Investigating Domain Names & Internet Numbers

ICANN Security Team | CERT-UK| January 2016

Syllabus

- Brief Overview of Internet Identifiers
- Common Uses for Criminal Domains
- Taking action on a host or domain
- Preparation
- Tools for Investigating Badness
  (Examples, hands-on, walk-thrus)

Time on Topic

About this course

- More than introductory but not advanced
- LOTS of information
- Fast paced
- Repetition is the key to learning

Try a simple investigation every day. These will make you familiar if not proficient with the methods and concepts

About the training materials

- The slides serve many purposes
  - Guide the discussion
  - Support live demonstration, encourage hands on
  - Record of the resources you can use
- Please do not post to a public site or repository
- Please contact us before you distribute outside your agency or organization

Course Scope and Limitations

We train how to gather information related to identifier systems abuse or misuse

The tools we demonstrate are freely available or offered commercially

All of the information we use is publicly available or commercially accessible via an API or for fee access

We do not train how to collect metadata or bulk personal data or for specific individuals or tangible things

Brief Overview of Internet Identifiers

What Are Internet Identifiers?

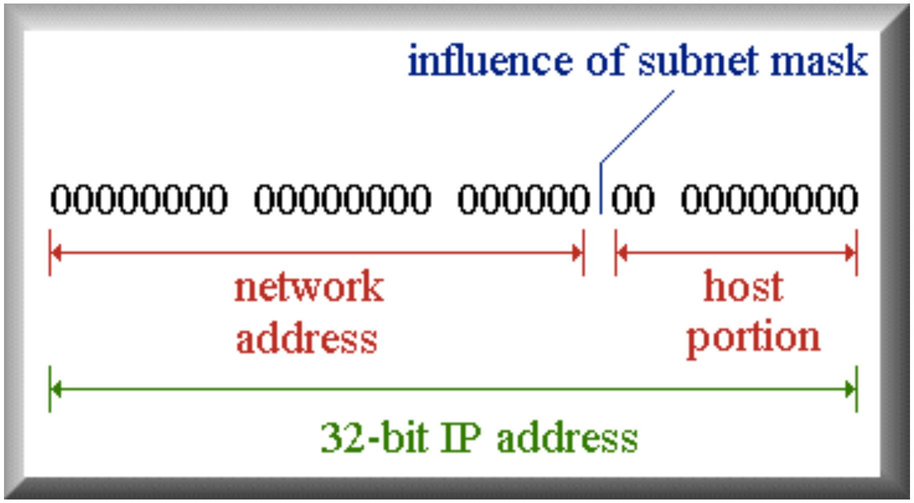
- The Internet is a mesh of networks whose operators agree to communicate using predefined protocols (“TCP/IP”)
- Networks use identifiers to name or number individual computers (hosts) so that these can communicate
  - IP addresses identify Internet’s streets and house numbers
  - Autonomous System Numbers identify the Internet’s “neighborhoods”
  - Domain Names provide user friendly ways to remember addresses

What Are Internet Protocol (IP) Addresses?

- IP addresses are 32-bit or 128-bit numbers that are used to identify networks and individual hosts of networks
  - IP version 4 number, e.g., 192.168.23.1 or
  - IP version 6 fe80::226:bbff:fe11:5b32
- A subnet mask distinguishes the number of bits in a number that represent the network part of the address

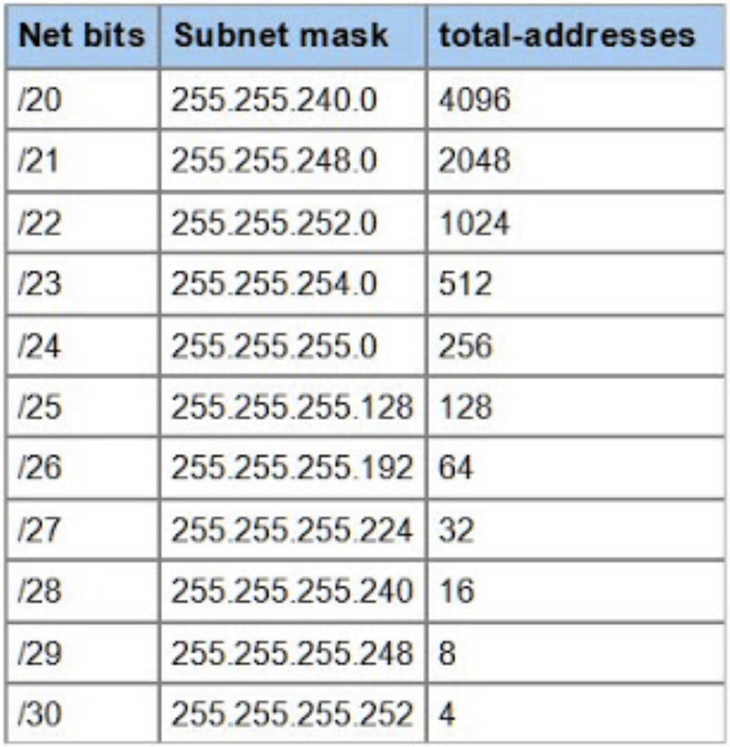
What is a subnet mask?

A number that identifies the number of bits of an IPv4 address that represent the local network identifier



IPv6 prefix numbers serve the same purpose

The remaining bits identify the number of hosts that can be addressed in the local network

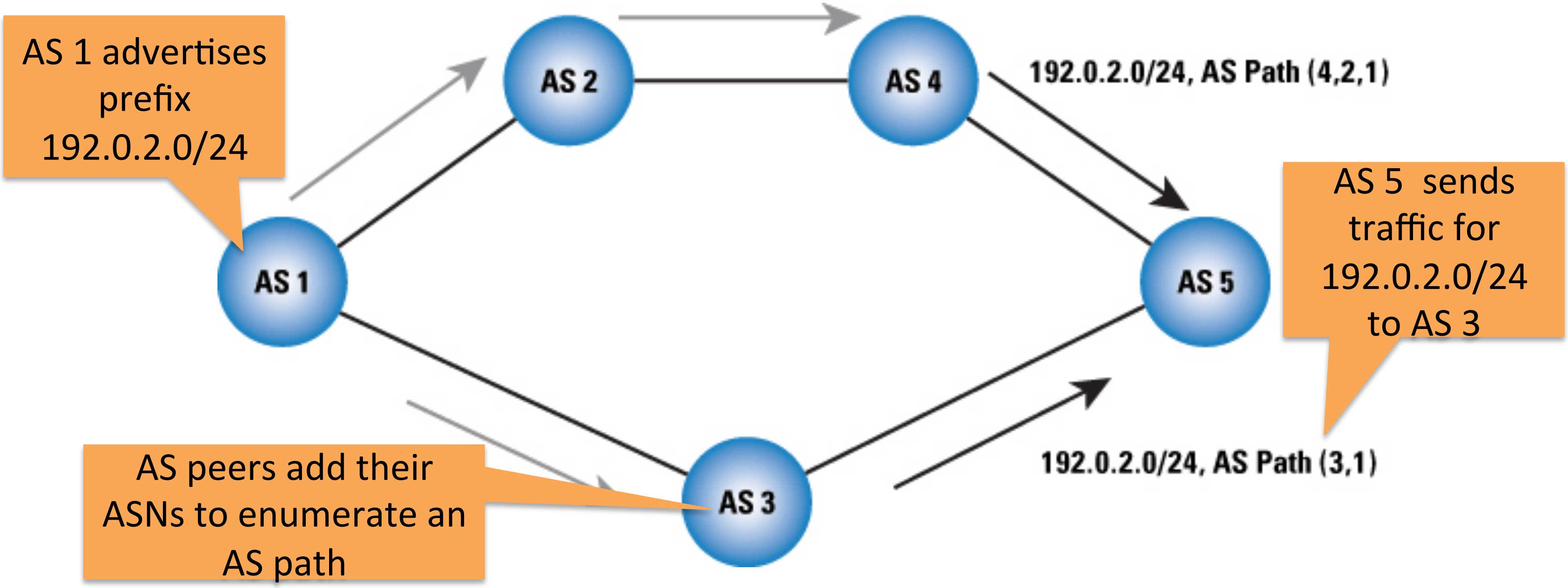


Net bits	Subnet mask	total-addresses
/20	255.255.240.0	4096
/21	255.255.248.0	2048
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4

Try http://www.tunnelsup.com/subnet-calculator

Autonomous System Number (ASN)

- ASNs identify operators who provide Internet access or transit routing service
  - ISPs, cable, mobile providers, hosting/cloud providers…
- ASNs are used to identify global routes (AS paths)



AS 1 advertises prefix 192.0.2.0/24

AS 5 sends traffic for 192.0.2.0/24 to AS 3

AS peers add their ASNs to enumerate an AS path

Try http://whatismyasn.org

What is the Domain Name System?

