Domain Name System

http://xkcd.com/302/

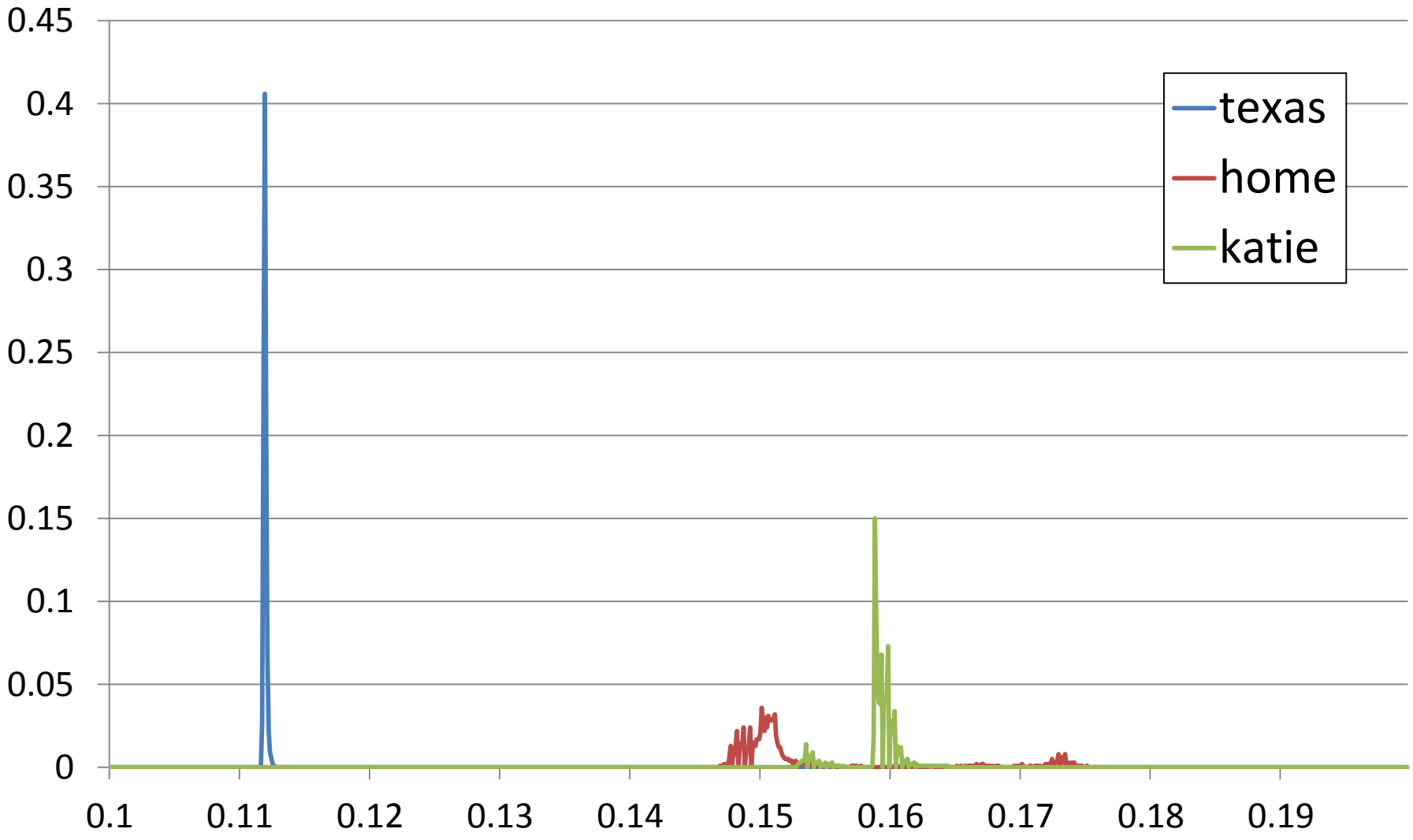
Overview

- Final project + presentation
- Some TCP and UDP experiments
- Domain Name System (DNS)
  - Hierarchical name space
  - Maps friendly names to IP address
  - Large distributed database of records

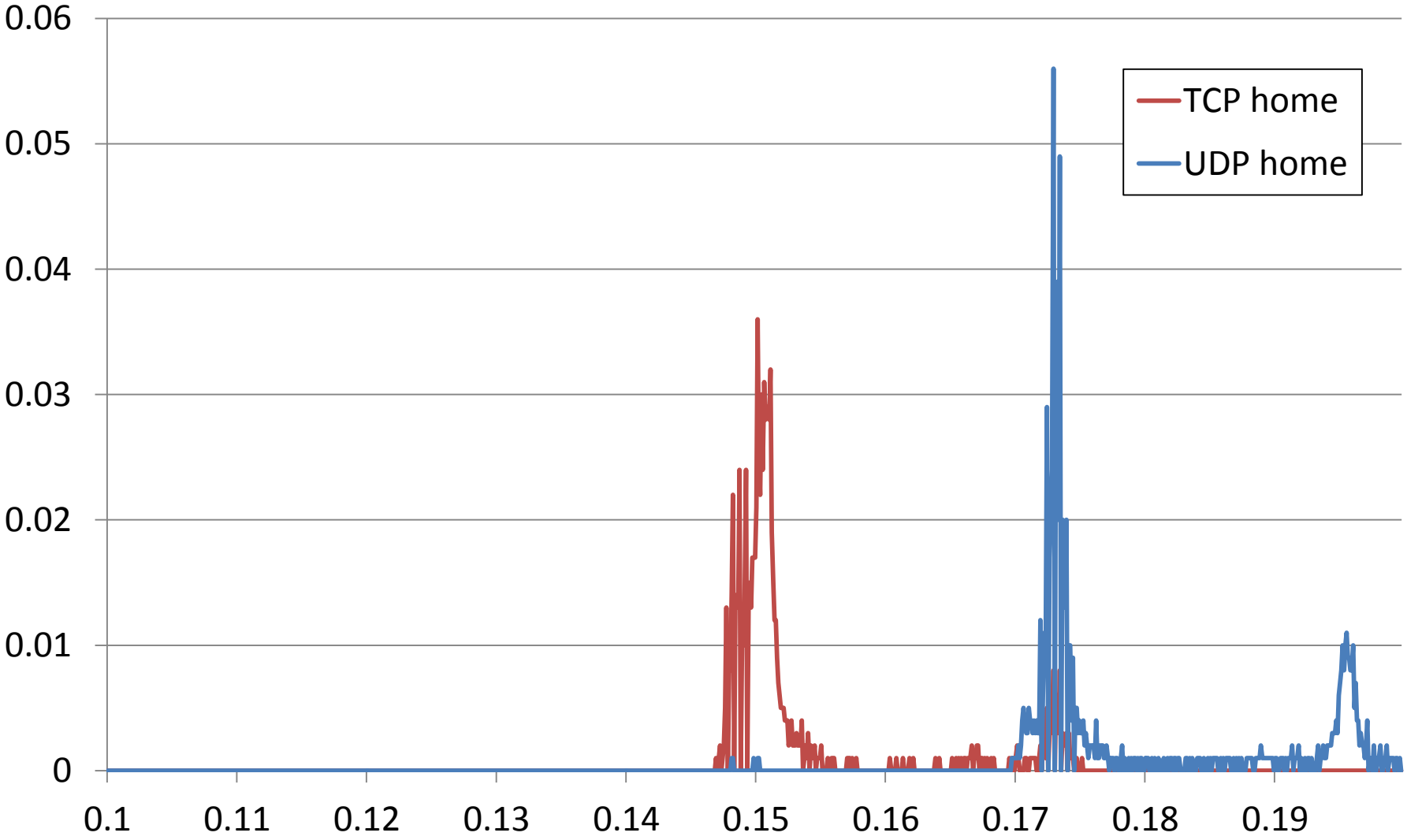
TCP/UDP experiments

- Send 1K of data, receive 1K back
  - Every ten seconds until something it failed
  - High resolution timing, start of send to end of receive
  - Endpoints:
    - home (cable modem) ↔ london
    - katie ↔ london
    - data center in Texas ↔ london
  - TCP and UDP
  - UDP no attempt to recover from packet loss
    - home, 6719 exchanges
    - katie, 151
    - texas, 842

TCP send/recv time



TCP vs UDP


0.06
0.05
0.04
0.03
0.02
0.01
0
0.1
0.11
0.12
0.13
0.14
0.15
0.16
0.17
0.18
0.19
TCP home
UDP home

Names and IP addresses

- Why use names instead of IP address?
  - Names are easier for humans to remember
    - www.bbc.co.uk versus 64.91.253.46
  - IP address could change if changing ISPs
  - Single name could map to multiple IP address
    - Load balance over several servers
    - Send user to nearest server to reduce latency
  - Allow multiple names to go to same place

Hierarchical network names

- **Host name:** www.cs.princeton.edu
  - Domain: registrar for each top-level domain (e.g., .edu)
  - Host name: local administrator assigns to each host
- **IP addresses:** 128.112.7.156
  - Prefixes: ICANN, regional Internet registries, and ISPs
  - Hosts: static configuration, or dynamic using DHCP
- **MAC addresses:** 00-15-C5-49-04-A9
  - Blocks: assigned to vendors by the IEEE
  - Adapters: assigned by the vendor from its block

Domain Name System

- Domain Name System (DNS)
  - Maps host name to IP address
  - DNS resolver, sends query
  - DNS server, provides response

- How does the server know the answer?

