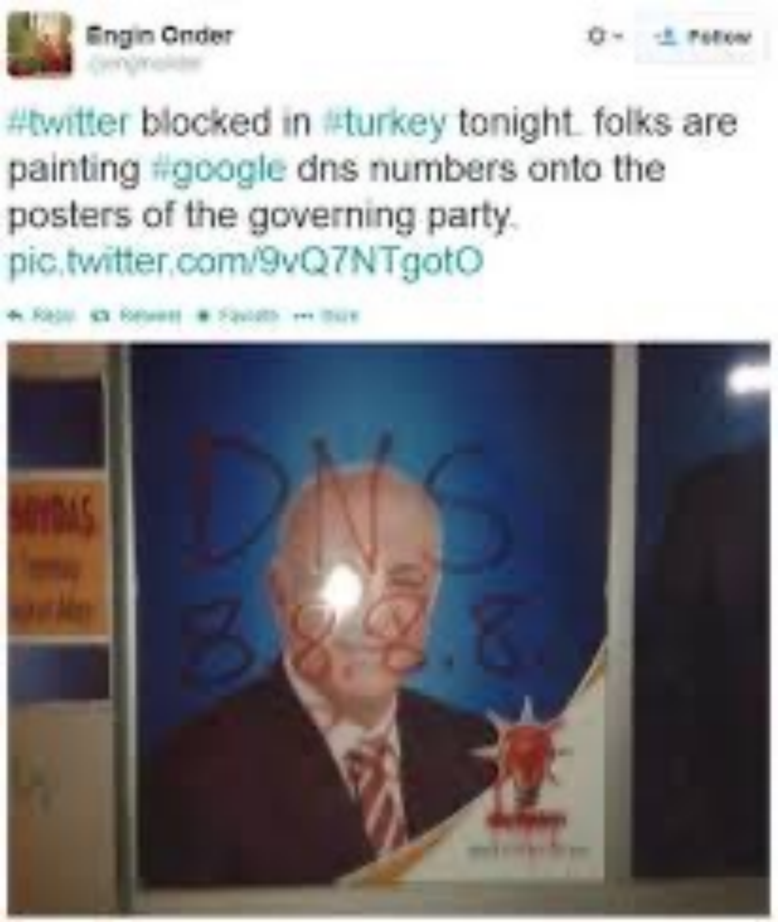
DNS SECURITY

VITALY SHMATIKOV

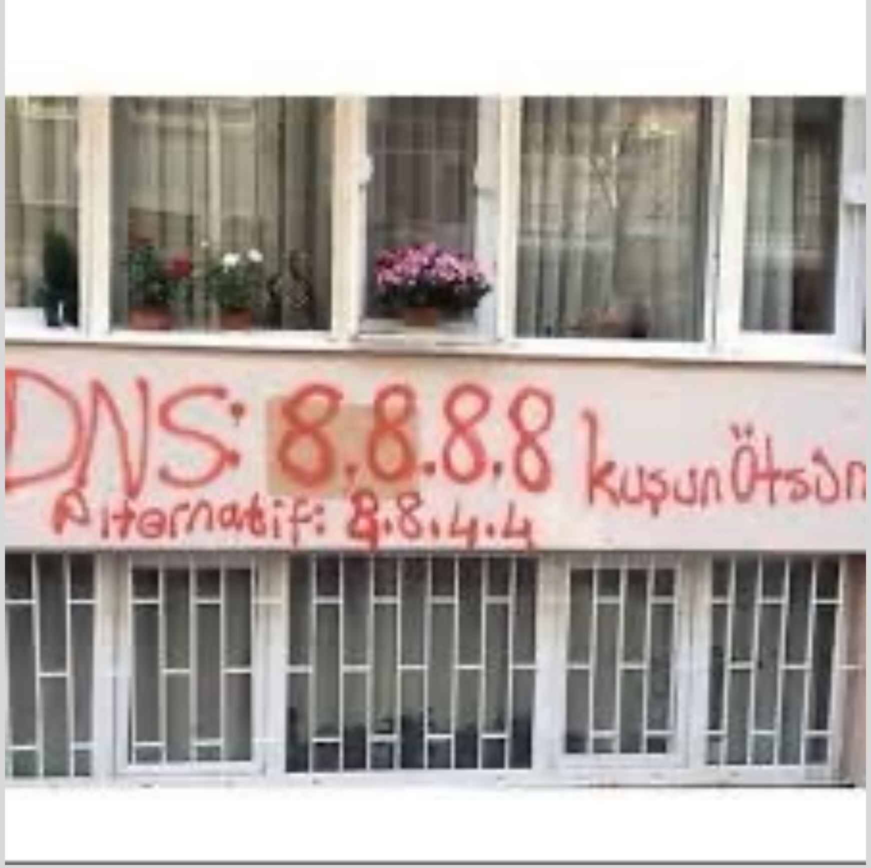
Turkey (2014)

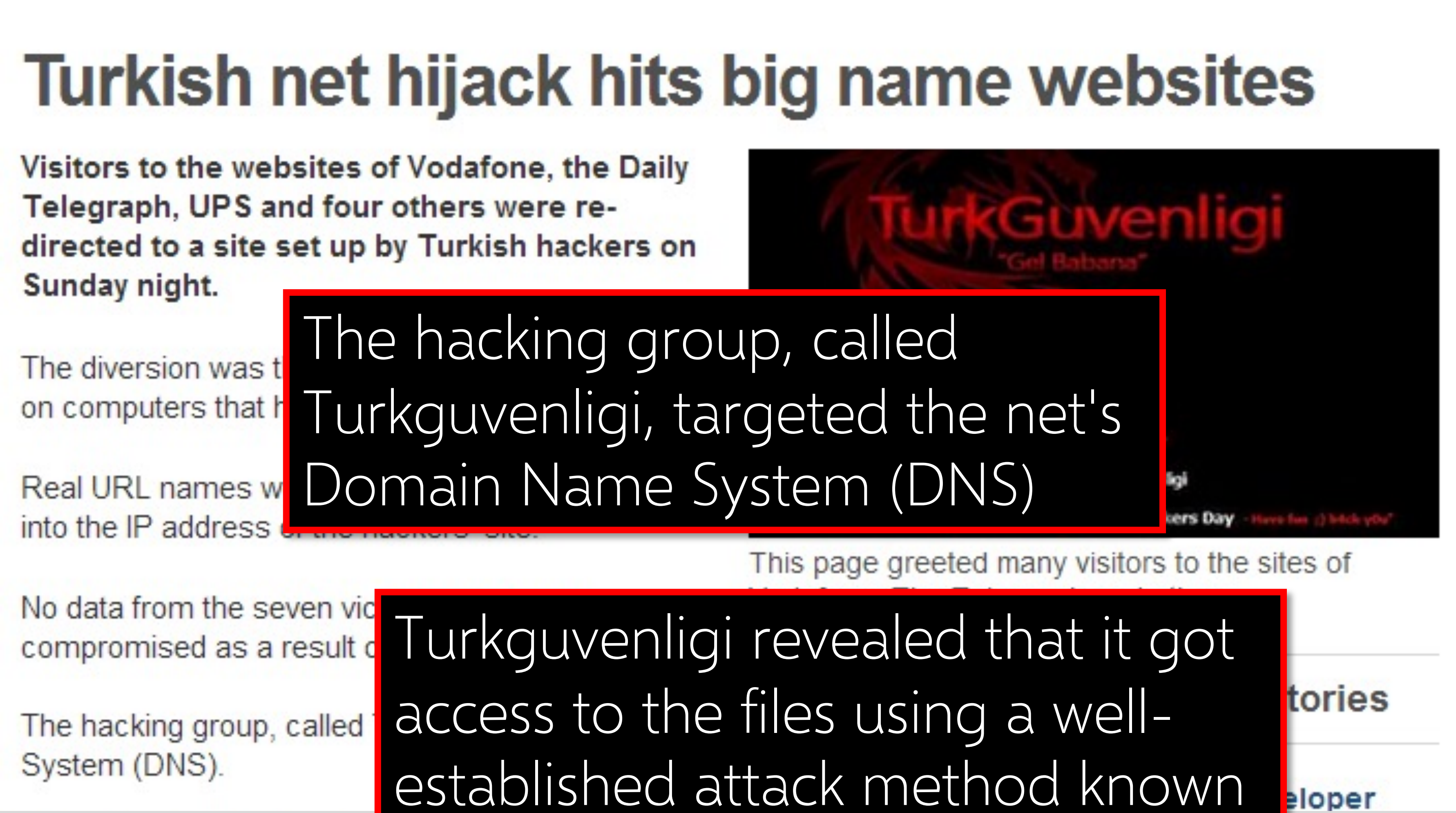


Engin Onder

@enginonder

#twitter blocked in #turkey tonight. folks are painting #google dns numbers onto the posters of the governing party. pic.twitter.com/9vQ7NTgotO





Turkish net hijack hits big name websites

Visitors to the websites of Vodafone, the Daily Telegraph, UPS and four others were re-directed to a site set up by Turkish hackers on Sunday night.

The diversion was t
on computers that h

Real URL names w
into the IP address o

No data from the seven vic
compromised as a result o

The hacking group, called
System (DNS).

This page greeted many visitors to the sites of

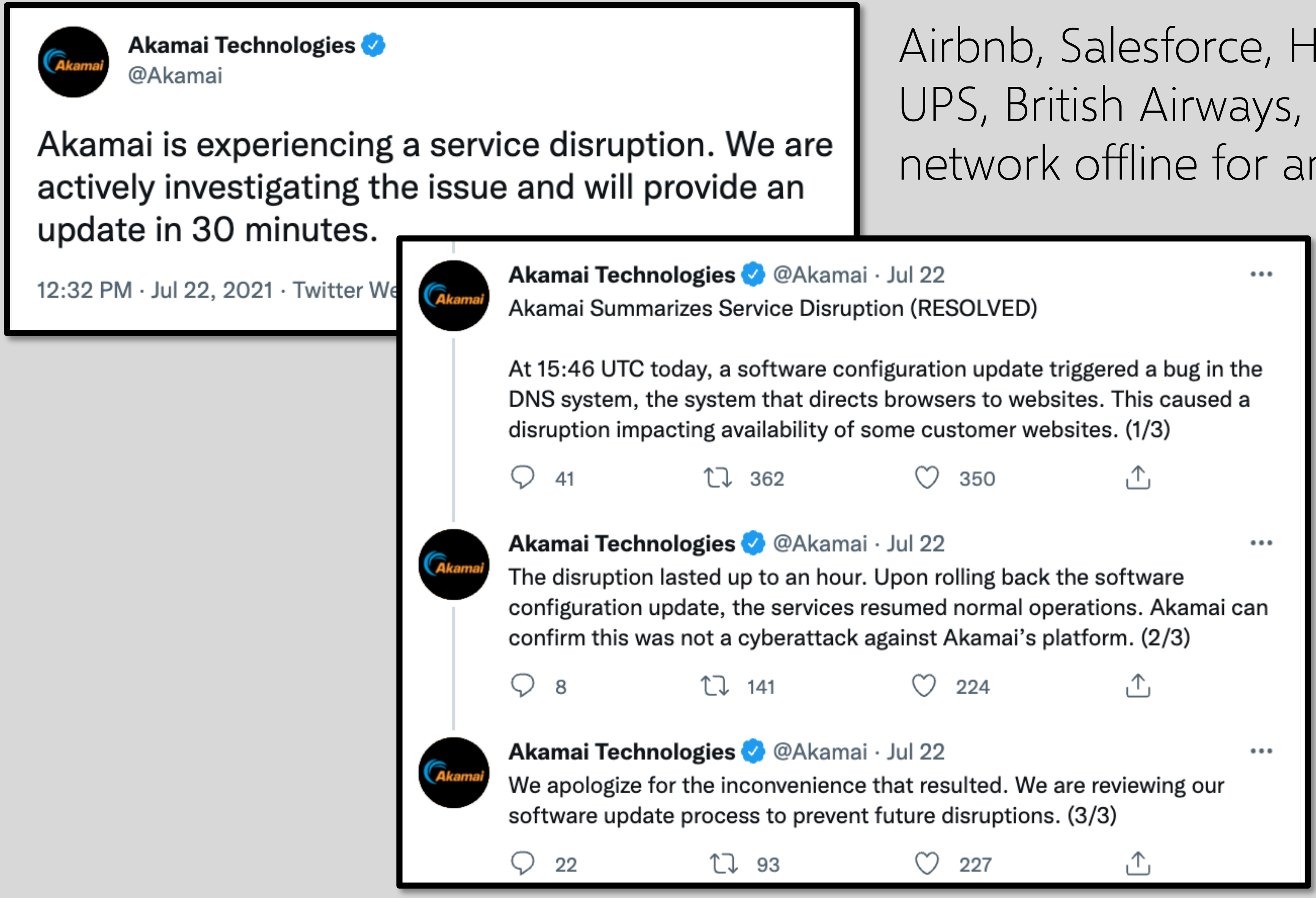
tories

eloper

The hacking group, called Turkguvenligi, targeted the net's Domain Name System (DNS)