A distributed database primarily used to obtain the

IP address, a number, e.g.,

192.168.23.1 or fe80::226:bbff:fe11:5b32

that is associated with a

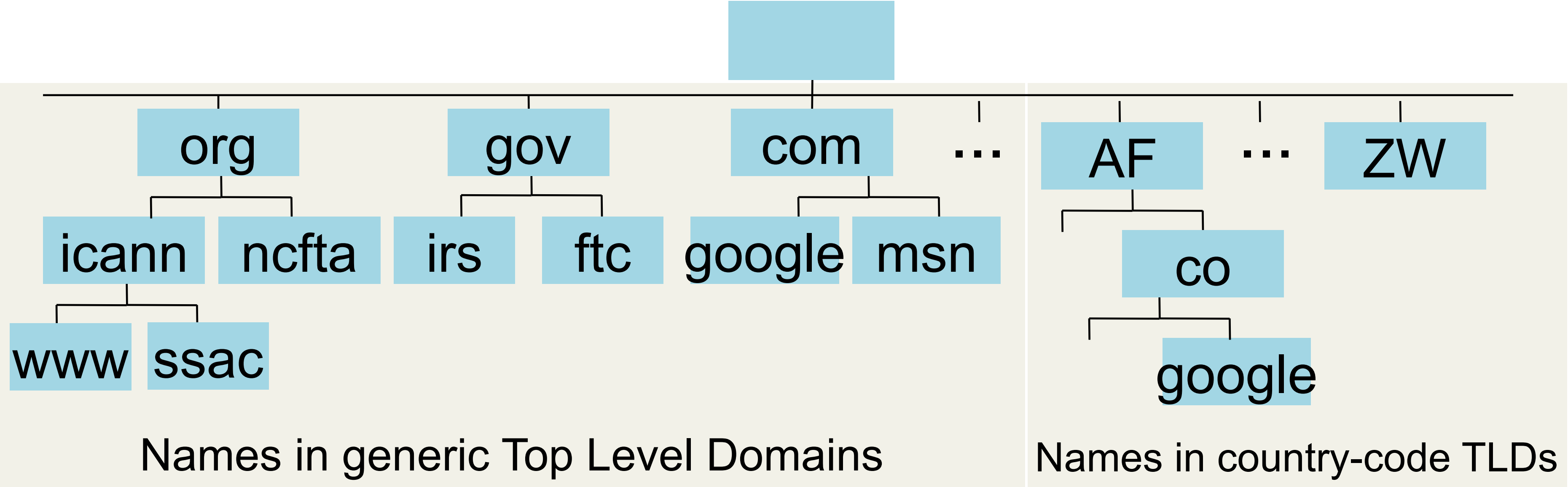
user-friendly name (www.example.com)

Why do we need a DNS?

- It’s hard to remember lots of four decimal numbers
- It’s impossibly hard to remember long hexadecimal ones

Top Level Domains

- Top Level Domains are delegated from the root of the DNS
- Generic Top Level Domains are operated by registry operators under contract to ICANN
- Country code Top Level Domains are operated by a registry operator designated by a sovereign nation
- Internationalized Domain names may use non-Latin characters


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

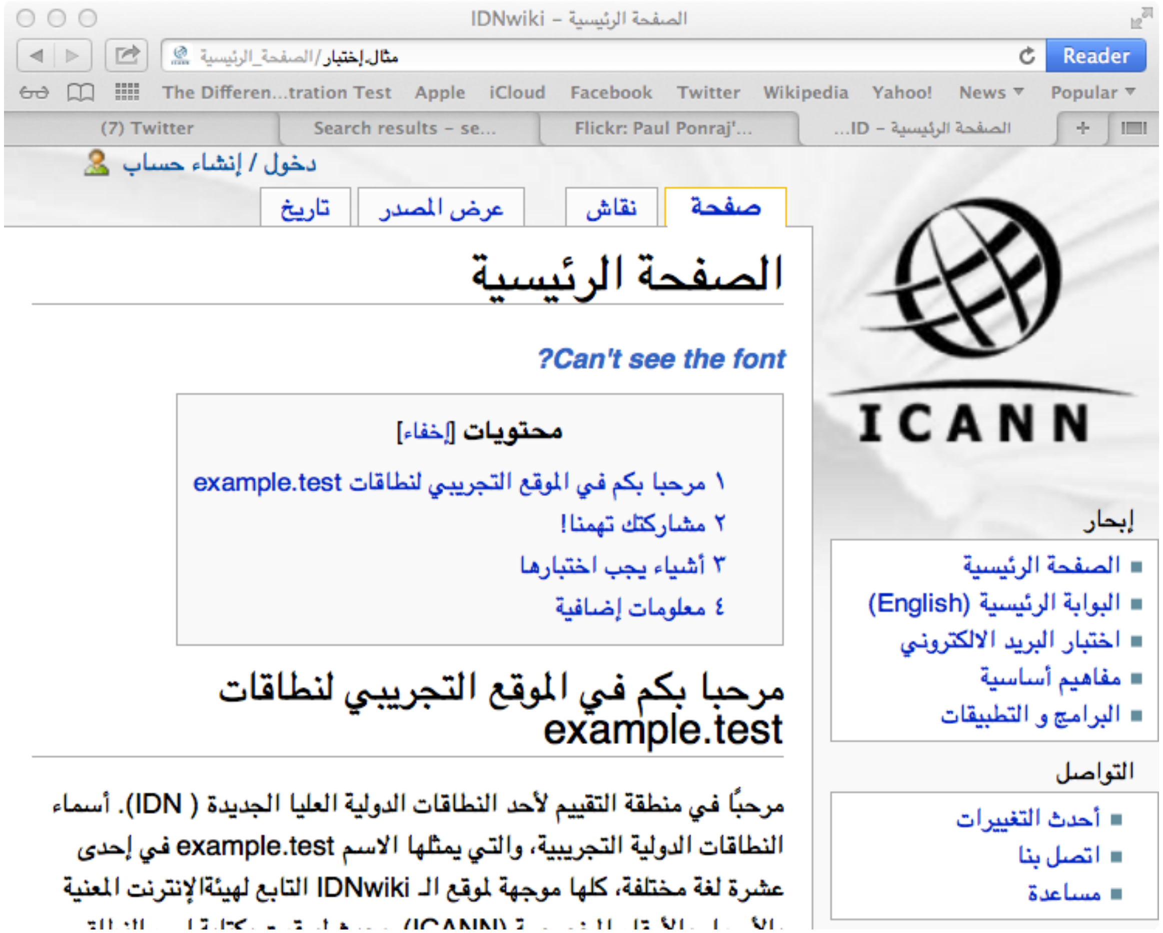
Internationalized Domain Names

- Characters for non-Latin scripted languages can be included in domain names

http://пример.испытание

http://παράδειγμα.δοκιμή

http://例子.测试



الصفحة الرئيسية

?Can't see the font

محتويات [إخفاء]

١ مرحبا بكم في الموقع التجريبي لنطاقات example.test

٢ مشاركتك تهمنا!