Option 1: Local file

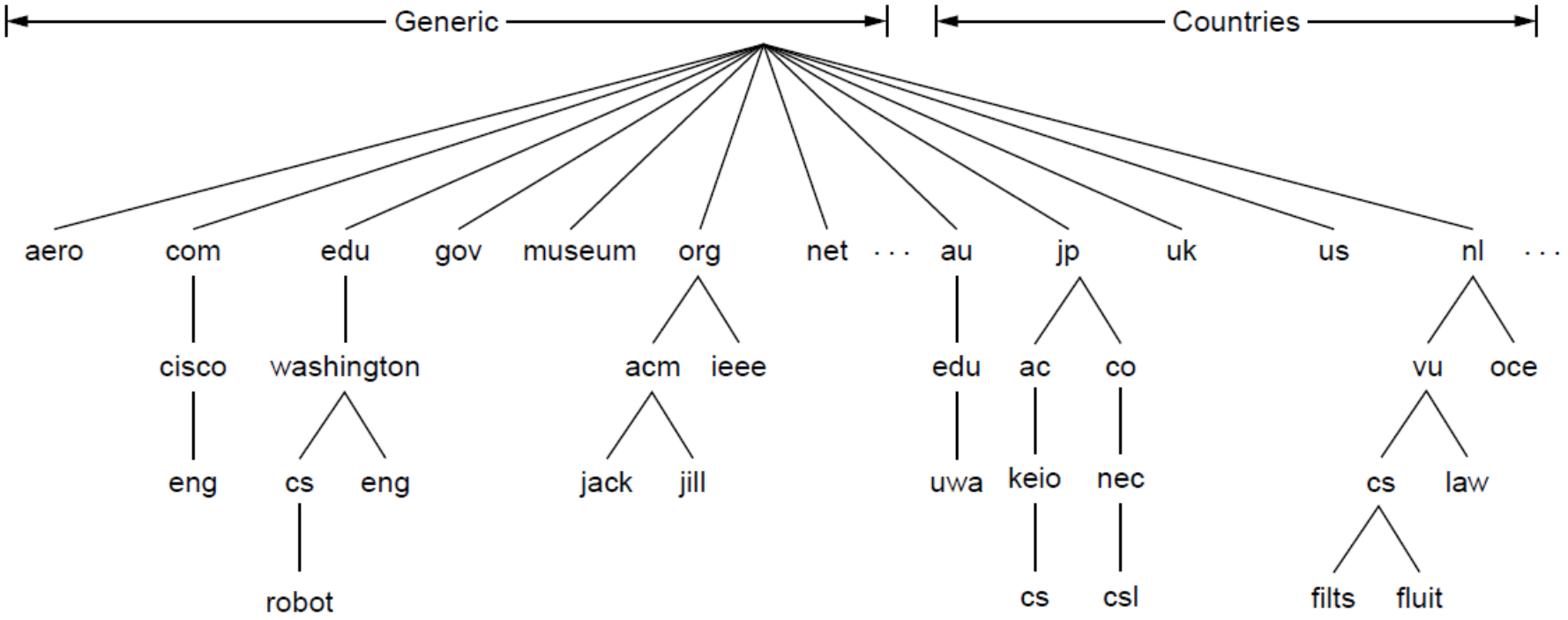
- Store name to address mapping in local file
  - ARPANET prior to 1983, hosts.txt
  - Flat namespace
  - SRI updated hosts.txt, others downloaded it
  - Worked in a world of a small number of large computers
  - Doesn't scale as more and more computers were placed on the network

Option 2: Central server

- Central server
  - All name to address mapping stored in one place
  - All queries go to central server
- Problems:
  - Single point of failure
  - Server may experience high volume of traffic
  - Server may be distant from a host wanting a lookup
  - Single point of update
  - Does not scale

Domain Name System (DNS)

- Distributed, hierarchical collection of servers
  - Name space is hierarchical



Generic Top Level Domains (TLDs)

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes
xxx	Sex industry	2010	No

Top level domains

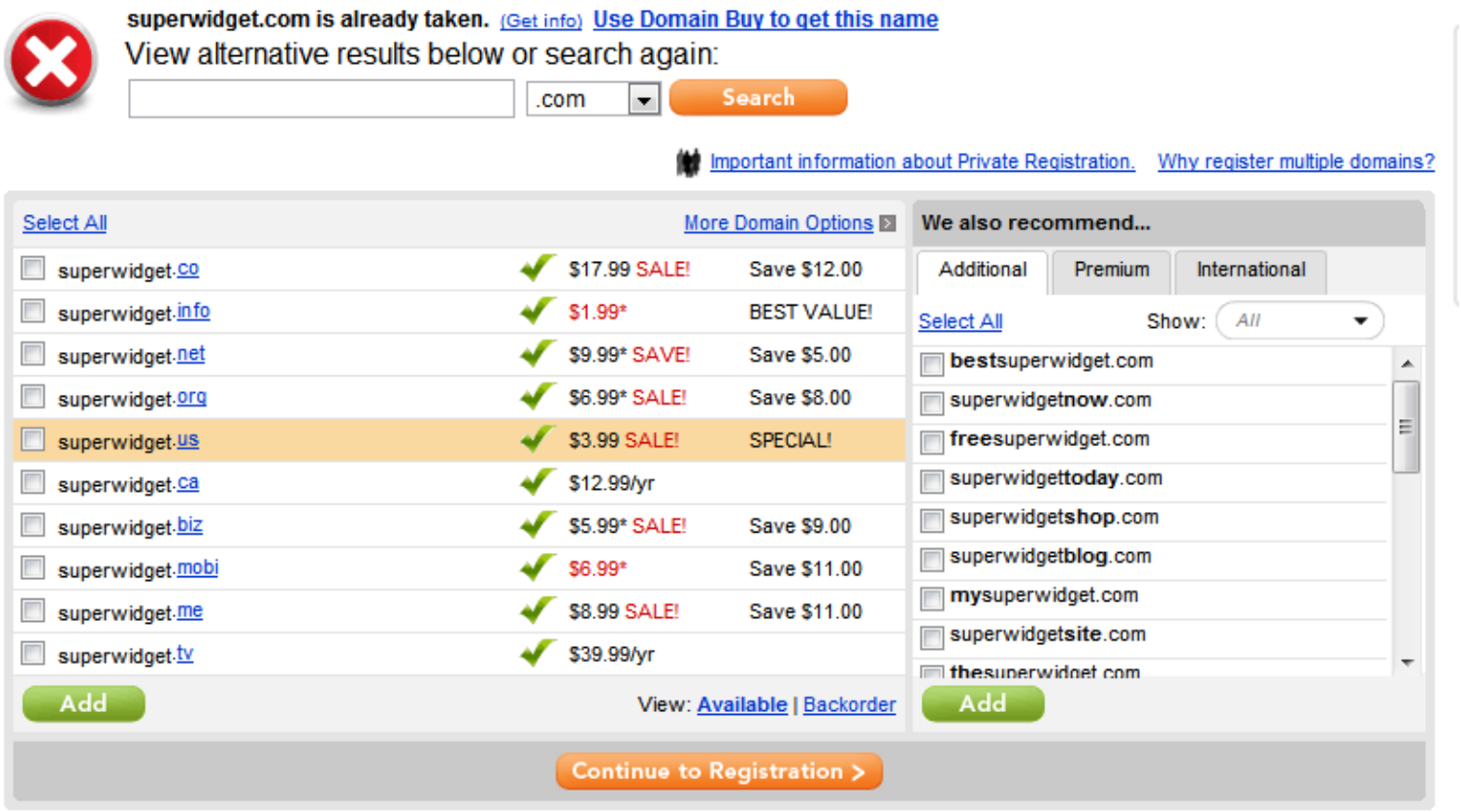
- Top-level domains (TLD)
  - Around 22 generic TLDs, e.g. com, net, org, edu
    - Most popular with US organizations
  - Around 250 country specific TLDs
    - Two letter ISO code, e.g. au, ch, se
    - Some violations, e.g. uk instead of gb
  - TLDs run by registrars appointed by Internet Corporation for Assigned Names and Numbers (ICANN)
  - Money in names
    - Cybersquatting
    - Country of Tavalu sold lease to .tv for 50 million

Top level domains

- Set to expand, you can buy your own TLD!
  - June 2011
    - ICANN approves creation of TLDs for brands a organizations
    - $185,000 initial application, $25,000 annual fee
  - Is an easy-to-remember domain name relevant anymore?
    - Google the name instead
    - What name should you type to get to General Motors?

Second-level domains

- Second-level domains
  - Getting name-of-company.com is easy
  - Buy from a registrar for the desired TLD, small annual fee



Subdomains

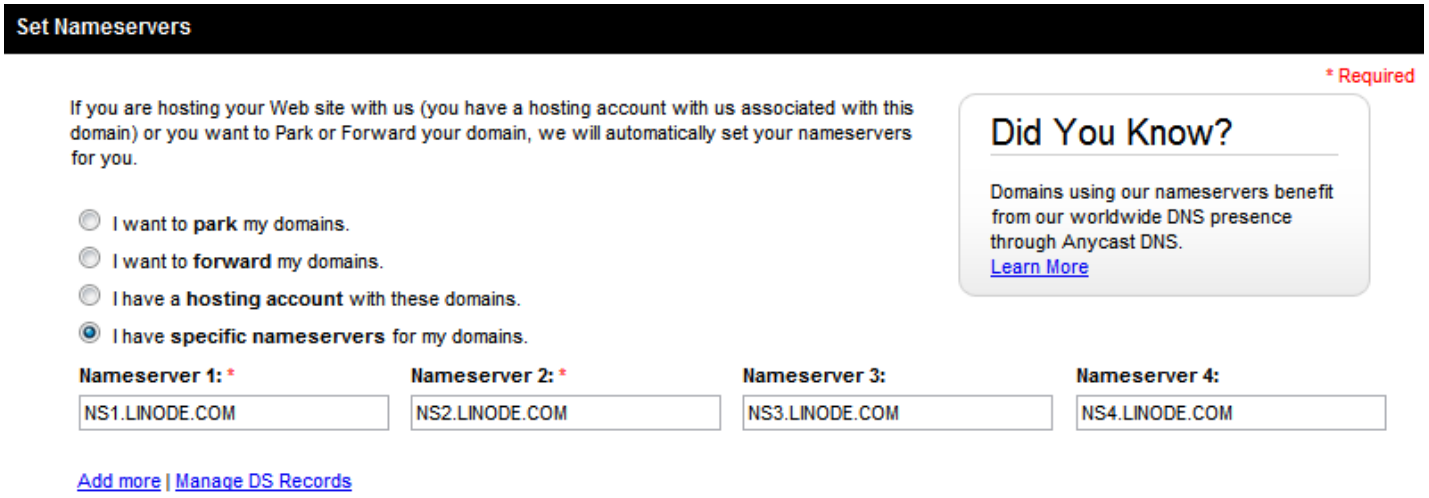
- Further hierarchy under a second-level domain
  - e.g. mail.company.com, www.company.com, inf.phy.cam.ac.uk
  - Each domain controls the subdomains under it
- Domain resource records
  - Each domain has a set of data about its server(s)
  - At a minimum, the IP address for a name

Domain resource record

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

- A - most important, maps hostnames to IPv4 addresses
- MX - username@company.com go to this server name
- NS - server that stores the record
- Fields have a TTL - time-to-live, for caching

Setting DNS resource record



DNS Manager » **keithv.com**

SOA Record

Primary DNS	Email	Default TTL	Refresh Rate	Retry Rate	Expire Time	Options
ns1.linode.com	a@b.com	Default	Default	Default	Default	Settings

NS Records

Name Server	Subdomain	TTL	Options
ns1.linode.com	keithv.com	Default	~~Edit~~ | ~~Remove~~
ns2.linode.com	keithv.com	Default	~~Edit~~ | ~~Remove~~
ns3.linode.com	keithv.com	Default	~~Edit~~ | ~~Remove~~
ns4.linode.com	keithv.com	Default	~~Edit~~ | ~~Remove~~
ns5.linode.com	keithv.com	Default	~~Edit~~ | ~~Remove~~

Add a new NS record

MX Records

Mail Server	Preference	Subdomain	TTL	Options
mx1.emailsrvr.com	10		Default	Edit | Remove
mx2.emailsrvr.com	20		Default	Edit | Remove

Add a new MX record

A/AAAA Records

Hostname	IP Address	TTL	Options
	69.164.194.211	Default	Edit | Remove
mail	69.164.194.211	Default	Edit | Remove
www	69.164.194.211	Default	Edit | Remove