Turkguvenligi revealed that it got access to the files using a well-established attack method known as SQL injection

Airbnb, Salesforce, Home Depot, UPS, British Airways, Sony PlayStation network offline for an hour



Akamai Technologies
@Akamai

Akamai is experiencing a service disruption. We are actively investigating the issue and will provide an update in 30 minutes.

12:32 PM · Jul 22, 2021 · Twitter We

Akamai Technologies @Akamai · Jul 22
Akamai Summarizes Service Disruption (RESOLVED)

At 15:46 UTC today, a software configuration update triggered a bug in the DNS system, the system that directs browsers to websites. This caused a disruption impacting availability of some customer websites. (1/3)

41 362 350

Akamai Technologies @Akamai · Jul 22
The disruption lasted up to an hour. Upon rolling back the software configuration update, the services resumed normal operations. Akamai can confirm this was not a cyberattack against Akamai's platform. (2/3)

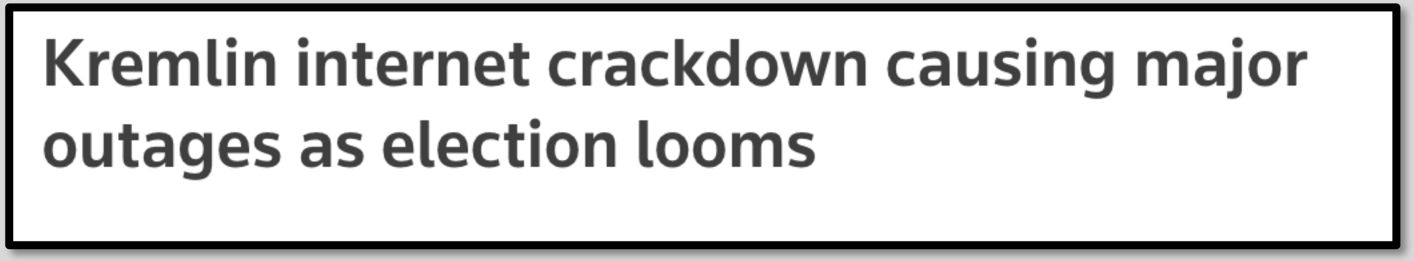
8 141 224

Akamai Technologies @Akamai · Jul 22
We apologize for the inconvenience that resulted. We are reviewing our software update process to prevent future disruptions. (3/3)

22 93 227

Not a security issue, apparently…

September 10, 2021



Kremlin internet crackdown causing major outages as election looms

There had been widespread disruption after Roskomnadzor blocked widely-used internet services in its bid to prevent access to a banned app backed by Navalny’s allies…

Roskomnadzor blocked Google and cybersecurity firm Cloudflare’s domain name system (DNS) services, which computers use to match website addresses with the correct servers.

https://www.reuters.com/article/us-russia-politics-internet-idCAKBN2G61MA

DNS Hostname vs. IP Address

DNS hostname (e.g., www.cs.cornell.edu)

- Mnemonic name understood by humans
- Variable length, full alphabet of characters
- Provides little (if any) information about location

IP address (e.g., 128.84.202.53)

- Numerical address understood by routers
- Fixed length, decimal number
- Hierarchical address space, related to host location

Uses of DNS

Hostname to IP address translation

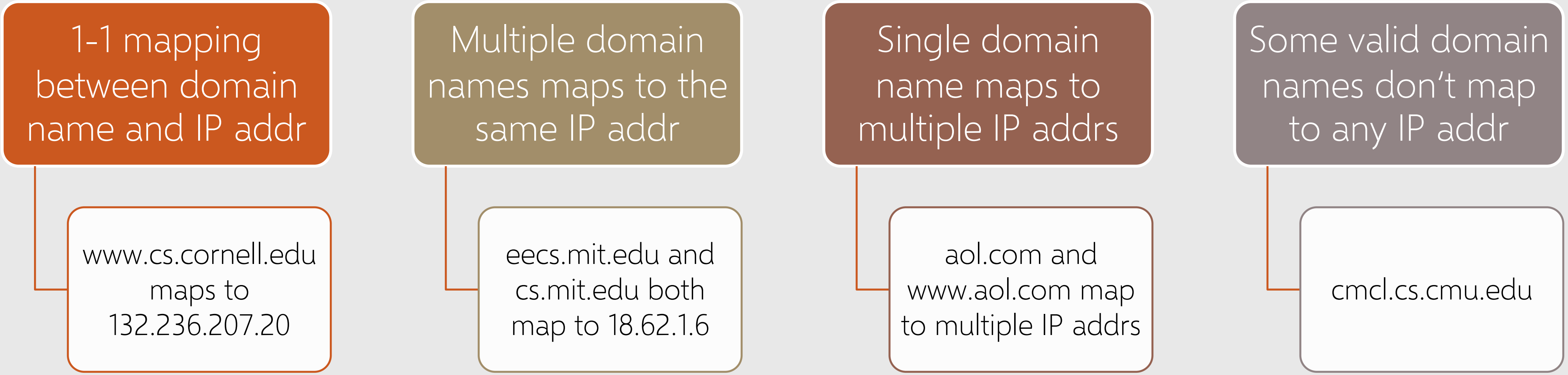
- Reverse lookup: IP address to hostname translation

Host name aliasing: other DNS names for a host

- Alias hostnames point to canonical hostname

Email: look up domain’s mail server by domain name

Different DNS Mappings



1-1 mapping between domain name and IP addr

www.cs.cornell.edu maps to 132.236.207.20

Multiple domain names maps to the same IP addr

eecs.mit.edu and cs.mit.edu both map to 18.62.1.6

Single domain name maps to multiple IP addrs

aol.com and www.aol.com map to multiple IP addrs

Some valid domain names don’t map to any IP addr

cmcl.cs.cmu.edu

Goals of DNS

A wide-area distributed database

Possibly biggest such database in the world!

Goals

- Scalability; decentralized maintenance
- Robustness
- Global scope
- Names mean the same thing everywhere
- Distributed updates/queries
- Good performance

DNS Structure

Hierarchical name space divided into contiguous sections called zones

- Zones are distributed over a collection of DNS servers

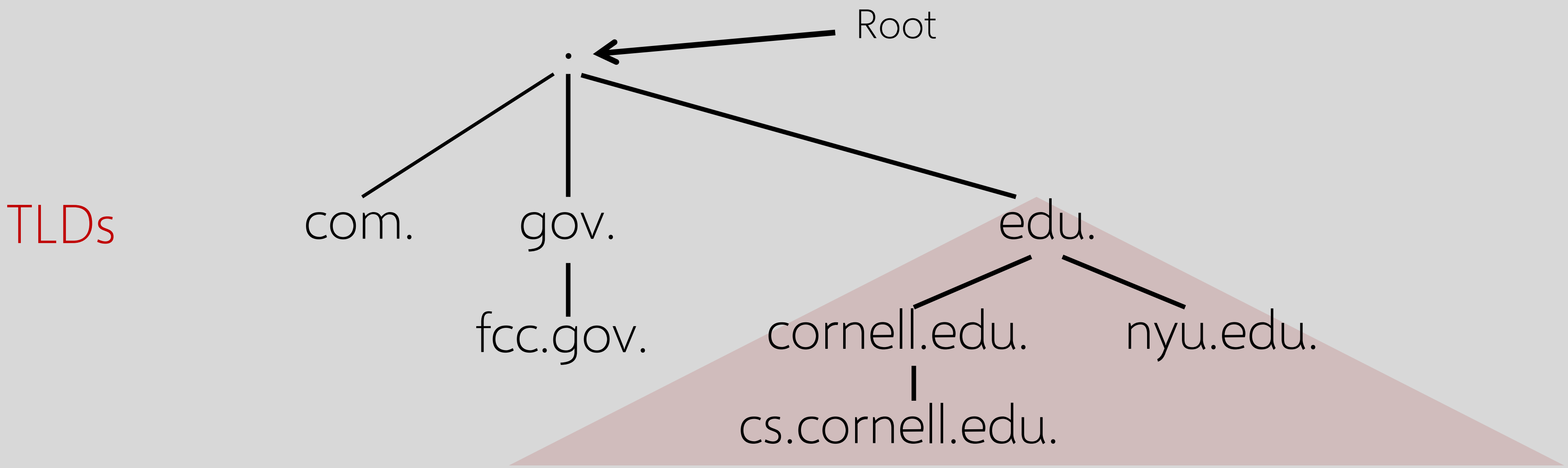
Hierarchy of DNS servers

- Root servers (identity hardwired into other servers)
- Top-level domain (TLD) servers
- Authoritative DNS servers

Performing the translations

- Local DNS servers located near clients
- Resolver software running on clients

Hierarchical Structure of DNS



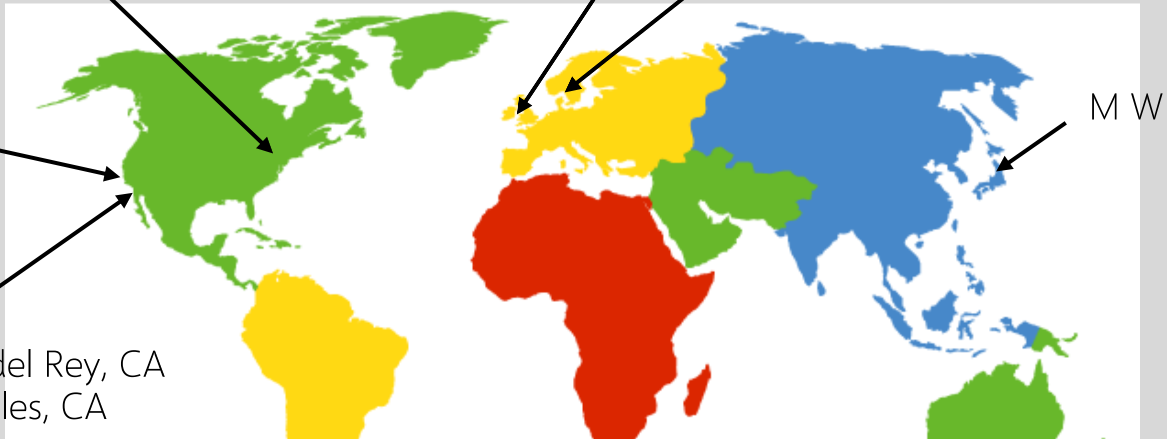
Hierarchy of namespace matches hierarchy of servers