٣ أشياء يجب اختبارها

٤ معلومات إضافية

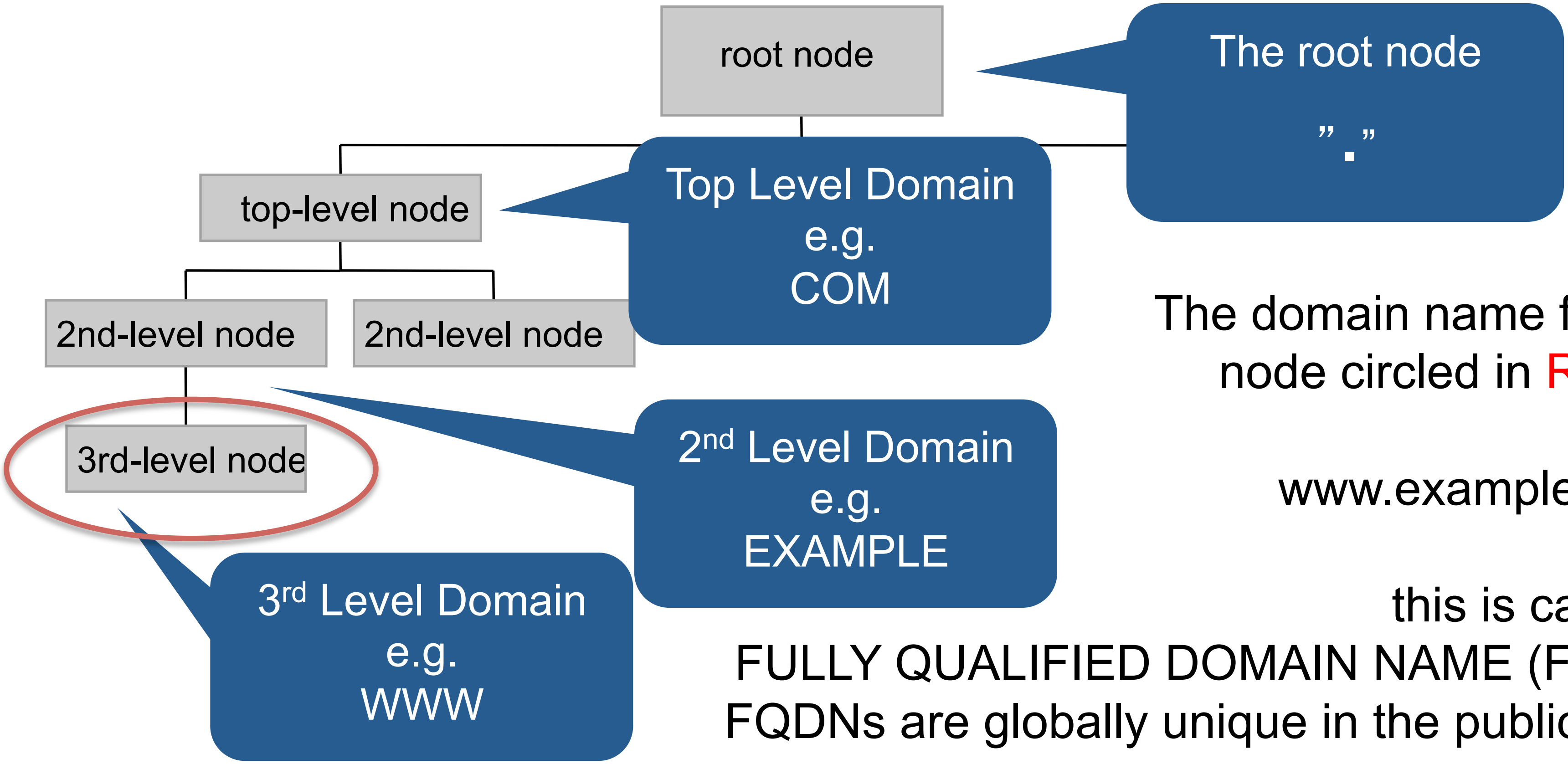
مرحبا بكم في الموقع التجريبي لنطاقات example.test

مرحبًا في منطقة التقييم لأحد النطاقات الدولية العليا الجديدة (IDN). أسماء النطاقات الدولية التجريبية، والتي يمثلها الاسم example.test في إحدى عشرة لغة مختلفة، كلها موجهة لموقع الـ IDNwiki التابع لهيئةالإنترنت المعنية

Brief Overview of the DNS Ecosystem

Labels and Domain Names

Each node in the DNS name space has a label
The domain name of a node is the list of the labels on the path from the node to the root of the DNS

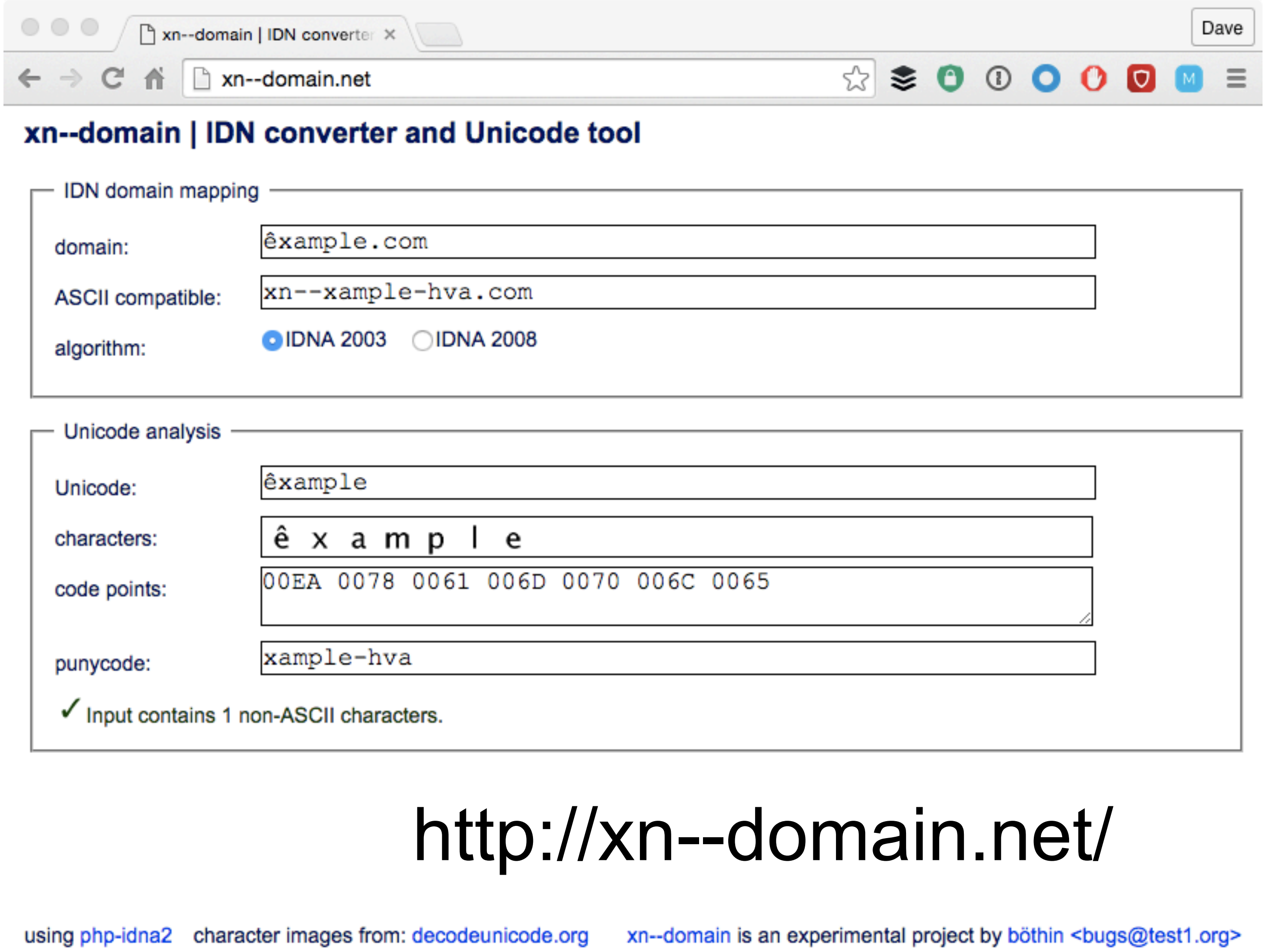


The domain name for the node circled in RED is

www.example.com.

this is called a
FULLY QUALIFIED DOMAIN NAME (FQDN)
FQDNs are globally unique in the public DNS

IDN Converter: Unicode-to-punycode



xn--domain | IDN converter and Unicode tool

IDN domain mapping

domain:	êxample.com
ASCII compatible:	xn--xample-hva.com
algorithm:	● IDNA 2003 ○ IDNA 2008

Unicode analysis

Unicode:	êxample
characters:	ê x a m p l e
code points:	00EA 0078 0061 006D 0070 006C 0065
punycode:	xample-hva

✓ Input contains 1 non-ASCII characters.

using php-idna2 character images from: decodeunicode.org xn--domain is an experimental project by böthin <bugs@test1.org>

http://xn--domain.net/

Who’s Who in the DNS Ecosytem?