Add a new A record

CNAME Records

Hostname	Aliases to	TTL	Options

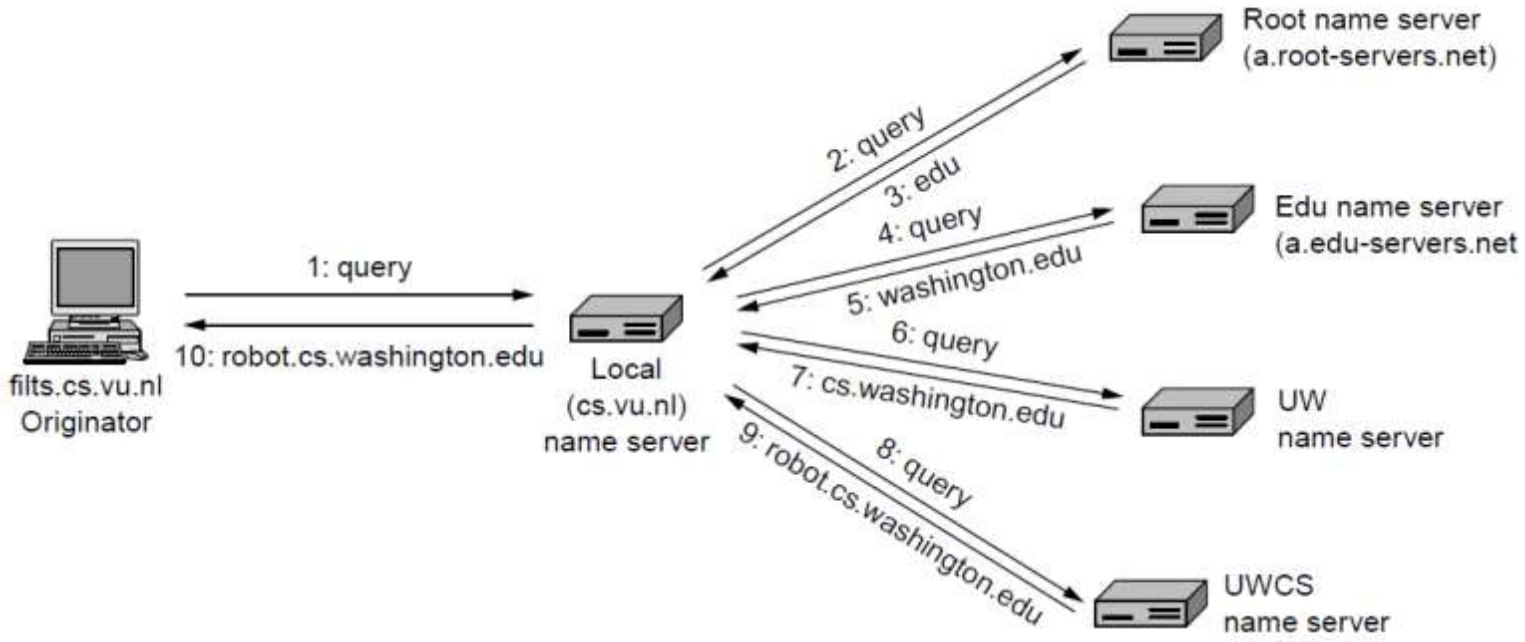
Add a new CNAME record

TXT Records

Name	Value	TTL	Options

Add a new TXT record

Name resolution

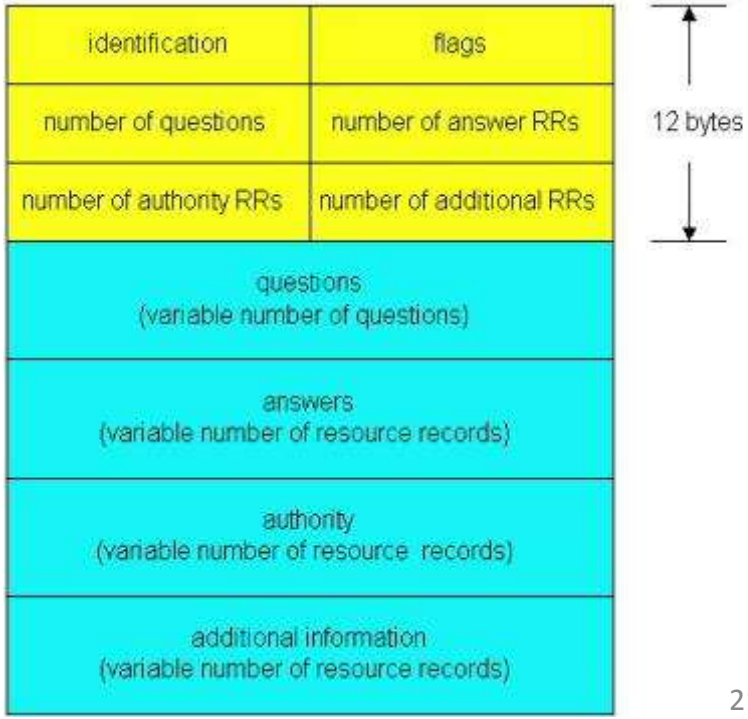


- Step 1: Host contacts its local DNS server
  - Host configured with local server
  - Manually configured (e.g. /etc/resolve.conf) or via DHCP
  - A "recursive query", originator waits for complete answer from local DNS server

DNS query

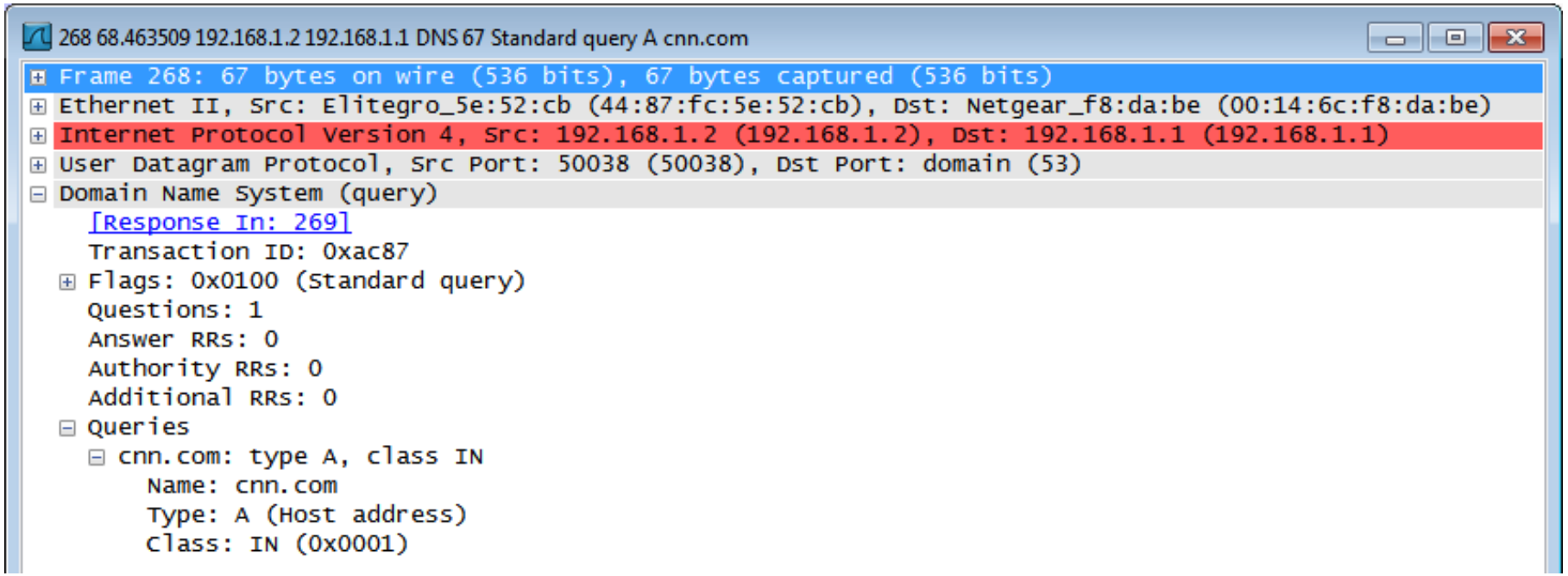
- Name lookup via DNS query
  - Transported over UDP
  - Retry same server with exponential backoff
  - Can switch to trying other DNS servers

- Identification:
  - 16 bit # for query, reply uses same #
- Flags:
  - Query or reply
  - Recursion desired
  - Recursion available
  - Reply is authoritative

