ns1.google.com
Using domain server:
Name: ns1.google.com
Address: 216.239.32.10#53
Aliases:

o-o.myaddr.l.google.com descriptive text "77.97.197.133"
```

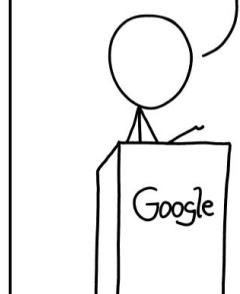
OpenDNS

```
[pgl-macbook-pro:pgl]:~ $ dig myip.opendns.com @resolver1.opendns.com +short
77.97.197.133
```

Tools and Toys

"My IP"

THE RUMORS ARE TRUE. GOOGLE
WILL BE SHUTTING DOWN PLUS—
ALONG WITH HANGOUTS, PHOTOS,
VOICE, DOCS, DRIVE, MAPS, GMAIL,
CHROME, ANDROID, AND SEARCH—
TO FOCUS ON OUR CORE PROJECT:
THE 8.8.8.8 DNS SERVER.



Tools and Toys

IP to ASN

```
[pgl-macbook-pro:pgl]:~ $ dig +short 8.8.8.0/24.origin.asn.cymru.com TXT  
"15169 | 8.8.8.0/24 | US | arin | 1992-12-01"
```

```
[pgl-macbook-pro:pgl]:~ $ dig +short 1.1.1.1.peer.asn.cymru.com TXT  
"1103 2914 3257 7195 | 1.1.1.0/24 | AU | apnic | 2011-08-11"
```

```
[pgl-macbook-pro:pgl]:~ $ dig +short 192.168.0.1.origin.asn.cymru.com TXT  
"23969 | 1.0.128.0/17 | TH | apnic | 2011-04-08"  
"23969 | 1.0.128.0/18 | TH | apnic | 2011-04-08"  
"23969 | 1.0.160.0/19 | TH | apnic | 2011-04-08"  
"23969 | 1.0.168.0/24 | TH | apnic | 2011-04-08"
```

From Team Cymru - similar to Whois but faster

Tools and Toys

Postcodes

```
[pgl-macbook-pro:pgl]:~ $ host -t LOC kt112ra.find.me.uk
kt112ra.find.me.uk location 51 19 42.141 N 0 23 56.076 W 0.00m 0.00m 0.00m 0.00m
```

```
[pgl-macbook-pro:pgl]:~ $ dig PASSAU.zipde.jpmens.net TXT
; <>> DiG 9.10.6 <>> PASSAU.zipde.jpmens.net TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 2408
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;PASSAU.zipde.jpmens.net.      IN      TXT

;; ANSWER SECTION:
PASSAU.zipde.jpmens.net. 604800 IN      TXT      "94036"
PASSAU.zipde.jpmens.net. 604800 IN      TXT      "94034"
PASSAU.zipde.jpmens.net. 604800 IN      TXT      "94032"
```

Tools and Toys

dns.toys

Currency conversion (forex)

```
dig 100USD-INR.fx @dns.toys  
dig 50CAD-AUD.fx @dns.toys
```

\$Value\$FromCurrency-\$ToCurrency. Daily rates are from [exchangerate.host](#).

Number to words

```
dig 987654321.words @dns.toys
```

Convert numbers to English words.

World time

```
dig mumbai.time @dns.toys  
dig newyork.time @dns.toys  
dig paris.fr.time @dns.toys
```

Pass city names without spaces suffixed with .time optionally.

IP echo

```
dig ip @dns.toys
```

Echo your IP address.

Usable CIDR Range

```
dig 10.0.0.0/24.cidr @dns.toys  
dig 2001:db8::/108.cidr @dns.toys
```

Parse CIDR notation to find out first and last usable IP address in the subnet.

From Kailash Nadh, CTO of Zerodha

Tools and Toys

Geocaching



Dort Nicht Suchen!

A cache by [Mockapetris_1876](#) & [bzlcache](#) Message this owner Hidden : 08/31/2015

Difficulty:

Terrain:

Size: (micro)

Geocache Description:

stage1.GC615NM.deebas.com

```
[pgl-macbook-pro:pgl]:~ $ host -t txt stage1.GC615NM.deebas.com  
stage1.GC615NM.deebas.com descriptive text "hint: reverse of six"
```

From Sebastian Haas:

*Mockapetris himself wasn't involved in the geocache. "Mockapetris_1876" is just a hint to DNS and RFC 1876 ;)
The cache is maintained by me.*

To solve the complete riddle you have to execute multiple queries (TXT, AAAA, PTR, LOC). You can find the solution in the screenshot.

Tools and Toys

Text adventure

By Craig
Mayhew,
[@craigmayhew](https://twitter.com/craigmayhew)

Uses round
robin DNS for
chance-based
actions