Registries

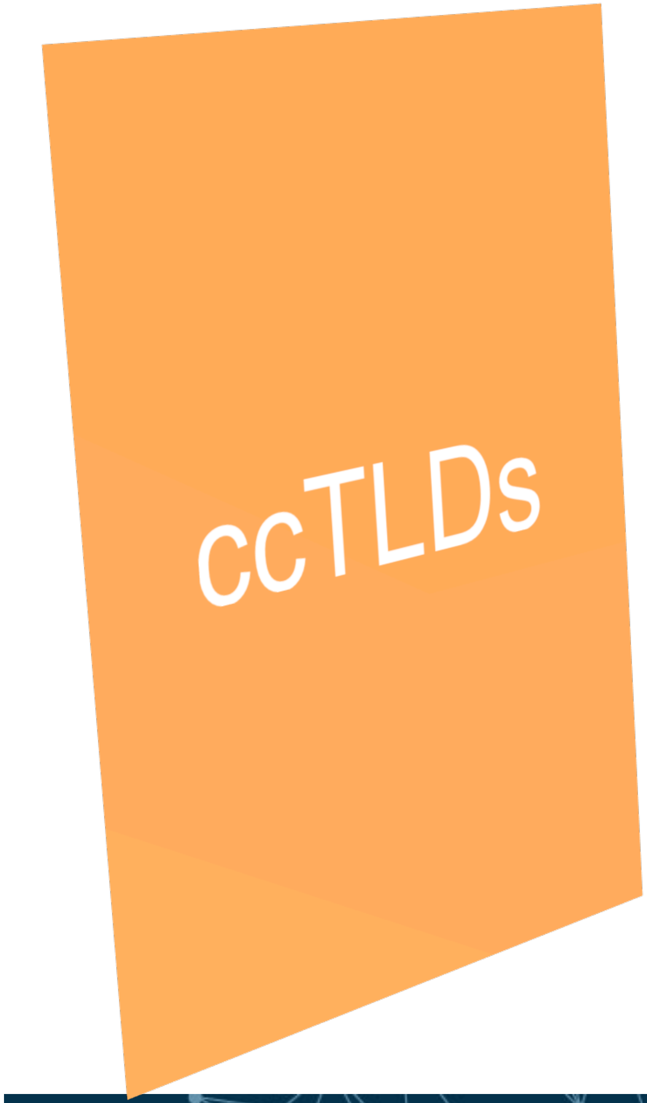
- Manage top-level domain (TLD) databases and generate TLD zone files
- Have diverse operations
  - Large corporations,
  - Small non-profits,
  - Departments in universities
- May outsource back-end operations

Generic Top Level Domain Registries

gTLDs

- gTLD registry operators contract with ICANN
  - Must comply with ICANN policy
  - http://www.icann.org/en/resources/registries/listing
- May outsource back-end operations to third party provider

Country Code TLD Operators (ccTLD)



- Do not have contracts with ICANN
  - http://www.iana.org/domains/root/db
- Participate in ICANN policy via the CC Name Supporting Organzation
  - http://ccnso.icann.org
- Diverse in operations and policies
  - Non-profit, for profit,
  - Run by government or external party
  - May have different registration or Whois services from gTLDs

Recursive DNS Operations Providers

Resolvers

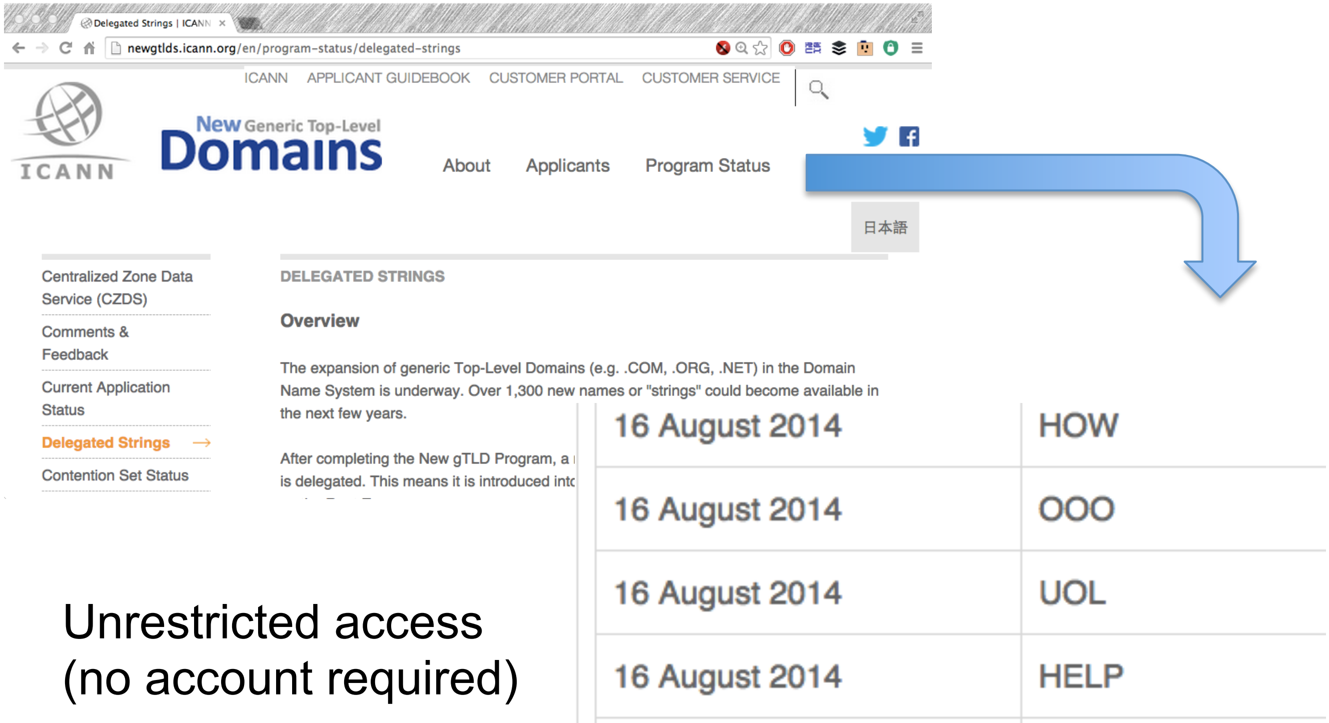
- ICANN does not have contracts with resolver operators
- Resolver operator space is diverse:
  - Internet Service Providers
  - Web or application hosting
  - Registrars (separate from ICANN contract)
  - Corporate resolvers
  - Public resolvers (Google, OpenDNS…)
- Home or personal use resolvers

New Top Level Domains

nTLDs

New TLDs are listed at ICANN as they are added to the root zone

- 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
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
is delegated. This means it is introduced int

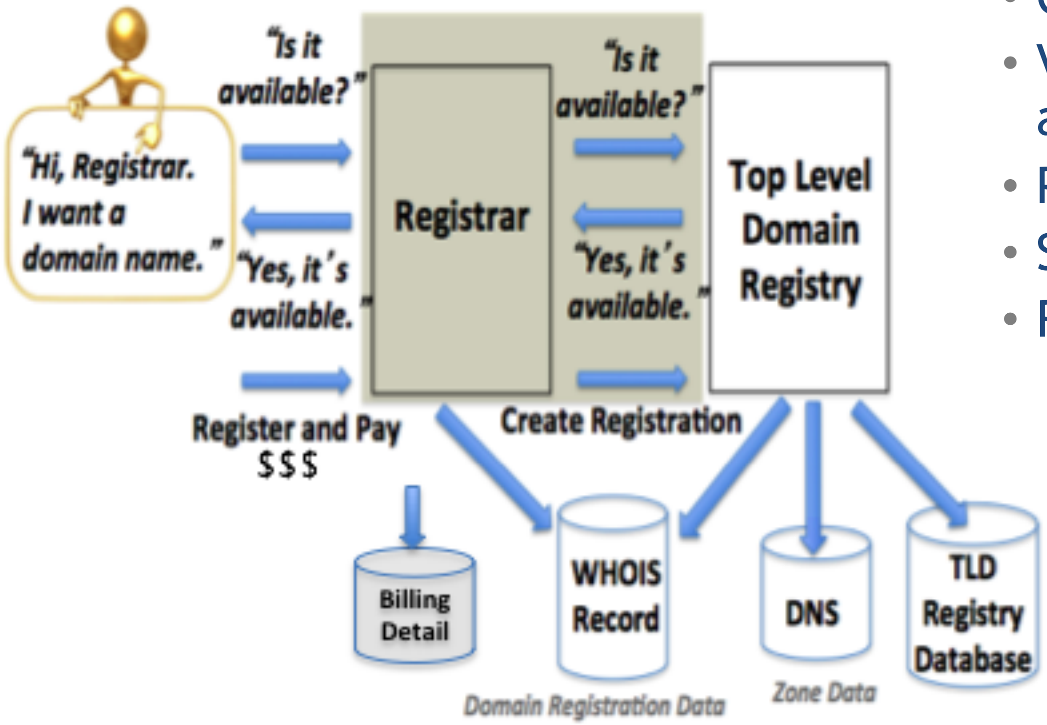
16 August 2014	HOW
16 August 2014	OOO
16 August 2014	UOL
16 August 2014	HELP

