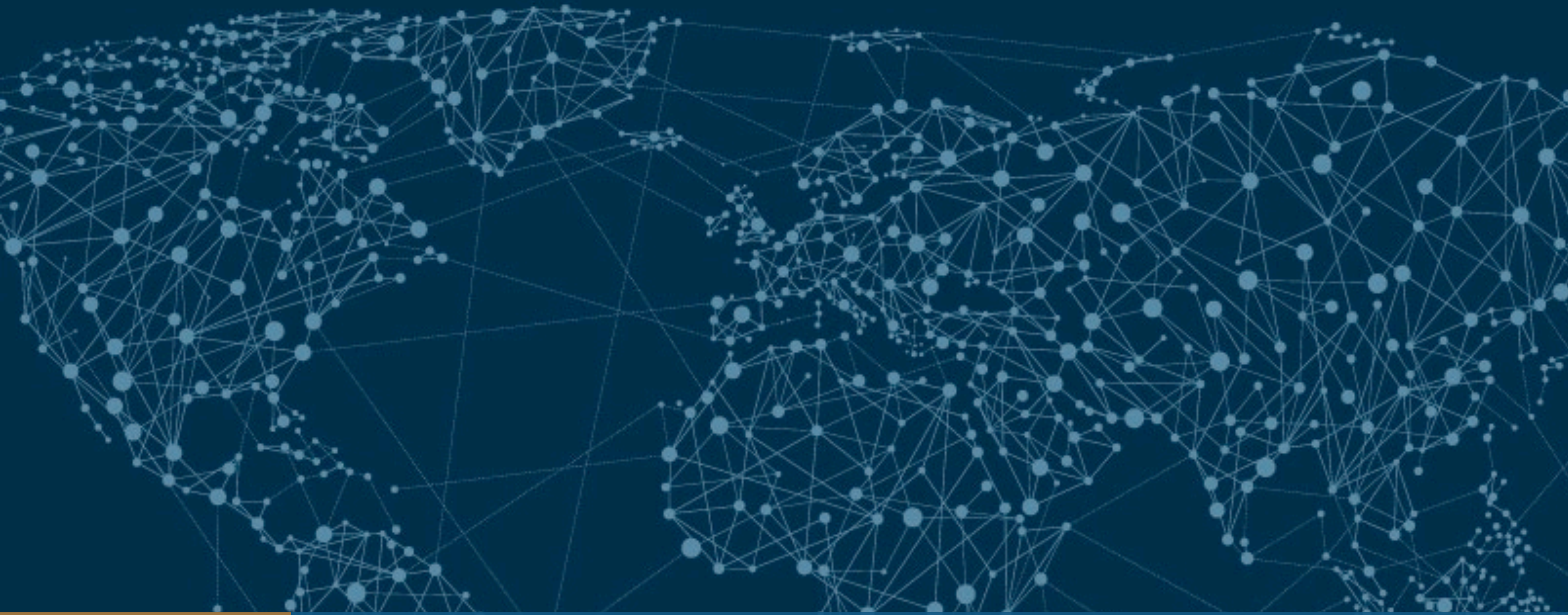


# DNS Abuse Handling

Champika Wijayatunga | APRICOT2015 – Fukuoka – Japan | Feb 2015

# Acknowledgements

- Dave Piscitello
  - Vice President, Security and ICT Coordination – ICANN

# Agenda

1
Brief Overview of DNS

2
Defining Badness in the DNS

3
Identifying Badness and Abuse Sources

4
Tools for Handling DNS Abuse or Misused Domains

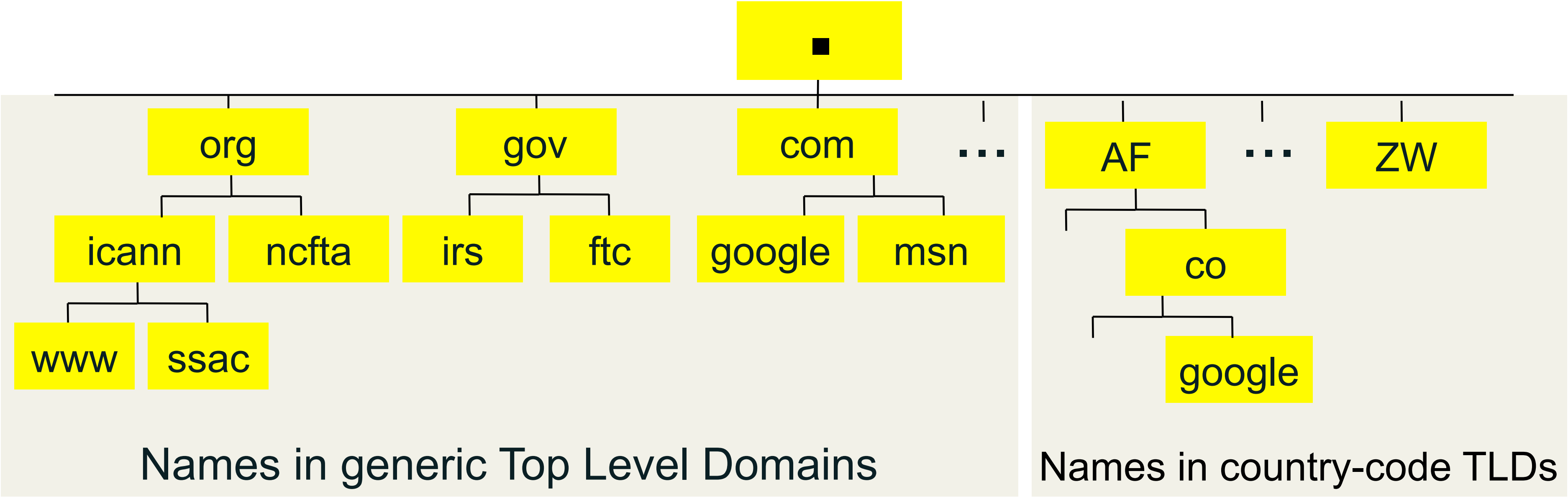
5
Importance of WHOIS

6
Summary / Demo

# Brief Overview of DNS

# DNS Recap

- A **domain** is a node in the Internet name space
  - A domain includes all its descendants
- Domains have names
  - Top-level domain (TLD) names are generic or country-specific
  - TLD *registries* administer domains in the top-level
  - TLD registries *delegate* labels beneath their top level delegation


.
org
gov
com
…
AF
…
ZW
icann
ncfta
irs
ftc
google
msn
co
www
ssac
google
Names in generic Top Level Domains
Names in country-code TLDs

# DNS Recap

- DNS is a distributed database
- Types of DNS servers
  - DNS Authoritative
    - Master
    - Slaves
  - DNS Resolver
    - Recursive
    - Cache
    - Stub resolver

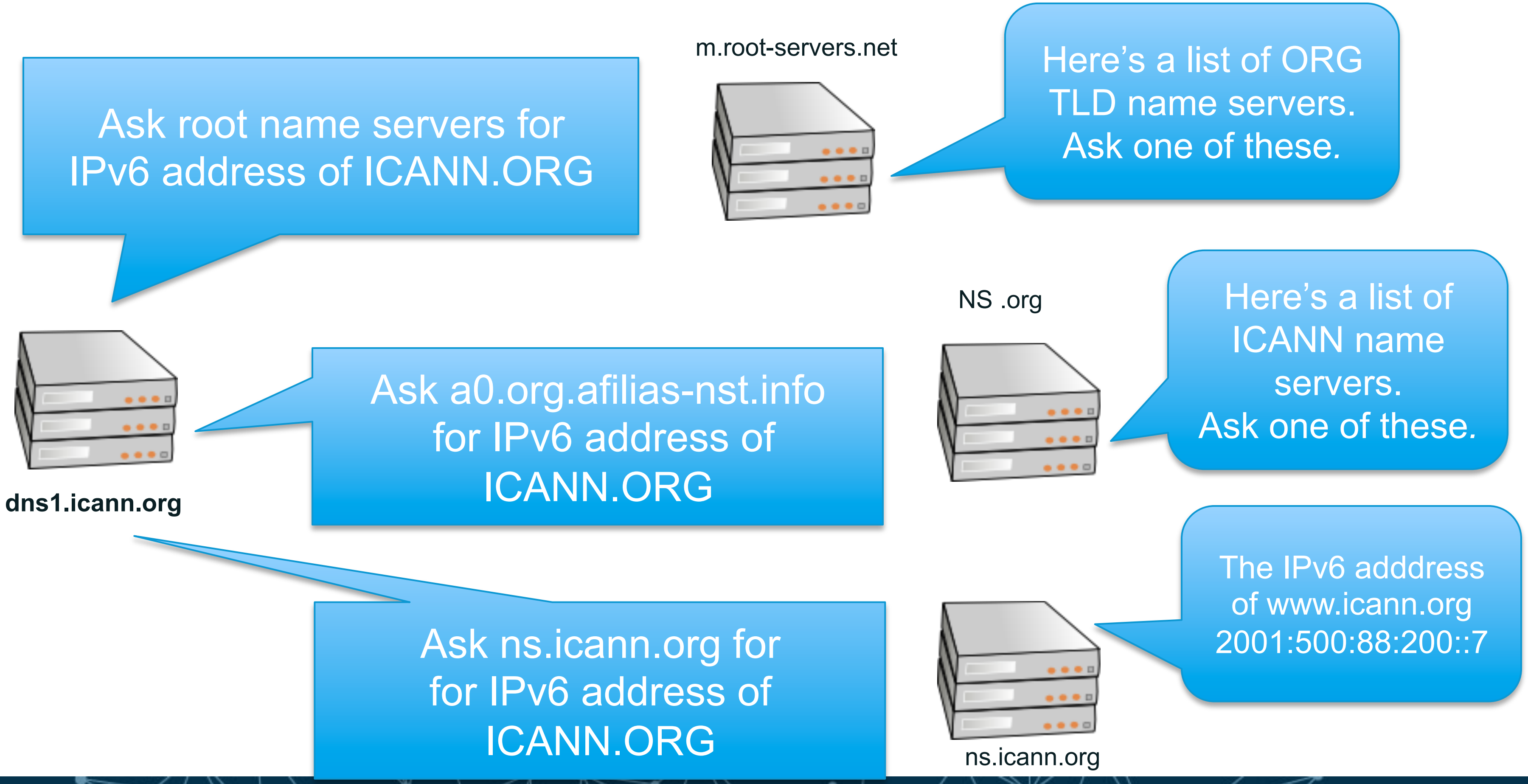
# Operational elements of the DNS

- Authoritative Name Servers host zone data
  - The set of “DNS data” that the registrant publishes
- Recursive Name Resolvers (“resolvers”)
  - Systems that find answers to queries for DNS data
- Caching resolvers
  - Recursive resolvers that not only find answers but also store answers locally for “TTL” period of time
- Client or “stub” resolvers
  - Software in applications, mobile apps or operating systems that query the DNS and process responses

# Domain name “directory assistance”

How does a resolver find the IP address of ICANN.ORG?

- Resolvers find answers by asking questions *iteratively*



dns1.icann.org

Ask root name servers for IPv6 address of ICANN.ORG

m.root-servers.net

Here’s a list of ORG TLD name servers. Ask one of these.