Set of nameservers answers queries for names within zone

Nameservers store names and links to other servers in tree

13 DNS Root Nameservers

Feb 6, 2007: Botnet DoS attack on root DNS servers



A Verisign, Dulles, VA
C Cogent, Herndon, VA
D U Maryland College Park, MD
G US DoD Vienna, VA
H ARL Aberdeen, MD
J Verisign

K RIPE, London

I Autonomica, Stockholm

E NASA Mt View, CA
F Internet Software
Consortium,
Palo Alto, CA

M WIDE Tokyo

B USC-ISI Marina del Rey, CA
L ICANN Los Angeles, CA

Each server is really a cluster of servers (some distributed over a small geographical region), replicated via IP anycast which routes DNS queries to any server in that cluster of servers, to spread the load

TLD and Authoritative Servers

Top-level domain (TLD) servers

- Responsible for com, org, net, edu, etc, and all top-level country domains: uk, fr, ca, jp
- Network Solutions maintains servers for .com TLD
- Educause (non-profit) for .edu TLD

Authoritative DNS servers

- An organization's DNS servers, providing authoritative information for that organization
- May be maintained by organization itself or ISP

Local Name Servers

- Each ISP (or company, or university) has one
  - No strict hierarchy
- Also called default or caching name server

When a host makes DNS query, query is sent to its local DNS server, which acts as proxy and forwards the query into the hierarchy

DNS Resource Records

DNS is a distributed database storing resource records.
A resource record includes (name, type, value, time-to-live).

Type = A (address)

- name = hostname
- value = IP address

Type = NS (name server)

- name = domain (e.g. cornell.edu)
- value = hostname of authoritative name server for this domain

Type = CNAME

- name = alias for some "canonical" (real) name
- value = canonical name

Type = MX (mail exchange)

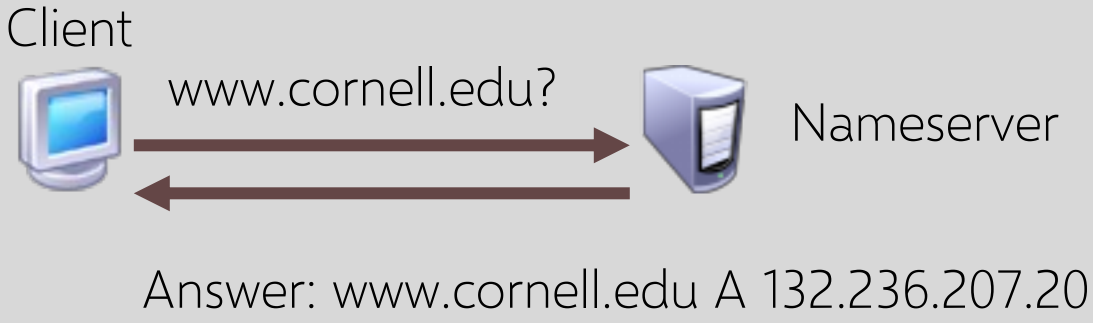
- name = domain
- value = name of mail server for that domain

Most queries and responses are UDP datagrams

DNS in Operation

Recursive

- Nameserver responds with answer or error



Client

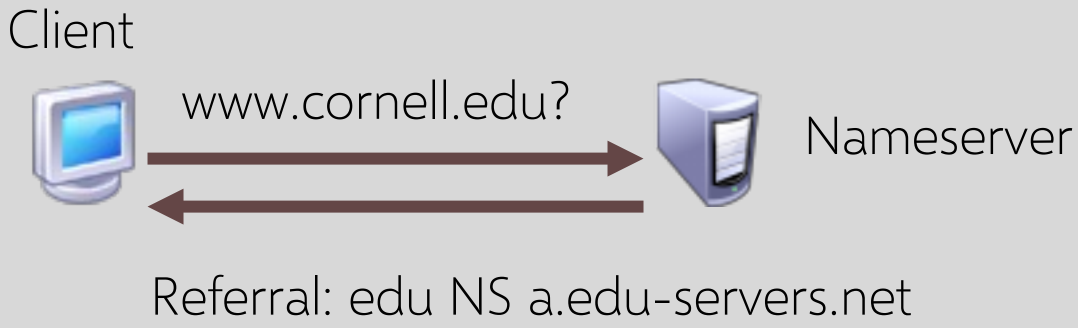
www.cornell.edu?

Nameserver

Answer: www.cornell.edu A 132.236.207.20

Iterative

- Nameserver may respond with a referral



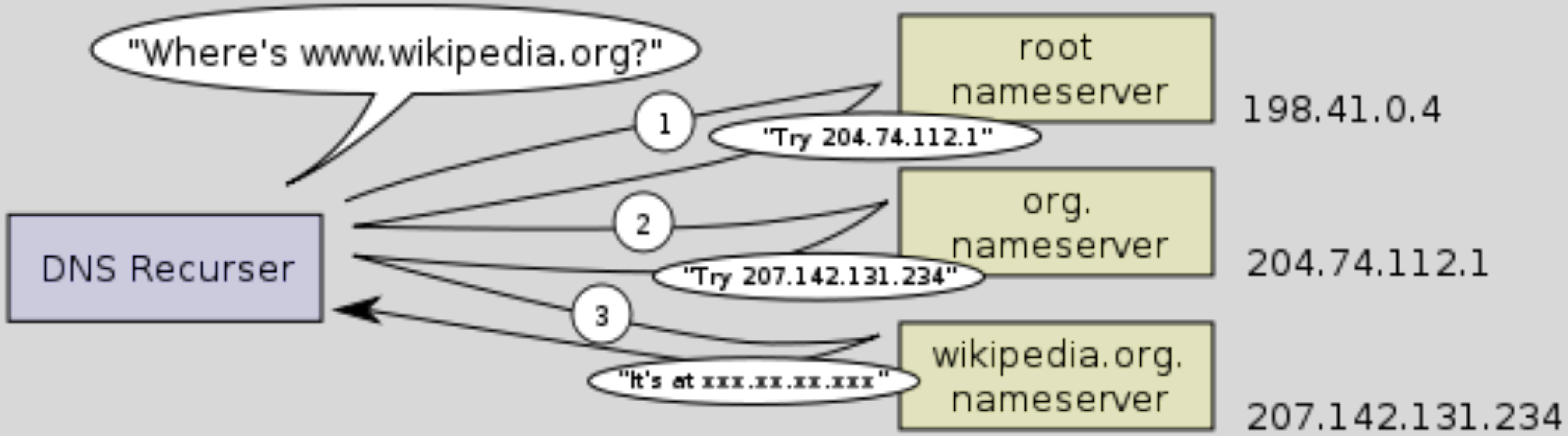
Client

www.cornell.edu?

Nameserver

Referral: edu NS a.edu-servers.net

Resolving Names



http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

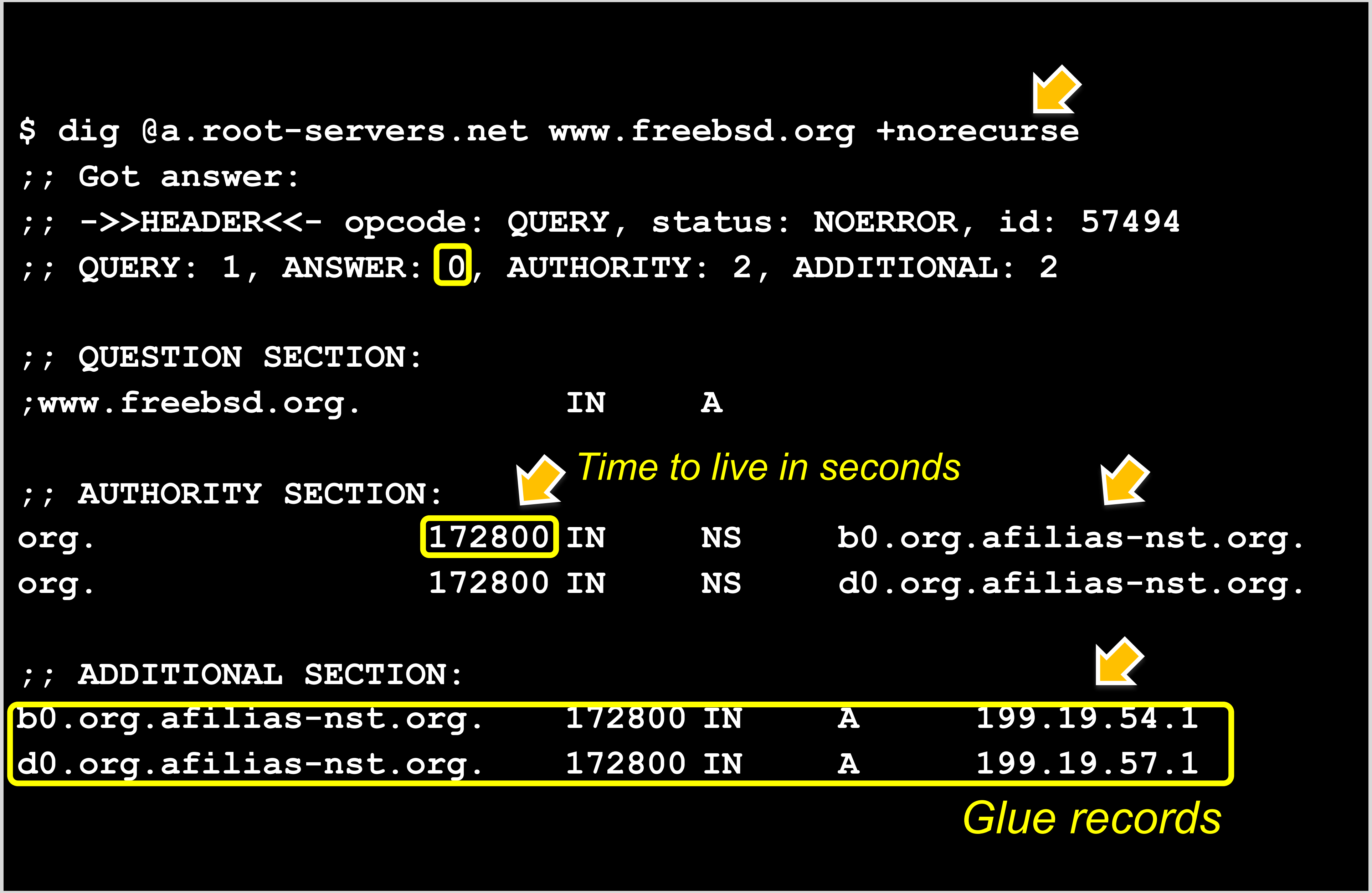
Recursive vs. Iterative Queries

Recursive

- Less burden on query initiator
- More burden on nameserver
  - Has to return an answer
- Most root and TLD servers won’t answer (shed load)
- Local name server answers recursive query