Unrestricted access
(no account required)

Registrars

- Business entities that process domain name registrations
  - In GTLD space all registrars must be ICANN accredited and are subject to Registrar Accreditation Agreement (RAA)
    - https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en
    - http://www.icann.org/registrar-reports/accredited-list.html
  - CcTLDs define their own registration processes
    - Some use ICANN accreditation or similar accreditation
- Retail and "wholesale" (reseller) business models
- Providing registration services is not an exclusive business

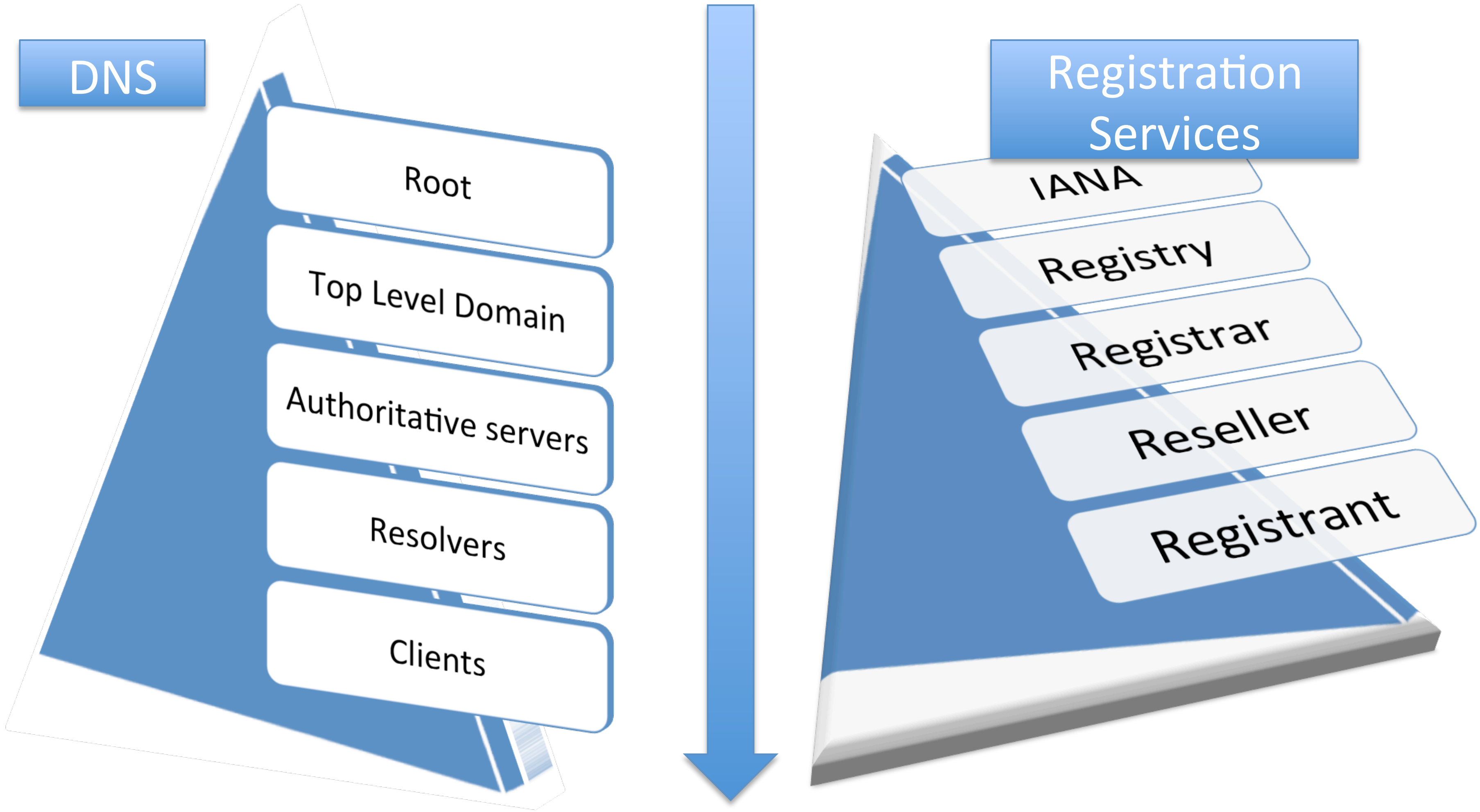
Domain name registration 101



How to register a gTLD 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

ICANN reach and remit



Number of actors increases, ICANN influence diminishes

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

DNS: Internet's directory assistance

- Stub resolvers ask questions
  - Software in applications, mobile apps or operating systems that issue DNS queries and process responses

What is the IPv6 address for www.icann.org?

- Recursive name resolvers find answers to queries for DNS data

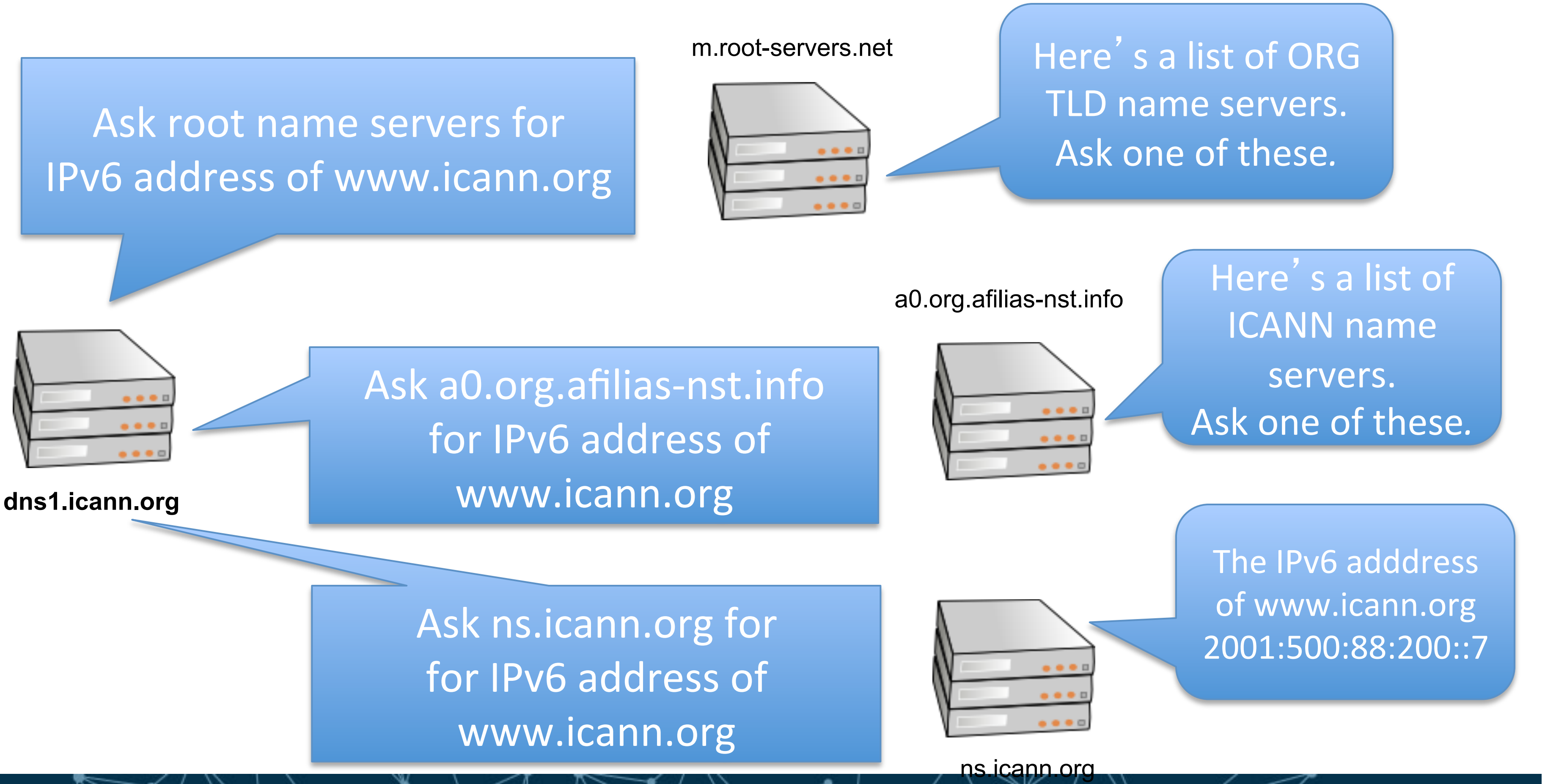
dns1.icann.org

I'll find that answer for you

Domain name “directory assistance”

