DNS is Still Lame

Why it’s a problem and what we can do about it

Ian Foster

$ whoami

Ian Foster

Way too interested in DNS & TLS

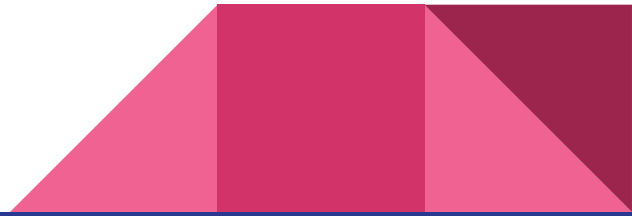
- DNS Researcher/Historian
  - dns.coffee
- Certgraph
- BygoneSSL

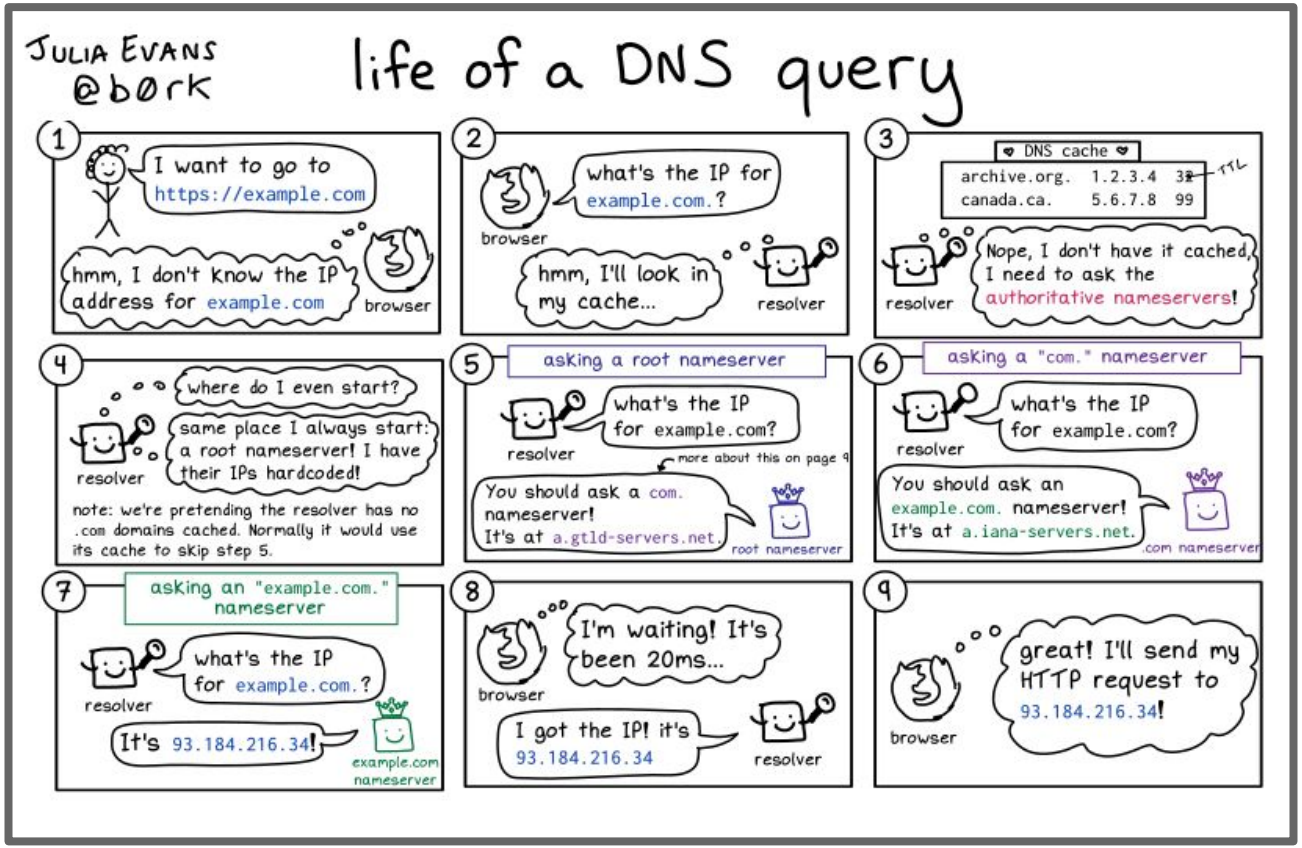
Red Team Lead @ Snap

@LANRAT

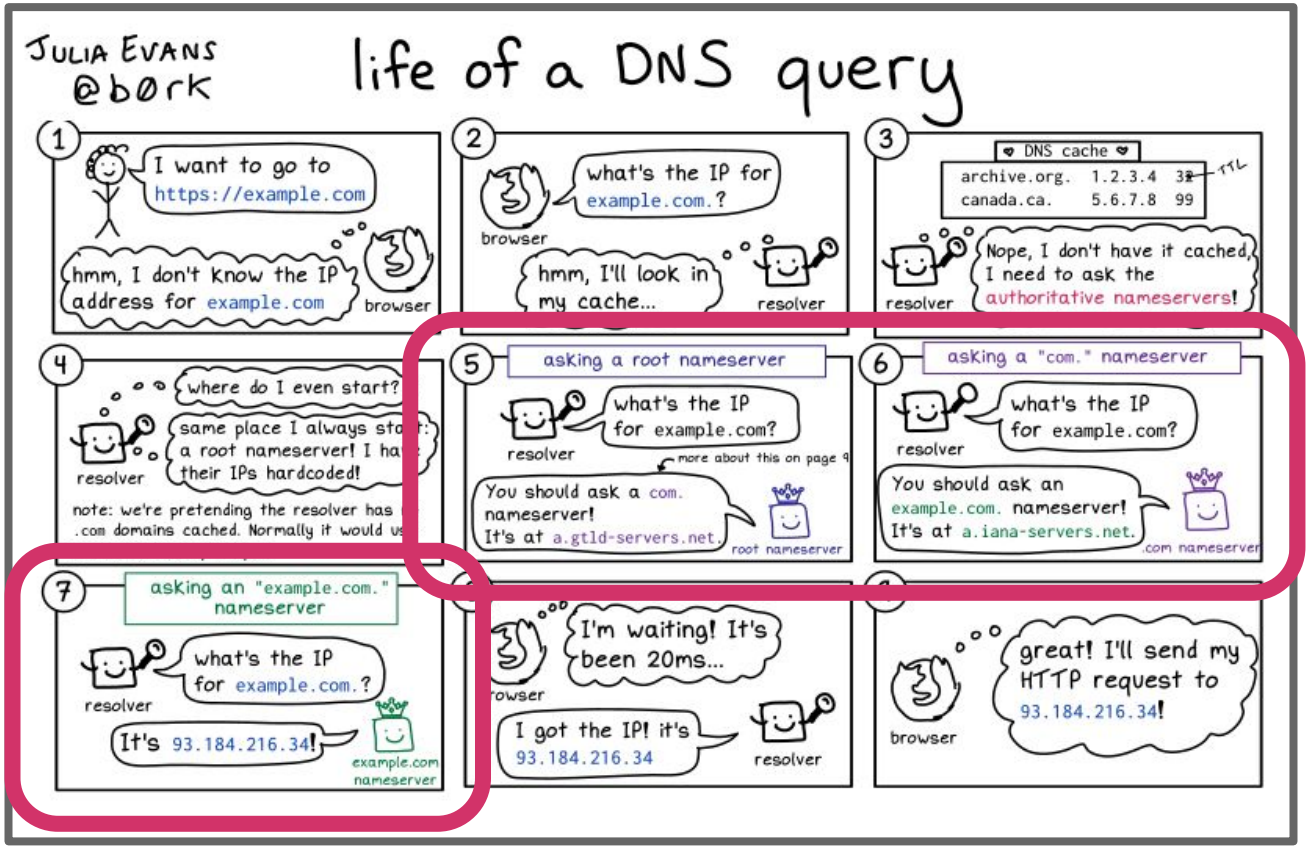
This Talk

- What is a DNS Lame Delegation
- DNS Dependency "trees"
- Examples of Lame Delegations
- Tool & Demo