Iterative

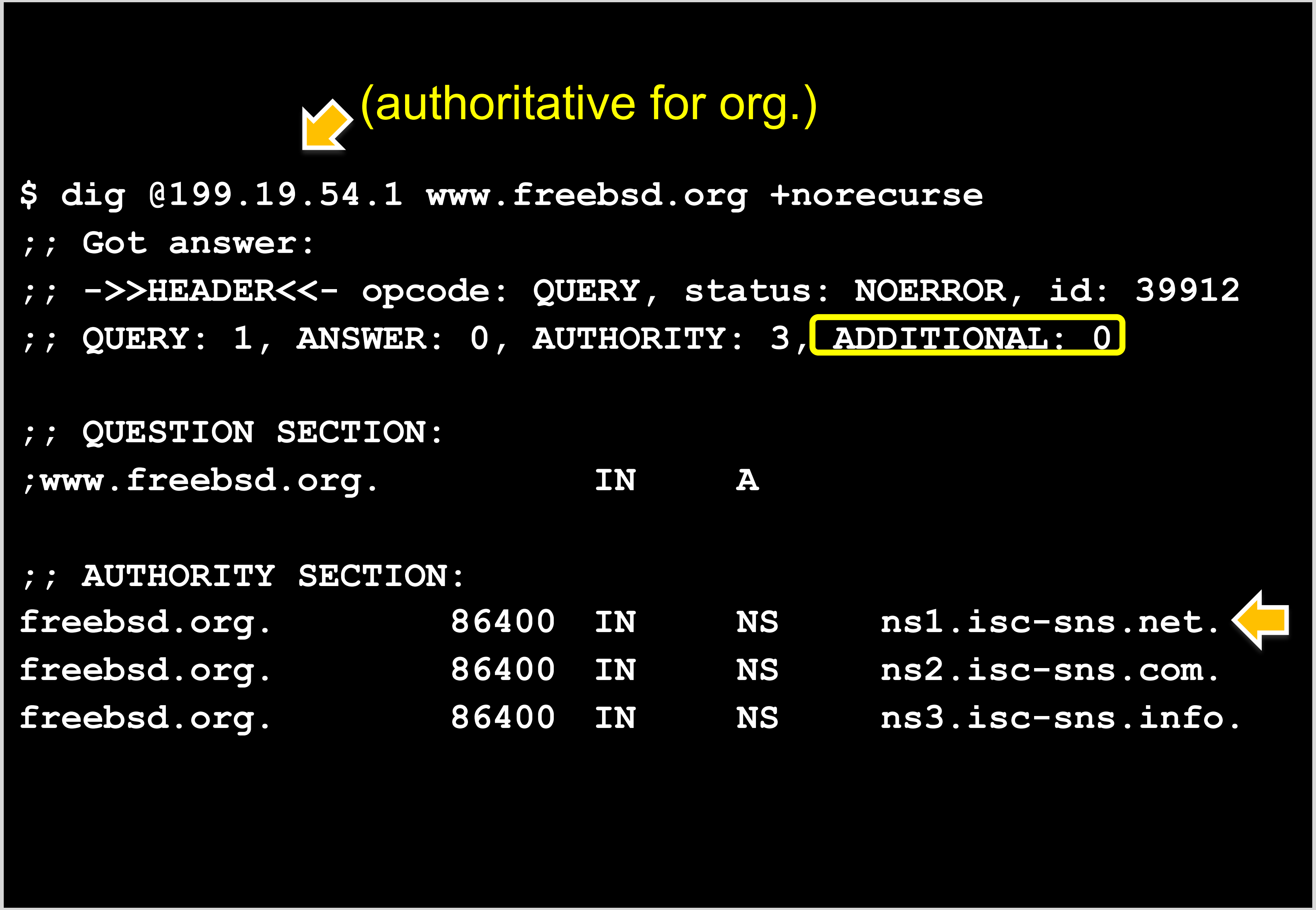
- More burden on query initiator
- Less burden on nameserver
  - Refers query to another nameserver



```
$ dig @a.root-servers.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57494
;; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.freebsd.org.               IN      A

;; AUTHORITY SECTION:
org.                    172800 IN      NS      b0.org.afilias-nst.org.
org.                    172800 IN      NS      d0.org.afilias-nst.org.

;; ADDITIONAL SECTION:
b0.org.afilias-nst.org. 172800 IN      A       199.19.54.1
d0.org.afilias-nst.org. 172800 IN      A       199.19.57.1
```

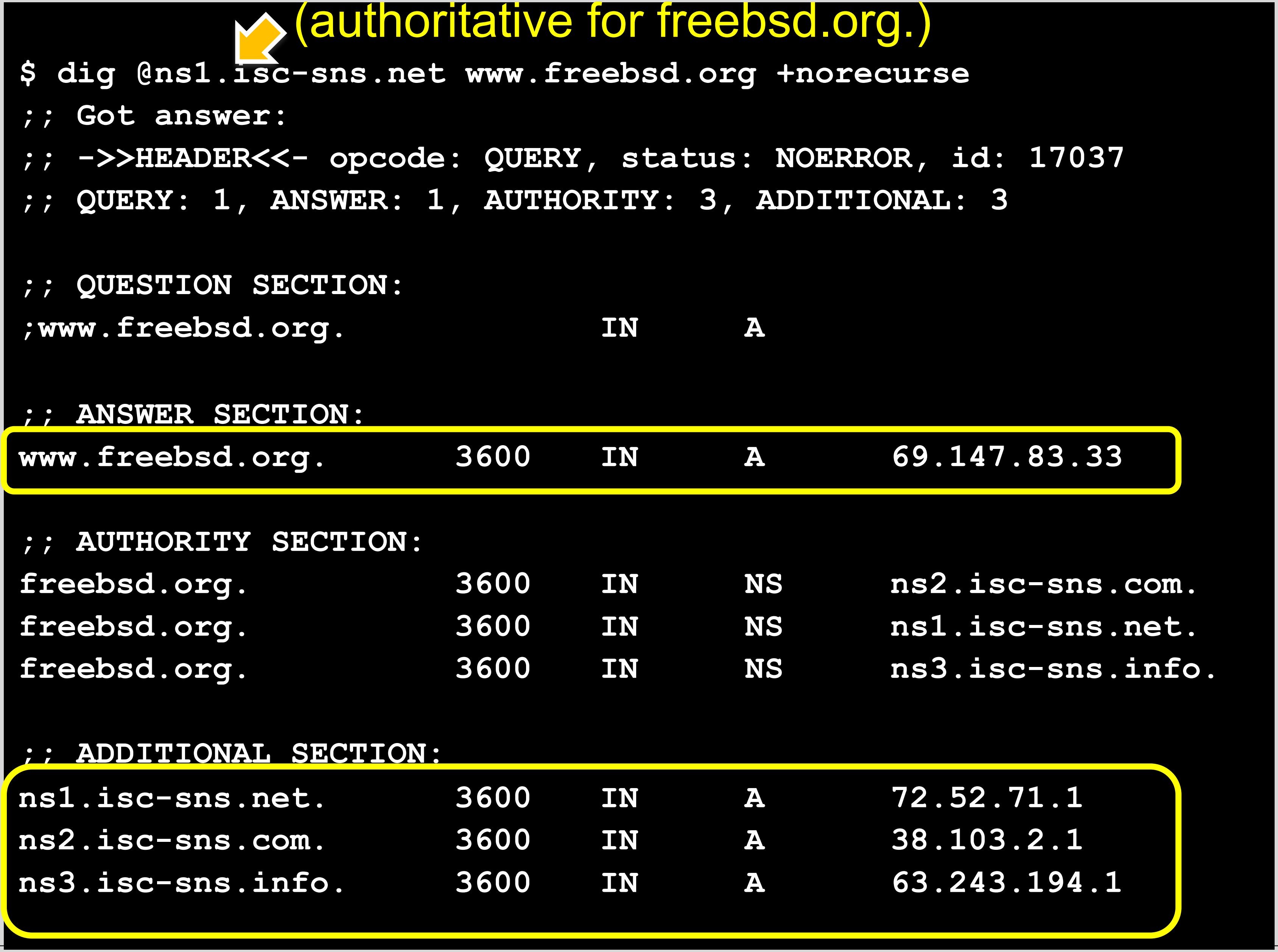
Time to live in seconds

Glue records



(authoritative for org.)

```
$ dig @199.19.54.1 www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39912
;; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.freebsd.org.          IN      A

;; AUTHORITY SECTION:
freebsd.org.        86400  IN      NS      ns1.isc-sns.net.
freebsd.org.        86400  IN      NS      ns2.isc-sns.com.
freebsd.org.        86400  IN      NS      ns3.isc-sns.info.
```

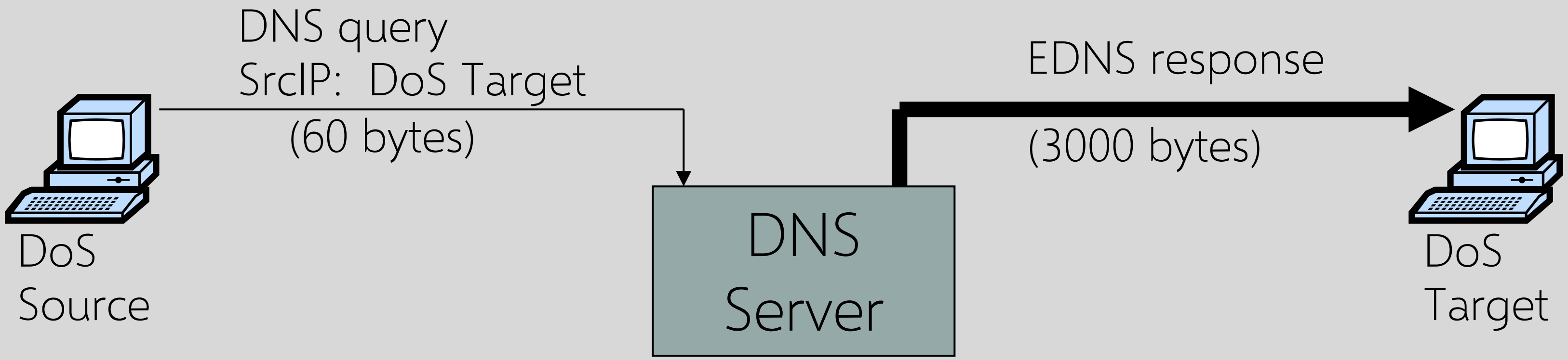


(authoritative for freebsd.org.)

```
$ dig @ns1.isc-sns.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17037
;; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.freebsd.org.              IN      A

;; ANSWER SECTION:
www.freebsd.org.       3600    IN      A       69.147.83.33

;; AUTHORITY SECTION:
freebsd.org.           3600    IN      NS      ns2.isc-sns.com.
freebsd.org.           3600    IN      NS      ns1.isc-sns.net.
freebsd.org.           3600    IN      NS      ns3.isc-sns.info.

;; ADDITIONAL SECTION:
ns1.isc-sns.net.       3600    IN      A       72.52.71.1
ns2.isc-sns.com.       3600    IN      A       38.103.2.1
ns3.isc-sns.info.      3600    IN      A       63.243.194.1
```

DNS Amplification Attack

x50 amplification



DNS query
SrcIP: DoS Target
(60 bytes)

EDNS response
(3000 bytes)