```
user@surf:/$ go() {
>     IN=$(dig -t txt +short $(echo $1).adventure.craig.mayhew.io @ns-236.awsdns-2
9.com | shuf -n 1)
>     IFS=''' read -ra ADDR <<< "$IN"
>     for i in "${ADDR[@]}"; do
>         echo "$i"
>     done
> }
```

Tools and Toys

Drink

```
[air:pgl]:~ $ host -t txt dyn.bortzmeyer.fr
dyn.bortzmeyer.fr descriptive text "Possible queries: " "hello/TXT to have a greeting. " "ip/TX
T,A,AAAA to have the IP address of the client. " "date/TXT to have the date. " "random/TXT,A,AA
AA to have a random integer or address. " "bgp/TXT to have the IP address of the client, its pr
efix in the DFZ and its origin AS number. " "country/TXT to have the country of the client. " "
Xorigin.Ydestination.unit/TXT to do unit conversions. " "Expr.op/TXT to evaluate an arithmetic
expression. " "full/TXT to have IP address, AS and country of the client. "
```

From Stéphane Bortzmeyer, [@bortzmeyer](https://twitter.com/bortzmeyer)

Amazing general purpose dynamic DNS server

Try `2+2.op.dyn.bortzmeyer.fr`, `LOC` and `URI` query types on
`random.dyn.bortzmeyer.fr`

Tunneling

Tunneling

General idea

General Approach to DNS tunneling [[back](#)]

DNS Tunneling works by abusing DNS records to traffic data in and out of a network. In principle, every type of record can be used, but the speed of the connection differs by the amount of data that can be stored in a single record. Below are some obvious ones:

- **TXT records** allow free-form data and can even include spaces. You can as such store information in it encoded with base64, allowing 220 bytes of data per record. TXT records are intended for "generic" use within the DNS framework. Users can place whichever data in it, as long as it meets the protocol requirements: a maximum length of 255 octets according to RFC 1035. In the recent past, TXT records had virtually been depreciated, which would have enabled highly security conscious environments to discard them at the enterprise DNS server. Today however, they have regained use as the carrier of the antispam-related SPF record.
- **CNAME records** allow only the characters A through Z, digits 0-9 and the hyphen. As such you require base32 encoding and are limited to about 110 bytes per record
- **EDNS0 messages** can be larger than the 512 byte maximum for UDP DNS, and can carry a 1280 byte payload by default. OzyManDNS uses a 768 byte payload for stability
- **A and MX records** can be used as well, but with more limitations. These cannot store all types of data.

Discussed on
Slashdot back
in 2000

Any record
types

<https://www.daemon.be/maarten/dnstunnel.html>

Tunneling

Wikipedia

```
$ host -t txt foo.wp.dg.cx
foo.wp.dg.cx descriptive text "Foo may refer to: Foo, bar, and baz: metasyntactic variables,
\"Fool\", as a nonstandard spelling to indicate a nonstandard pronunciation, Foo Fighters, a post-
grunge group formed by Dave Grohl, Foo fighters, a World War II term for various UFOs or
mysterio\" \"us aerial phenomena seen in the skies over Europe and the Pacific theatre, Foo, also
a known surname or last name of a... http://a.vu/w:Foo"
```

```
$ dig +short txt '新疆.wp.dg.cx' | perl -pe's/\\"(\d{1,3})/chr $1/eg'
"Xinjiang (Uyghur: , Shinjang\; \; Postal map spelling: Sinkiang) is an autonomous region
(Xinjiang Uyghur Autonomous Region) of the People's Republic of China. It is a large, sparsely
populated area (spanning over 1.6 million sq. km) which takes up about one sixth of the
country's territory. Xinjiang borders the Tibet Autonomous Region to the south and Qinghai and
Gansu... http://a.vu/w:Xinjiang"
```

David Leadbetter

Add TXT records to "publish" a post

By Harshad
Sharm - trying to
"break coder's
block"

Tunneling

Blogging

- View latest post:

```
$ dig @127.0.0.1 -p 10053 TXT +short rex.latest
"# Hello"
"This is a test."
```

- See recent posts:

```
$ dig @127.0.0.1 -p 10053 TXT +short rex.index
"Latest: rex.latest"
"Recent:"
"  rex.hello"
"  rex.trying.something.silly"
```

- Read a specific post:

```
$ dig @127.0.0.1 -p 10053 TXT +short rex.trying.something.silly
"# Woohoo!"
"This actually works?!"
```

Tunneling

IP over DNS

Erik Eckman -
@yarrick on
GitHub

IPv4 only inside
the tunnel, but
server can listen
on IPv6

Iodine has the
atomic number 53

Try it out within your own LAN! Follow these simple steps:

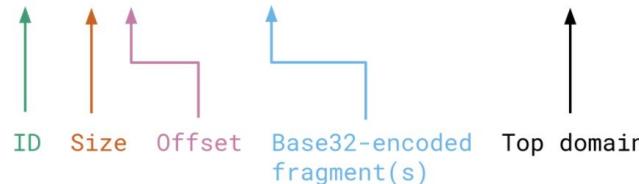
- On your server, run: `./iodined -f 10.0.0.1 test.com`. If you already use the `10.0.0.0` network, use another internal net like `172.16.0.0`.
- Enter a password.
- On the client, run: `./iodine -f -r 192.168.0.1 test.com`. Replace `192.168.0.1` with your server's ip address.
- Enter the same password.
- Now the client has the tunnel ip `10.0.0.2` and the server has `10.0.0.1`.
- Try pinging each other through the tunnel.
- Done! :)

Tunneling

HTTP over DNS

Browsertunnel can send arbitrary strings over DNS by encoding the string in a subdomain, which is forwarded to the browsertunnel server when the browser attempts to recursively resolve the domain.

gmr02c.16.0.nbswy3dpea5cs000.tunnel.example.com



Jessie Li,
@veggiedefender
on GitHub

HTTP over DNS
over HTTPS?

Longer messages that cannot fit in one domain (253 bytes) are automatically split into multiple queries, which are reassembled and decoded by the server.

ya4iee.40.0.orugs4zanf.zsayjanr.tunnel.example.com

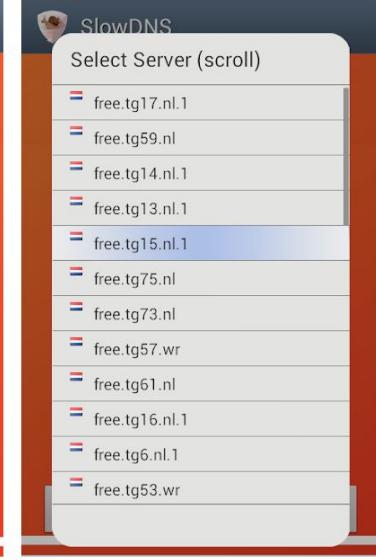
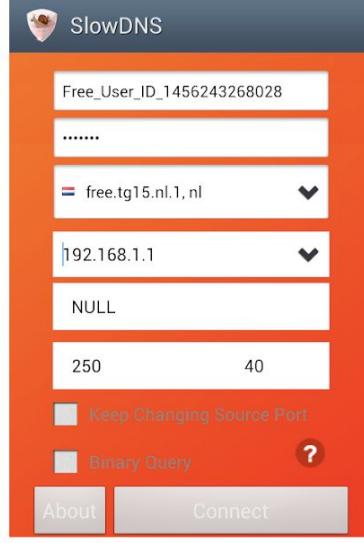
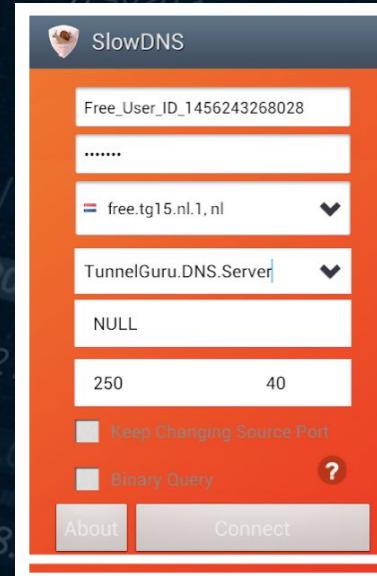
ya4iee.40.18.xw4z3foiqg.2zltonq.tunnel.example.com

ya4iee.40.35.wozi0.tunnel.example.com

Tunneling

VPN over DNS

"Contains ads"



Tunneling

dnscat2

lagox86 on GitHub, or
"Ron"

Doesn't need a domain

Looks exactly like
normal DNS traffic

```
dnscat2> window -i dns1
New window created: dns1
Starting Dnscat2 DNS server on 0.0.0.0:53531
[domains = skullseclabs.org]...
```

Assuming you have an authoritative DNS server, you can run
the client anywhere with the following:
./dnscat2 skullseclabs.org

To talk directly to the server without a domain name, run:
./dnscat2 --dns server=x.x.x.x,port=53531

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53531.