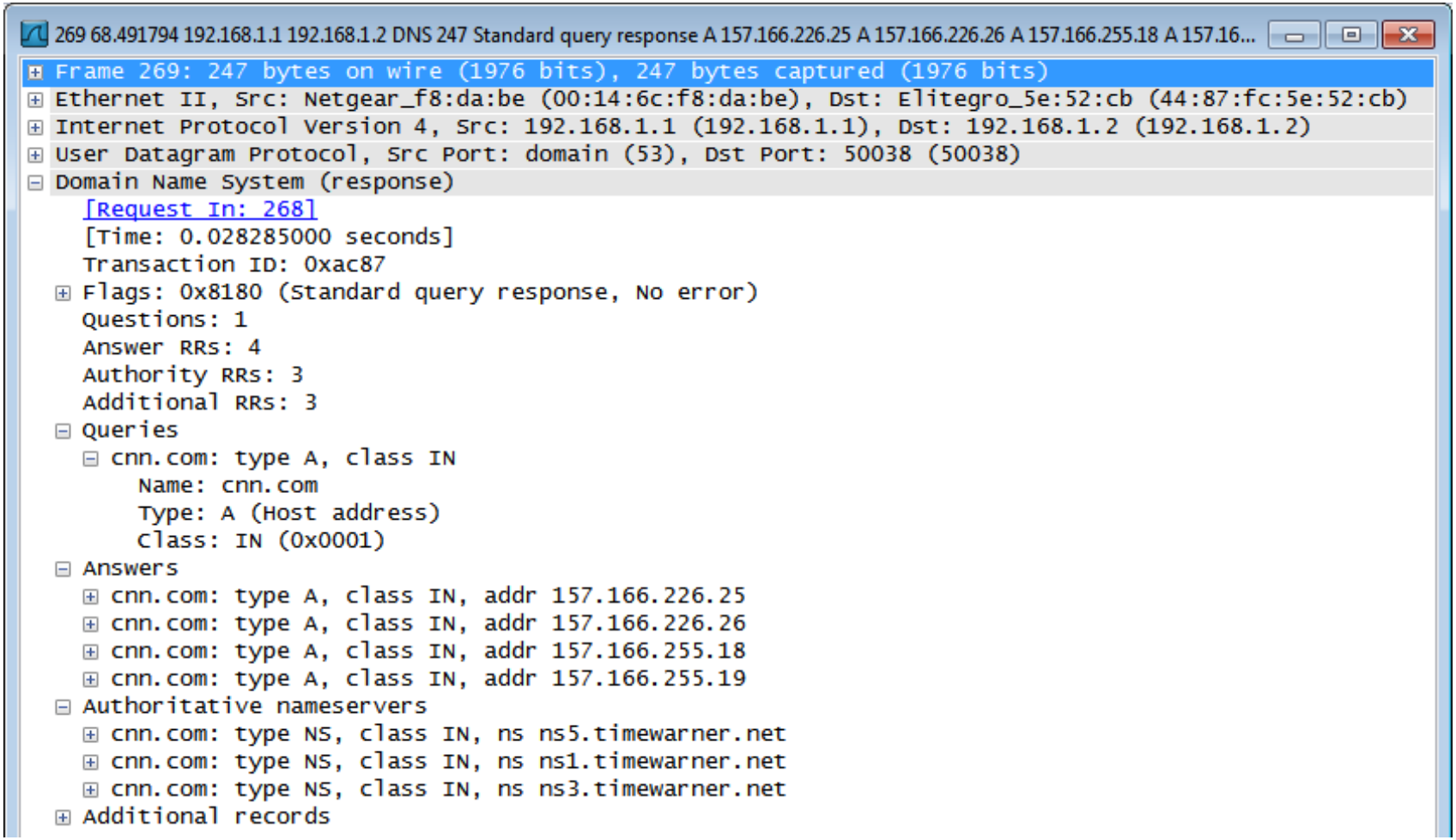


Example DNS query

```
status = getaddrinfo("cnn.com", "80", &hints, &res);
```



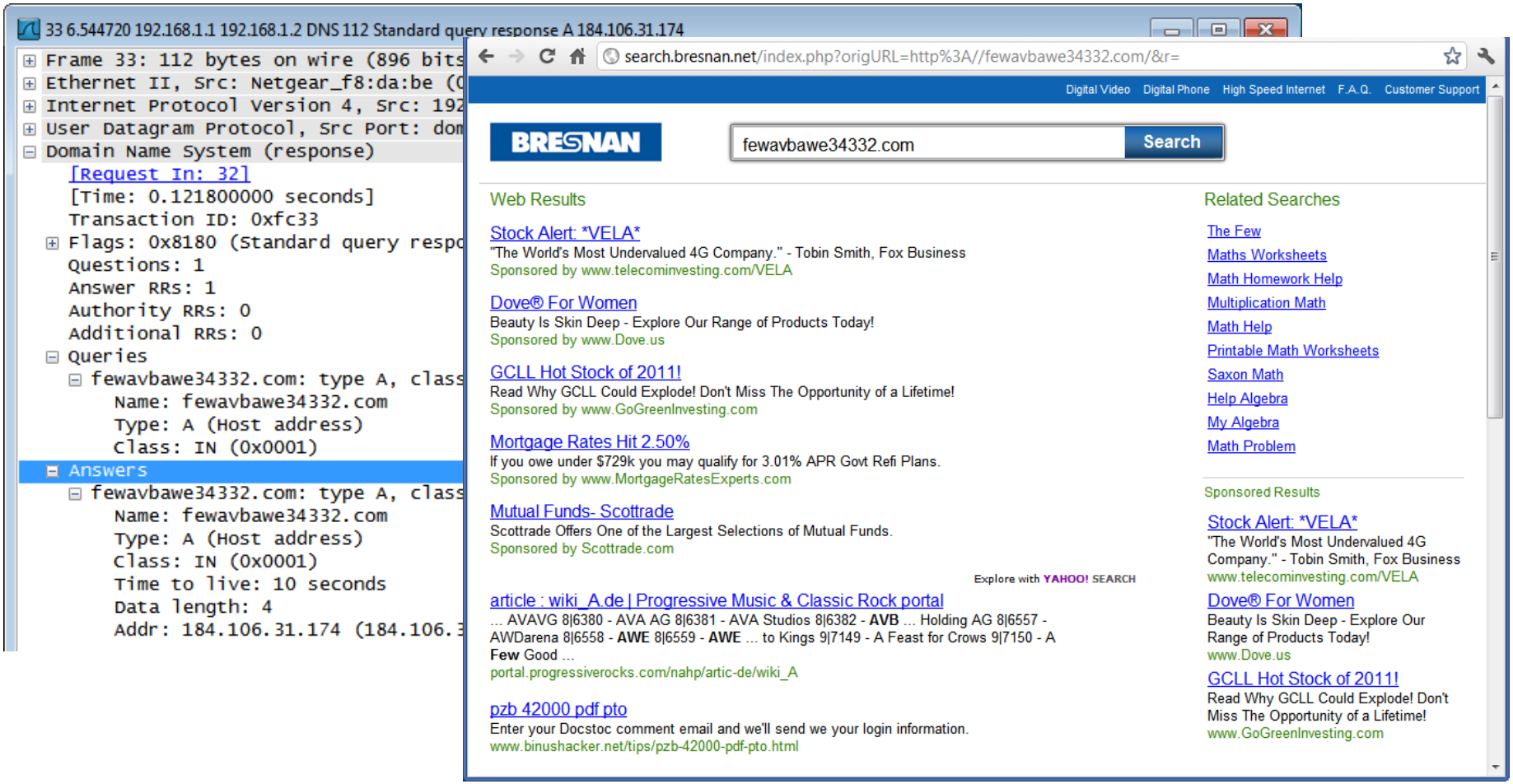
Example DNS response



DNS query to nowhere?

- Request lookup of a bogus domain name

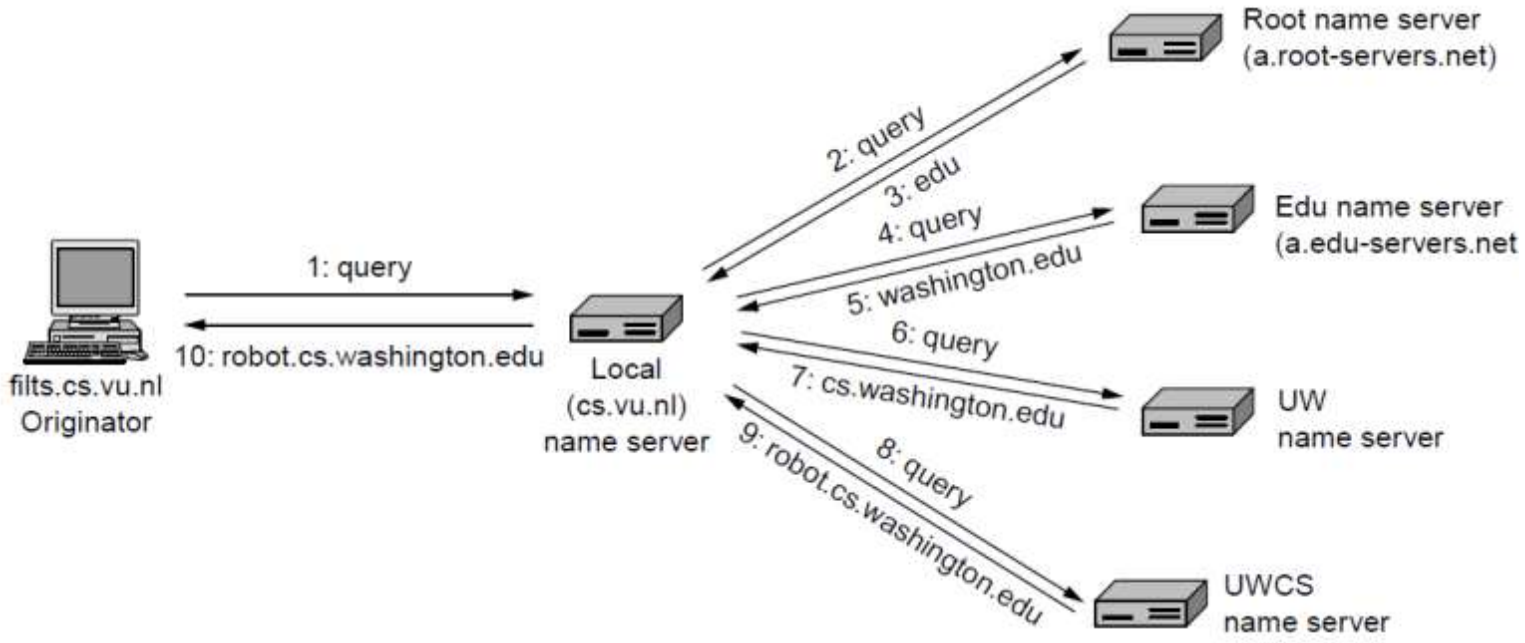
```
status = getaddrinfo("fewavbawe34332.com", "80", &hints, &res);
```



Domain Name Servers

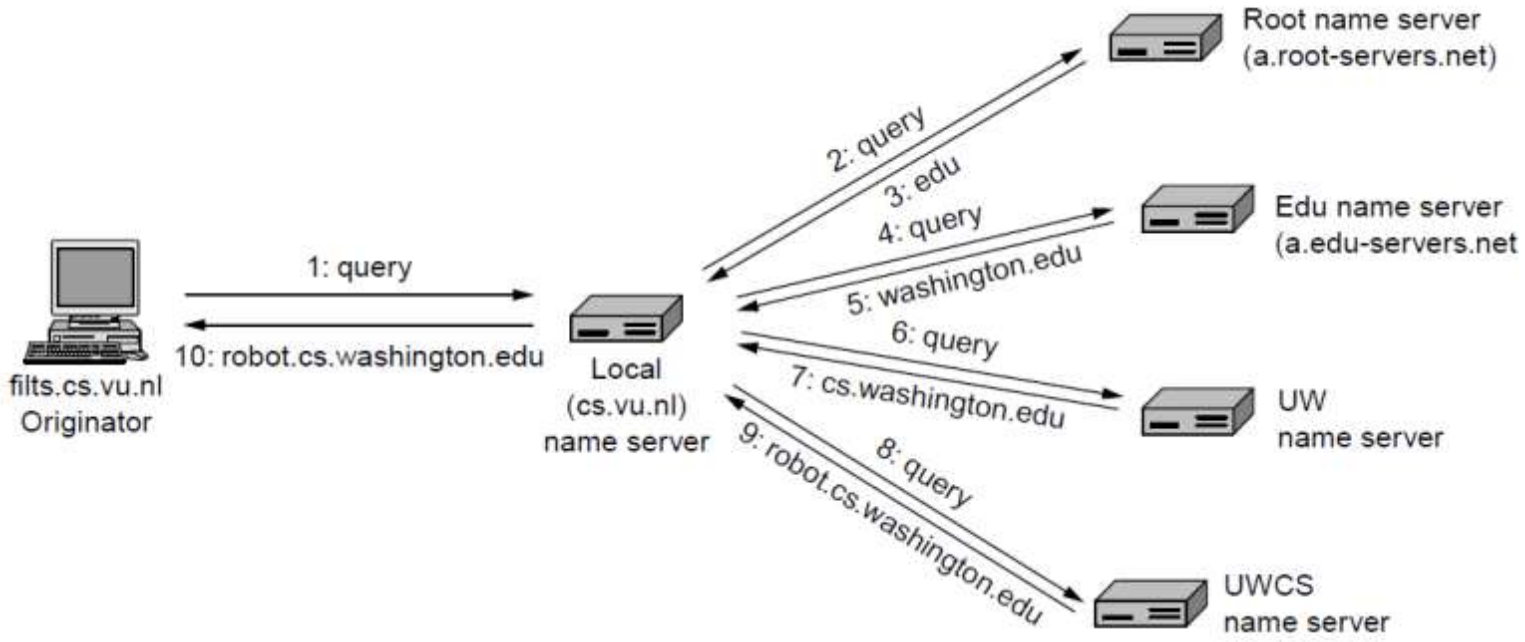
- Distributed, hierarchical collection of servers
  - Root servers, named: letter.root-servers.net, A-M
  - a.root-servers.net, actually a geographically distributed set of servers reached via anycast routing