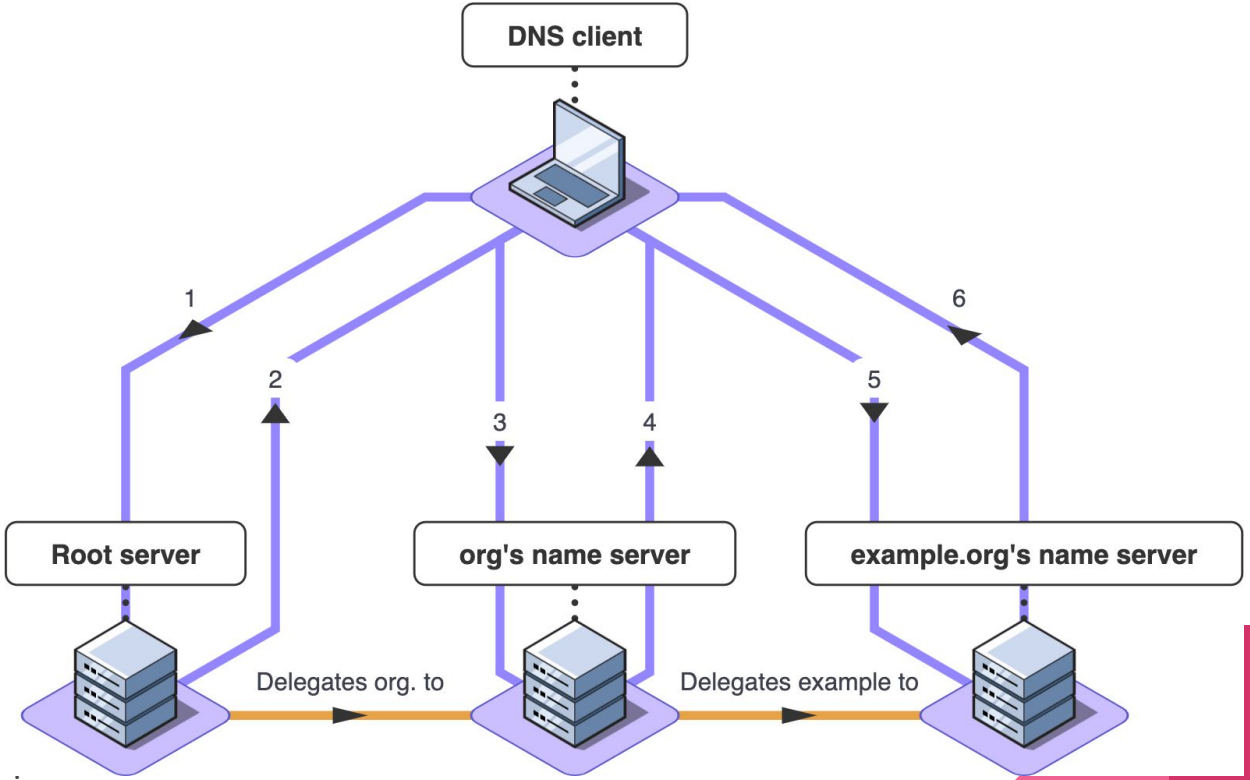


https://wizardzines.com/comics/life-of-a-dns-query



https://wizardzines.com/comics/life-of-a-dns-query

DNS Delegation & Authoritative DNS Servers

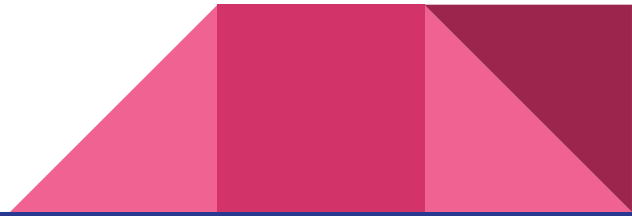


Source: nslookup.io

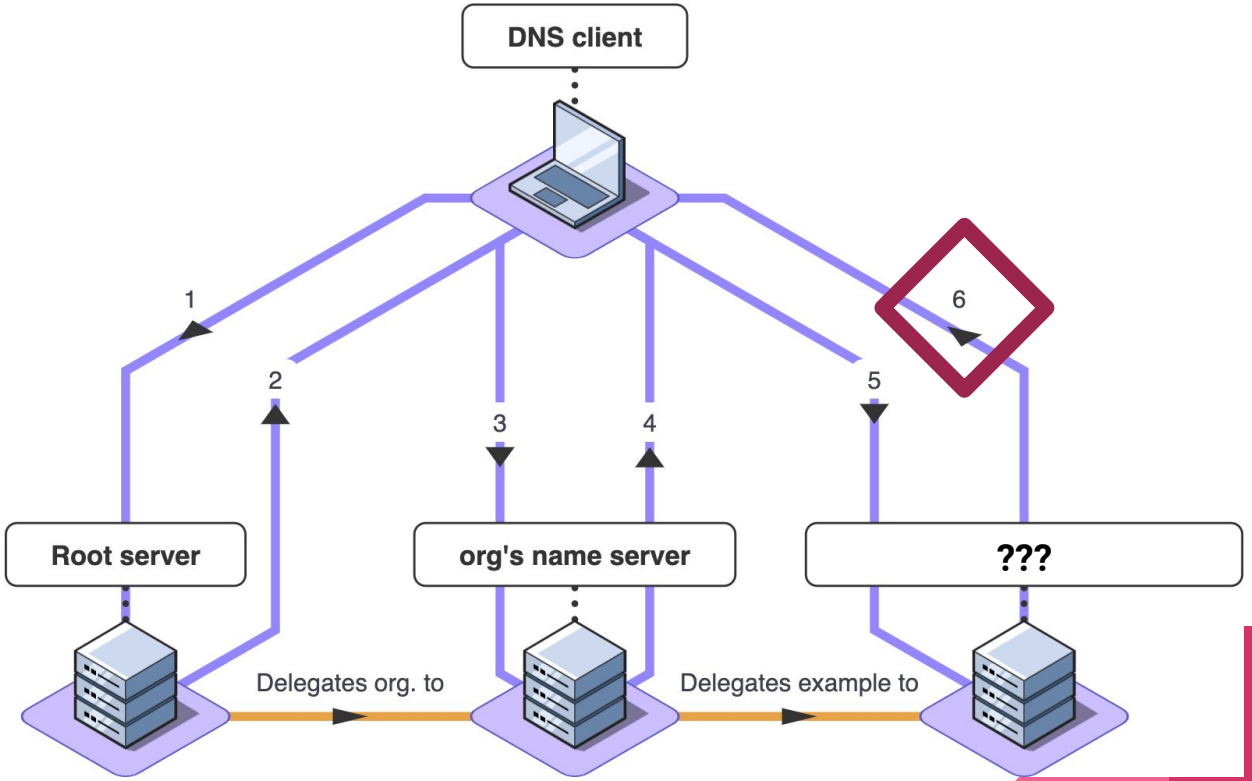
Lame Delegations

- Defined in RFC 8499