Ask a0.org.afilias-nst.info for IPv6 address of ICANN.ORG

NS .org

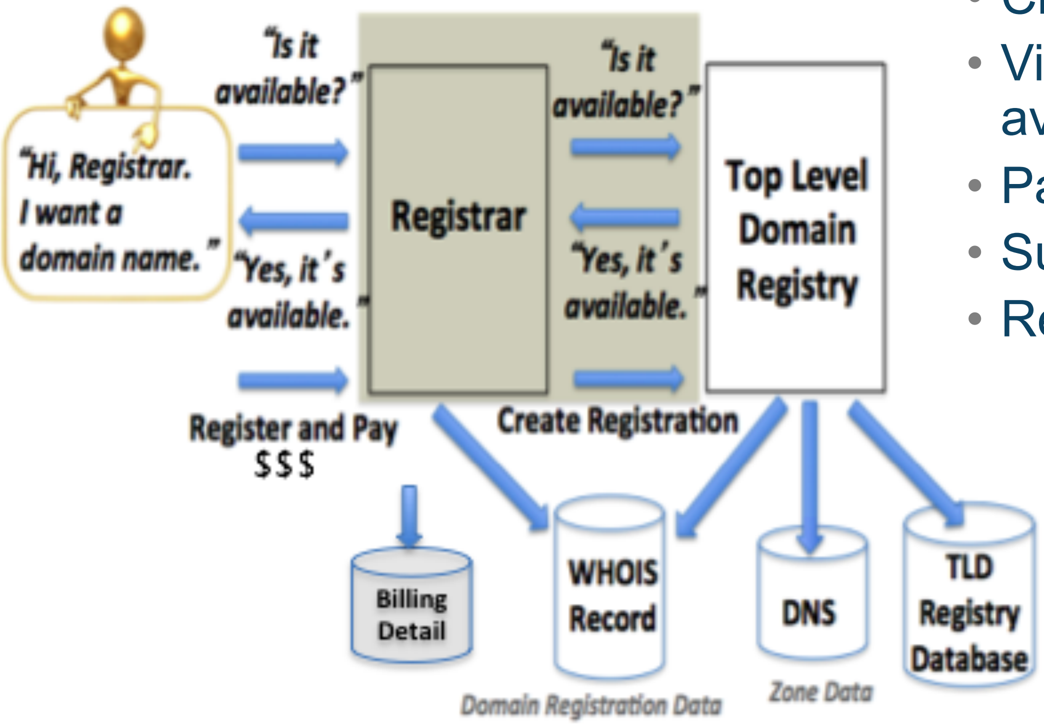
Here’s a list of ICANN name servers. Ask one of these.

Ask ns.icann.org for for IPv6 address of ICANN.ORG

ns.icann.org

The IPv6 adddress of www.icann.org 2001:500:88:200::7

# Domain Name Registration 101

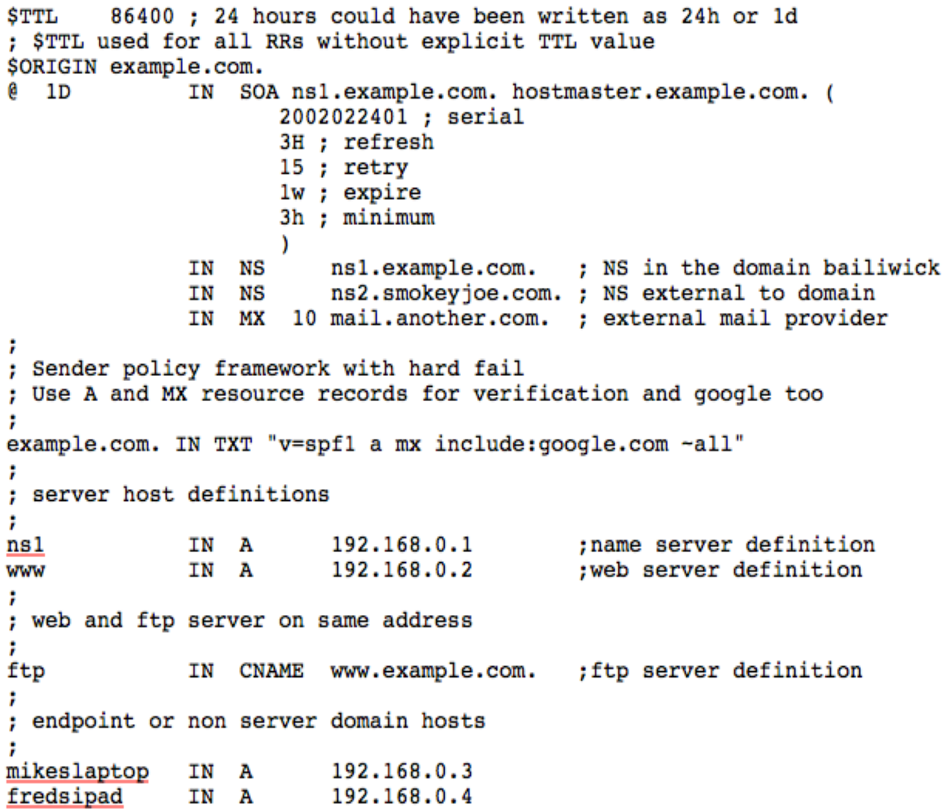


How to register a domain:

- Choose a string e.g., `example`
- Visit a registrar to check string availability in a TLD
- Pay a fee to register the name
- Submit registration information
- Registrar and registries manage:
  - "string" + TLD (managed in registry DB)
  - Contacts, DNS (managed in Whois)
  - DNS, status (managed in Whois DBs)
  - Payment information

# What is a DNS zone *data*?

- DNS zone data are hosted at an *authoritative name server*
  - Each “cut” has zone data (root, TLD, delegations)
- DNS zones contain *resource records that* describe
  - name servers,
  - IP addresses,
  - Hosts,
  - Services
  - Cryptographic keys & signatures…

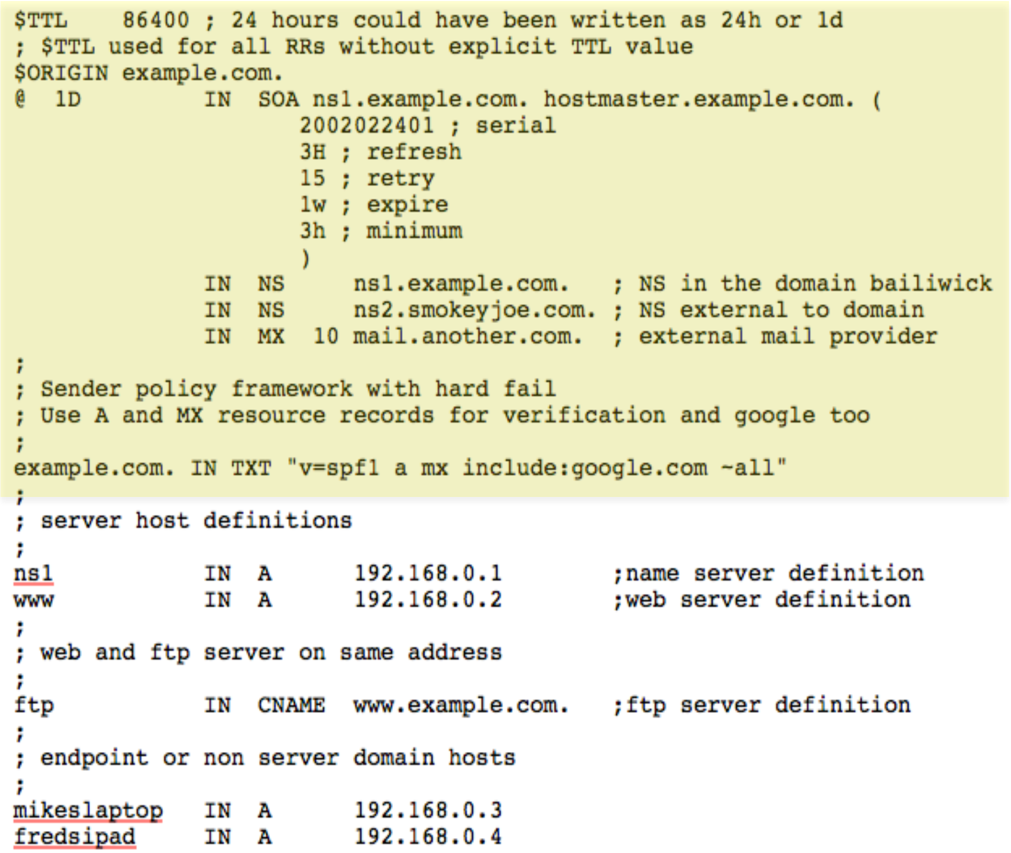


```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
; $TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@  1D          IN  SOA ns1.example.com. hostmaster.example.com. (
                          2002022401 ; serial
                          3H ; refresh
                          15 ; retry
                          1w ; expire
                          3h ; minimum
                          )
               IN  NS     ns1.example.com.   ; NS in the domain bailiwick
               IN  NS     ns2.smokeyjoe.com. ; NS external to domain
               IN  MX  10 mail.another.com.  ; external mail provider
;
; Sender policy framework with hard fail
; Use A and MX resource records for verification and google too
;
example.com. IN TXT "v=spf1 a mx include:google.com ~all"
;
; server host definitions
;
ns1            IN  A      192.168.0.1        ;name server definition
www            IN  A      192.168.0.2        ;web server definition
;
; web and ftp server on same address
;
ftp            IN  CNAME  www.example.com.   ;ftp server definition
;
; endpoint or non server domain hosts
;
mikeslaptop    IN  A      192.168.0.3
fredsipad      IN  A      192.168.0.4
```

*Only US ASCII-7 letters, digits, and hyphens can be used as zone data.*

*In a zone, IDNs strings begin with XN--*

# Common DNS Resource Records



```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
; $TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@  1D          IN  SOA nsl.example.com. hostmaster.example.com. (
                      2002022401 ; serial
                      3H ; refresh
                      15 ; retry
                      1w ; expire
                      3h ; minimum
                      )
              IN  NS     nsl.example.com.   ; NS in the domain bailiwick
              IN  NS     ns2.smokeyjoe.com. ; NS external to domain
              IN  MX  10 mail.another.com.  ; external mail provider
;
; Sender policy framework with hard fail
; Use A and MX resource records for verification and google too
;
example.com. IN TXT "v=spf1 a mx include:google.com ~all"
;
; server host definitions
;
nsl           IN  A      192.168.0.1        ;name server definition
www           IN  A      192.168.0.2        ;web server definition
;
; web and ftp server on same address
;
ftp           IN  CNAME  www.example.com.   ;ftp server definition
;
; endpoint or non server domain hosts
;
mikeslaptop   IN  A      192.168.0.3
fredsipad     IN  A      192.168.0.4
```

Time to live (TTL)

- *How long RRs are accurate*

Start of Authority (SOA) RR

- *Source: zone created here*
- *Administrator's email*
- *Revision number of zone file*

Name Server (NS)

- *IN (Internet)*
- *Name of authoritative server*

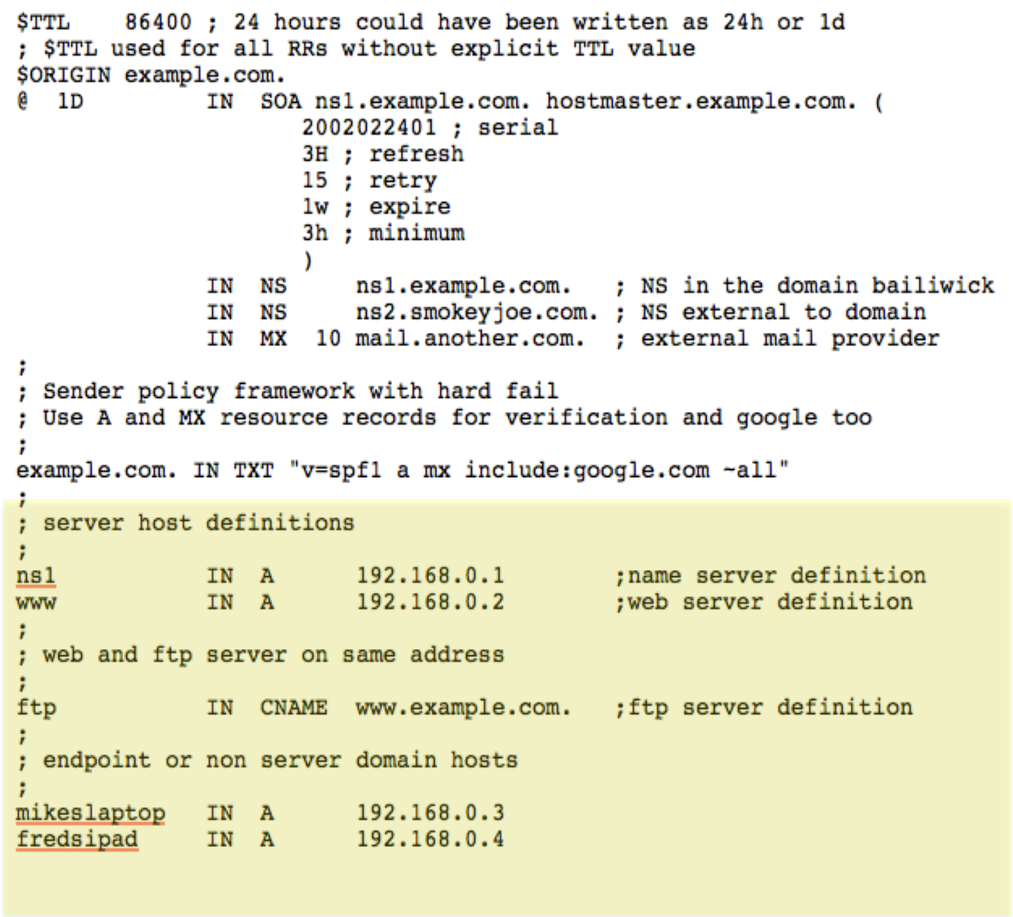
Mail Server (MX)