2006: 0.58M open resolvers on Internet (Kaminsky-Shiffman)
2013: 21.7M open resolvers (openresolverproject.org)

March 2013: 300 Gbps DDoS attack on Spamhaus

Sven Olaf Kamphuis and his "mobile computing office"

DNS Caching

Performing all these queries takes time

- … before actual communication takes place

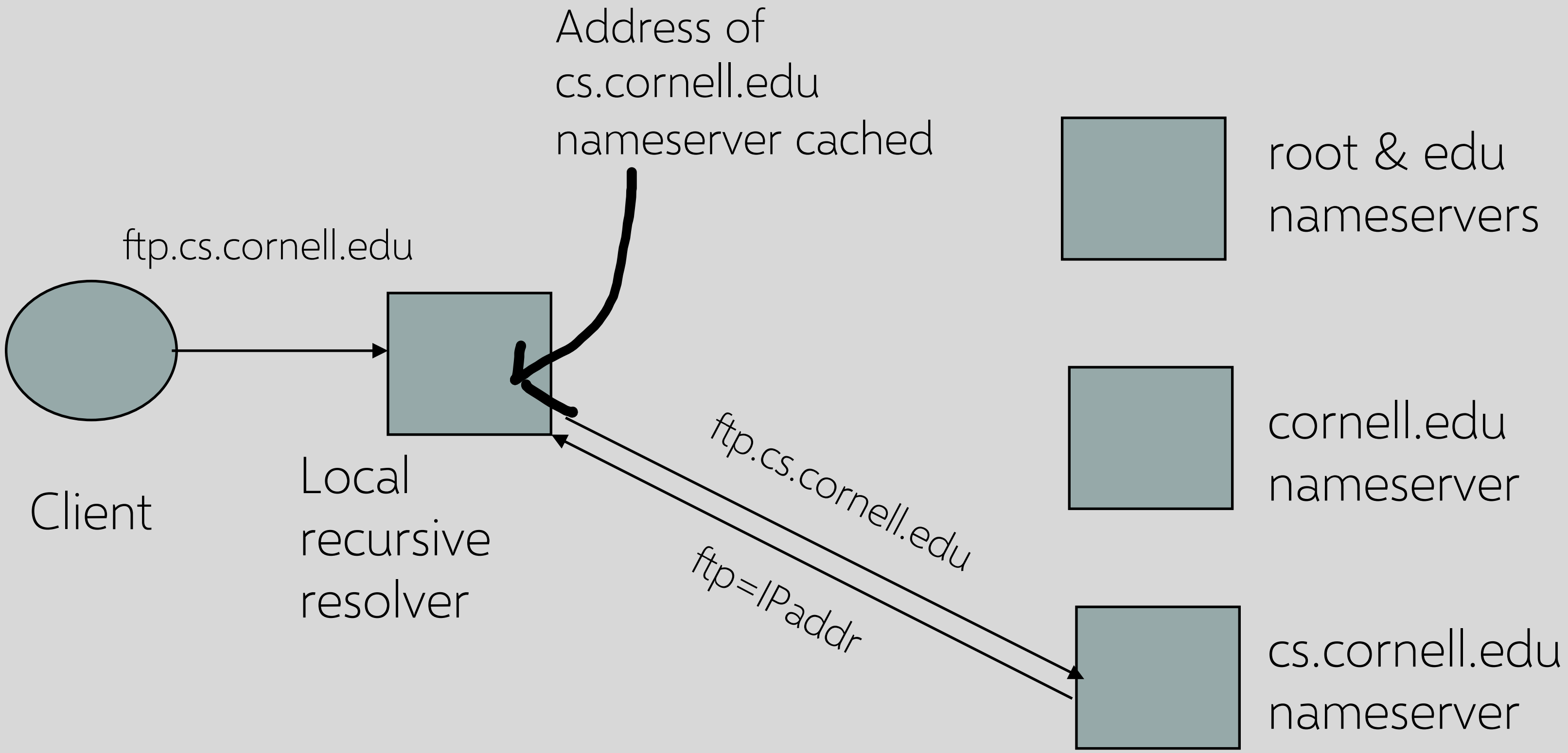
Caching can greatly reduce overhead

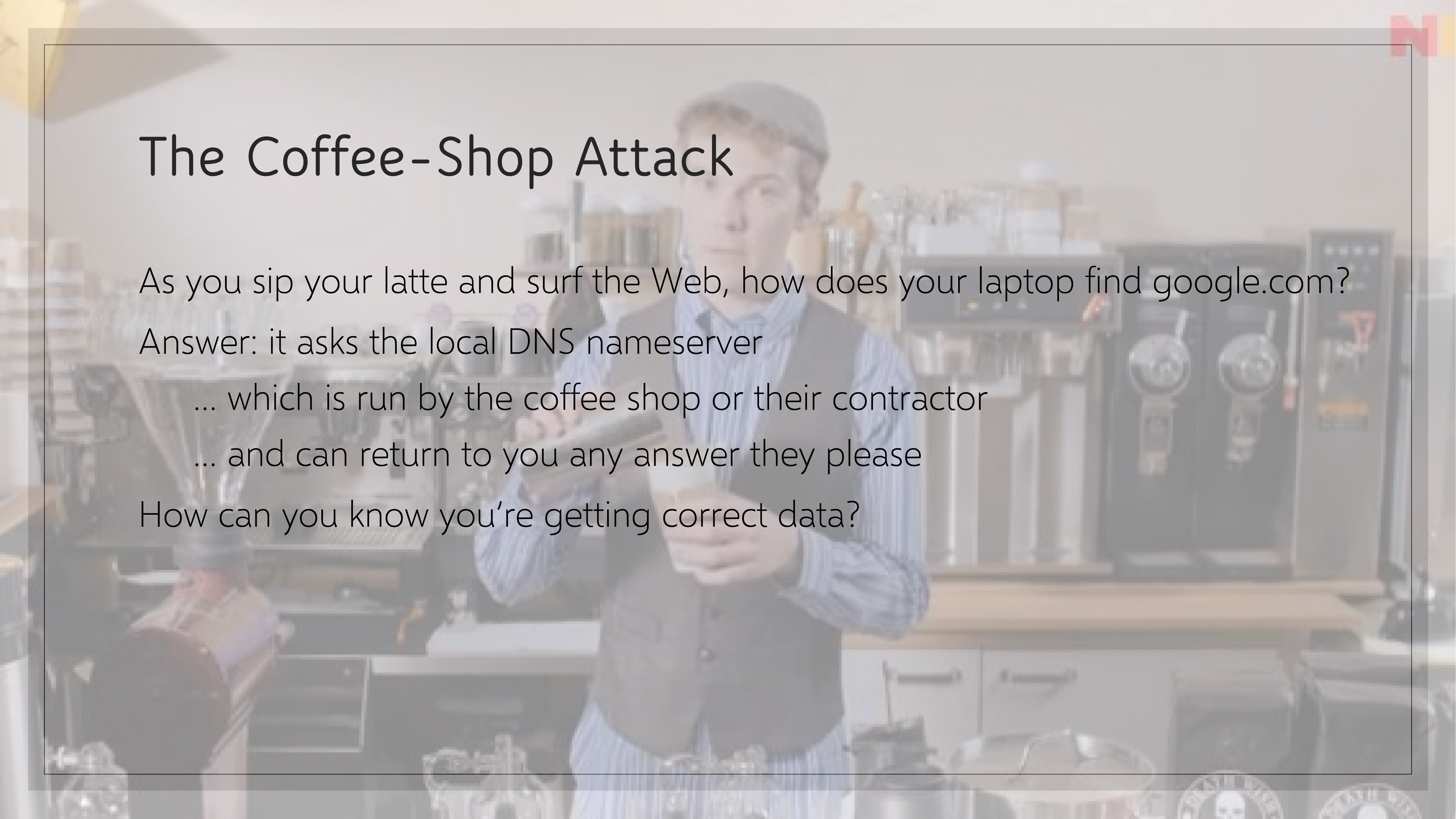
- Top-level servers very rarely change
- Popular sites visited often

How DNS caching works

- All DNS servers cache responses to queries
  - Including negative responses (e.g., misspellings)
- Responses include a time-to-live (TTL) field
- Server deletes cached entry after TTL expires

Cached Lookup Example





The Coffee-Shop Attack

As you sip your latte and surf the Web, how does your laptop find google.com?

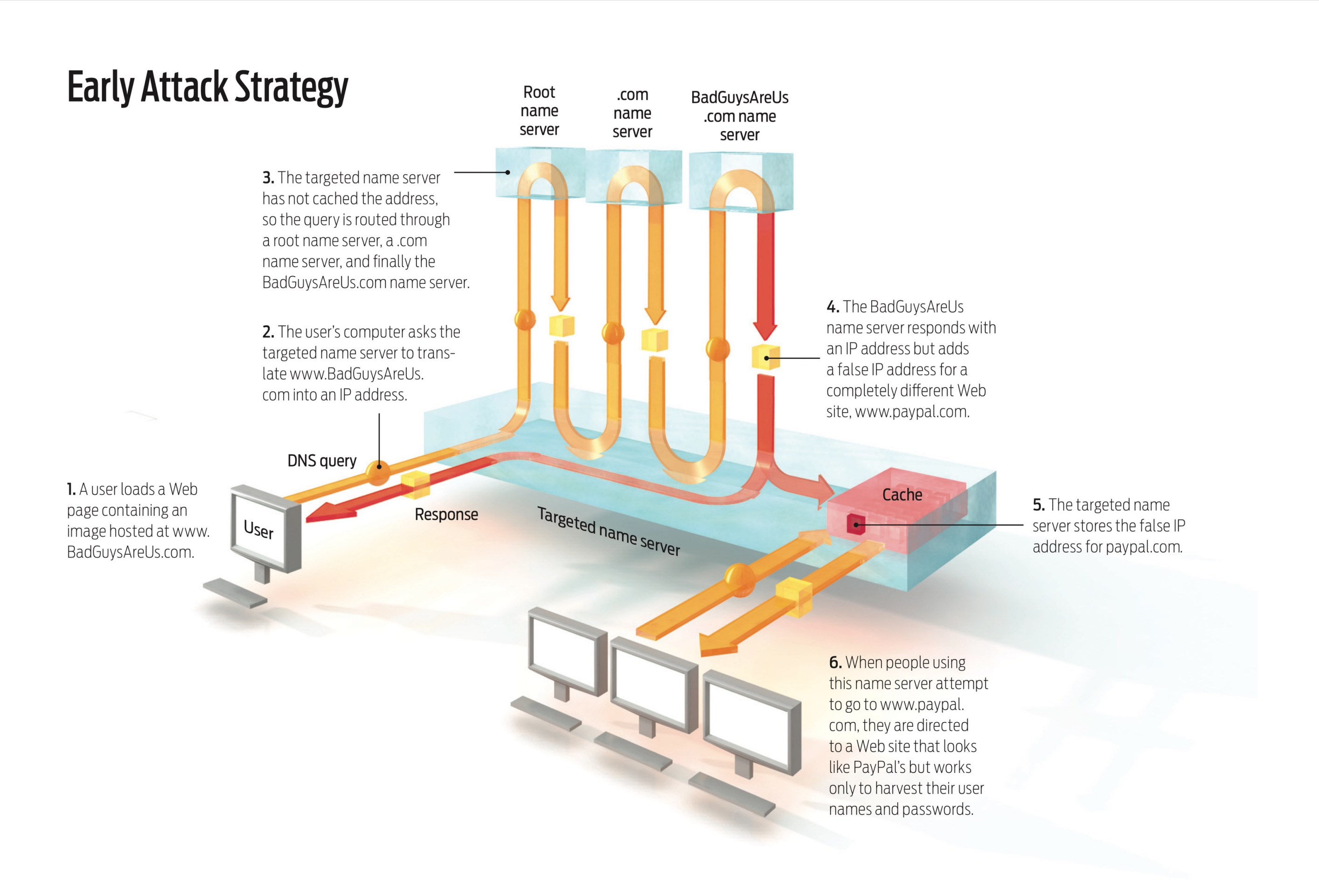
Answer: it asks the local DNS nameserver

… which is run by the coffee shop or their contractor

… and can return to you any answer they please

How can you know you're getting correct data?