- Put very simply: The NS responses are not correct

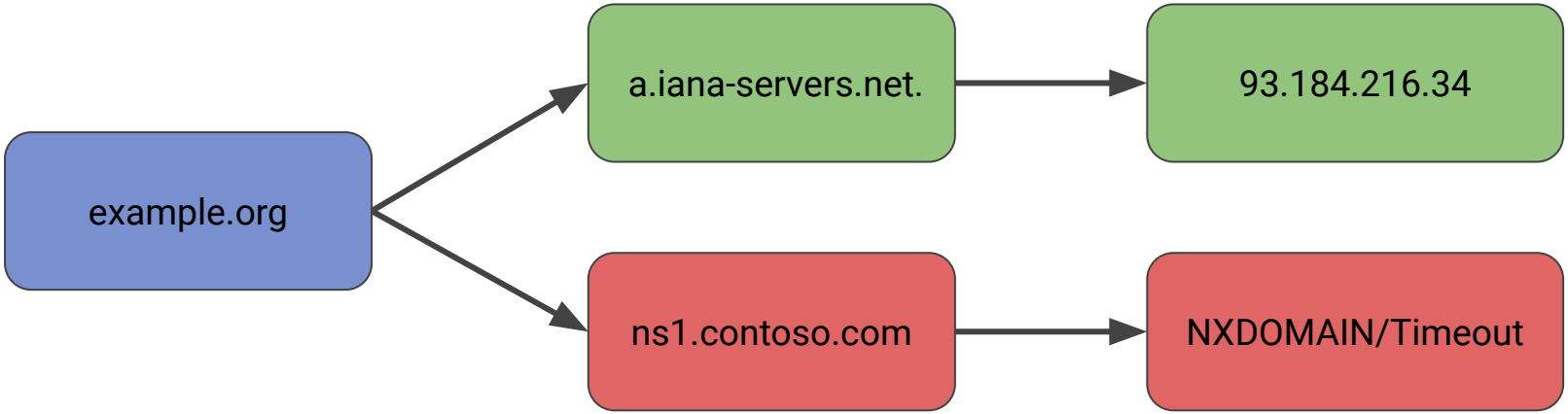
- Example:
  - NS answer 1:
    - `example.org 86400 NS ns1.example.org.`
    - `example.org 86400 NS ns2.example.org.`
  - NS answer 2:
    - `example.org 86400 NS ns1.foo.com.`
    - `example.org 86400 NS ns2.foo.com.`