- *IN (Internet)*
- *Name of mail server*

Sender Policy Framework (TXT)

- *Authorized mail senders*

# Common DNS Resource Records



```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
; $TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@  1D         IN  SOA ns1.example.com. hostmaster.example.com. (
                     2002022401 ; serial
                     3H ; refresh
                     15 ; retry
                     1w ; expire
                     3h ; minimum
                     )
              IN  NS     ns1.example.com.   ; NS in the domain bailiwick
              IN  NS     ns2.smokeyjoe.com. ; NS external to domain
              IN  MX  10 mail.another.com.  ; external mail provider
;
; Sender policy framework with hard fail
; Use A and MX resource records for verification and google too
;
example.com. IN TXT "v=spf1 a mx include:google.com ~all"
;
; server host definitions
;
ns1           IN  A      192.168.0.1        ;name server definition
www           IN  A      192.168.0.2        ;web server definition
;
; web and ftp server on same address
;
ftp           IN  CNAME  www.example.com.   ;ftp server definition
;
; endpoint or non server domain hosts
;
mikeslaptop   IN  A      192.168.0.3
fredsipad     IN  A      192.168.0.4
```

Name server address record

- *NS1 (name server name)*
- *IN (Internet)*
- *A (IPv4)   * AAAA is IPv6*
- *IPv4 address (192.168.0.1)*

Web server address record

- *www (world wide web)*
- *IN (Internet)*
- *A (IPv4)   * AAAA is IPv6*

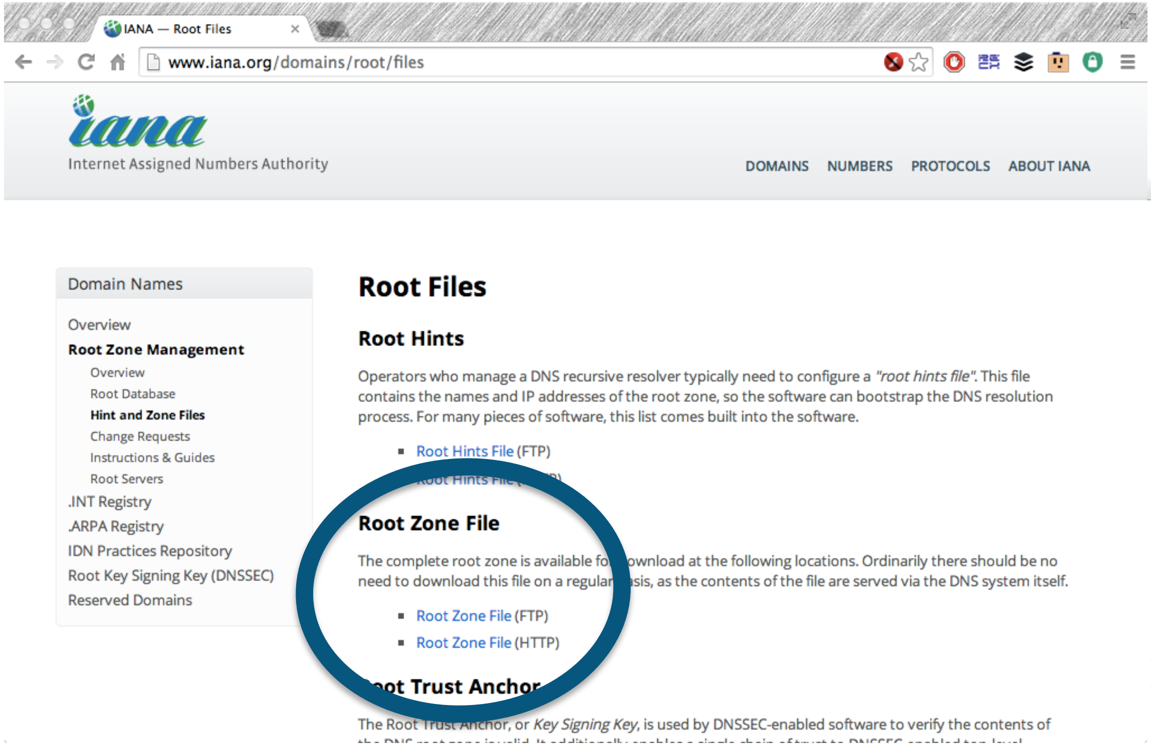
*IPv4 address (192.168.0.2)*

File server address record

- *FTP (file transfer protocol)*
- *IN (Internet)*
- *CNAME means “same address spaces and numbers as www”*

# Where can I get root zone data?

- IANA Root Zone Management
  - http://www.iana.org/domains/root/files



## Root Files

### Root Hints

Operators who manage a DNS recursive resolver typically need to configure a *"root hints file"*. This file contains the names and IP addresses of the root zone, so the software can bootstrap the DNS resolution process. For many pieces of software, this list comes built into the software.

- Root Hints File (FTP)
- Root Hints File (HTTP)

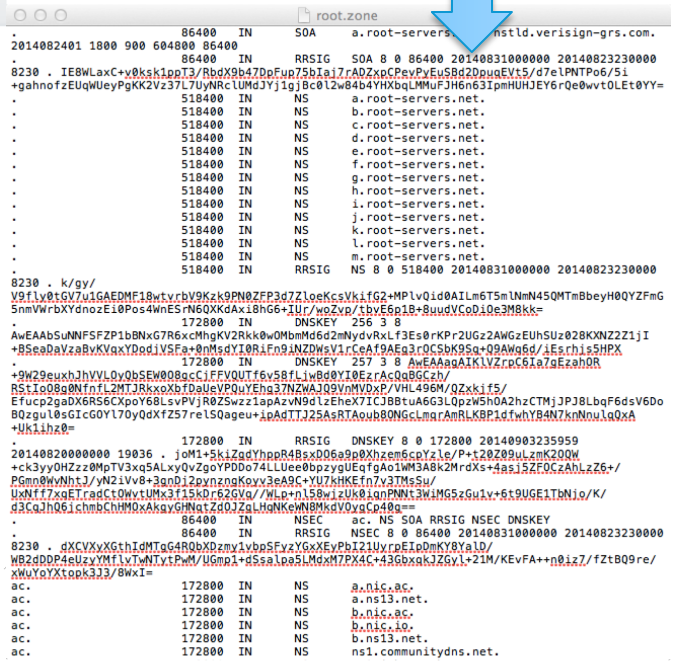
### Root Zone File

The complete root zone is available fo ownload at the following locations. Ordinarily there should be no need to download this file on a regular sis, as the contents of the file are served via the DNS system itself.

- Root Zone File (FTP)
- Root Zone File (HTTP)

### oot Trust Anchor

The Root Trust Anchor, or *Key Signing Key*, is used by DNSSEC-enabled software to verify the contents of



```
.                       86400   IN      SOA     a.root-servers       nstld.verisign-grs.com.
2014082401 1800 900 604800 86400
.                       86400   IN      RRSIG   SOA 8 0 86400 20140831000000 20140823230000
8230 . IE8WLaxC+v0ksk1ppT3/RbdX9b47DpFup75bIaj7rADZxpCPevPyEuSBd2DpuqEVt5/d7elPNTPo6/5i
+gahnofzEUqWUeyPgKK2Vz37L7UyNRclUMdJYj1gjBc0l2w84b4YHXbqLMMuFJH6n63IpmHUHJEY6rQe0wvtOLEt0YY=
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      RRSIG   NS 8 0 518400 20140831000000 20140823230000
8230 . k/gy/
V9fly0tGV7u1GAEDMF18wtvrbV9Kzk9PN0ZFP3d7ZloeKcsVkifG2+MPlvQid0AILm6T5mlNmN45QMTmBbeyH0QYZFmG
5nmVWrbXYdnozEi0Pos4WnESrN6QXKdAxi8hG6+IUr/woZvp/tbvE6p1B+8uudVCoDiOe3M8kk=
.                       172800  IN      DNSKEY  256 3 8
AwEAAbSuNNFSFZP1bBNxG7R6xcMhgKV2Rkk0wOMbmMd6d2mNydvRxLf3Es0rKPr2UGz2AWGzEUhSUz028KXNZ2Z1jI
+BSeaDaVzaBvKVqxYDodjVSFa+0nMsdYI0RiFn9iNZDWsV1rCeAf9AEg3rOCSbK9Sg+Q9AWg6d/iEsrhjs5HPX
.                       172800  IN      DNSKEY  257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR
+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/
RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/
Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6Do
BQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA
+Uk1ihz0=
.                       172800  IN      RRSIG   DNSKEY 8 0 172800 20140903235959
20140820000000 19036 . joM1+5kiZgdYhppR4BsxDO6a9p0Xhzem6cpYzle/P+t20Z09uLzmK2OQW
+ck3yyOHZzz0MpTV3xq5ALxyQvZgoYPDDo74LLUee0bpzygUEqfgAo1WM3A8k2MrdXs+4asj5ZFOCzAhLzZ6+/
PGmn0WvNhtJ/yN2iVv8+3gnDj2pynzngKoyv3eA9C+YU7kHKEfn7v3TMsSu/
UxNff7xqETradCtOWvtUMx3f15kDr62GVq//WLp+nl58wjzUk0iqnPNNt3WiMG5zGu1v+6t9UGE1TbNjo/K/
d3CqJhQ6jchmbChHMOxAkgyGHNqtZdOJZgLHqNKeWN8MkdVOygCp40g==
.                       86400   IN      NSEC    ac. NS SOA RRSIG NSEC DNSKEY
.                       86400   IN      RRSIG   NSEC 8 0 86400 20140831000000 20140823230000
8230 . dXCVXyXGthIdMTgG4RQbXDzmy1vbpSFyzYGxXEyPbI21UyrpEIpDmKY8YalD/
WB2dDDP4eUzyYMflvTwNTytPwM/UGmp1+dSsalpa5LMdxM7PX4C+43GbxqkJZGyl+21M/KEvFA++n0iz7/fZtBQ9re/
xWuYoYXtopk3J3/8WxI=
ac.                     172800  IN      NS      a.nic.ac.
ac.                     172800  IN      NS      a.ns13.net.
ac.                     172800  IN      NS      b.nic.ac.
ac.                     172800  IN      NS      b.nic.io.
ac.                     172800  IN      NS      b.ns13.net.
ac.                     172800  IN      NS      ns1.communitydns.net.
```

# Registration Data Directory Services

## Whois

Databases containing records of registrations

- Domain Whois
  - Sponsoring Registrar
  - Domain Name Servers
  - Domain Status
  - Creation/Expiry dates
  - Point of Contact
  - DNSSEC data

- Address Whois
  - Regional Internet Registry
  - IPv4/v6 address allocation
  - ASN allocation
  - Creation/Expiry dates
  - Point of Contact

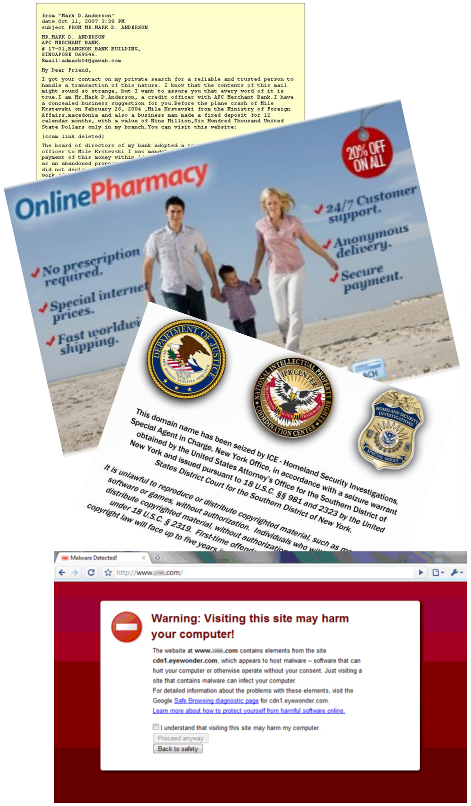
# Relevance to Abuse Handlers

Abuse investigations typically involve collection of most/all of these identifiers