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

- Resolvers find answers by asking questions *iteratively*



Ask root name servers for IPv6 address of www.icann.org

m.root-servers.net

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

dns1.icann.org

Ask a0.org.afilias-nst.info for IPv6 address of www.icann.org

a0.org.afilias-nst.info

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

Ask ns.icann.org for for IPv6 address of www.icann.org

ns.icann.org

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

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…

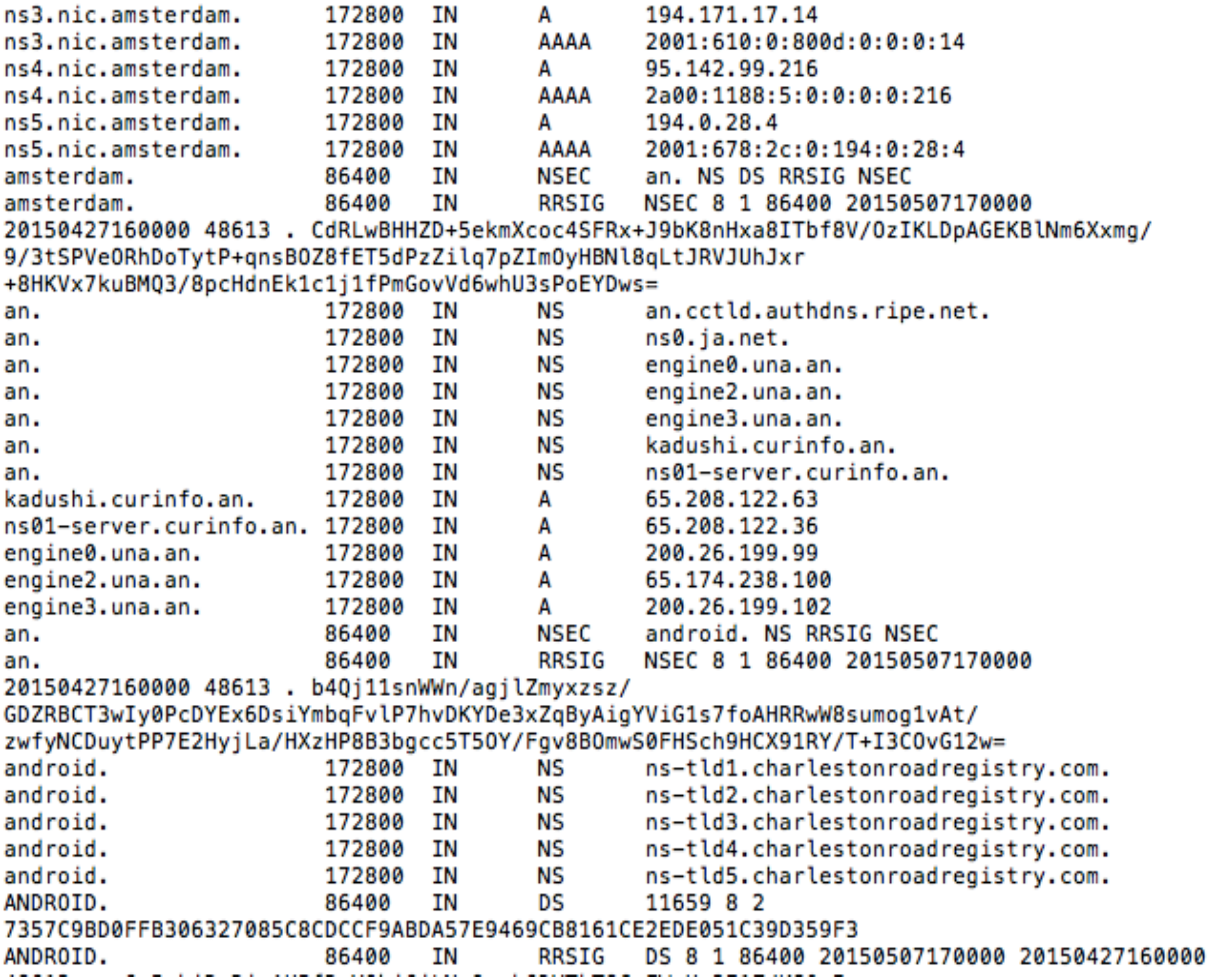
Zone data can only contain US ASCII-7 letters, digits, and hyphens.

In a zone, IDN strings will Always begin with XN--

Root zone data

The root zone contains delegated top level domain information

- Name server records (NS)
- Name server addresses (A, AAAA)
- Cryptographic records (DS, RRSIG, DNSKEY, NSEC)