Name resolution



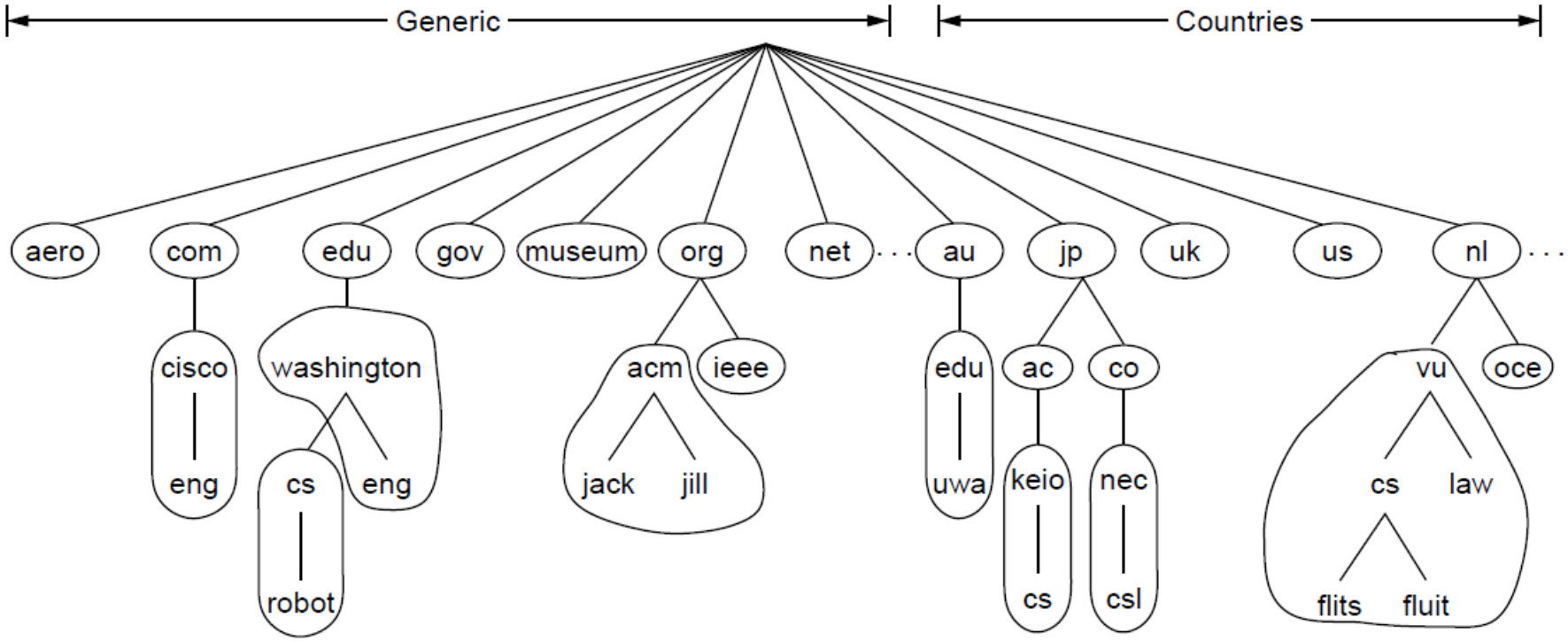
- Step 2/3: Root NS responds with NS handling .edu
  - An "iterative query"
  - Local NS has ongoing conversation with multiple servers to find answer for originator

Name resolution

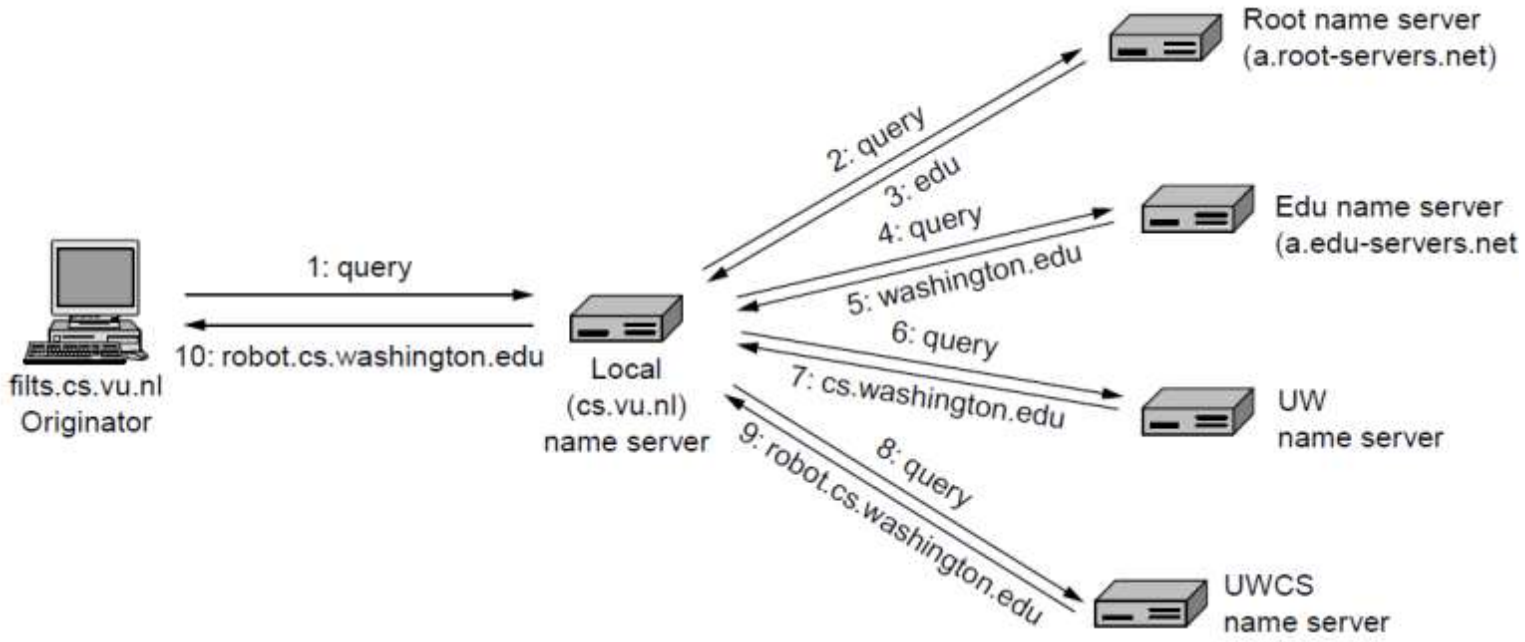


- Step 4/5: edu NS responds with NS for UW
  - Name space divided into non-overlapping zones
  - Zone has a primary name server, 1+ secondary
  - Zone boundaries controlled by domain owner

Name space zones



Name resolution



- Step 6/7: UW NS responds with NS for UWCS
  - UW CS department runs their own DNS server
- Step 8/9: UWCS NS responds with address of robot
  - UWCS NS is the authoritative server
  - The actual DNS record is stored here

Caching

- Recursive queries sufficient to find mapping
  - But expensive, loads root servers
  - Time consuming, incur many RTTs
  - Cache records for certain amount of time (TTL)
- Different levels of caching
  - In the resolver's operating system
  - Local DNS server
    - Can remember steps in the recursive query
    - Go directly to authoritative server for a new hostname at a previous found domain name

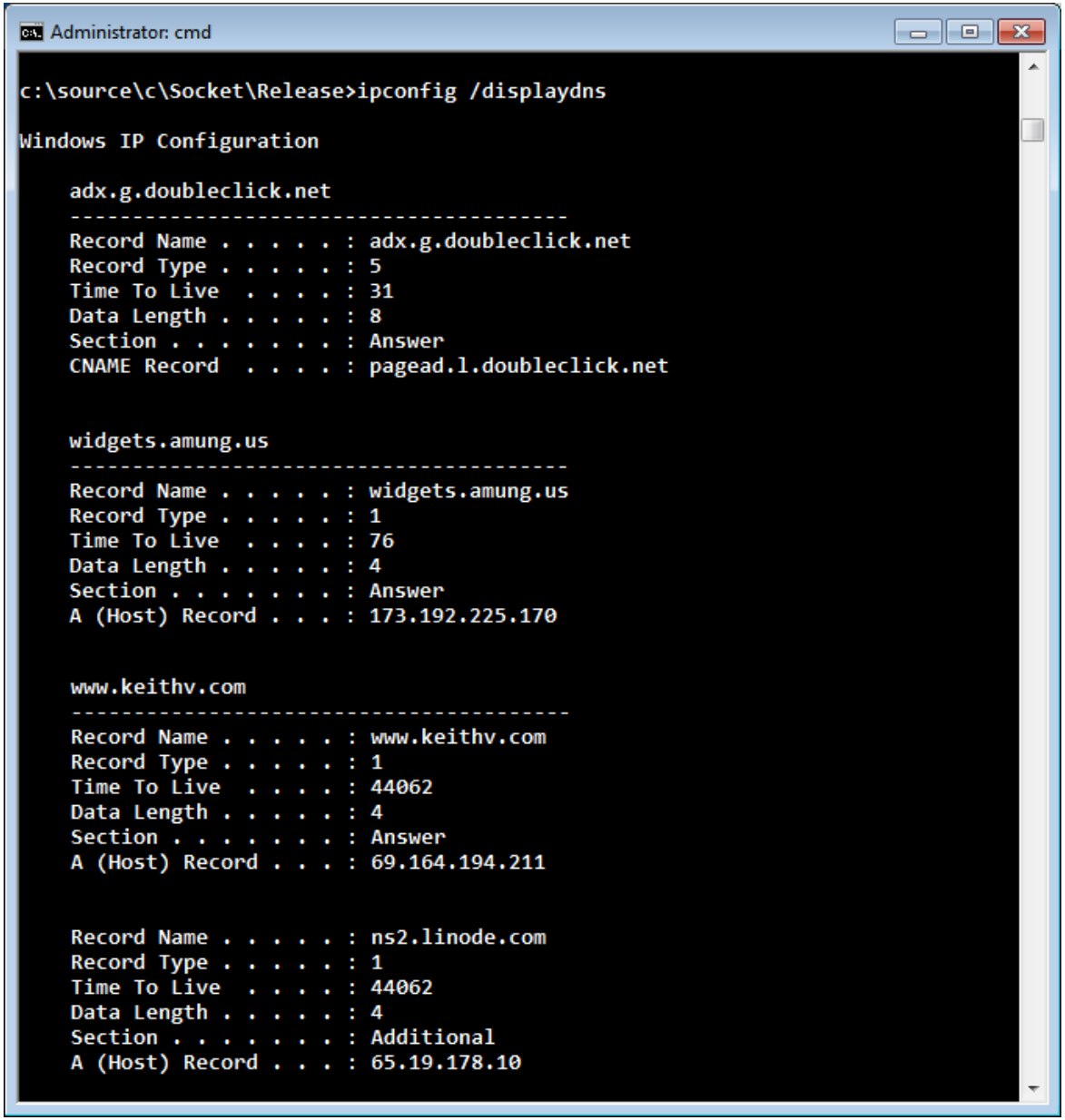
Negative caching

- Negative caching
  - Normally DNS cache stores only successful name resolutions
  - But common misspellings can be expensive to lookup
    - Talk to root server and then TLD server before discovering it is a bogus domain name
  - DNS servers can store negative entries and quickly return that name can't be resolved