- Domain Names
- Name Servers
- IP networks and addresses
- Autonomous Systems
- Registration data

# Defining Badness in the DNS

# Common Uses for Maliciously Registered Domains



from "Mark D.Anderson"
date Oct 11, 2007 3:38 PM
subject FROM MR.MARK D. ANDERSON

MR.MARK D. ANDERSON
AFC MERCHANT BANK.
# 17-01,BANGKOK BANK BUILDING,
SINGAPORE 069546.
Email:admark04@gawab.com

My Dear Friend,

I got your contact on my private search for a reliable and trusted person to handle a transaction of this nature. I know that the contents of this mail might sound so strange, but I want to assure you that every word of it is true.I am Mr.Mark D.Anderson, a credit officer with AFC Merchant Bank.I have a concealed business suggestion for you.Before the plane crash of Mile Krstevski on February 26, 2004 ,Mile Krstevski from the Ministry of Foreign Affairs,macedonia and also a business man made a fixed deposit for 12 calendar months, with a value of Nine Million,Six Hundred Thousand United State Dollars only in my branch.You can visit this website:

[scam link deleted]

The board of directors of my bank adopted a re
officer to Mile Krstevski I was mandat
payment of this money within
as an abandoned proper
did not decl
work

OnlinePharmacy
20% OFF ON ALL
✓ 24/7 Customer support.
✓ Anonymous delivery.
✓ Secure payment.
✓ No prescription required.
✓ Special internet prices.
✓ Fast worldwide shipping.
DEPARTMENT OF JUSTICE
NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER
IPR CENTER
HOMELAND SECURITY INVESTIGATIONS
SPECIAL AGENT

This domain name has been seized by ICE - Homeland Security Investigations, Special Agent in Charge, New York Office, in accordance with a seizure warrant obtained by the United States Attorney's Office for the Southern District of New York and issued pursuant to 18 U.S.C. §§ 981 and 2323 by the United States District Court for the Southern District of New York.

*It is unlawful to reproduce or distribute copyrighted material, such as mo software or games, without authorization. Individuals who wi distribute copyrighted material, without authorization under 18 U.S.C. § 2319. First-time offende copyright law will face up to five years i*

Malware Detected!

http://www.[redacted].com/

**Warning: Visiting this site may harm your computer!**

The website at **www.[redacted].com** contains elements from the site **cdn1.eyewonder.com**, which appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that contains malware can infect your computer.

For detailed information about the problems with these elements, visit the Google Safe Browsing diagnostic page for cdn1.eyewonder.com.

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer.

Proceed anyway

Back to safety

- Counterfeit goods
- Data exfiltration
- Exploit attacks
- Illegal pharma
- Infrastructure (ecrime name resolution)
- Malware C&C
- Malware distribution (drive-by pages)
- Phishing
- Scams (419, reshipping, stranded traveler…)

# Abuses of other peoples' Domains & DNS

redLine owNz yOu! - Microsoft Internet Explo...
File Edit View Favorites Tools Help
Back Search
Address http://experts.microsoft.fr/
Go Links
Done
Internet

HACKED!

Hi Master (: Your System OwNed By Turkish Hackers!

redLine & rudeb0y & Ejder & The_Bekir & SaCReDSeeR & ASH owNed you!

next target: microsoft.com

TiTHacK.CoM & SavSaK.CoM

- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Tunneling (covert communications)
- Attack obfuscation
- Host file modification (infected devices)
- Changing default resolvers (DNSChanger)
- Poisoning (resolver/ISP)
- Man in the Middle attacks (insertion, capture)

# How Abusers acquire DNS resources

- Purchase using stolen credit cards, compromised accounts
- Abuse“free” services
- Leverage bullet-proof or grey hat hosting/ domain providers
- Hack and exploit legitimate hosts
- Phish registration account credentials and use to modify domain zone data or buy domains

# Abuse (Malicious) Domain
# or a
# Misused (Exploited) Domain?

- *Not always easy to differentiate*

# Collecting Evidence of DNS Abuse/Misuse

- Recent domain registration creation date
- Questionable Whois contact data
- Privacy protection service
- Suspicious values in DNS Zone data (e.g., TTL)
- Spoofing or confusing use of a brand
- Known DGA or malware control point
- Hosted on suspicious (notorious) name servers
- High frequency/volume of name errors
- Suspicious (notorious) hosting location
- Suspicious (notorious) service operator
- Base site content is non-existent or bad
- Linked content is suspicious or bad
- Suspicious mail headers, sender, or content

# Not always easy to identify badness

- Abusers Use Obfuscation
  - Redirection: hacked sites use URL shorteners
  - Recursion: Shortened URLs are shortened
  - One-time use URLs
  - Add subdomains to zone at a hacked DNS server
  - Country- or script-specific content; non-visible content
  - Privacy-protected domain registrations or bogus Whois
- Abusers use ACLs
  - Prevent registrars, Google, LE, investigators from seeing sites
- “Abuse” behaviors can emulate legitimate behavior
  - EXAMPLE: Fast flux versus adaptive networking (e.g., CDNs)

# What is Fast Flux Hosting?

- An evasion technique
- Using fast flux hosting, an attacker
  - Hosts illegal content at a web site
  - Sends phishing email containing URLs that point to compromised computers he commands
  - Commands the compromised computers (proxies) to forward user requests to the attacker's web site
  - Rapidly changes the IP addresses of the proxies to avoid detection and takedown
- Several variants
  - Double flux changes addresses of name servers as well as proxies
  - Domain names are key element of FF attacks

# Steps to investigate & suspend domains

1. Collect evidence of abuse
   A. The purpose of this course is to show ways to do this
2. Determine registrar
   A. Is there a reseller of that registrar involved?
3. Contact registrar abuse desk
   A. Provide evidence of abuse
   B. Point out registration problems
   C. Ask if TOS ,ICANN, ccTLD registry domain suspension policy applies
4. No success?  Contact registry
   A. Same supporting info as registrar
5. Escalate
   A. Sharing/intel networks
   B. National CERT or local LE
   C. ICANN compliance

If you are looking at a suspicious domain, someone else is, too.

# Collecting Evidence of Abuse/Misuse

- Domain names
- Name servers, resolvers
- DNS zone data
- DNS traffic
- Name registration data
- Registry
- Registrar

- Host IP addresses
- IP networks
- Address registration data
- Autonomous systems
- Service providers
- Hosting providers
- Content

**Reputation**

# Tools for Identifying Badness and Abuse Sources

# Tools for Abuse Handlers

- Many tools to help you you identify the abused or malicious resource
  - Domain names, host names, IP addresses, ASNs
  - Hosting location (web, DNS, mail) or origin
  - Content (URL, file, email, attachment)
- Many tools to identify whom to contact or report the resource
  - Databases of domain registrants, operators, ISPs
  - Block list and analysis sites and data providers

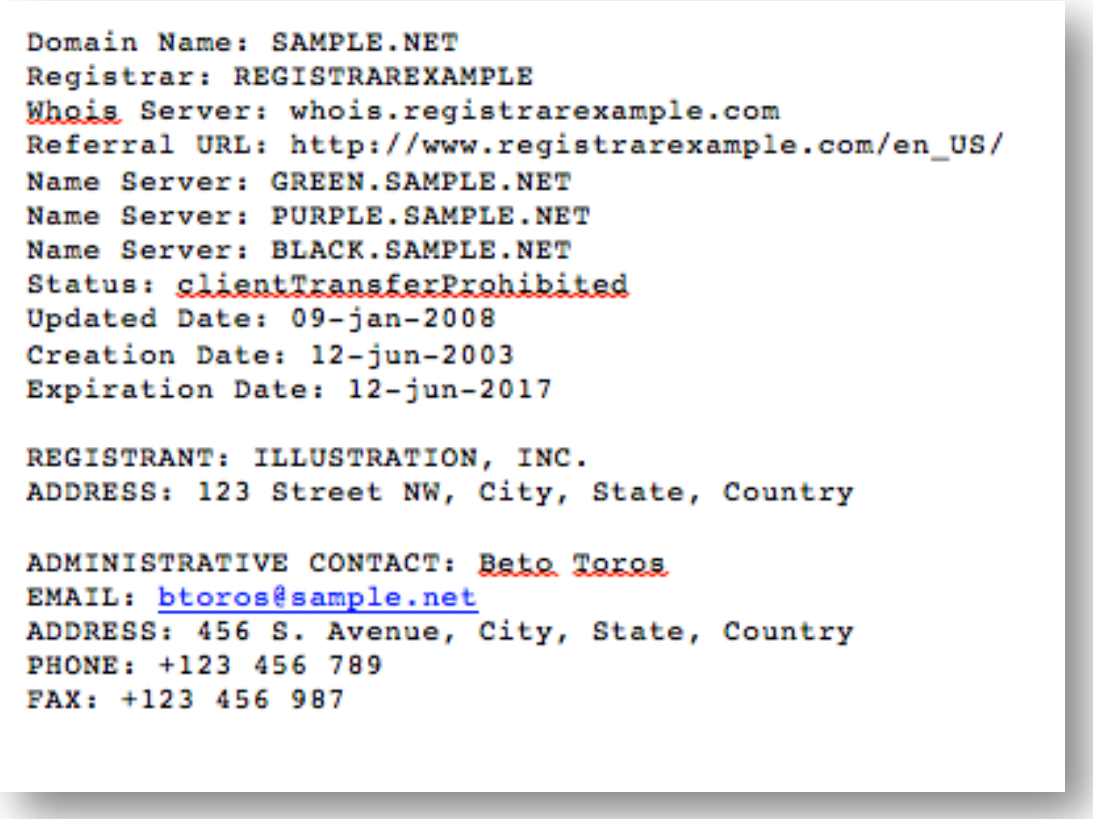
SAVE A COPY OF EVERYTHING YOU VISIT OR QUERY

# WHOIS Database

- Internet Protocol you can use to search registry and registrar databases and discover who registered a domain name or IP address
- Includes contact information for registrant

# A typical WHOIS entry

- Registrant name
- Street address
- Email
- Telephone number
- Creation date
- Expiration date



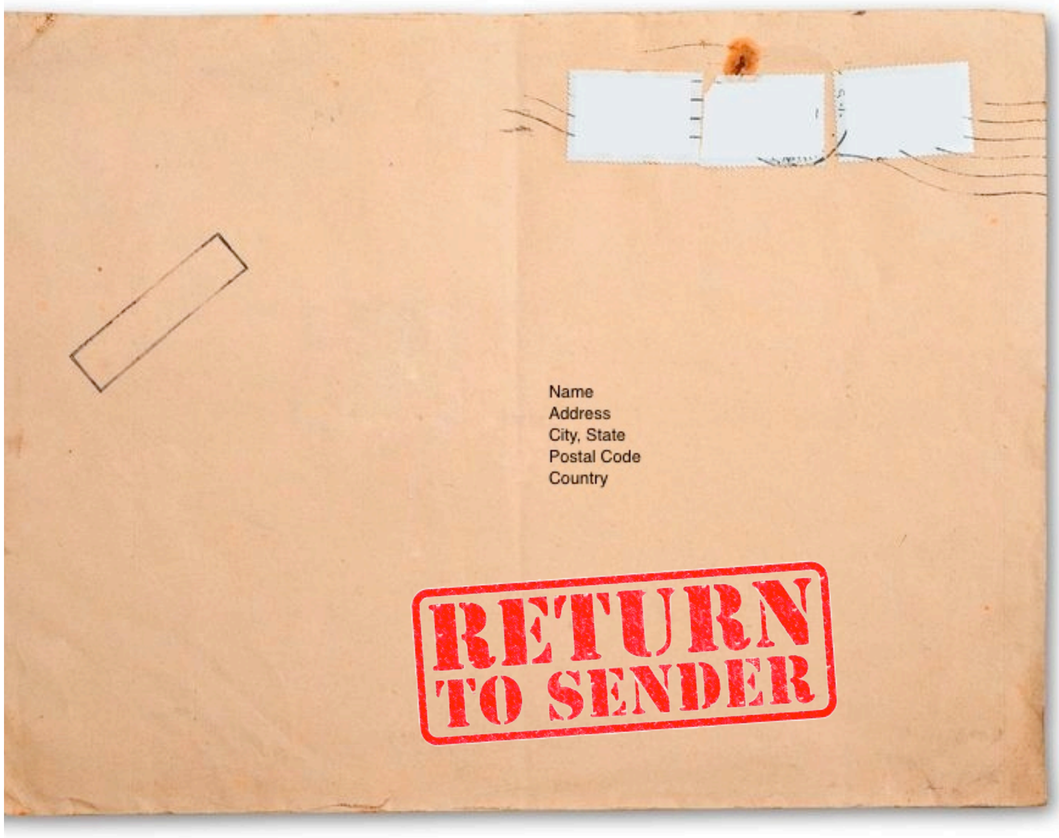
```
Domain Name: SAMPLE.NET
Registrar: REGISTRAREXAMPLE
Whois Server: whois.registrarexample.com
Referral URL: http://www.registrarexample.com/en_US/
Name Server: GREEN.SAMPLE.NET
Name Server: PURPLE.SAMPLE.NET
Name Server: BLACK.SAMPLE.NET
Status: clientTransferProhibited
Updated Date: 09-jan-2008
Creation Date: 12-jun-2003
Expiration Date: 12-jun-2017

REGISTRANT: ILLUSTRATION, INC.
ADDRESS: 123 Street NW, City, State, Country

ADMINISTRATIVE CONTACT: Beto Toros
EMAIL: btoros@sample.net
ADDRESS: 456 S. Avenue, City, State, Country
PHONE: +123 456 789
FAX: +123 456 987
```