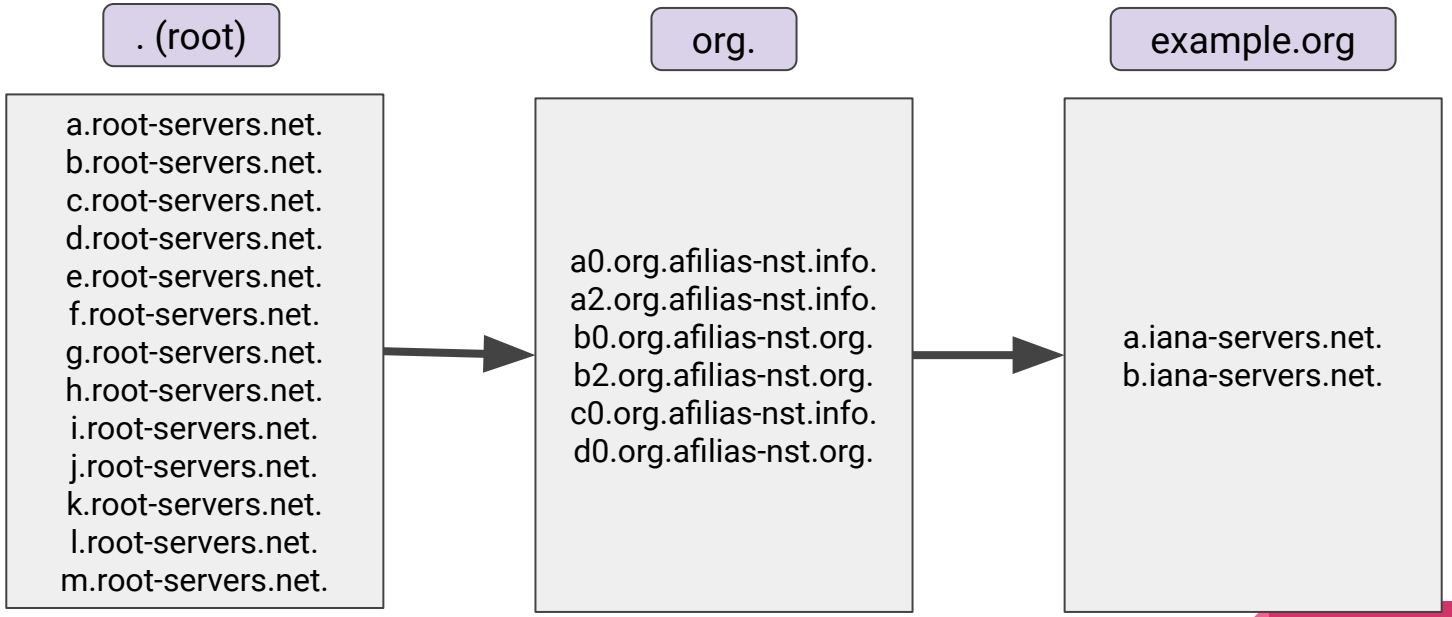
Lame Delegations



Partially Lame Delegation



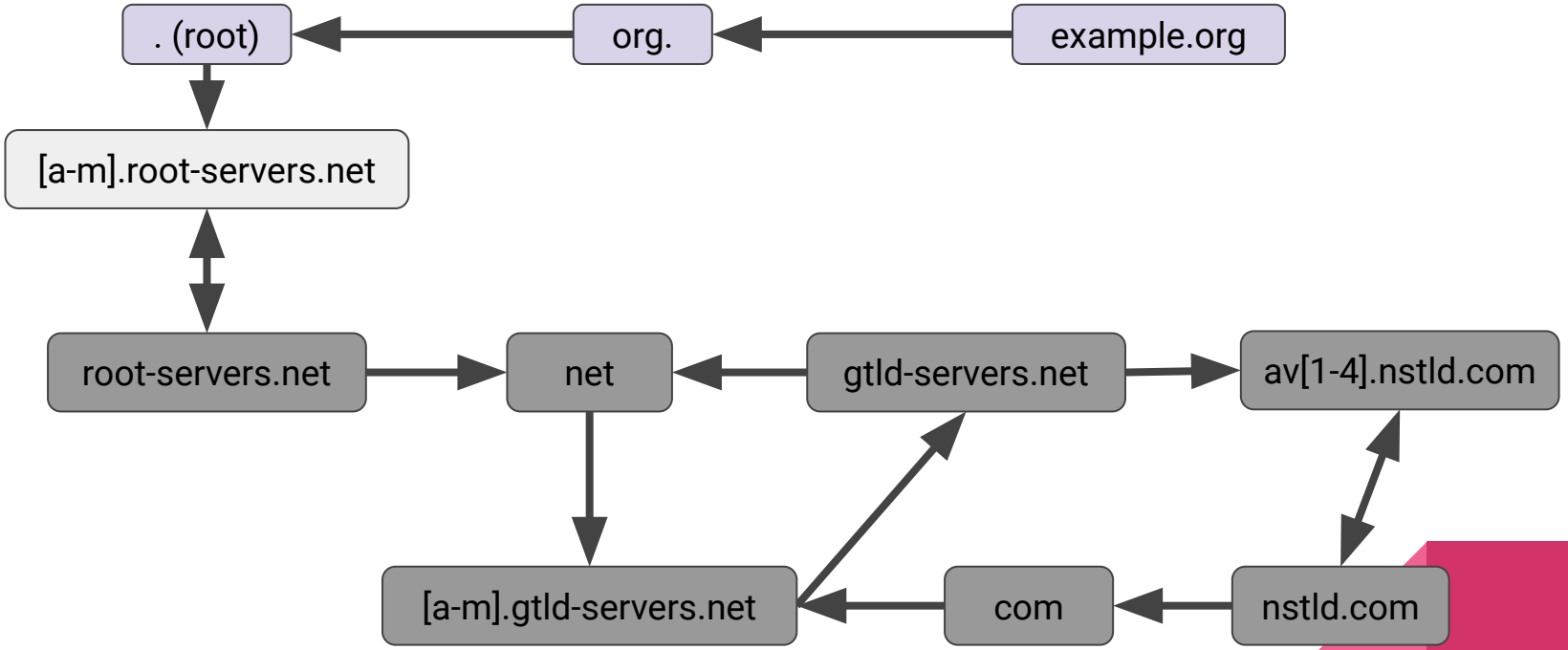
DNS Dependencies



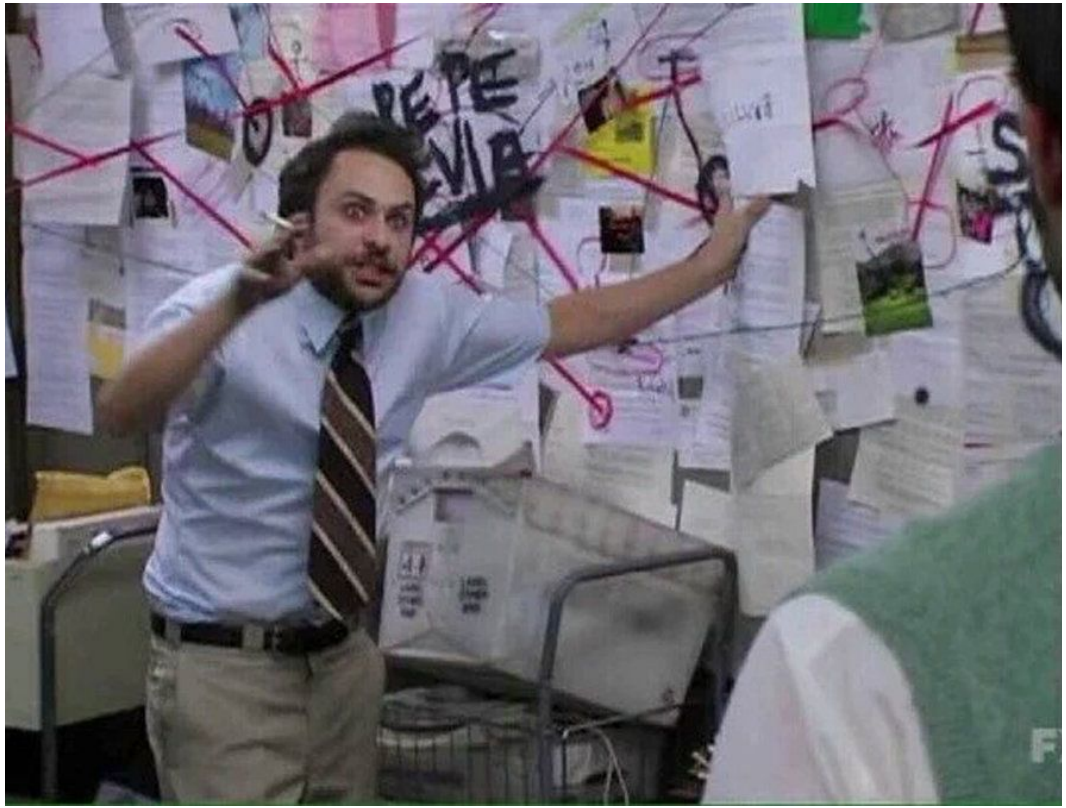
DNS Dependencies

- Nameservers
  - Root Nameservers
  - TLD Nameservers
  - Chain of delegating Nameservers
  - Authoritative Nameservers
- IP Addresses for every nameservers
- Recursive Dependencies for every parent domain used by all Nameservers