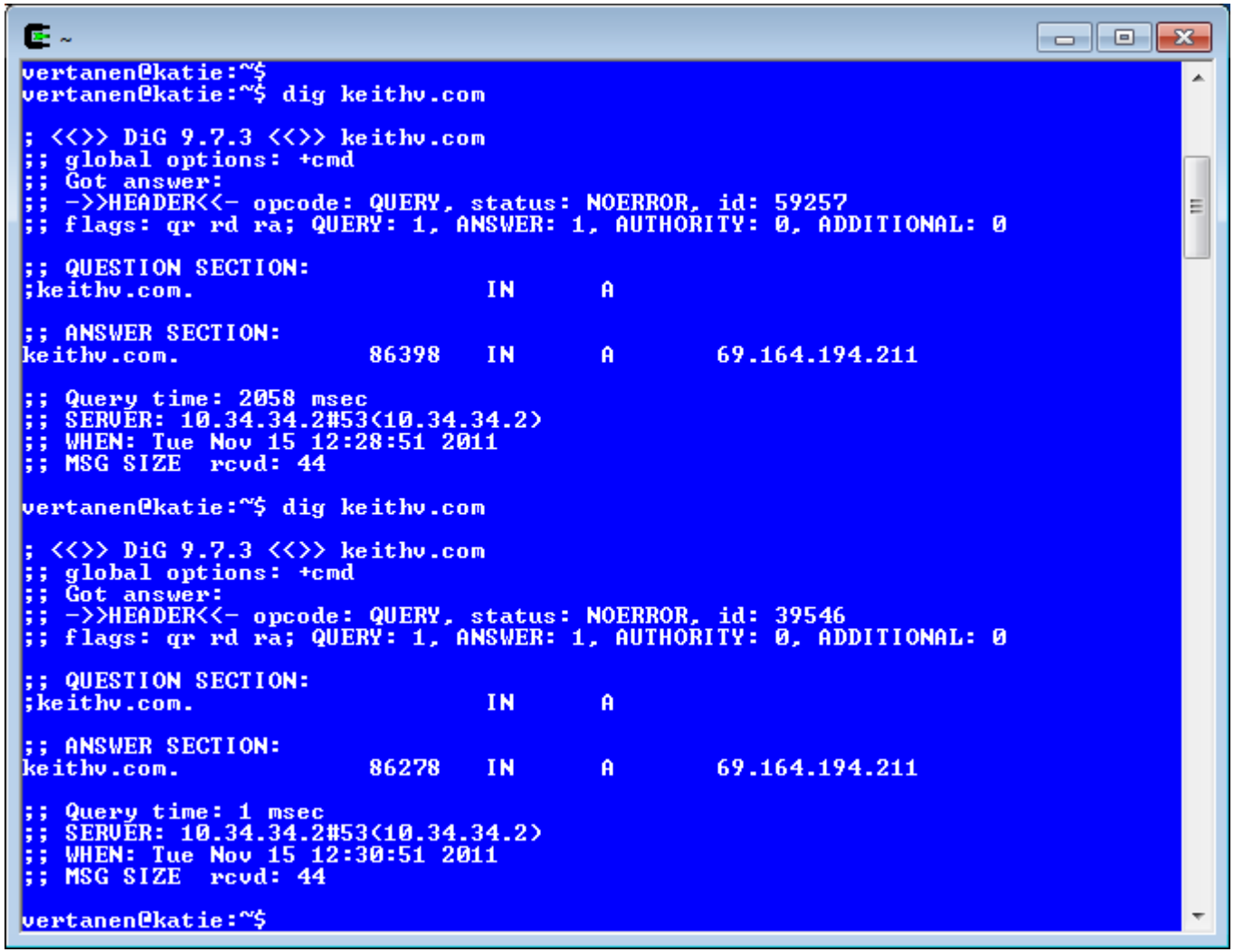
Cache poisoning

- DNS cache poisoning
  - Fool DNS server into entering a non-authoritative entry
  - Users get sent to wrong IP address
  - Controller of spoofed domain name can:
    - Spread malicious software
    - Steal information
    - e.g. http://www.wellsfargo.com now goes a web server running a site very similar to real site… User sees the correct URL in their browser.
  - http://www.youtube.com/watch?v=1d1tUefYn4U