```
Received: dnscat.9fa0ff178f72686d6c716c6376697968657a6d716800 (TXT)
Sending: 9fa0ff178f72686d6c716c6376697968657a6d716800
Received: d17cff3e747073776c776d70656b73786f646f616200.skullseclabs.org (MX)
Sending: d17cff3e747073776c776d70656b73786f646f616200.skullseclabs.org
```

And more

Bigger things

DNS for config

Corey Quinn

Using Route 53
for config
management

@quinnypig on
Twitter



About the Author

Corey is the Chief Cloud Economist at The Duckbill Group, where he specializes in helping companies improve their AWS bills by making them

Episode Summary

Join me as I launch a new series called Whiteboard Confessional that explores how whiteboard architecture diagrams might look pretty but rarely work as designed in production. To kick off the series, we're taking a look at everyone's favorite database, AWS Route 53, while touching upon a number of topics, including what data centers used to look like, the emergence of virtualization and the impact it had, configuration management databases and how they differ from configuration management tools like Chef and Puppet, why using DNS as a configuration management database is inherently an awful idea, how there's almost always a better solution than whatever you built in your own isolated environment, how just because someone built something doesn't mean they knew what they were doing, and more.

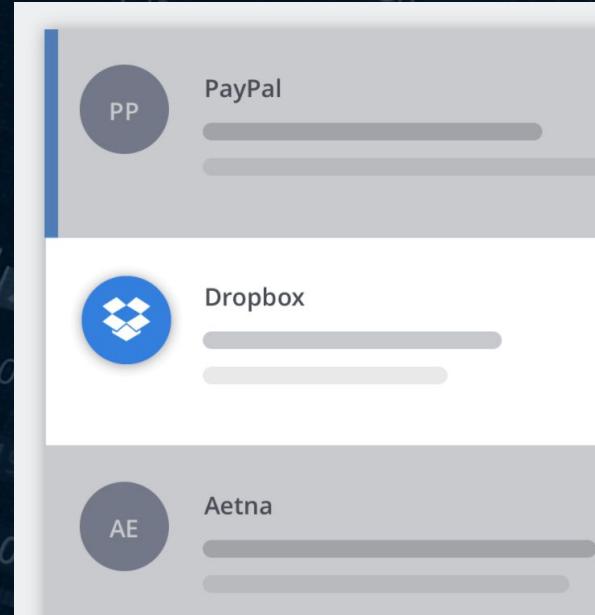
Bigger things

Brands

BIMI records

Really just TXT
records starting
`_bimi`

<https://bimi.agari.com/>



With brand indicators,
your brand will be
integrated into every
email.

When customers scan
their inboxes, your
email will stand out.

Bigger things

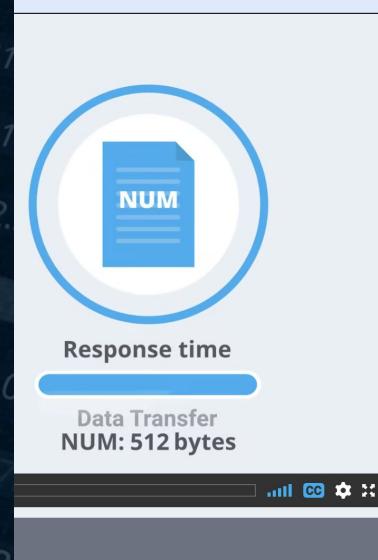
Contacts DB

"Free, unlimited, unrestricted access to data about every company in the UK**"

npm modules, developer docs

Numprotocol.com

NUM technology



What is NUM?

A new way to store and retrieve data

NUM is like the Web but for machines. Websites are built for browsing but are an inefficient way to find precise pieces of data like a telephone number, address and more. NUM makes useful data machine-readable so it can be built into devices, apps and services to make your life easier.

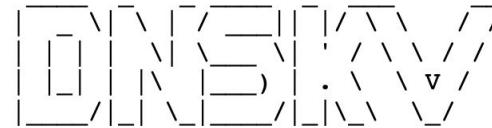
NUM is built on top of the Domain Name System (DNS) – a system we all use every day. Watch the 90-second explainer to find out more.

Bigger things

Key-value store

**Generic service offered
to allow people to set
and retrieve values**

**Not sure who's behind
this!**



DNS Key Value Storage (dnskv.com)

The packet messaging service for true hackers. Simple and free to use.

Too complex? See: [simplified tutorial](#)

Structure:

- Suffix all names with this domain
- options.value.key.

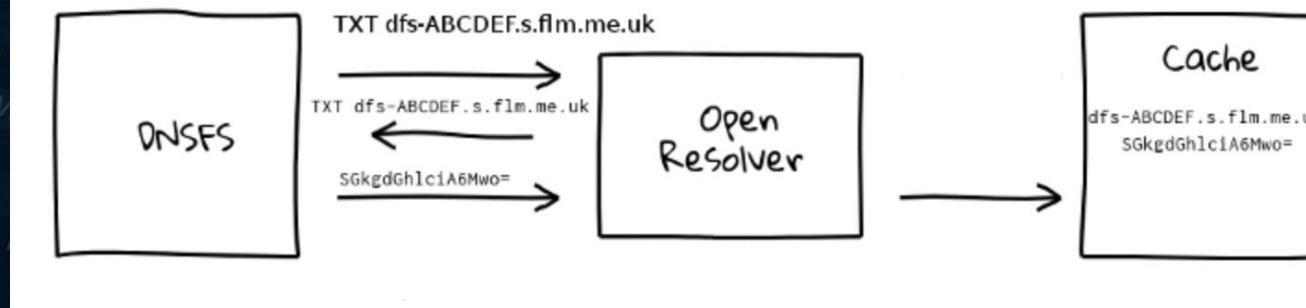
Insert:

- value.key.

Bigger things

DNSFS

Putting data into cache



Ben Cox, benjojo.co.uk

Bigger things

MP3s

One use of DNSFS



Ben Cox
@Benjojo12

Replying to @Manawymr

oh god that actually works. Here is a bash 1 liner:

```
let counter=0; while true; do sleep 1; dig TXT +short  
$counter.mp3.nodialtone.de @ns1.resellerinterface.de  
| tr -d ' ' | tr -d '"' | base64 -d; let counter++; done | vlc
```

Links

- <https://dnsfilter.com/> - DNSFilter
- <https://github.com/sehaas/fakert> - Sebastian Haas' fakert
- <https://beaglenetworks.net/post/42707829171/star-wars-traceroute> - Star Wars traceroute
- <https://dgl.cx/wikipedia-dns> - Wikipedia over DNS
- https://www.youtube.com/watch?v=_y36fG2Oba0 - The Day The Router Died
- <https://www.youtube.com/watch?v=O03kODV2m1k> - Bad Horse
- <https://asciinema.org/a/15020> - Christmas traceroute
- <https://team-cymru.com/community-services/ip ASN-mapping/#dns> - IP to ASN mapping
- <https://www.cambus.net/interesting-dns-hacks/> - few things including the calculator, My IP
- <https://jpmens.net/2020/10/04/airports-of-the-world/> - Airports
- <https://github.com/gryphius/ch-loc> - Oli Schacher's Swiss location stuff
- <https://www.daemon.be/maarten/dnstunnel.html> - Discussion of DNS tunneling
- <https://coord.info/GC615NM> - Geocache
- <https://github.com/craigmayhew/dns-adventure-game> - text adventure over DNS
- <https://github.com/hiway/txtrex> - blogging via DNS (Harshad Sharma - @hiway)
- <https://gist.github.com/ManawyrM/718cf8ab6ba59ba95d9743d01b1763dd> - MP3 streaming
- <https://github.com/yarrick/iodine> - iodine - IP over DNS
- <https://github.com/veggiedefender/browsertunnel> - HTTP over DNS
- <https://www.lastweekinaws.com/podcast/aws-morning-brief/whiteboard-confessional-route-53-db/> - DNS for config management
- <https://play.google.com/store/apps/details?id=com.in.troiddns> - SlowDNS - VPN over DNS
- <https://dnsvk.com/> - DNS Key Value Storage
- <https://github.com/ligox86/dnscat2> - dnscat2
- <https://bimi.agari.com/> - Brand Indicator Records
- <https://tools.ietf.org/id/draft-blank-ietf-bimi-00.html> - BIMI draft
- <https://www.num.uk/> - num.uk business
- <https://www.numprotocol.com/> - the NUM protocol
- <https://github.com/benjojo/dnsfs> - DNSFS
- <https://xkcd.com/1361/>
- <https://team-cymru.com/community-services/ip ASN-mapping/#dns> - IP to ASN mapping
- <https://www.bortzmeyer.org/drink.html> - Drink DNS server
- <https://github.com/pgl/rule53> - Rule53 list on GitHub
- <https://twitter.com/pgl/status/1405614755000295427> - Twitter thread

Questions?



Principal Museum of DNS Curator
Security Researcher @ **DNSFilter**
Open for work

twitter.com/pql
infosec.exchange/@pql

peter@dnsfilter.com / pql@yoyo.org