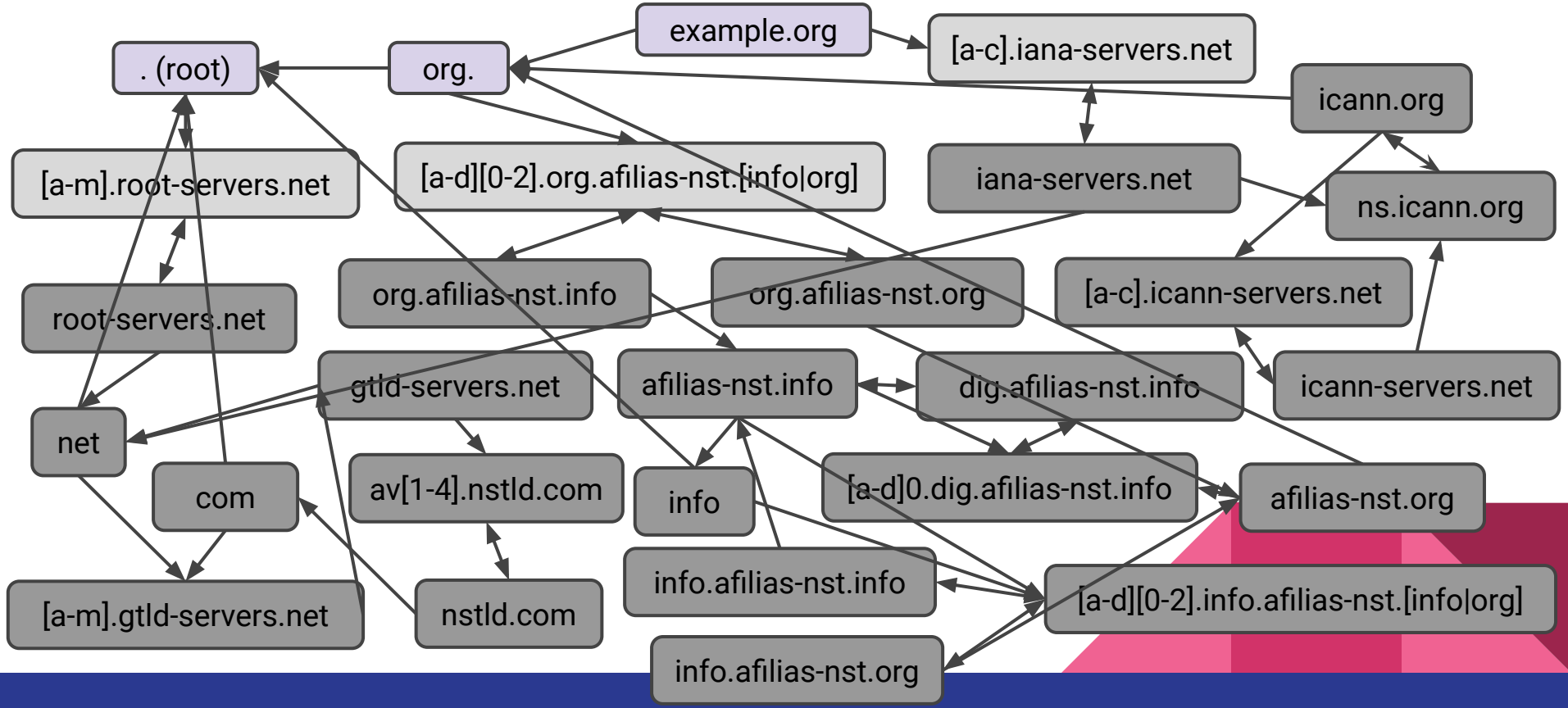
DNS Dependencies



WARNING



DNS Dependencies



Identifying Authoritative Responses

```
lanrat@firefly:~$ dig +noadditional +norecurse +noquestion -t a shmoocon.org @8.8.8.8

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> +noadditional +norecurse +noquestion -t a shmoocon.org @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 58689
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

```
lanrat@firefly:~$ dig +noadditional +norecurse +noquestion -t a shmoocon.org @krusty.shmoo.com.

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> +noadditional +norecurse +noquestion -t a shmoocon.org @krusty.shmoo.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61224
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; ANSWER SECTION:
shmoocon.org.           400     IN      A       23.185.0.2
```

Manually Recursive Resolving a Domain

```
lanrat@firefly:~$ dig +norecurse -t ns .

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> +norecurse -t ns .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9965
;; flags: qr ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       7109    IN      NS      i.root-servers.net.
.                       7109    IN      NS      a.root-servers.net.
.                       7109    IN      NS      j.root-servers.net.
.                       7109    IN      NS      d.root-servers.net.
.                       7109    IN      NS      e.root-servers.net.
.                       7109    IN      NS      f.root-servers.net.
.                       7109    IN      NS      g.root-servers.net.
.                       7109    IN      NS      l.root-servers.net.
.                       7109    IN      NS      h.root-servers.net.
.                       7109    IN      NS      b.root-servers.net.
.                       7109    IN      NS      k.root-servers.net.
```

```
lanrat@firefly:~$ dig +noadditional +norecurse -t a  shmoocon.org @a.root-servers.net.

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> +noadditional +norecurse -t a shmoocon.org @a.root-servers.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48894
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;shmoocon.org.                  IN      A

;; AUTHORITY SECTION:
org.                    172800  IN      NS      d0.org.afilias-nst.org.
org.                    172800  IN      NS      a0.org.afilias-nst.info.
org.                    172800  IN      NS      c0.org.afilias-nst.info.
org.                    172800  IN      NS      a2.org.afilias-nst.info.
org.                    172800  IN      NS      b0.org.afilias-nst.org.
org.                    172800  IN      NS      b2.org.afilias-nst.org.

;; Query time: 4 msec
;; SERVER: 2001:503:ba3e::2:30#53(a.root-servers.net.) (UDP)
;; WHEN: Wed Jan 10 11:01:48 PST 2024
```

```
lanrat@firefly:~$ dig +noadditional +norecurse -t a  shmoocon.org @b0.org.afilias-nst.org.

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> +noadditional +norecurse -t a shmoocon.org @b0.org.afilias-nst.org.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28339
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;shmoocon.org.                  IN      A

;; AUTHORITY SECTION:
shmoocon.org.           3600    IN      NS      krusty.shmoo.com.
shmoocon.org.           3600    IN      NS      archimedes.shmoo.com.

;; Query time: 136 msec
;; SERVER: 2001:500:c::1#53(b0.org.afilias-nst.org.) (UDP)
;; WHEN: Wed Jan 10 11:02:45 PST 2024
;; MSG SIZE  rcvd: 96
```

```
lanrat@firefly:~$ dig +noadditional +norecurse -t a  shmoocon.org @krusty.shmoo.com.

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> +noadditional +norecurse -t a shmoocon.org @krusty.shmoo.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14592
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;shmoocon.org.                  IN      A

;; ANSWER SECTION:
shmoocon.org.           400     IN      A       23.185.0.2
```

An Alternate Route?