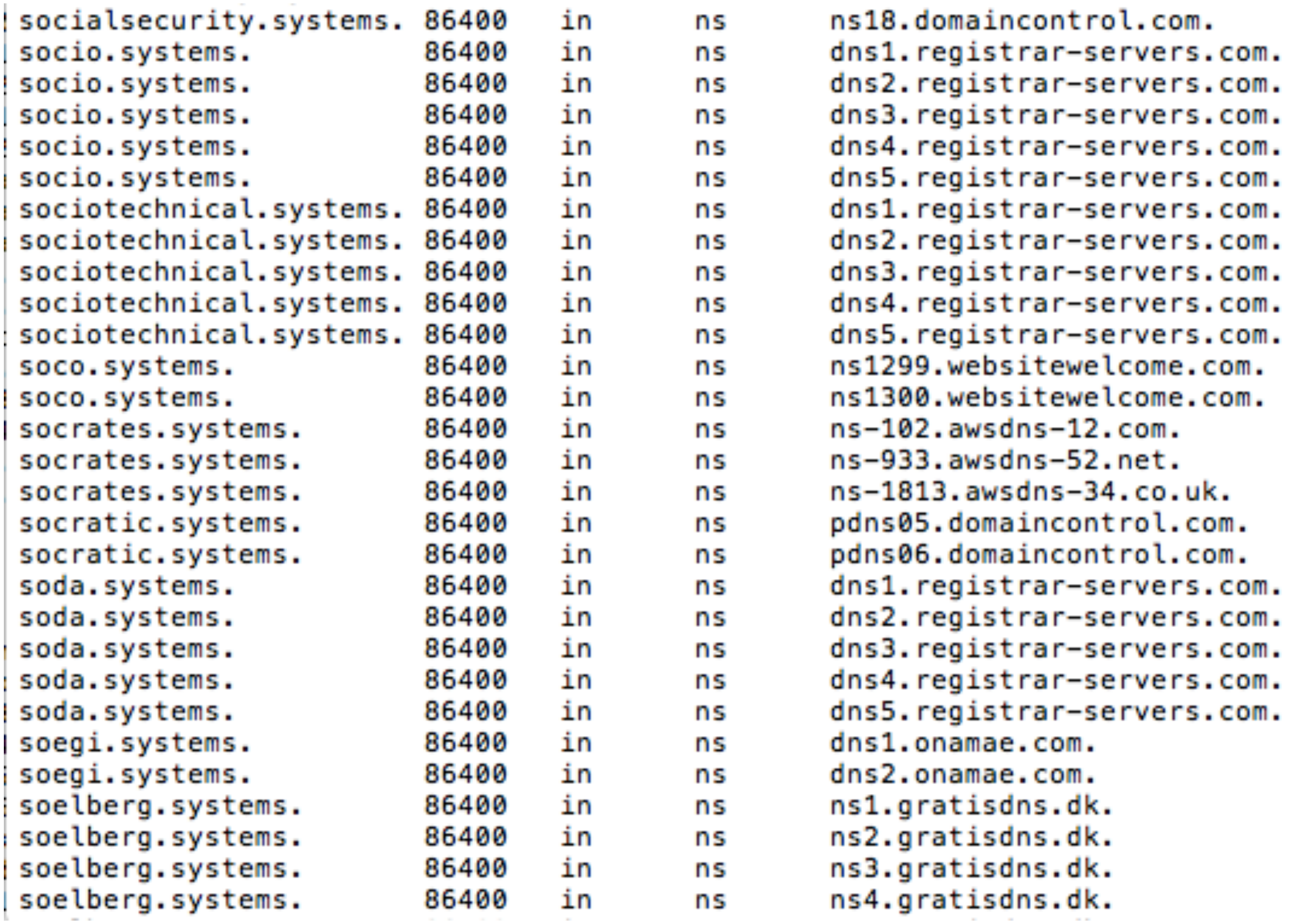


```
ns3.nic.amsterdam.      172800  IN      A       194.171.17.14
ns3.nic.amsterdam.      172800  IN      AAAA    2001:610:0:800d:0:0:0:14
ns4.nic.amsterdam.      172800  IN      A       95.142.99.216
ns4.nic.amsterdam.      172800  IN      AAAA    2a00:1188:5:0:0:0:0:216
ns5.nic.amsterdam.      172800  IN      A       194.0.28.4
ns5.nic.amsterdam.      172800  IN      AAAA    2001:678:2c:0:194:0:28:4
amsterdam.              86400   IN      NSEC    an. NS DS RRSIG NSEC
amsterdam.              86400   IN      RRSIG   NSEC 8 1 86400 20150507170000
20150427160000 48613 . CdRLwBHHZD+5ekmXcoc4SFRx+J9bK8nHxa8ITbf8V/OzIKLDpAGEKBlNm6Xxmg/
9/3tSPVeORhDoTytP+qnsBOZ8fET5dPzZilq7pZImOyHBNl8qLtJRVJUhJxr
+8HKVx7kuBMQ3/8pcHdnEk1c1j1fPmGovVd6whU3sPoEYDws=
an.                     172800  IN      NS      an.cctld.authdns.ripe.net.
an.                     172800  IN      NS      ns0.ja.net.
an.                     172800  IN      NS      engine0.una.an.
an.                     172800  IN      NS      engine2.una.an.
an.                     172800  IN      NS      engine3.una.an.
an.                     172800  IN      NS      kadushi.curinfo.an.
an.                     172800  IN      NS      ns01-server.curinfo.an.
kadushi.curinfo.an.     172800  IN      A       65.208.122.63
ns01-server.curinfo.an. 172800  IN      A       65.208.122.36
engine0.una.an.         172800  IN      A       200.26.199.99
engine2.una.an.         172800  IN      A       65.174.238.100
engine3.una.an.         172800  IN      A       200.26.199.102
an.                     86400   IN      NSEC    android. NS RRSIG NSEC
an.                     86400   IN      RRSIG   NSEC 8 1 86400 20150507170000
20150427160000 48613 . b4Qj11snWWn/agjlZmyxzsz/
GDZRBCT3wIy0PcDYEx6DsiYmbqFvlP7hvDKYDe3xZqByAigYViG1s7foAHRRwW8sumog1vAt/
zwfyNCDuytPP7E2HyjLa/HXzHP8B3bgcc5T5OY/Fgv8BOmwS0FHSch9HCX91RY/T+I3COvG12w=
android.                172800  IN      NS      ns-tld1.charlestonroadregistry.com.
android.                172800  IN      NS      ns-tld2.charlestonroadregistry.com.
android.                172800  IN      NS      ns-tld3.charlestonroadregistry.com.
android.                172800  IN      NS      ns-tld4.charlestonroadregistry.com.
android.                172800  IN      NS      ns-tld5.charlestonroadregistry.com.
ANDROID.                86400   IN      DS      11659 8 2
7357C9BD0FFB306327085C8CDCCF9ABDA57E9469CB8161CE2EDE051C39D359F3
ANDROID.                86400   IN      RRSIG   DS 8 1 86400 20150507170000 20150427160000
```

Top Level Domain zone data

The TLD zones contain delegated sub-domain information

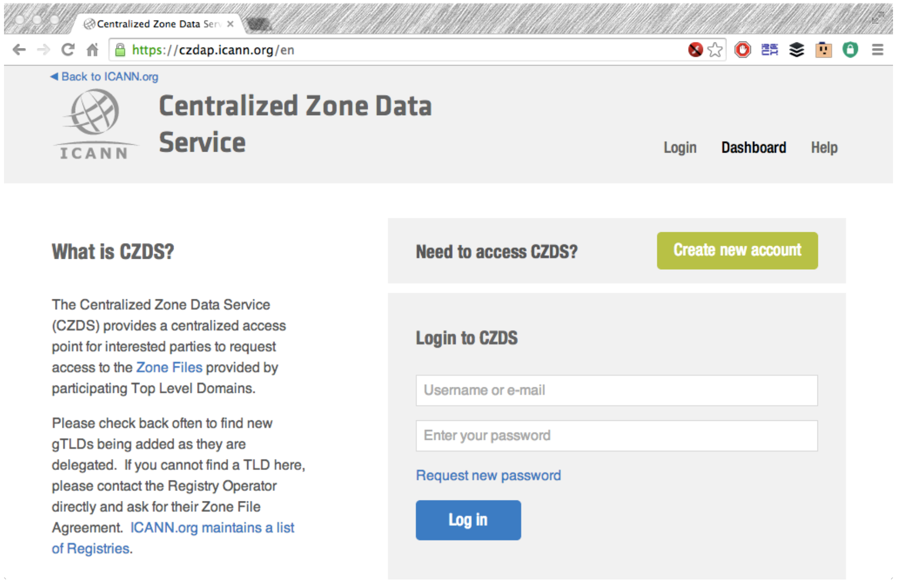
- Name server records (NS)
- Cryptographic records



```
socialsecurity.systems. 86400   in      ns      ns18.domaincontrol.com.
socio.systems.          86400   in      ns      dns1.registrar-servers.com.
socio.systems.          86400   in      ns      dns2.registrar-servers.com.
socio.systems.          86400   in      ns      dns3.registrar-servers.com.
socio.systems.          86400   in      ns      dns4.registrar-servers.com.
socio.systems.          86400   in      ns      dns5.registrar-servers.com.
sociotechnical.systems. 86400   in      ns      dns1.registrar-servers.com.
sociotechnical.systems. 86400   in      ns      dns2.registrar-servers.com.
sociotechnical.systems. 86400   in      ns      dns3.registrar-servers.com.
sociotechnical.systems. 86400   in      ns      dns4.registrar-servers.com.
sociotechnical.systems. 86400   in      ns      dns5.registrar-servers.com.
soco.systems.           86400   in      ns      ns1299.websitewelcome.com.
soco.systems.           86400   in      ns      ns1300.websitewelcome.com.
socrates.systems.       86400   in      ns      ns-102.awsdns-12.com.
socrates.systems.       86400   in      ns      ns-933.awsdns-52.net.
socrates.systems.       86400   in      ns      ns-1813.awsdns-34.co.uk.
socratic.systems.       86400   in      ns      pdns05.domaincontrol.com.
socratic.systems.       86400   in      ns      pdns06.domaincontrol.com.
soda.systems.           86400   in      ns      dns1.registrar-servers.com.
soda.systems.           86400   in      ns      dns2.registrar-servers.com.
soda.systems.           86400   in      ns      dns3.registrar-servers.com.
soda.systems.           86400   in      ns      dns4.registrar-servers.com.
soda.systems.           86400   in      ns      dns5.registrar-servers.com.
soegi.systems.          86400   in      ns      dns1.onamae.com.
soegi.systems.          86400   in      ns      dns2.onamae.com.
soelberg.systems.       86400   in      ns      ns1.gratisdns.dk.
soelberg.systems.       86400   in      ns      ns2.gratisdns.dk.
soelberg.systems.       86400   in      ns      ns3.gratisdns.dk.
soelberg.systems.       86400   in      ns      ns4.gratisdns.dk.
```

Where can I get TLD zone data?

- Freely available from Centralized Zone Data Access
  - https://czdap.icann.org/en



Centralized Zone Data Service

What is CZDS?

The Centralized Zone Data Service (CZDS) provides a centralized access point for interested parties to request access to the Zone Files provided by participating Top Level Domains.