DNS Cache Poisoning



Early Attack Strategy

1. A user loads a Web page containing an image hosted at www.BadGuysAreUs.com.

2. The user's computer asks the targeted name server to translate www.BadGuysAreUs.com into an IP address.

3. The targeted name server has not cached the address, so the query is routed through a root name server, a .com name server, and finally the BadGuysAreUs.com name server.

4. The BadGuysAreUs name server responds with an IP address but adds a false IP address for a completely different Web site, www.paypal.com.

5. The targeted name server stores the false IP address for paypal.com.

6. When people using this name server attempt to go to www.paypal.com, they are directed to a Web site that looks like PayPal's but works only to harvest their user names and passwords.

What if DNS Is Subverted?

Redirect victim’s web traffic to rogue servers

Redirect victim’s email to rogue email servers (MX records in DNS)

Does TLS/SSL provide protection?

- Yes—user will get “wrong certificate” if SSL enabled
- No—SSL not enabled or user ignores warnings
- No—how is SSL trust established? Often, by email!

Pharming

Many anti-phishing defenses rely on DNS

Can bypass them by poisoning DNS cache and/or forging DNS responses

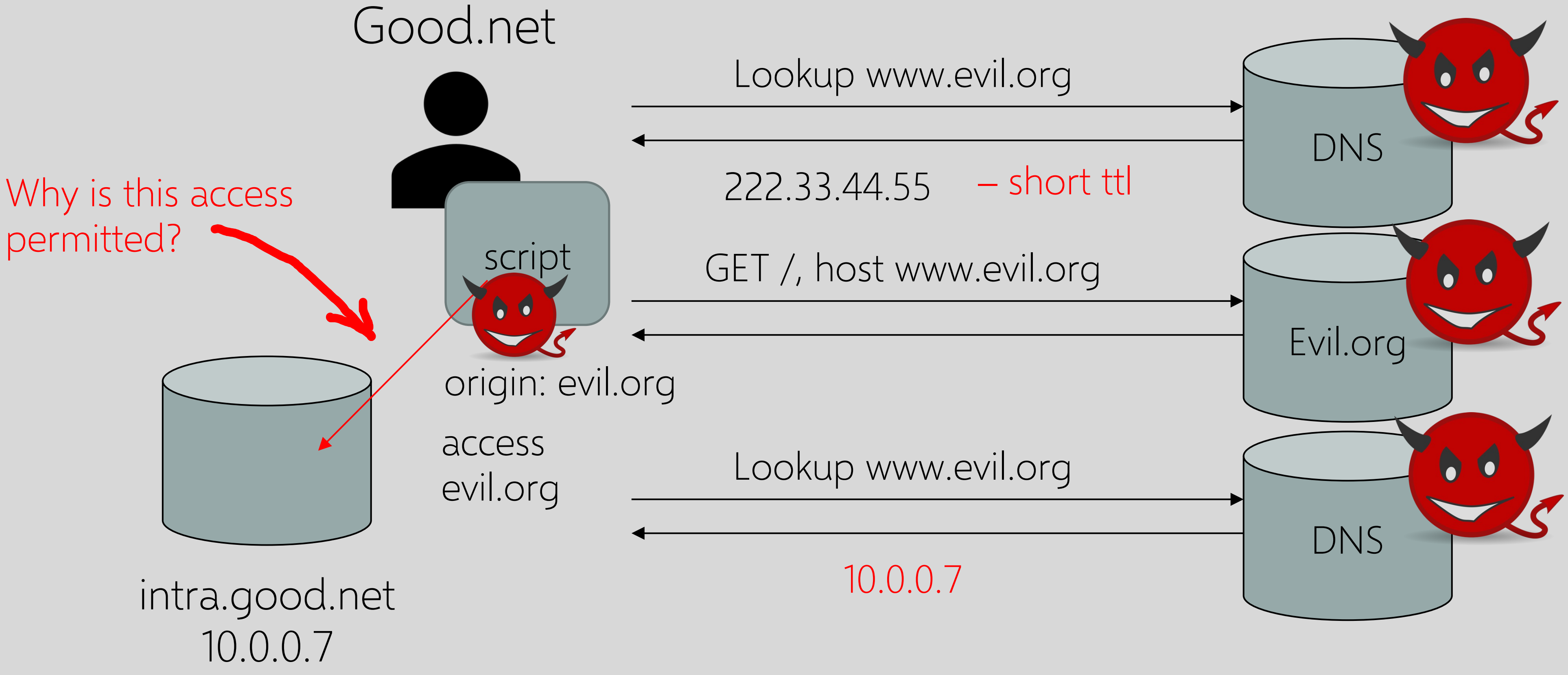
- Browser: “give me the address of www.paypal.com”
- Attacker: “sure, it’s 6.6.6.6” (attacker-controlled site)

Dynamic pharming / DNS rebinding

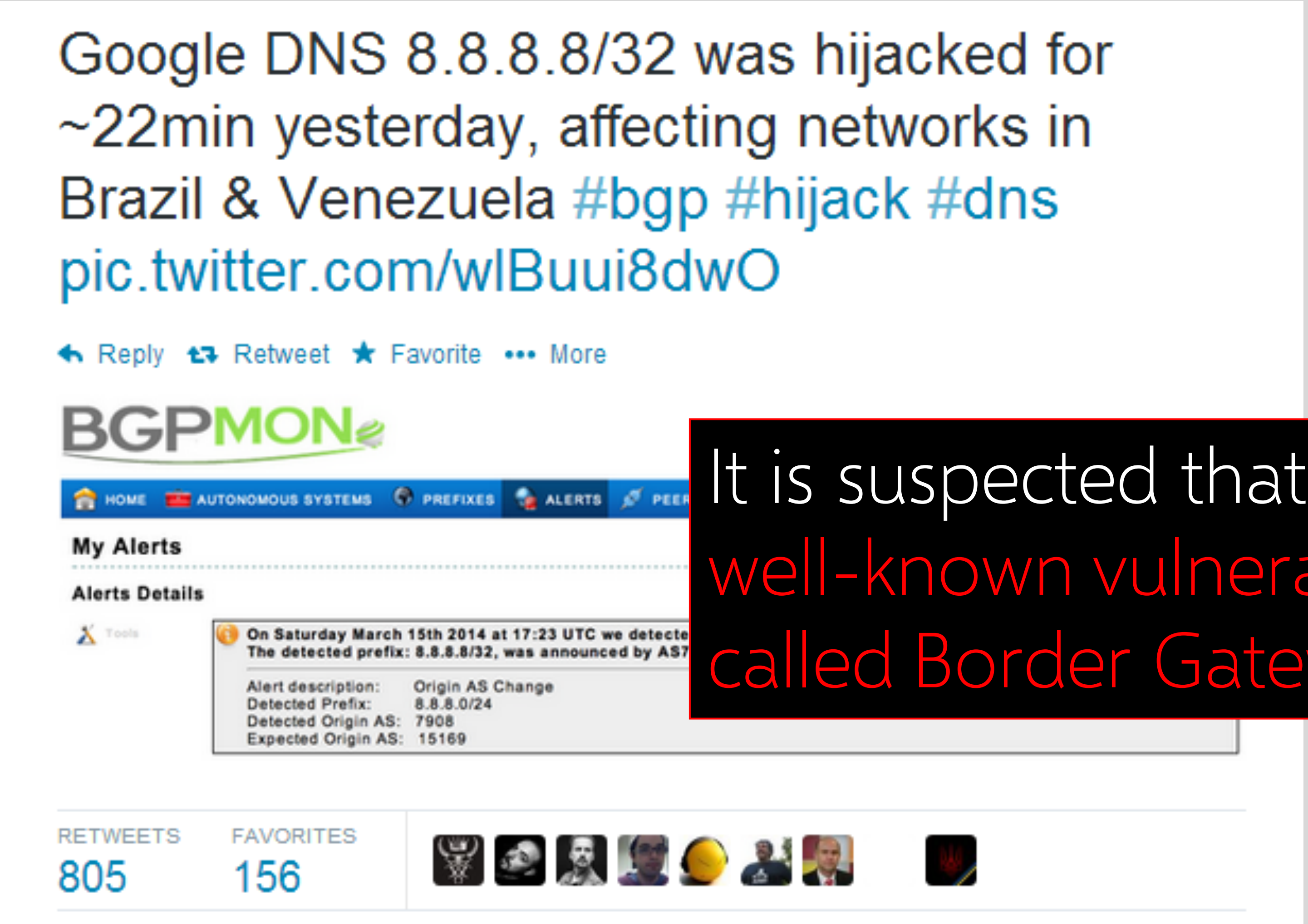
- Provide bogus DNS mapping for a trusted server, trick user into downloading a malicious script
- Force user to download content from the real server, temporarily provide correct DNS mapping
- Malicious script and content have the same origin!

Why?

DNS Rebinding for an Intranet Attack



March 16, 2014



Google DNS 8.8.8.8/32 was hijacked for ~22min yesterday, affecting networks in Brazil & Venezuela #bgp #hijack #dns pic.twitter.com/wIBuui8dwO

My Alerts

Alerts Details

On Saturday March 15th 2014 at 17:23 UTC we detecte
The detected prefix: 8.8.8.8/32, was announced by AS7