```
lanrat@firefly:~$ dig +noadditional +norecurse -t a  shmoocon.org @archimedes.shmoo.com.
;; communications error to 216.137.208.30#53: timed out
;; communications error to 216.137.208.30#53: timed out
;; communications error to 216.137.208.30#53: timed out

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> +noadditional +norecurse -t a shmoocon.org @archimedes.shmoo.com.
;; global options: +cmd
;; no servers could be reached
```

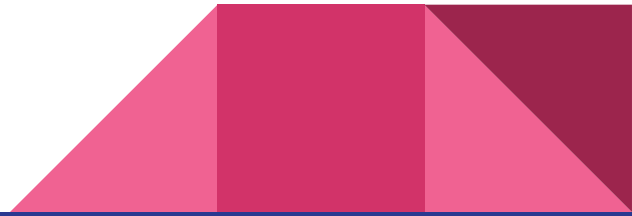
What can we do about this?

- Continuously monitor for changes in your domains and DNS dependencies
  - Make it automatic!
- If the problem is upstream of you, then notify the network operators
- Setup your DNS infrastructure to have fewer dependencies
  - As few NS or CNAME chains as possible

Tool: Broken DNS

https://github.com/lanrat/broken-dns

- Enumerates DNS dependency tree
- Tests all possible servers along resolution paths
- Fast!
- Can alert on:
  - Lame Delegations
  - Unexpected NS in answers
  - Any hidden problems anywhere in the dependency tree
  - Authoritative NS providing different answers



Demo Time!

```
lanrat@geary:~/code/broken-dns$ ./broken-dns shmoocon.org
2024/01/11 11:04:31 starting 10 threads
[FINDING] lame delegation: "archimedes.shmoo.com" is not authoritative for "shmoocon.org"
STATS: 1/1 lame delegations and 1 problems
lanrat@geary:~/code/broken-dns$
```

Can we take over shmoocon.org?

```
lanrat@firefly:~$ dig -t NS shmoocon.org

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> -t NS shmoocon.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11463
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;shmoocon.org.                  IN      NS

;; ANSWER SECTION:
shmoocon.org.           400     IN      NS      krusty.shmoo.com.
shmoocon.org.           400     IN      NS      archimedes.shmoo.com.

;; Query time: 148 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Jan 10 10:03:25 PST 2024
;; MSG SIZE  rcvd: 96
```

```
lanrat@firefly:~$ dig @krusty.shmoo.com. -t NS shmoocon.org

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @krusty.shmoo.com. -t NS shmoocon.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17997
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;shmoocon.org.                  IN      NS

;; ANSWER SECTION:
shmoocon.org.           400     IN      NS      archimedes.shmoo.com.
shmoocon.org.           400     IN      NS      krusty.shmoo.com.

;; ADDITIONAL SECTION:
krusty.shmoo.com.       3600    IN      A       205.134.188.162
archimedes.shmoo.com.   3600    IN      A       216.137.208.30

;; Query time: 60 msec
;; SERVER: 205.134.188.162#53(krusty.shmoo.com.) (UDP)
;; WHEN: Wed Jan 10 10:05:21 PST 2024
;; MSG SIZE  rcvd: 128
```

```
^Clanrat@firefly:~$ dig @archimedes.shmoo.com. -t NS shmoocon.org
;; communications error to 216.137.208.30#53: timed out
;; communications error to 216.137.208.30#53: timed out
;; communications error to 216.137.208.30#53: timed out

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @archimedes.shmoo.com. -t NS shmoocon.org
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

```
lanrat@firefly:~[130]$ host krusty.shmoo.com
krusty.shmoo.com has address 205.134.188.162
```

```
lanrat@firefly:~[130]$ host archimedes.shmoo.com.
archimedes.shmoo.com has address 216.137.208.30
```

```
lanrat@firefly:~$ whois 205.134.188.162 | grep -v \# | grep \.

NetRange:       205.134.160.0 - 205.134.191.255
CIDR:           205.134.160.0/19
NetName:        AINET-BLK
NetHandle:      NET-205-134-160-0-1
Parent:         NET205 (NET-205-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   American Information Network (AI)
RegDate:        1995-04-27
Updated:        1998-09-29
Ref:            https://rdap.arin.net/registry/ip/205.134.160.0
OrgName:        American Information Network
OrgId:          AI
Address:        11700 Montgomery Road
City:           Beltsville
StateProv:      MD
PostalCode:     20705
Country:        US
RegDate:        1995-04-27
Updated:        2016-06-07
Ref:            https://rdap.arin.net/registry/entity/AI
```

```
lanrat@firefly:~$ whois 216.137.208.30 |  grep -v \# | grep \. | head
NetRange:       216.137.192.0 - 216.137.255.255
CIDR:           216.137.192.0/18
NetName:        NET-216-137-192-0-1
NetHandle:      NET-216-137-192-0-1
Parent:         NET216 (NET-216-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS11090
Organization:   Matanuska Telecom Association, Incorporated (MTAONL)
RegDate:        2008-03-25
Updated:        2022-08-17
Ref:            https://rdap.arin.net/registry/ip/216.137.192.0
OrgName:        Matanuska Telecom Association, Incorporated
OrgId:          MTAONL
Address:        1740 S. Chugach
City:           Palmer
StateProv:      AK
PostalCode:     99645
Country:        US
RegDate:        1998-04-06
Updated:        2023-08-15
Ref:            https://rdap.arin.net/registry/entity/MTAONL
```

A note on ccTLDs

Demo Time!

FIN

https://github.com/lanrat/broken-dns
https://dns.coffee

ian@ian.do