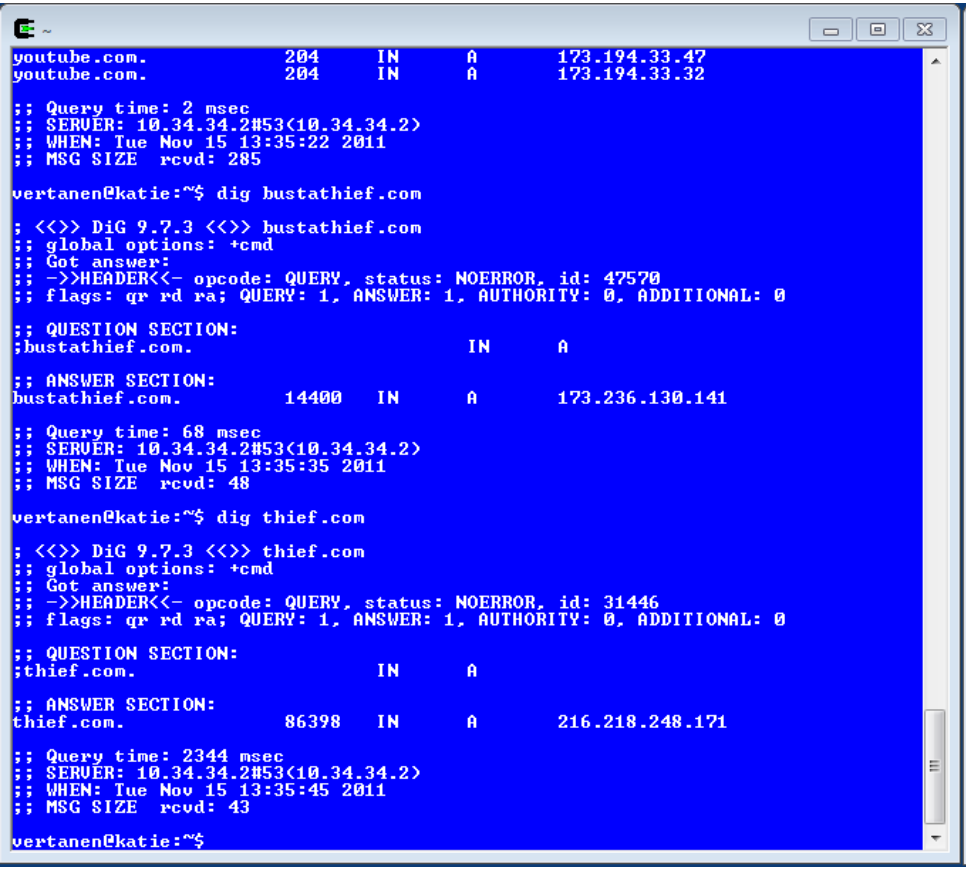
Example Windows DNS cache

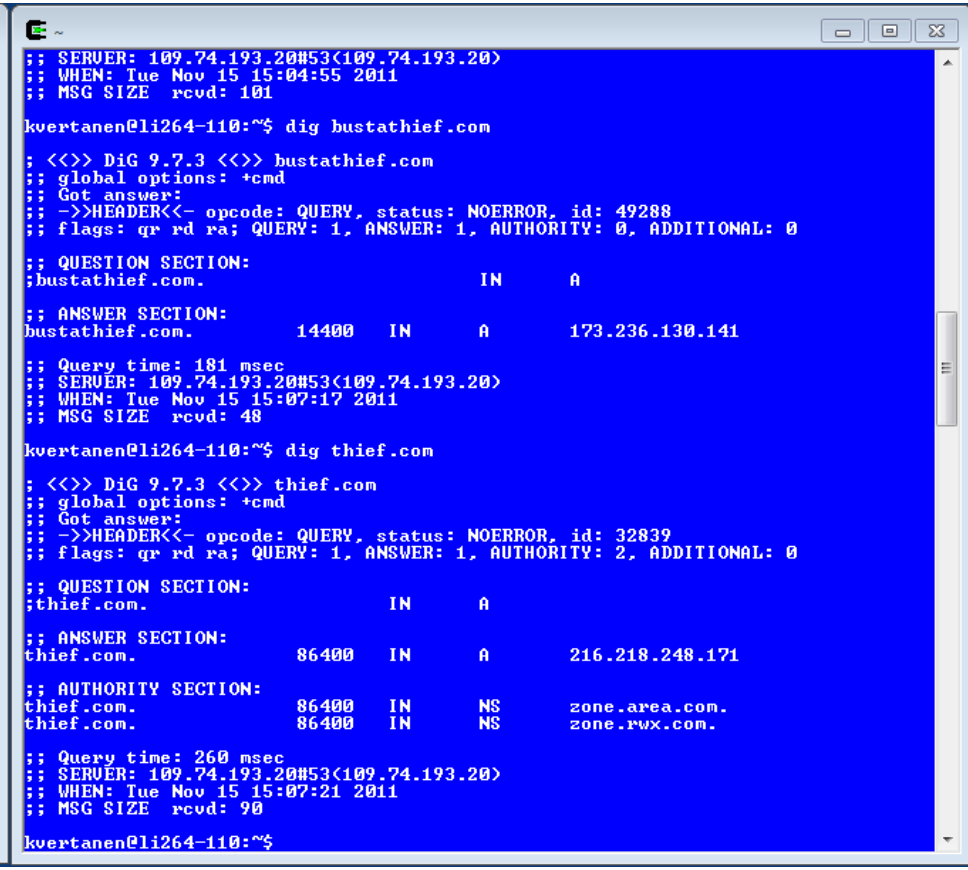


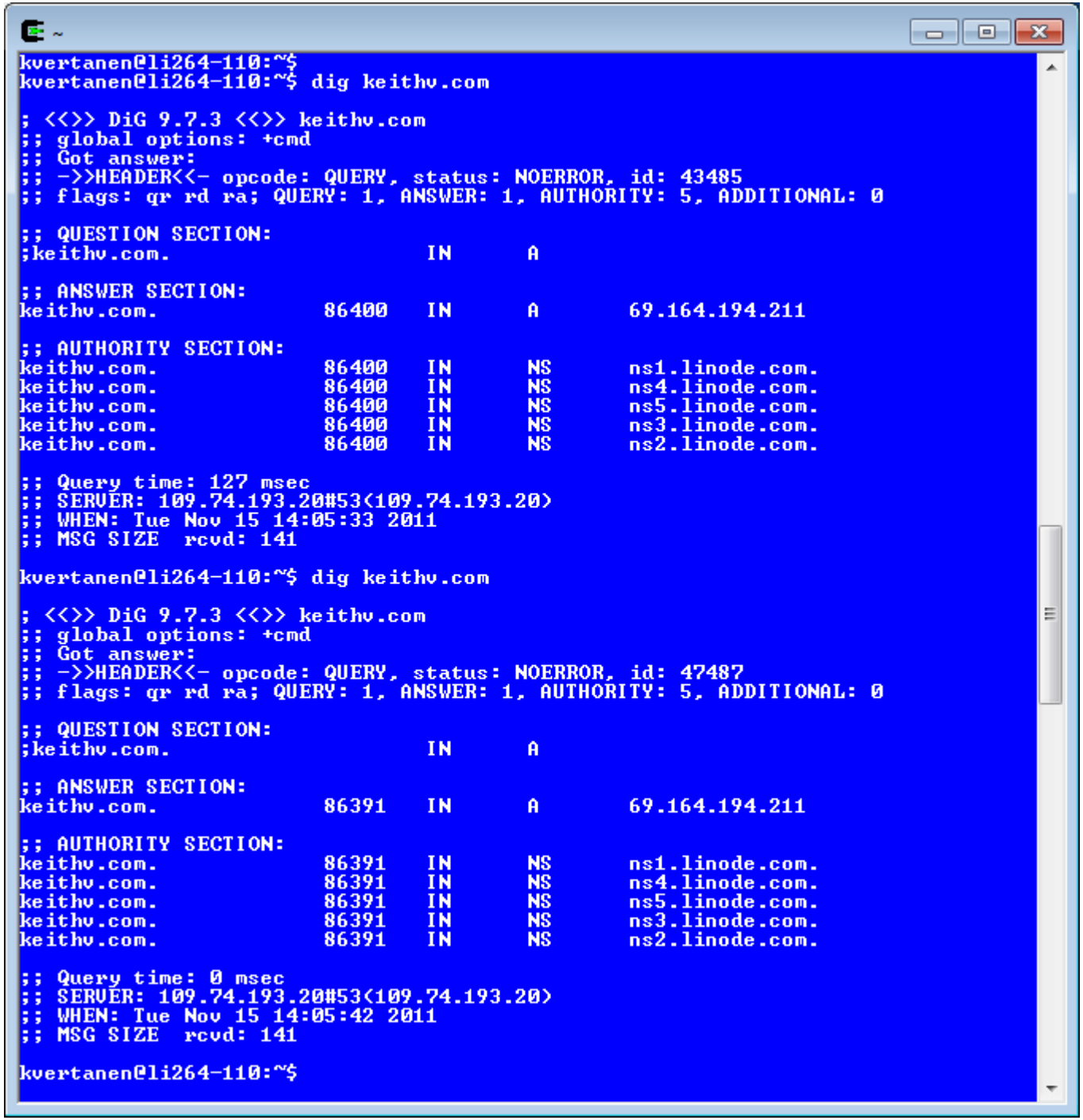
Exploring DNS with dig

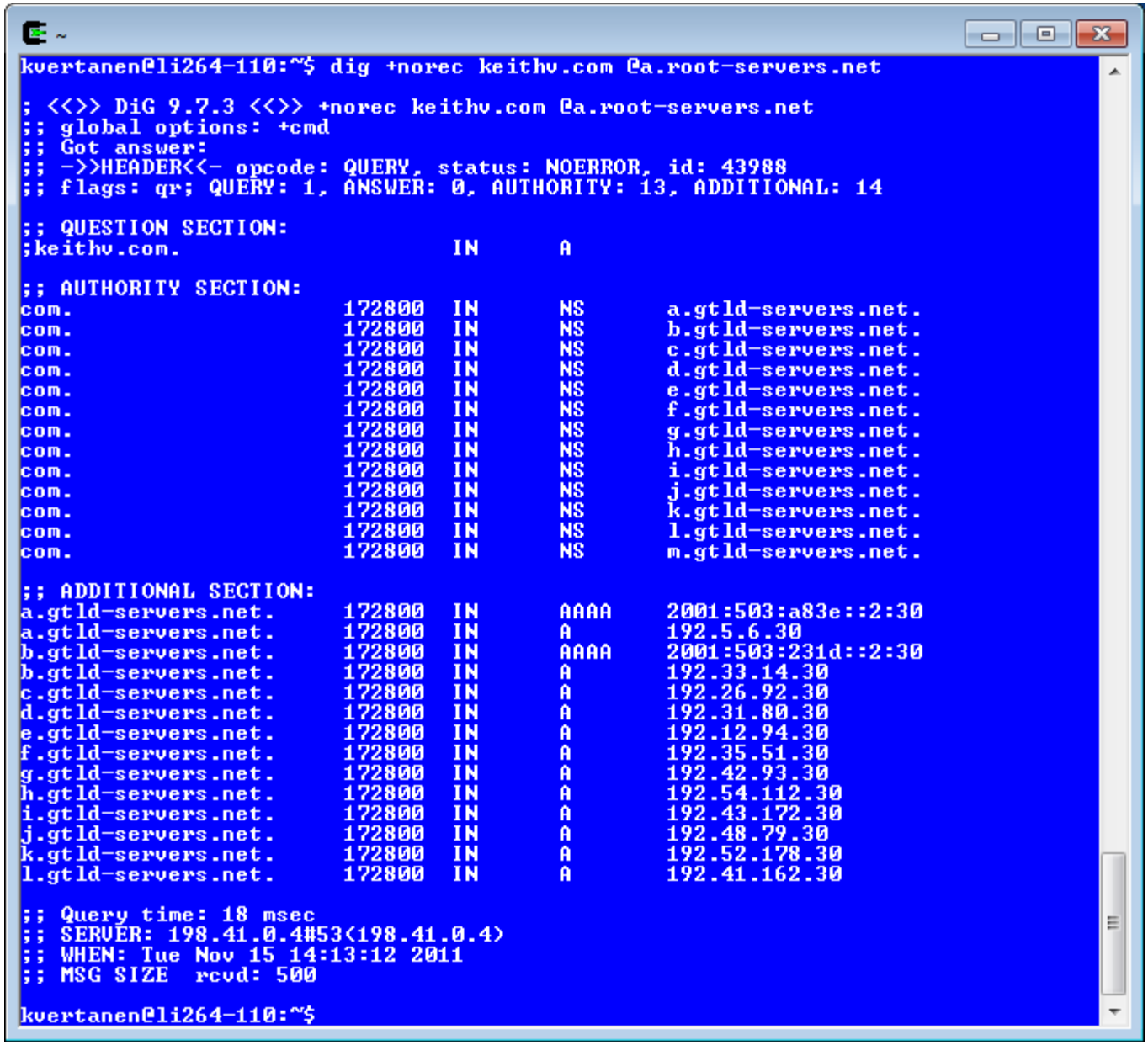


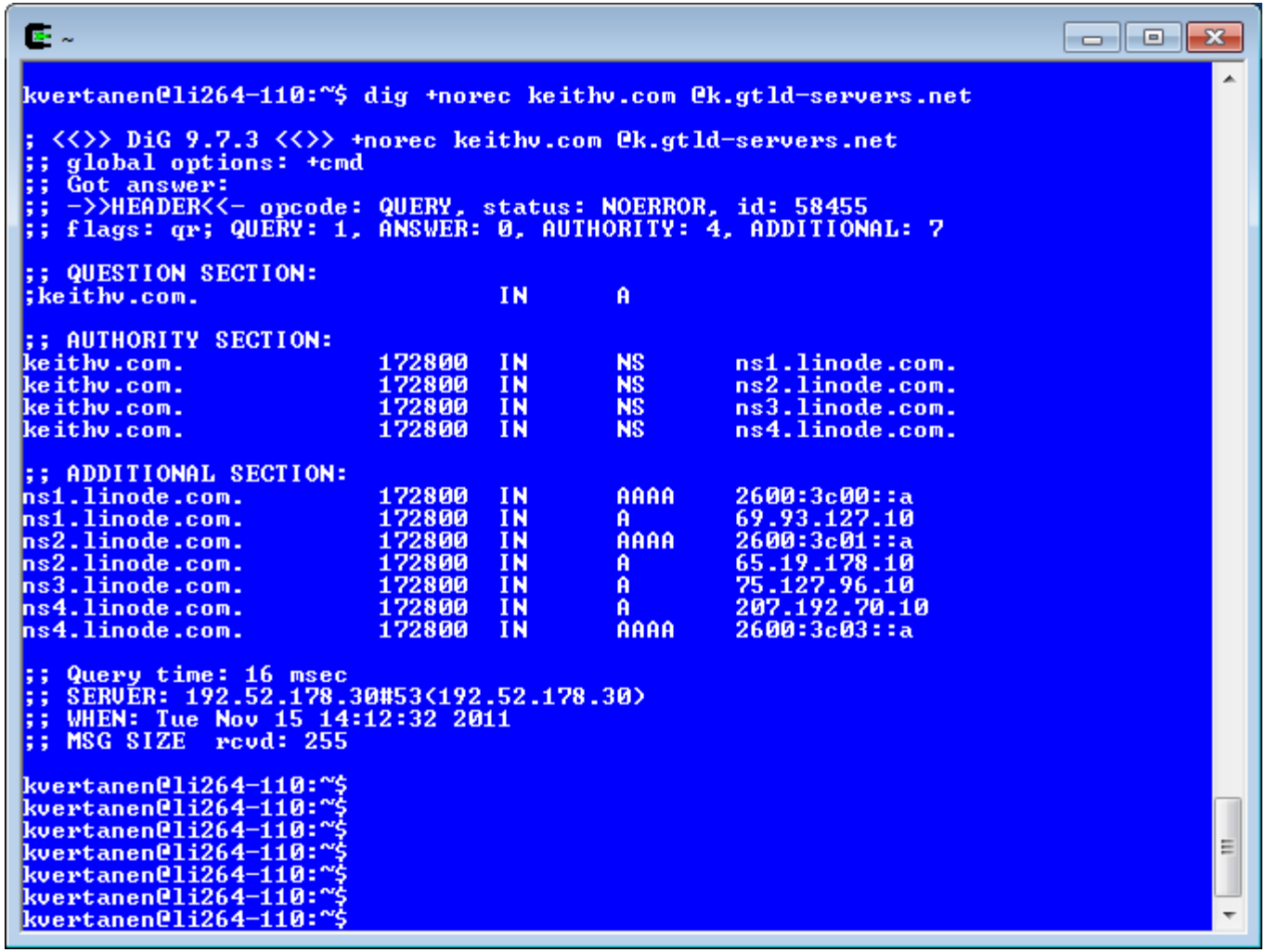
What the heck?