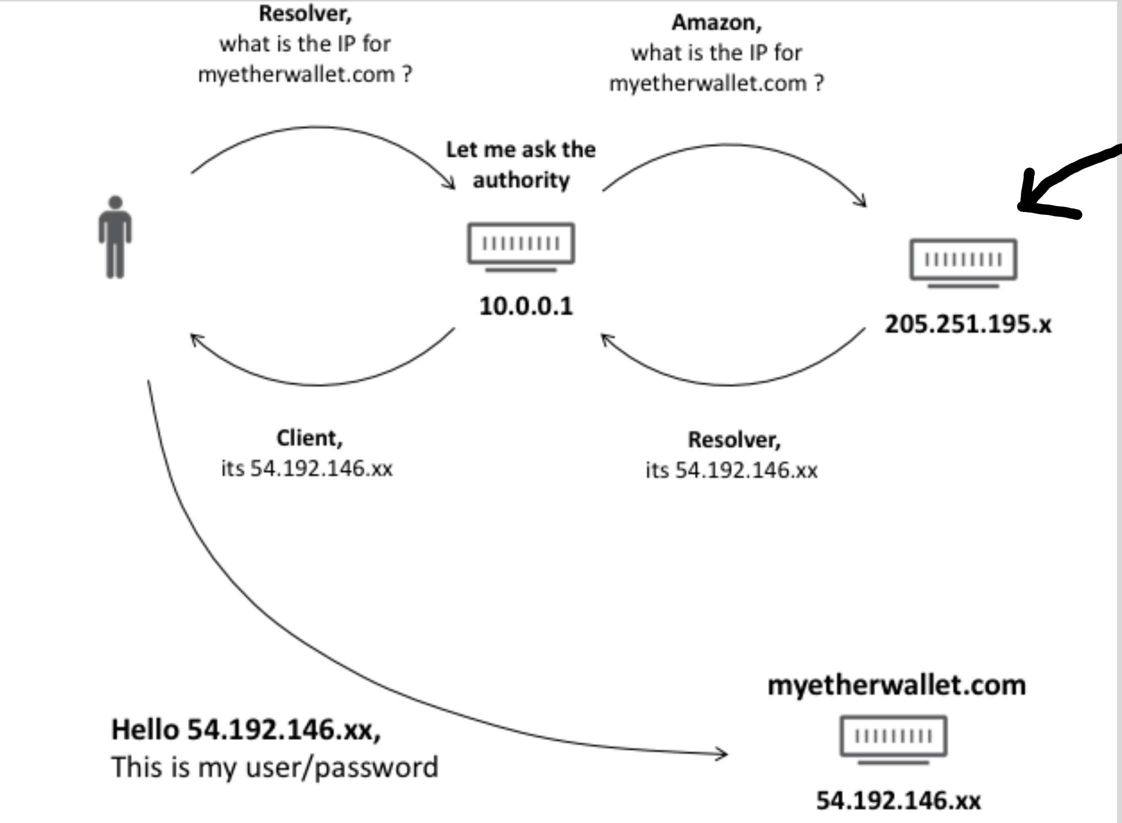
```
Alert description:     Origin AS Change
Detected Prefix:       8.8.8.0/24
Detected Origin AS:    7908
Expected Origin AS:    15169
```

RETWEETS 805

FAVORITES 156

It is suspected that hackers exploited a well-known vulnerability in the so-called Border Gateway Protocol (BGP)

Amazon DNS Hijack via BGP Hijack (2018)

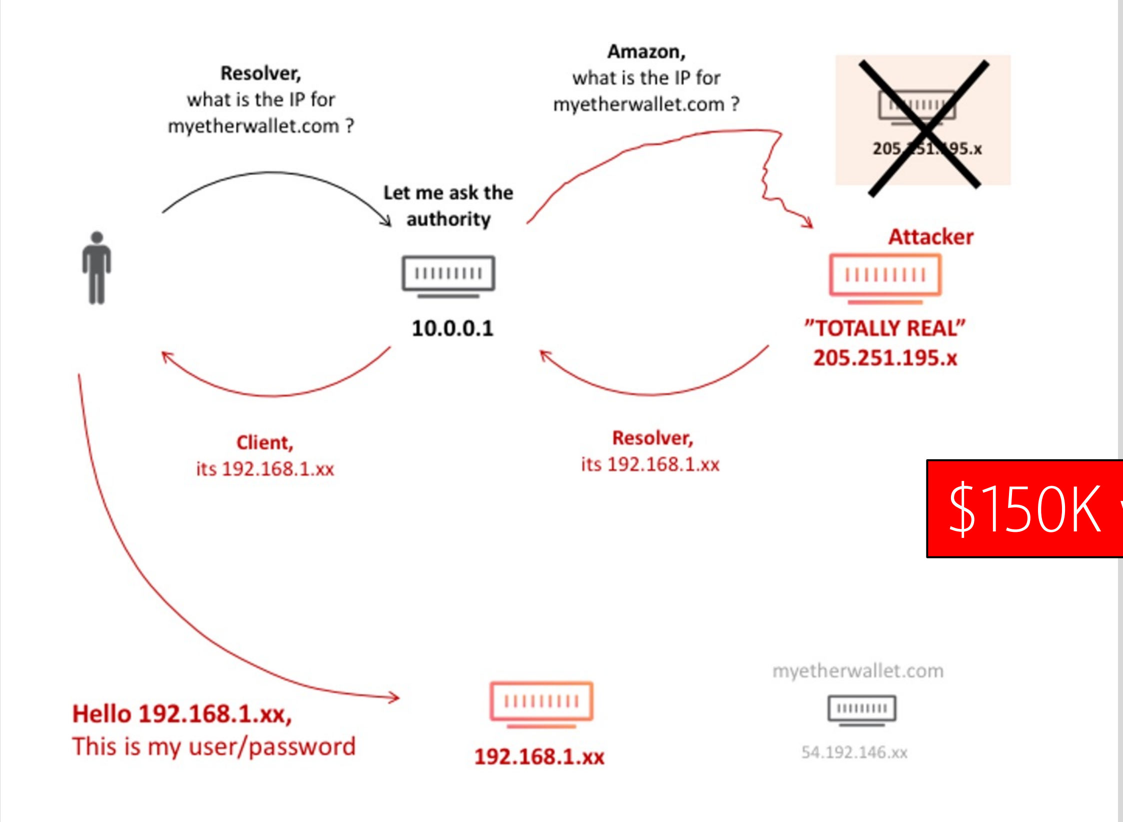


This IP space is allocated to Amazon

Instead, routes to it were announced by eNet and forwarded to Hurricane Electric

https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/

Amazon DNS Hijack via BGP Hijack (2018)



Resolver,
what is the IP for
myetherwallet.com ?

Let me ask the authority

10.0.0.1

Amazon,
what is the IP for
myetherwallet.com ?

~~205.251.195.x~~

Attacker

"TOTALLY REAL"
205.251.195.x

Client,
its 192.168.1.xx

Resolver,
its 192.168.1.xx

Hello 192.168.1.xx,
This is my user/password

192.168.1.xx

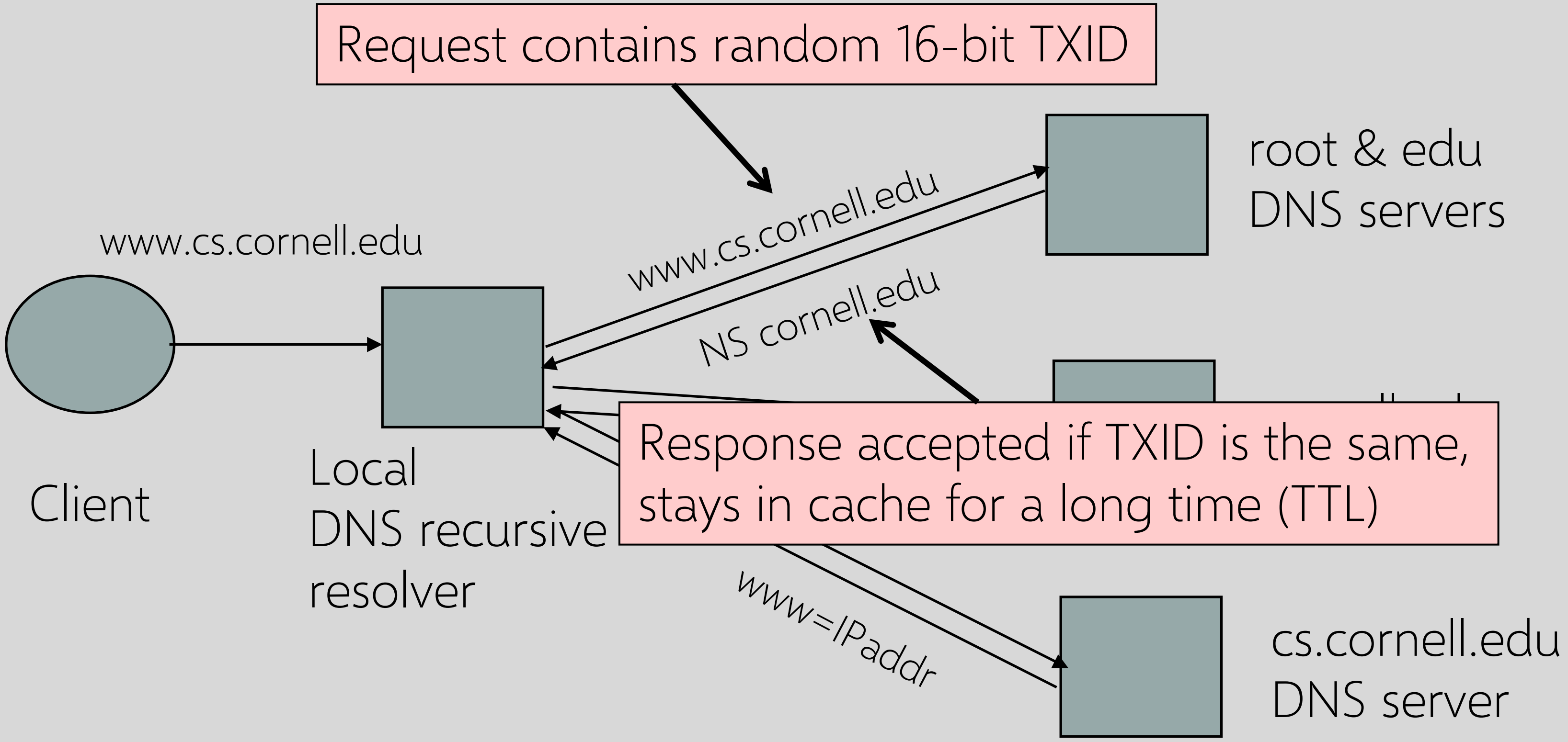
myetherwallet.com

54.192.146.xx

$150K worth of cryptocurrency stolen

https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/

DNS “Authentication”

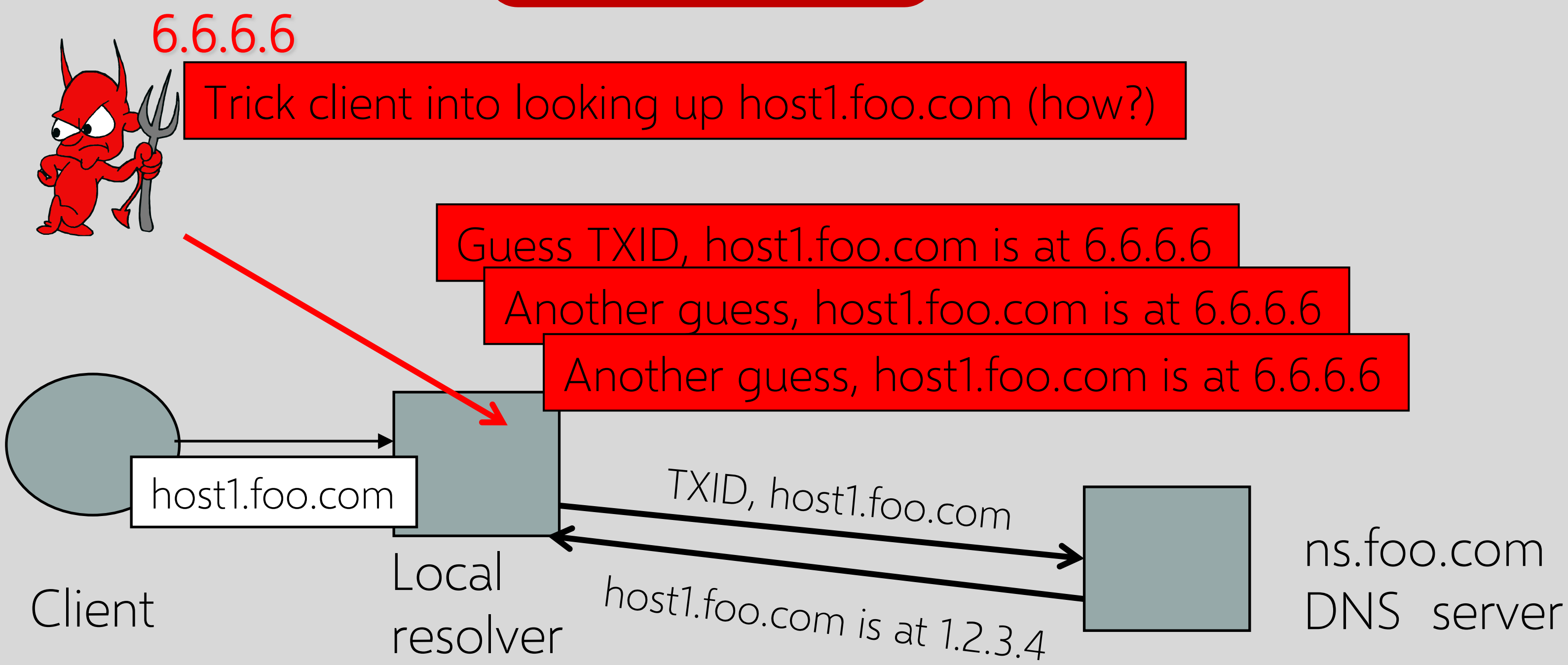


Request contains random 16-bit TXID

Response accepted if TXID is the same, stays in cache for a long time (TTL)

How is this different from the coffee-shop scenario?