# Why is WHOIS important?

- Helps network administrators find and fix system problems and maintain Internet stability
- Manages registration status of domain names
- Assists in fighting abusive use of Internet

# Accuracy of WHOIS data is important

- WHOIS records are created when a domain name is registered
- Information changes over time and should be updated so that registrants can be easily contacted
- Inaccurate records can lead to the domain name's cancellation



# Who do I tell if WHOIS information is wrong or missing?

- Send complaint to ICANN about inaccurate or missing WHOIS data
- http://www.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form

# What if I don't want to share my personal information in the WHOIS database?

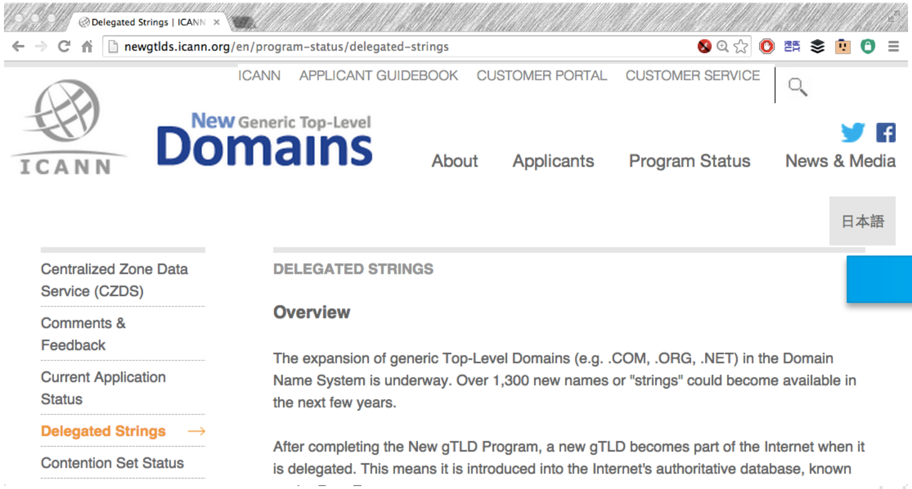
- ICANN requires all accredited registrars and registries to provide contact information for registrants and managers via WHOIS.
- Some registrars offer privacy or proxy services that show the contact information of the service instead of the registrant's.
- These are not truly anonymous. A registrar may be legally compelled to release information in some cases or will voluntarily release information in accordance with its policies.

# WHOIS may change dramatically in future

- An Expert Working Group has proposed a complete overhaul to how registrant information is provided to users.
- Next Generation gTLD Directory Services Model would streamline the way data is retrieved and validated.
- It would also help safeguard data against illegitimate uses.

# Delegation Records for new TLDs

- http://newgtlds.icann.org/en/program-status/delegated-strings
- https://newgtlds.icann.org/newgtlds.csv



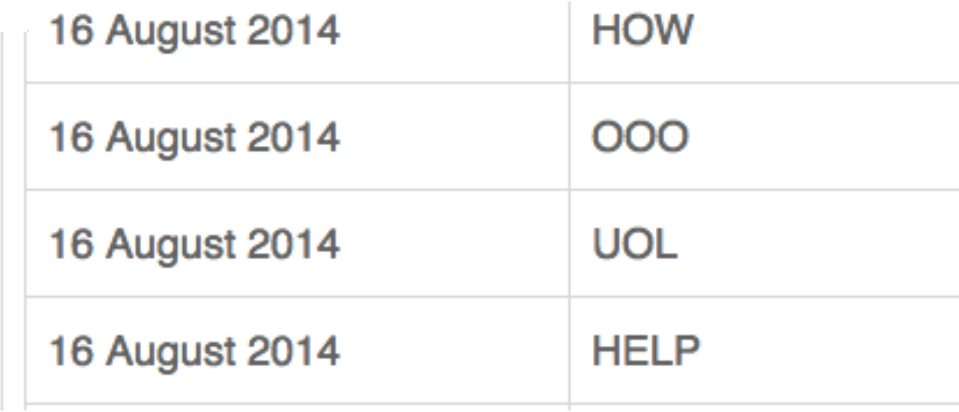
Delegated Strings | ICANN
newgtlds.icann.org/en/program-status/delegated-strings
ICANN
APPLICANT GUIDEBOOK
CUSTOMER PORTAL
CUSTOMER SERVICE
ICANN
New Generic Top-Level Domains
About
Applicants
Program Status
News & Media
日本語
Centralized Zone Data Service (CZDS)
Comments & Feedback
Current Application Status
Delegated Strings →
Contention Set Status

DELEGATED STRINGS

**Overview**

The expansion of generic Top-Level Domains (e.g. .COM, .ORG, .NET) in the Domain Name System is underway. Over 1,300 new names or "strings" could become available in the next few years.

After completing the New gTLD Program, a new gTLD becomes part of the Internet when it is delegated. This means it is introduced into the Internet's authoritative database, known



| | |
|---|---|
| 16 August 2014 | HOW |
| 16 August 2014 | OOO |
| 16 August 2014 | UOL |
| 16 August 2014 | HELP |

# Tools for Investigating DNS

- nslookup (Win), host

  http://support.microsoft.com/kb/200525

- dig (Linux, BSD, MacOS),

  https://library.linode.com/linux-tools/common-commands/dig

- Robtex

  http://www.robtex.com/dns/

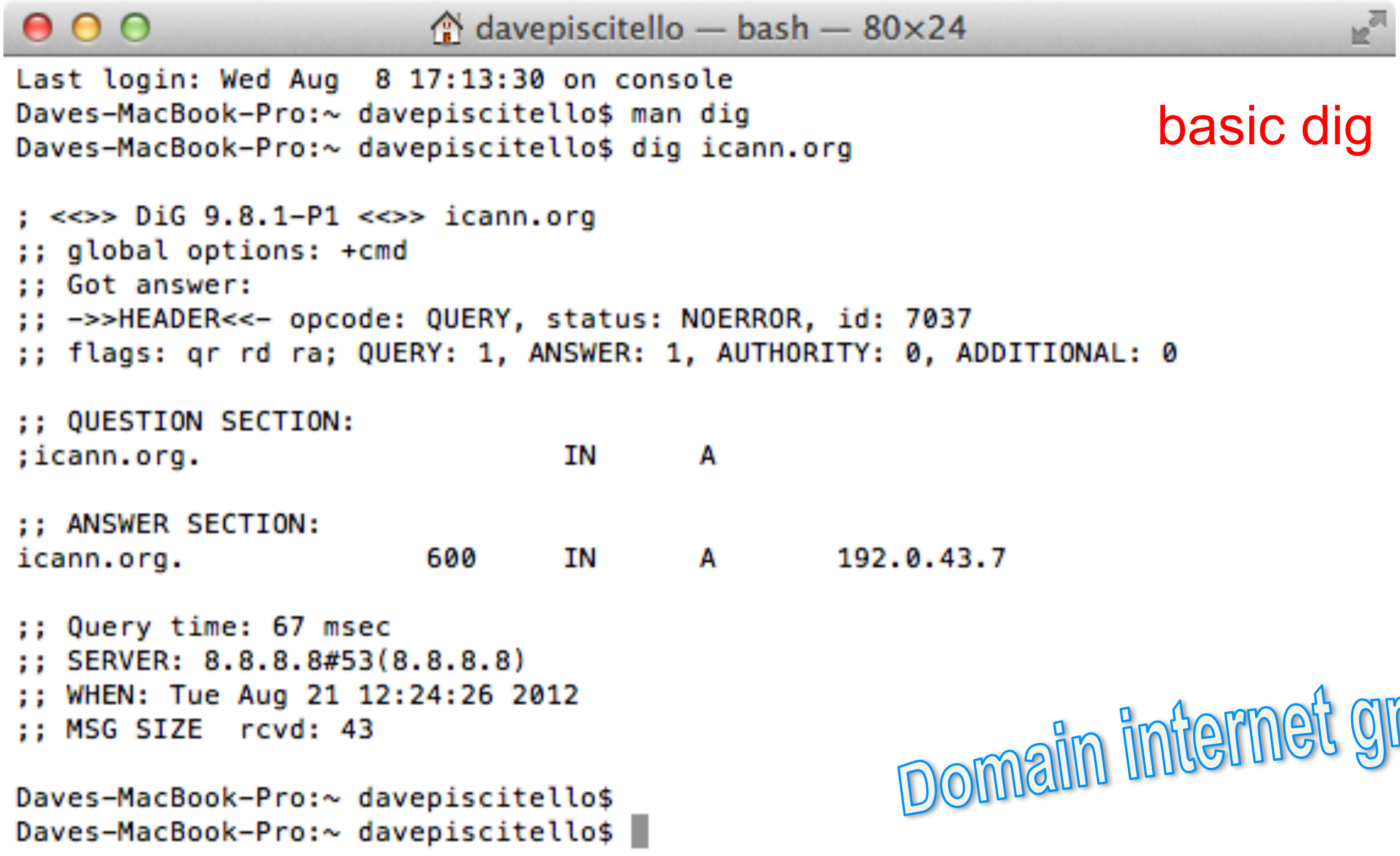
- Passive DNS at BFK.DE

  http://www.bfk.de/bfk_dnslogger.html

- Passive DNS at DNSDB

  https://www.dnsdb.info/

# Using dig (Linux, BSD)

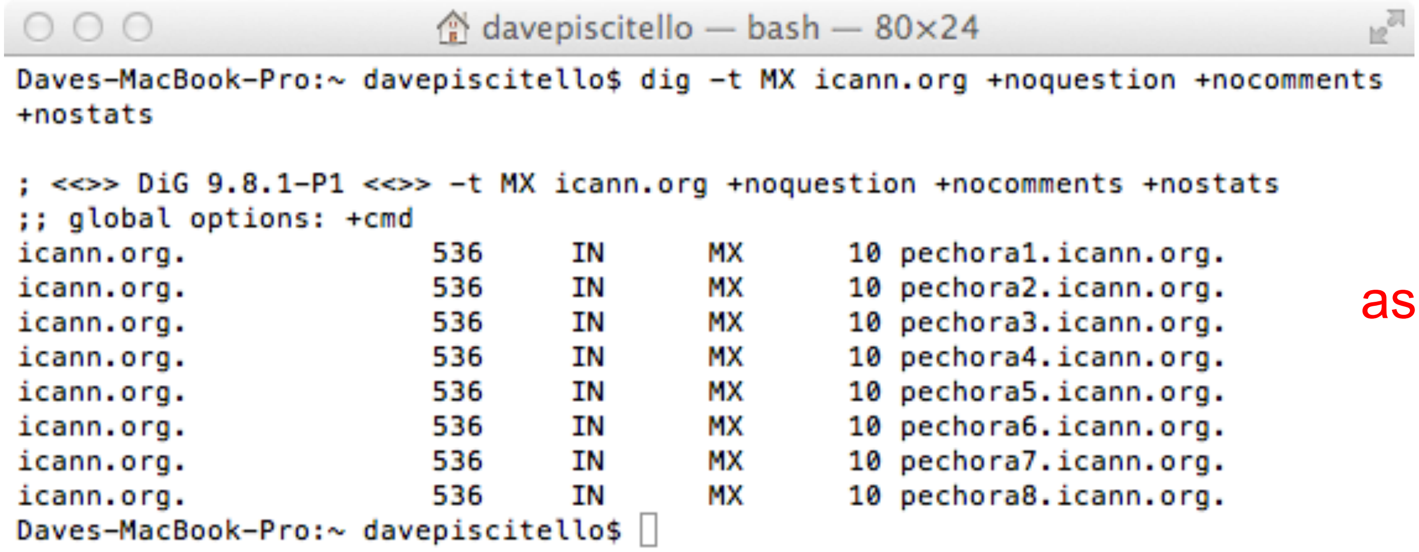


```
Last login: Wed Aug  8 17:13:30 on console
Daves-MacBook-Pro:~ davepiscitello$ man dig
Daves-MacBook-Pro:~ davepiscitello$ dig icann.org

; <<>> DiG 9.8.1-P1 <<>> icann.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7037
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;icann.org.                     IN      A

;; ANSWER SECTION:
icann.org.              600     IN      A       192.0.43.7

;; Query time: 67 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Aug 21 12:24:26 2012
;; MSG SIZE  rcvd: 43

Daves-MacBook-Pro:~ davepiscitello$
Daves-MacBook-Pro:~ davepiscitello$
```