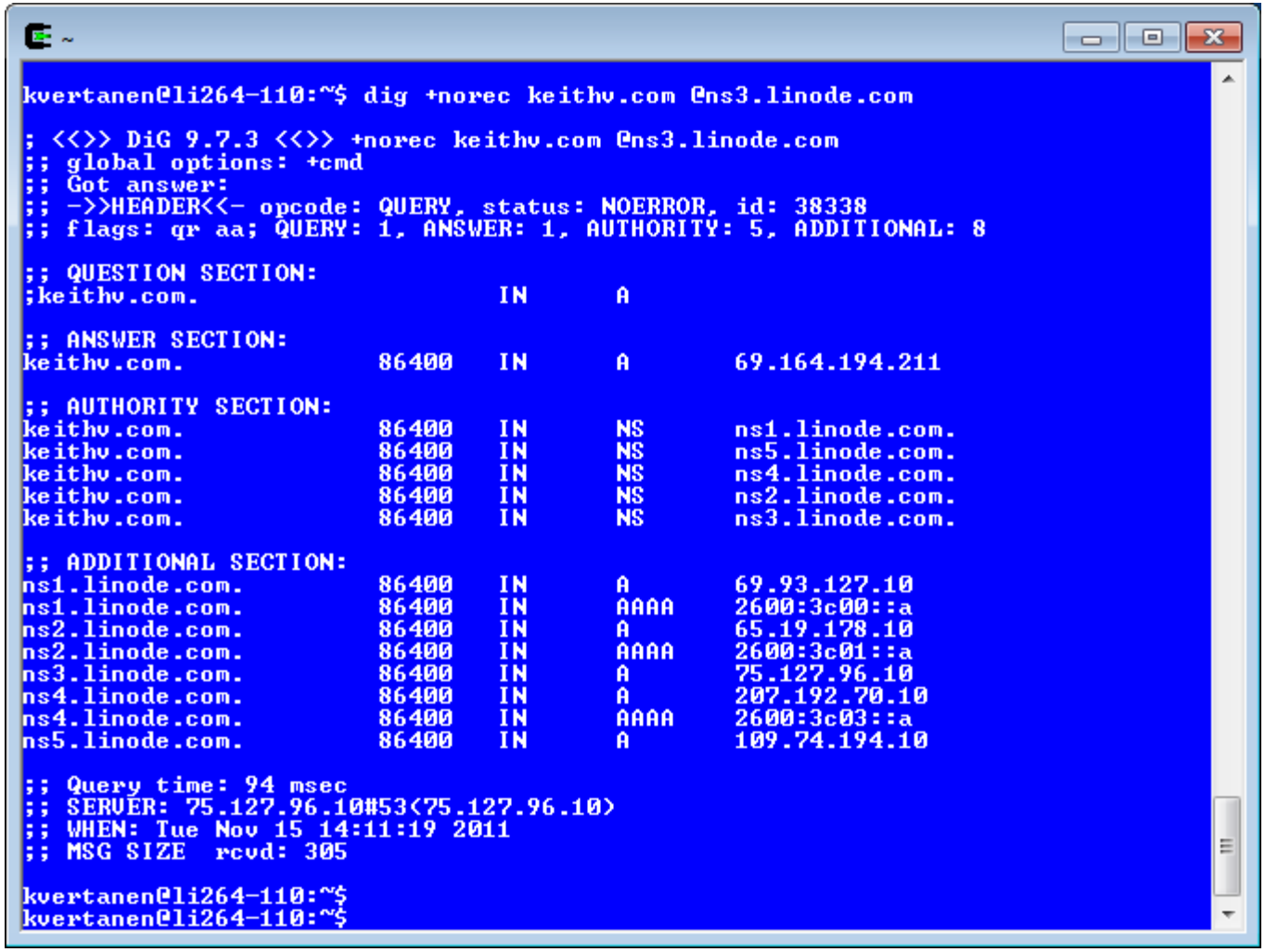





~
kvertanen@li264-110:~$
kvertanen@li264-110:~$ dig keithv.com
; <<>> DiG 9.7.3 <<>> keithv.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43485
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0
;; QUESTION SECTION:
;keithv.com. IN A
;; ANSWER SECTION:
keithv.com. 86400 IN A 69.164.194.211
;; AUTHORITY SECTION:
keithv.com. 86400 IN NS ns1.linode.com.
keithv.com. 86400 IN NS ns4.linode.com.
keithv.com. 86400 IN NS ns5.linode.com.
keithv.com. 86400 IN NS ns3.linode.com.
keithv.com. 86400 IN NS ns2.linode.com.
;; Query time: 127 msec
;; SERVER: 109.74.193.20#53(109.74.193.20)
;; WHEN: Tue Nov 15 14:05:33 2011
;; MSG SIZE rcvd: 141
kvertanen@li264-110:~$ dig keithv.com
; <<>> DiG 9.7.3 <<>> keithv.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47487
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0
;; QUESTION SECTION:
;keithv.com. IN A
;; ANSWER SECTION:
keithv.com. 86391 IN A 69.164.194.211
;; AUTHORITY SECTION:
keithv.com. 86391 IN NS ns1.linode.com.
keithv.com. 86391 IN NS ns4.linode.com.
keithv.com. 86391 IN NS ns5.linode.com.
keithv.com. 86391 IN NS ns3.linode.com.
keithv.com. 86391 IN NS ns2.linode.com.
;; Query time: 0 msec
;; SERVER: 109.74.193.20#53(109.74.193.20)
;; WHEN: Tue Nov 15 14:05:42 2011
;; MSG SIZE rcvd: 141
kvertanen@li264-110:~$


~
kvertanen@li264-110:~$ dig +norec keithv.com @a.root-servers.net
; <<>> DiG 9.7.3 <<>> +norec keithv.com @a.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43988
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14
;; QUESTION SECTION:
;keithv.com. IN A
;; AUTHORITY SECTION:
com. 172800 IN NS a.gtld-servers.net.
com. 172800 IN NS b.gtld-servers.net.
com. 172800 IN NS c.gtld-servers.net.
com. 172800 IN NS d.gtld-servers.net.
com. 172800 IN NS e.gtld-servers.net.
com. 172800 IN NS f.gtld-servers.net.
com. 172800 IN NS g.gtld-servers.net.
com. 172800 IN NS h.gtld-servers.net.
com. 172800 IN NS i.gtld-servers.net.
com. 172800 IN NS j.gtld-servers.net.
com. 172800 IN NS k.gtld-servers.net.
com. 172800 IN NS l.gtld-servers.net.
com. 172800 IN NS m.gtld-servers.net.
;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800 IN AAAA 2001:503:a83e::2:30
a.gtld-servers.net. 172800 IN A 192.5.6.30
b.gtld-servers.net. 172800 IN AAAA 2001:503:231d::2:30
b.gtld-servers.net. 172800 IN A 192.33.14.30
c.gtld-servers.net. 172800 IN A 192.26.92.30
d.gtld-servers.net. 172800 IN A 192.31.80.30
e.gtld-servers.net. 172800 IN A 192.12.94.30
f.gtld-servers.net. 172800 IN A 192.35.51.30
g.gtld-servers.net. 172800 IN A 192.42.93.30
h.gtld-servers.net. 172800 IN A 192.54.112.30
i.gtld-servers.net. 172800 IN A 192.43.172.30
j.gtld-servers.net. 172800 IN A 192.48.79.30
k.gtld-servers.net. 172800 IN A 192.52.178.30
l.gtld-servers.net. 172800 IN A 192.41.162.30
;; Query time: 18 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Nov 15 14:13:12 2011
;; MSG SIZE rcvd: 500
kvertanen@li264-110:~$


~
kvertanen@li264-110:~$ dig +norec keithv.com @k.gtld-servers.net
; <<>> DiG 9.7.3 <<>> +norec keithv.com @k.gtld-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58455
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 7
;; QUESTION SECTION:
;keithv.com. IN A
;; AUTHORITY SECTION:
keithv.com. 172800 IN NS ns1.linode.com.
keithv.com. 172800 IN NS ns2.linode.com.
keithv.com. 172800 IN NS ns3.linode.com.
keithv.com. 172800 IN NS ns4.linode.com.
;; ADDITIONAL SECTION:
ns1.linode.com. 172800 IN AAAA 2600:3c00::a
ns1.linode.com. 172800 IN A 69.93.127.10
ns2.linode.com. 172800 IN AAAA 2600:3c01::a
ns2.linode.com. 172800 IN A 65.19.178.10
ns3.linode.com. 172800 IN A 75.127.96.10
ns4.linode.com. 172800 IN A 207.192.70.10
ns4.linode.com. 172800 IN AAAA 2600:3c03::a
;; Query time: 16 msec
;; SERVER: 192.52.178.30#53(192.52.178.30)
;; WHEN: Tue Nov 15 14:12:32 2011
;; MSG SIZE rcvd: 255
kvertanen@li264-110:~$
kvertanen@li264-110:~$
kvertanen@li264-110:~$
kvertanen@li264-110:~$
kvertanen@li264-110:~$
kvertanen@li264-110:~$
kvertanen@li264-110:~$


~
kvertanen@li264-110:~$ dig +norec keithv.com @ns3.linode.com
; <<>> DiG 9.7.3 <<>> +norec keithv.com @ns3.linode.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38338
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 8
;; QUESTION SECTION:
;keithv.com. IN A
;; ANSWER SECTION:
keithv.com. 86400 IN A 69.164.194.211
;; AUTHORITY SECTION:
keithv.com. 86400 IN NS ns1.linode.com.
keithv.com. 86400 IN NS ns5.linode.com.
keithv.com. 86400 IN NS ns4.linode.com.
keithv.com. 86400 IN NS ns2.linode.com.
keithv.com. 86400 IN NS ns3.linode.com.
;; ADDITIONAL SECTION:
ns1.linode.com. 86400 IN A 69.93.127.10
ns1.linode.com. 86400 IN AAAA 2600:3c00::a
ns2.linode.com. 86400 IN A 65.19.178.10
ns2.linode.com. 86400 IN AAAA 2600:3c01::a
ns3.linode.com. 86400 IN A 75.127.96.10
ns4.linode.com. 86400 IN A 207.192.70.10
ns4.linode.com. 86400 IN AAAA 2600:3c03::a
ns5.linode.com. 86400 IN A 109.74.194.10
;; Query time: 94 msec
;; SERVER: 75.127.96.10#53(75.127.96.10)
;; WHEN: Tue Nov 15 14:11:19 2011
;; MSG SIZE rcvd: 305
kvertanen@li264-110:~$
kvertanen@li264-110:~$

Summary

- Domain Name System (DNS)
  - Global distributed database
    - Maps human friendly names to IP addresses
    - Critical for the functioning of the Internet
  - DNS resolution multistep process involving:
    - Root servers, top-level domain servers, authoritative servers
  - Caching to improve performance