DNS Spoofing by Off-Path Attacker



6.6.6.6

Trick client into looking up host1.foo.com (how?)

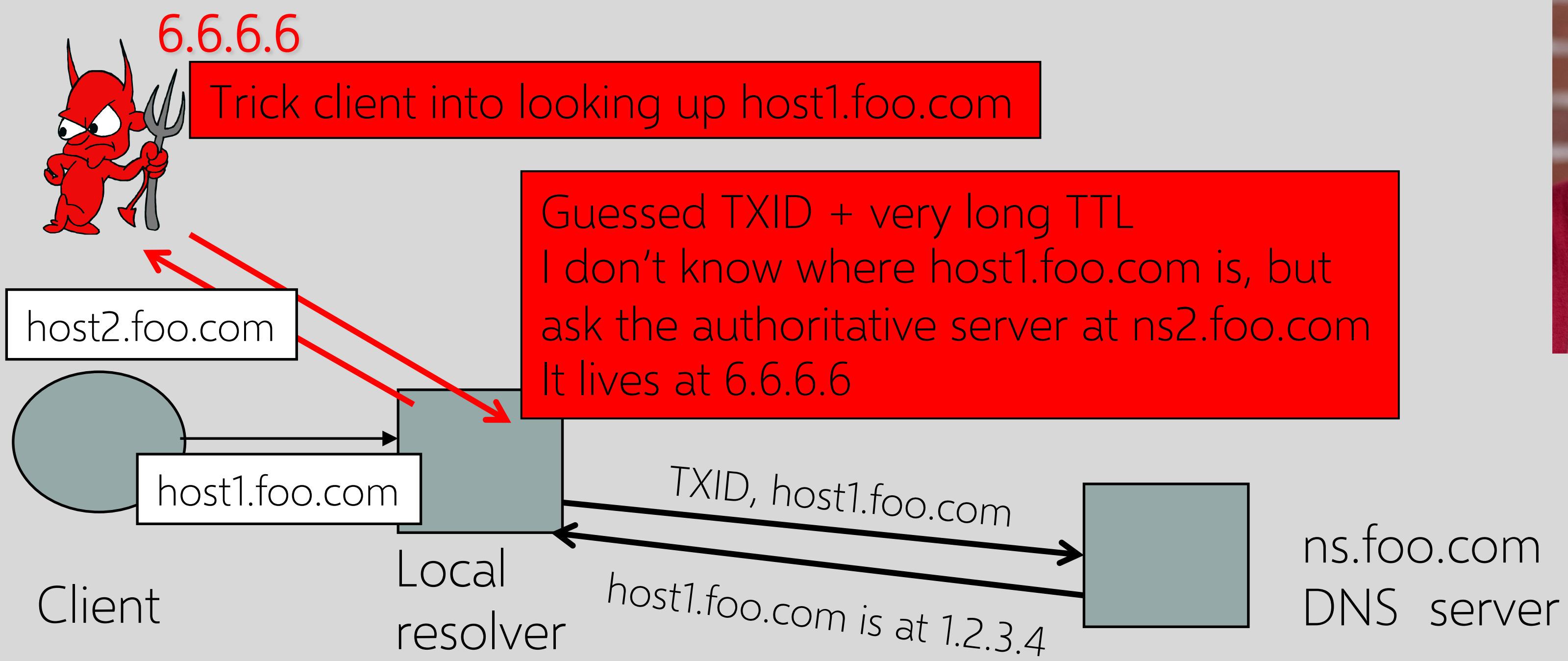
Guess TXID, host1.foo.com is at 6.6.6.6

Another guess, host1.foo.com is at 6.6.6.6

Another guess, host1.foo.com is at 6.6.6.6

Several opportunities to win the race.
If attacker loses, has to wait until TTL expires…
… but can try again with host2.foo.com, host3.foo.com, etc.
… but what’s the point of hijacking host3.foo.com?

Kaminsky’s Attack



6.6.6.6

Trick client into looking up host1.foo.com

Guessed TXID + very long TTL
I don’t know where host1.foo.com is, but
ask the authoritative server at ns2.foo.com
It lives at 6.6.6.6

If win the race, any request for XXX.foo.com will go to 6.6.6.6

The cache is poisoned… for a very long time!

No need to win future races!

If lose, try again with <ANYTHING>.foo.com

Triggering a Race

Any link, any image, any ad, anything can cause a DNS lookup

- No JavaScript required, though it helps

Mail servers will look up what bad guy wants

- On first greeting: HELO
- On first learning who they' re talking to: MAIL FROM
- On spam check (oops!)
- When trying to deliver a bounce
- When trying to deliver a newsletter
- When trying to deliver an actual response from an actual employee

Reverse DNS Spoofing

Trusted access is often based on host names

- Example: permit all hosts in .rhosts to run remote shell

Network requests such as rsh or rlogin arrive from numeric source addresses

- System performs reverse DNS lookup to determine requester's host name and checks if it's in .rhosts

If attacker can spoof the answer to reverse DNS query, he can fool target machine into thinking that request comes from an authorized host

- No authentication for DNS responses and typically no double-checking (numeric → symbolic → numeric)

Solving the DNS Spoofing Problem

Long TTL for legitimate responses

- Does it really help?

Randomize port in addition to TXID

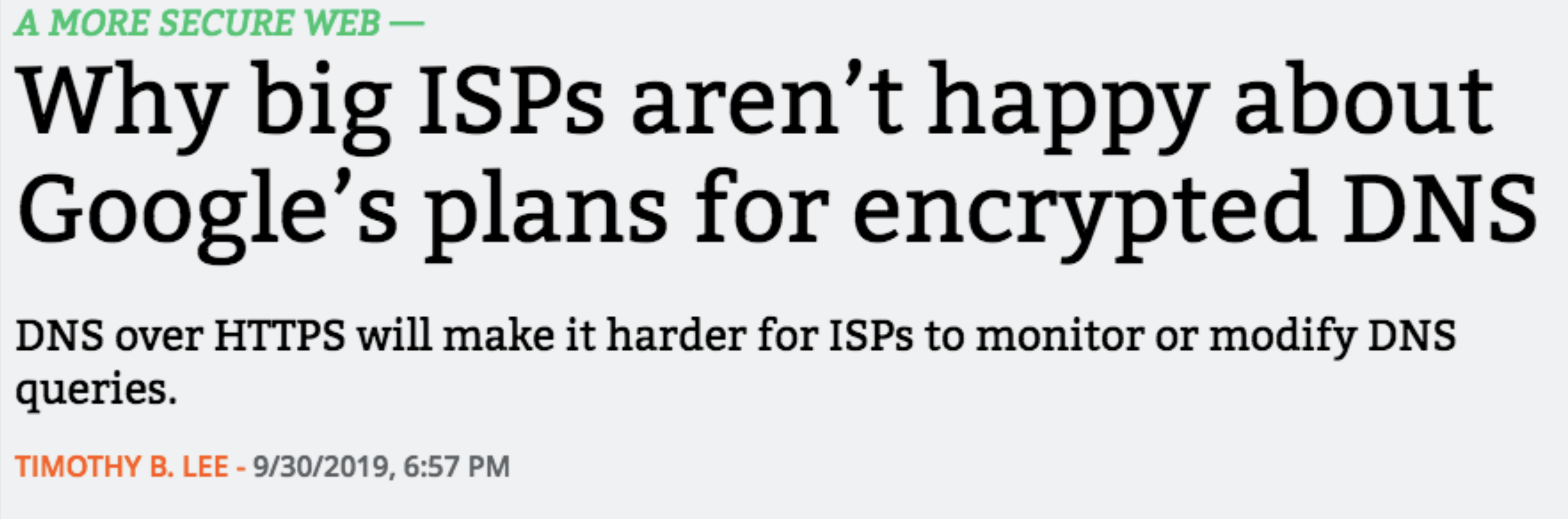
- 32 bits of randomness, makes it harder for attacker to guess TXID+port

DNSSEC

- Cryptographic authentication of host-address mappings

Encrypted DNS

Not the same!
DNSSEC does not encrypt DNS requests and responses.

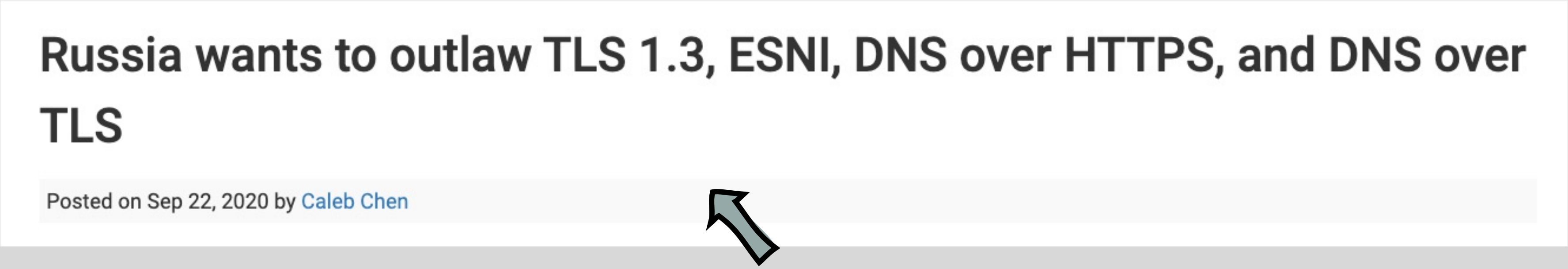


A MORE SECURE WEB —

Why big ISPs aren’t happy about Google’s plans for encrypted DNS

DNS over HTTPS will make it harder for ISPs to monitor or modify DNS queries.

TIMOTHY B. LEE - 9/30/2019, 6:57 PM



Russia wants to outlaw TLS 1.3, ESNI, DNS over HTTPS, and DNS over TLS

Posted on Sep 22, 2020 by Caleb Chen

[draft law] “... bans the use of encryption protocols allowing for hiding the name (identifier) of a web page or Internet site on the territory of the Russian Federation.”