basic dig

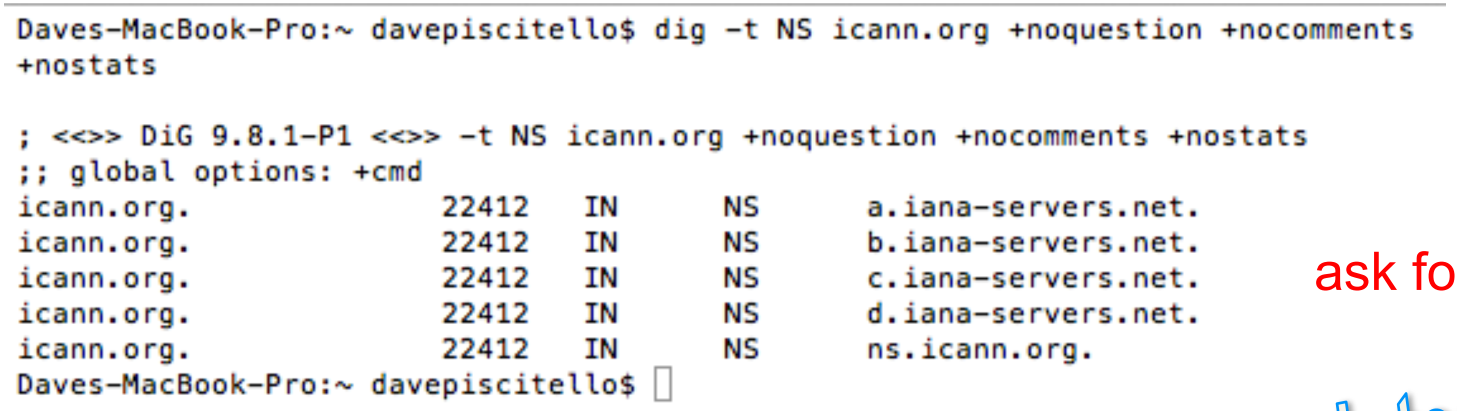
Domain internet groper

# Using dig (Linux, BSD)



```
Daves-MacBook-Pro:~ davepiscitello$ dig -t MX icann.org +noquestion +nocomments
+nostats

; <<>> DiG 9.8.1-P1 <<>> -t MX icann.org +noquestion +nocomments +nostats
;; global options: +cmd
icann.org.              536     IN      MX      10 pechora1.icann.org.
icann.org.              536     IN      MX      10 pechora2.icann.org.
icann.org.              536     IN      MX      10 pechora3.icann.org.
icann.org.              536     IN      MX      10 pechora4.icann.org.
icann.org.              536     IN      MX      10 pechora5.icann.org.
icann.org.              536     IN      MX      10 pechora6.icann.org.
icann.org.              536     IN      MX      10 pechora7.icann.org.
icann.org.              536     IN      MX      10 pechora8.icann.org.
Daves-MacBook-Pro:~ davepiscitello$ 
```

ask for mail servers

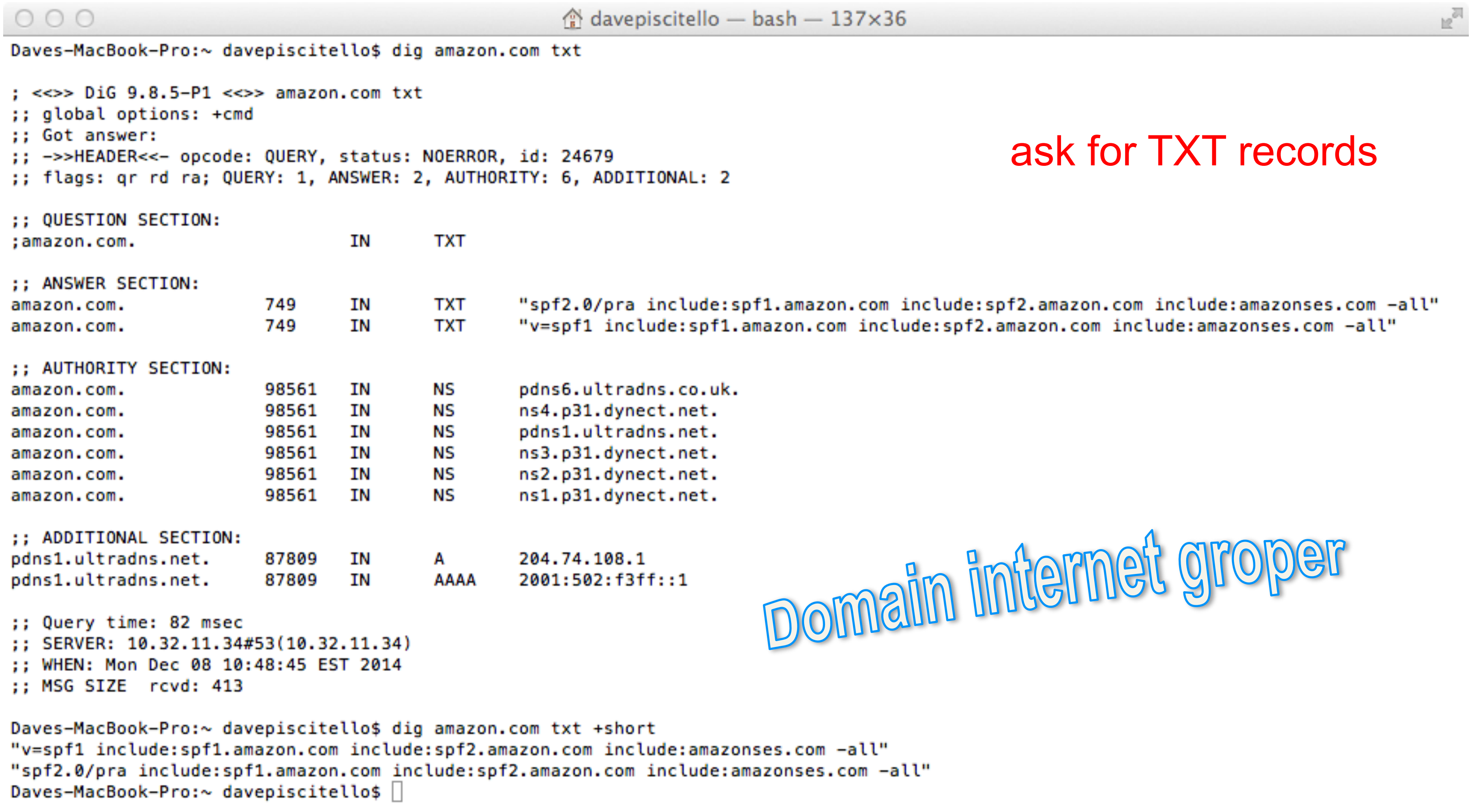


```
Daves-MacBook-Pro:~ davepiscitello$ dig -t NS icann.org +noquestion +nocomments
+nostats

; <<>> DiG 9.8.1-P1 <<>> -t NS icann.org +noquestion +nocomments +nostats
;; global options: +cmd
icann.org.              22412   IN      NS      a.iana-servers.net.
icann.org.              22412   IN      NS      b.iana-servers.net.
icann.org.              22412   IN      NS      c.iana-servers.net.
icann.org.              22412   IN      NS      d.iana-servers.net.
icann.org.              22412   IN      NS      ns.icann.org.
Daves-MacBook-Pro:~ davepiscitello$ 
```

ask for name servers

Domain internet groper

# Using dig (Linux, BSD)

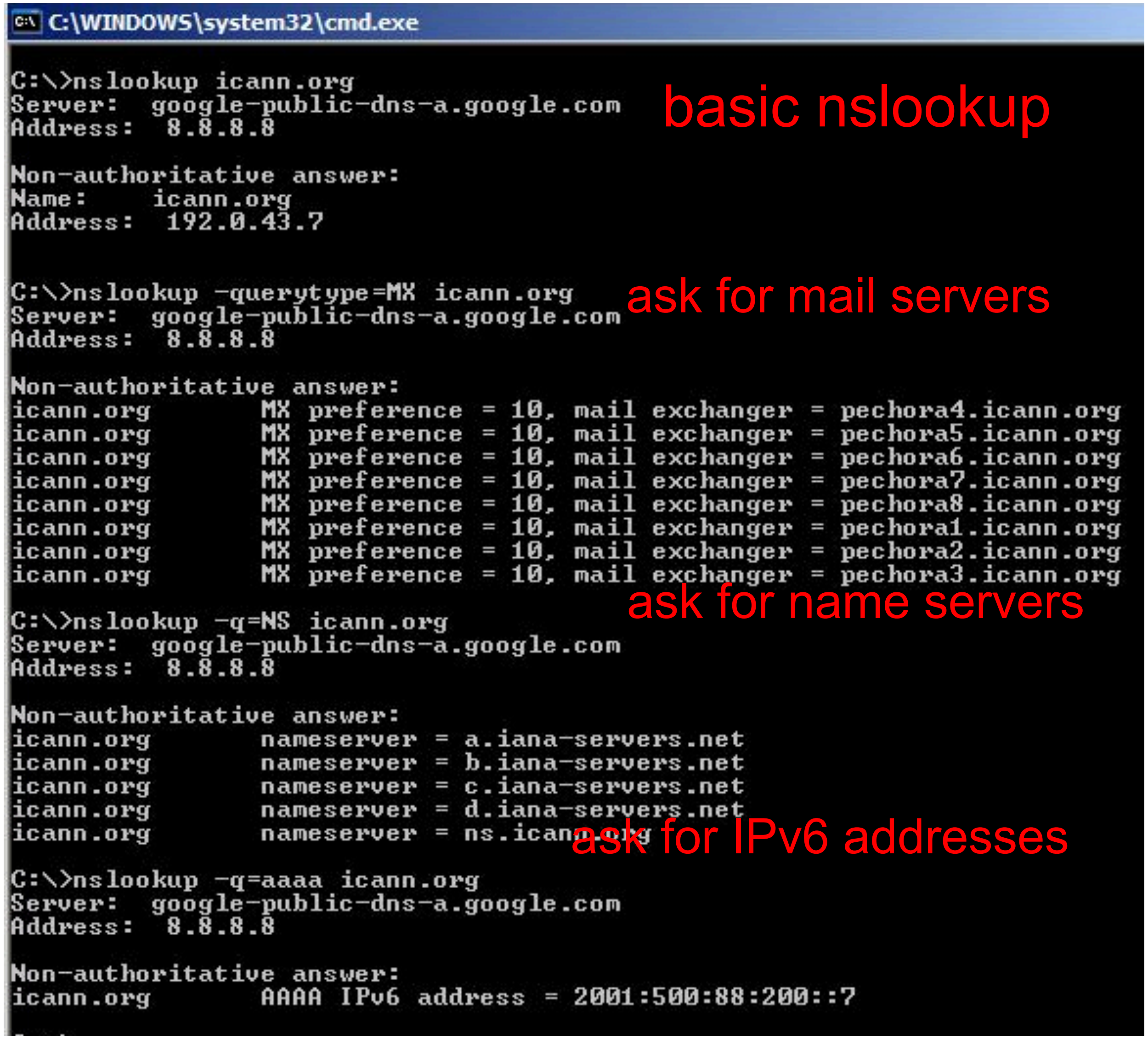


```
Daves-MacBook-Pro:~ davepiscitello$ dig amazon.com txt

; <<>> DiG 9.8.5-P1 <<>> amazon.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24679
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 2

;; QUESTION SECTION:
;amazon.com.                    IN      TXT

;; ANSWER SECTION:
amazon.com.             749     IN      TXT     "spf2.0/pra include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
amazon.com.             749     IN      TXT     "v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"

;; AUTHORITY SECTION:
amazon.com.             98561   IN      NS      pdns6.ultradns.co.uk.
amazon.com.             98561   IN      NS      ns4.p31.dynect.net.
amazon.com.             98561   IN      NS      pdns1.ultradns.net.
amazon.com.             98561   IN      NS      ns3.p31.dynect.net.
amazon.com.             98561   IN      NS      ns2.p31.dynect.net.
amazon.com.             98561   IN      NS      ns1.p31.dynect.net.

;; ADDITIONAL SECTION:
pdns1.ultradns.net.     87809   IN      A       204.74.108.1
pdns1.ultradns.net.     87809   IN      AAAA    2001:502:f3ff::1

;; Query time: 82 msec
;; SERVER: 10.32.11.34#53(10.32.11.34)
;; WHEN: Mon Dec 08 10:48:45 EST 2014
;; MSG SIZE  rcvd: 413

Daves-MacBook-Pro:~ davepiscitello$ dig amazon.com txt +short
"v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
"spf2.0/pra include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
Daves-MacBook-Pro:~ davepiscitello$
```

ask for TXT records

Domain internet groper

# Using nslookup



C:\WINDOWS\system32\cmd.exe

```
C:\>nslookup icann.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    icann.org
Address:  192.0.43.7


C:\>nslookup -querytype=MX icann.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
icann.org       MX preference = 10, mail exchanger = pechora4.icann.org
icann.org       MX preference = 10, mail exchanger = pechora5.icann.org
icann.org       MX preference = 10, mail exchanger = pechora6.icann.org
icann.org       MX preference = 10, mail exchanger = pechora7.icann.org
icann.org       MX preference = 10, mail exchanger = pechora8.icann.org
icann.org       MX preference = 10, mail exchanger = pechora1.icann.org
icann.org       MX preference = 10, mail exchanger = pechora2.icann.org
icann.org       MX preference = 10, mail exchanger = pechora3.icann.org

C:\>nslookup -q=NS icann.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
icann.org       nameserver = a.iana-servers.net
icann.org       nameserver = b.iana-servers.net
icann.org       nameserver = c.iana-servers.net
icann.org       nameserver = d.iana-servers.net
icann.org       nameserver = ns.icann.org

C:\>nslookup -q=aaaa icann.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
icann.org       AAAA IPv6 address = 2001:500:88:200::7
```

basic nslookup

ask for mail servers

ask for name servers

ask for IPv6 addresses

Also try:

“q=any”

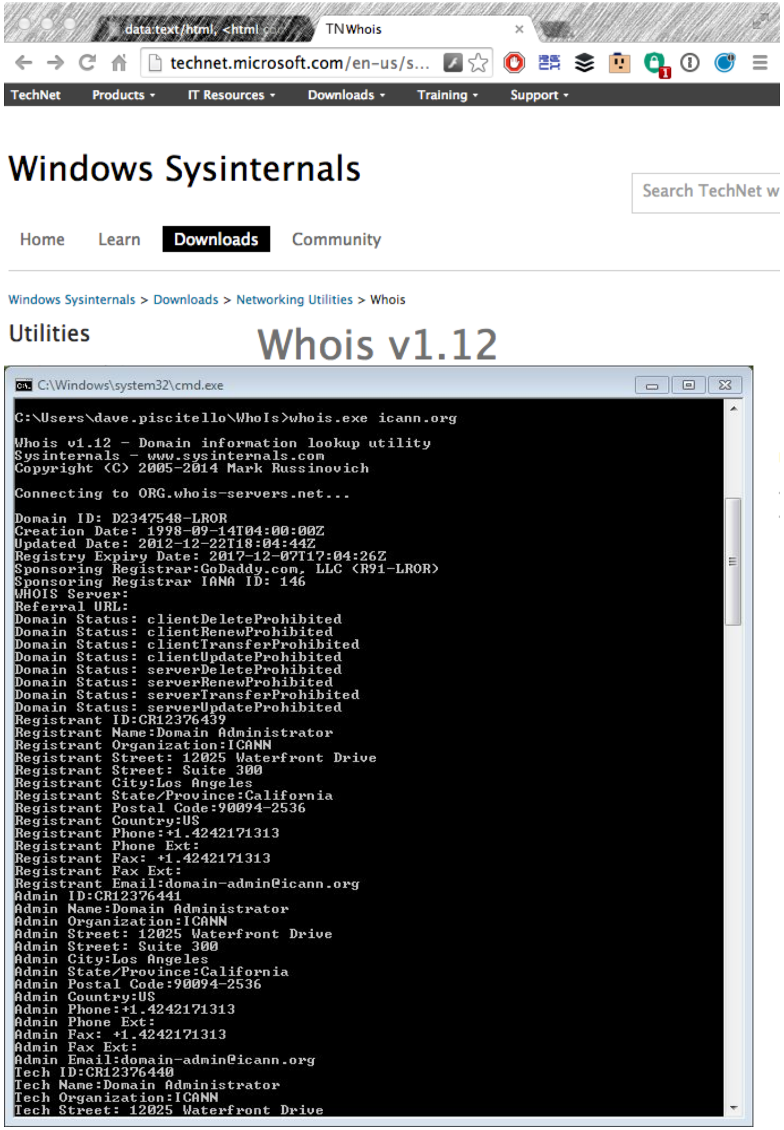
“q=“txt”

Name system lookup

# Passive DNS Replication (PDNS)

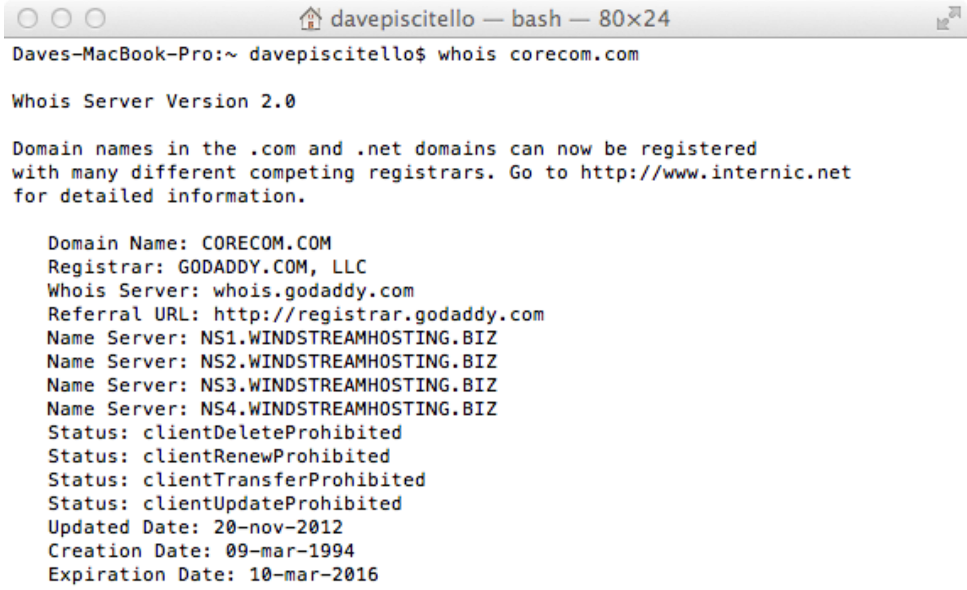
- What does Passive DNS do?
  - Shows query and response traffic, i.e.,
    - The DNS records clients are asking to resolve and
    - The Responses resolvers receives back from authoritative servers
- How does Passive DNS work?
  - Monitor DNS queries & responses (near recursive servers)
  - Put all of the data you monitor into a database
- Query the database to extract behavior
- Best results at big ISPs
  - Physical network location with visibility
  - Filter down to just the DNS queries/responses

# Command line Whois



```
C:\Users\dave.piscitello\WhoIs>whois.exe icann.org

Whois v1.12 - Domain information lookup utility
Sysinternals - www.sysinternals.com
Copyright (C) 2005-2014 Mark Russinovich

Connecting to ORG.whois-servers.net...

Domain ID: D2347548-LROR
Creation Date: 1998-09-14T04:00:00Z
Updated Date: 2012-12-22T18:04:44Z
Registry Expiry Date: 2017-12-07T17:04:26Z
Sponsoring Registrar:GoDaddy.com, LLC (R91-LROR)
Sponsoring Registrar IANA ID: 146
WHOIS Server:
Referral URL:
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: clientUpdateProhibited
Domain Status: serverDeleteProhibited
Domain Status: serverRenewProhibited
Domain Status: serverTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID:CR12376439
Registrant Name:Domain Administrator
Registrant Organization:ICANN
Registrant Street: 12025 Waterfront Drive
Registrant Street: Suite 300
Registrant City:Los Angeles
Registrant State/Province:California
Registrant Postal Code:90094-2536
Registrant Country:US
Registrant Phone:+1.4242171313
Registrant Phone Ext:
Registrant Fax: +1.4242171313
Registrant Fax Ext:
Registrant Email:domain-admin@icann.org
Admin ID:CR12376441
Admin Name:Domain Administrator
Admin Organization:ICANN
Admin Street: 12025 Waterfront Drive
Admin Street: Suite 300
Admin City:Los Angeles
Admin State/Province:California
Admin Postal Code:90094-2536
Admin Country:US
Admin Phone:+1.4242171313
Admin Phone Ext:
Admin Fax: +1.4242171313
Admin Fax Ext:
Admin Email:domain-admin@icann.org
Tech ID:CR12376440
Tech Name:Domain Administrator
Tech Organization:ICANN
Tech Street: 12025 Waterfront Drive
```

Linux, BSD have it:



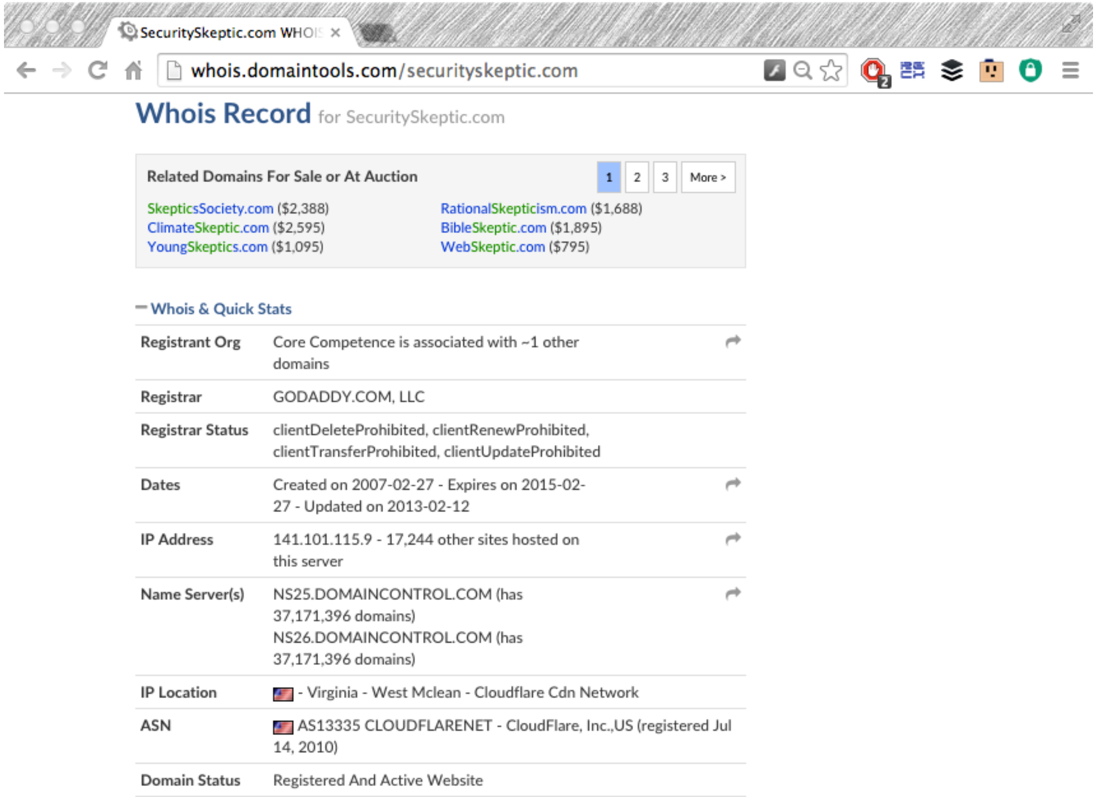
```
Daves-MacBook-Pro:~ davepiscitello$ whois corecom.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: CORECOM.COM
   Registrar: GODADDY.COM, LLC
   Whois Server: whois.godaddy.com
   Referral URL: http://registrar.godaddy.com
   Name Server: NS1.WINDSTREAMHOSTING.BIZ
   Name Server: NS2.WINDSTREAMHOSTING.BIZ
   Name Server: NS3.WINDSTREAMHOSTING.BIZ
   Name Server: NS4.WINDSTREAMHOSTING.BIZ
   Status: clientDeleteProhibited
   Status: clientRenewProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 20-nov-2012
   Creation Date: 09-mar-1994
   Expiration Date: 10-mar-2016
```

Use whois domain.tld > domainwhois.txt to save output

Download for DOS here:

http://technet.microsoft.com/en-us/sysinternals/bb897435.aspx

# Web based Whois tools



SecuritySkeptic.com WHOIS ×
whois.domaintools.com/securityskeptic.com

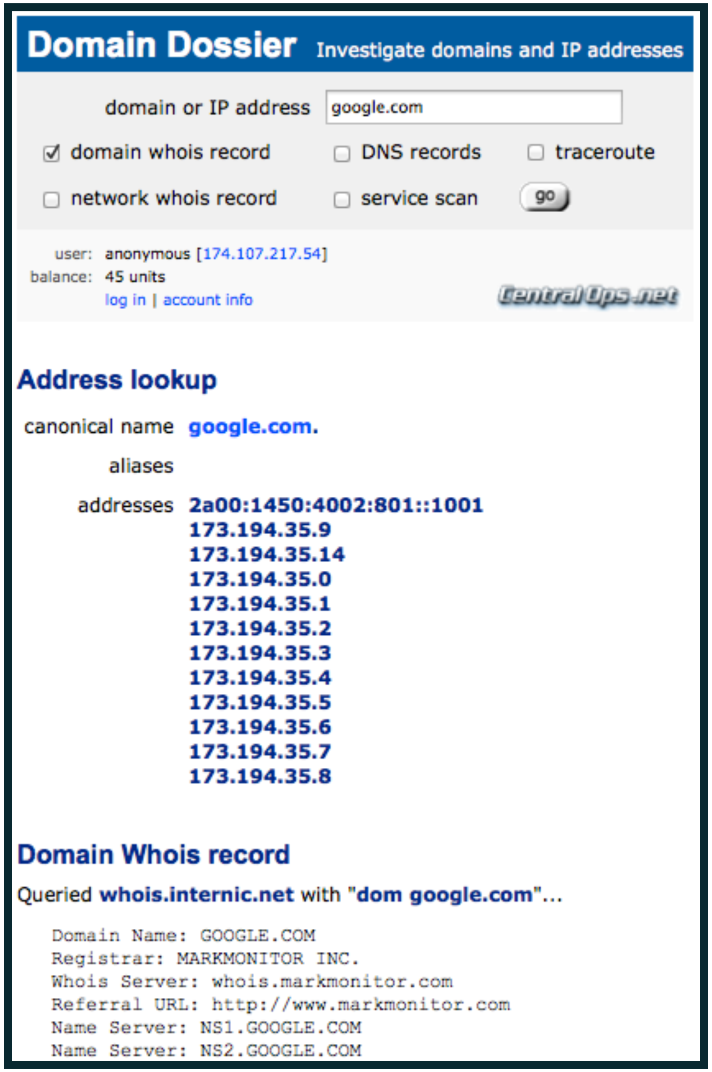
## Whois Record for SecuritySkeptic.com

Related Domains For Sale or At Auction

| | |
|---|---|
| SkepticsSociety.com ($2,388) | RationalSkepticism.com ($1,688) |
| ClimateSkeptic.com ($2,595) | BibleSkeptic.com ($1,895) |
| YoungSkeptics.com ($1,095) | WebSkeptic.com ($795) |

– Whois & Quick Stats

| | |
|---|---|
| Registrant Org | Core Competence is associated with ~1 other domains |
| Registrar | GODADDY.COM, LLC |
| Registrar Status | clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited |
| Dates | Created on 2007-02-27 - Expires on 2015-02-27 - Updated on 2013-02-12 |
| IP Address | 141.101.115.9 - 17,244 other sites hosted on this server |
| Name Server(s) | NS25.DOMAINCONTROL.COM (has 37,171,396 domains)<br>NS26.DOMAINCONTROL.COM (has 37,171,396 domains) |
| IP Location | - Virginia - West Mclean - Cloudflare Cdn Network |
| ASN | AS13335 CLOUDFLARENET - CloudFlare, Inc.,US (registered Jul 14, 2010) |
| Domain Status | Registered And Active Website |



**Domain Dossier** Investigate domains and IP addresses

domain or IP address: google.com

☑ domain whois record ☐ DNS records ☐ traceroute
☐ network whois record ☐ service scan

user: anonymous [174.107.217.54]
balance: 45 units
log in | account info

### Address lookup

canonical name google.com.

aliases

addresses 2a00:1450:4002:801::1001
173.194.35.9
173.194.35.14
173.194.35.0
173.194.35.1
173.194.35.2
173.194.35.3
173.194.35.4
173.194.35.5
173.194.35.6
173.194.35.7
173.194.35.8

### Domain Whois record

Queried **whois.internic.net** with "**dom google.com**"...

```
Domain Name: GOOGLE.COM
Registrar: MARKMONITOR INC.
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
```

- Domain Tools
- http://domaintools.com
- Domain Dossier
  - http://centralops.net/co/DomainDossier.aspx

# Identifying IPs and ASNs

Address Whois:

- AfriNIC.net
- APNIC.net
- ARIN.net
- LACNIC.net
- RIPE.net

- Shadowserver Whois
  - http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP
- Team Cymru
  - https://asn.cymru.com/
- Robtex (Share Tab)
  - http://robtex.com
- DNSSTuff

  http://www.dnsstuff.com

# Tools for Investigating Reputation

Reputation services, Block lists, Malware Analysis

Spamhaus
SURBL
ZeusTracker
Team Cymru
Alexa
Clean MX
CBL
Stopbadware

Google
VirusTotal
Anubis
ThreatExpert
URLquery
SiteVet
Wepawet
MalwareTracker

# Reputation Services

- Organizations that classify
  - IP address allocations,
  - Domain names,
  - hosting providers,
  - ISPs,
- As legitimate or malicious using a scoring system

- URLQuery.net
- sitevet.com
- HOSTexploit.com
- Spamhaus.org
- ProjectHoneypot.org
- MalwareDomainList

# Tracking down malware domains

I’ve got what I think is malware

- – How do I figure out if it’s a malware?
- How do I figure out if it’s controlled via a domain or host?

- Malware analysis methodologies include:
  - Grab a sample: fingerprint files, dissect, disassemble…
  - Run wireshark to capture traffic
  - Catalog the IPs and ASNs of hosts exchanging traffic with my botted machine
  - Passively map DNS
  - Share what I find with other skilled white hats
- Not your day job? Consider publicly available tools
- Web based malware analysis tools
  - Virustotal, for malware analysis
    - http://www.virustotal.com

# Summary

1
Brief Overview of DNS

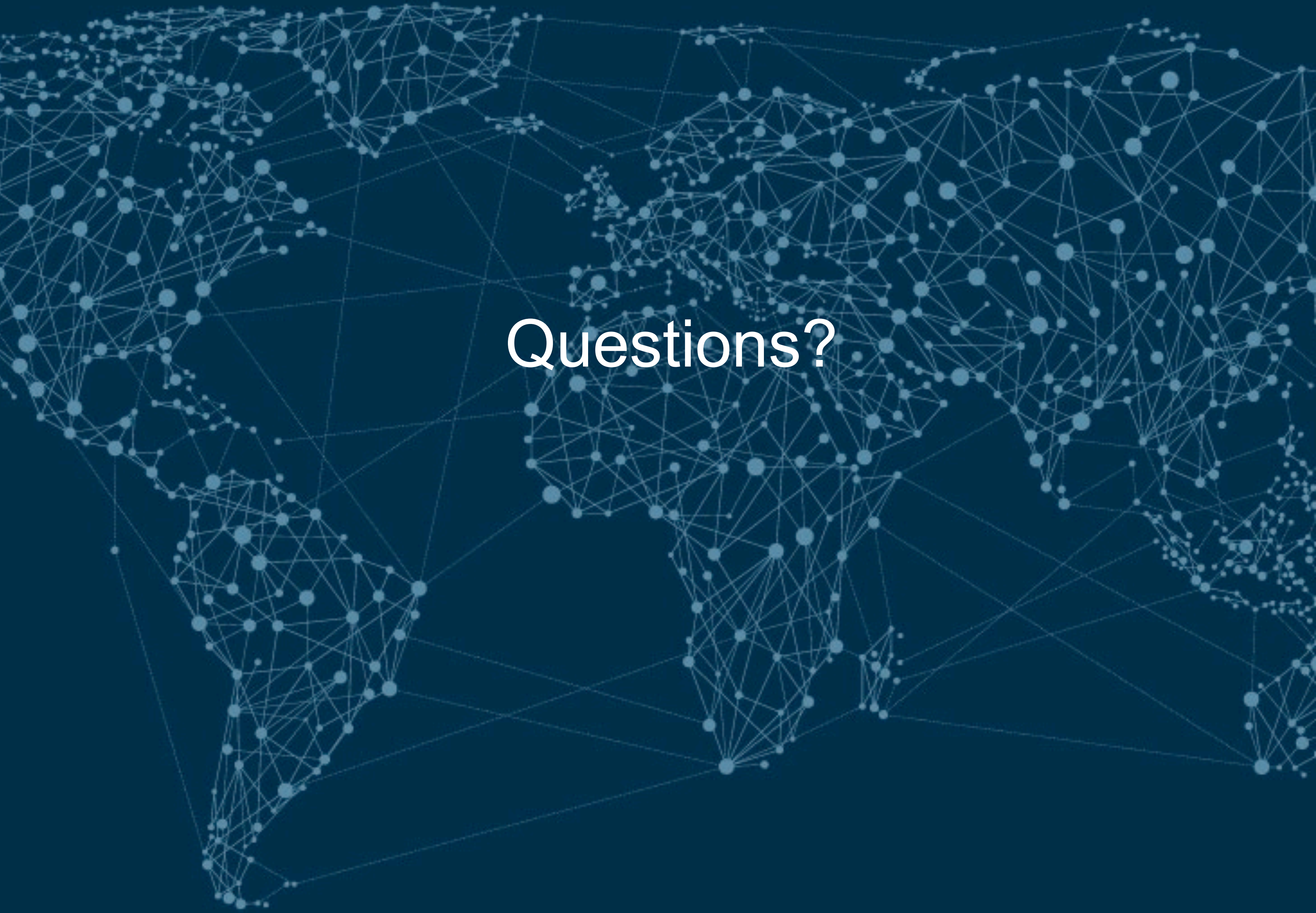
2
Defining Badness in the DNS

3
Identifying Badness and Abuse Sources

4
Tools for Handling DNS Abuse or Misused Domains

5
Importance of WHOIS

6
Summary / Demo



# Questions?

# Thank You!

<champika.wijayatunga@icann.org>