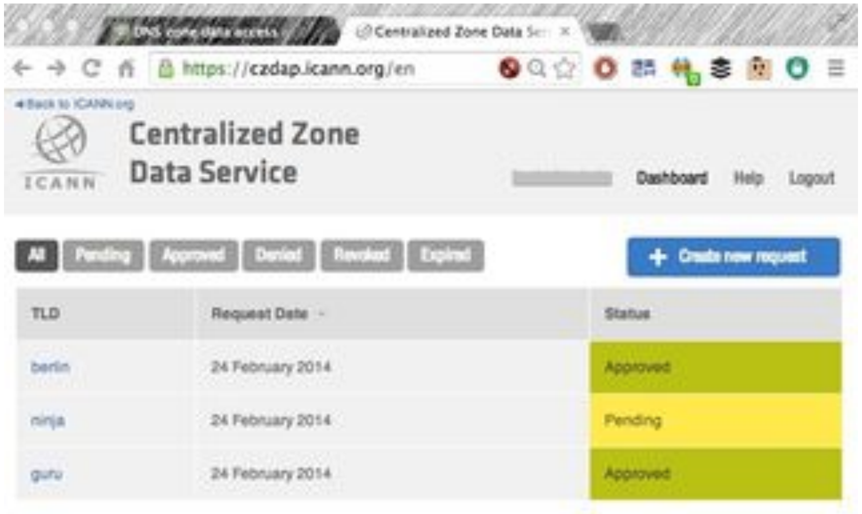
Please check back often to find new gTLDs being added as they are delegated. If you cannot find a TLD here, please contact the Registry Operator directly and ask for their Zone File Agreement. ICANN.org maintains a list of Registries.

Need to access CZDS?

Login to CZDS

1. create an account,
2. create cryptographic keys for SFTP
3. select the TLD zone files
4. agree to terms and conditions
5. Provide IP address for SFTP

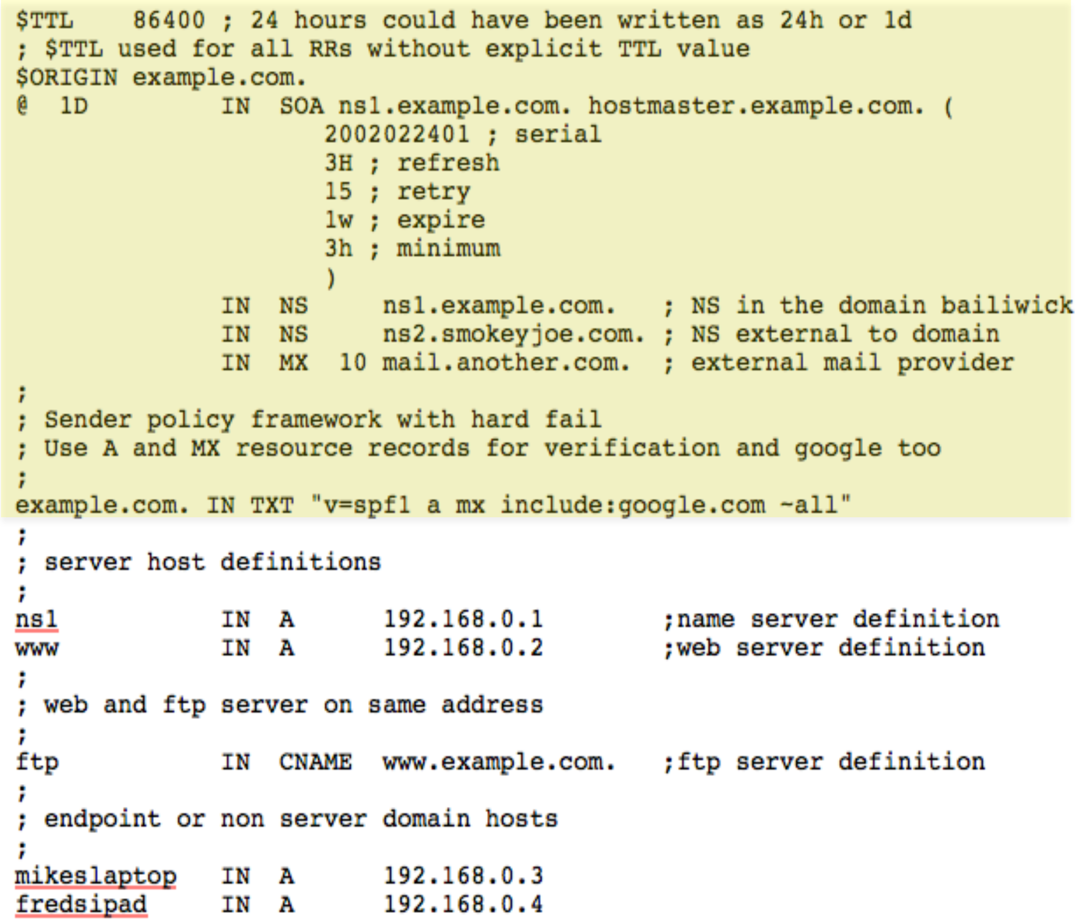
6. Request zone data from registry
7. Manage access



Centralized Zone Data Service

TLD	Request Date	Status
berlin	24 February 2014	Approved
ninja	24 February 2014	Pending
guru	24 February 2014	Approved

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
```

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*

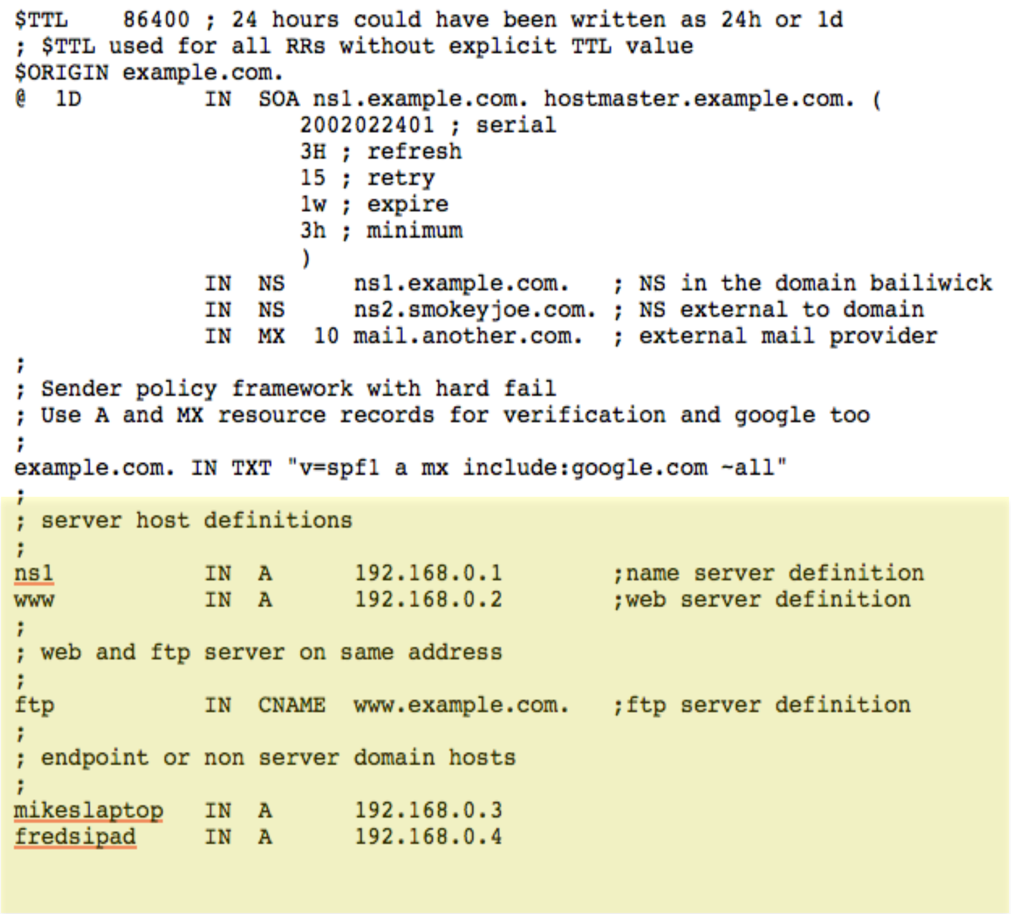
Mail Server (MX)

- *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

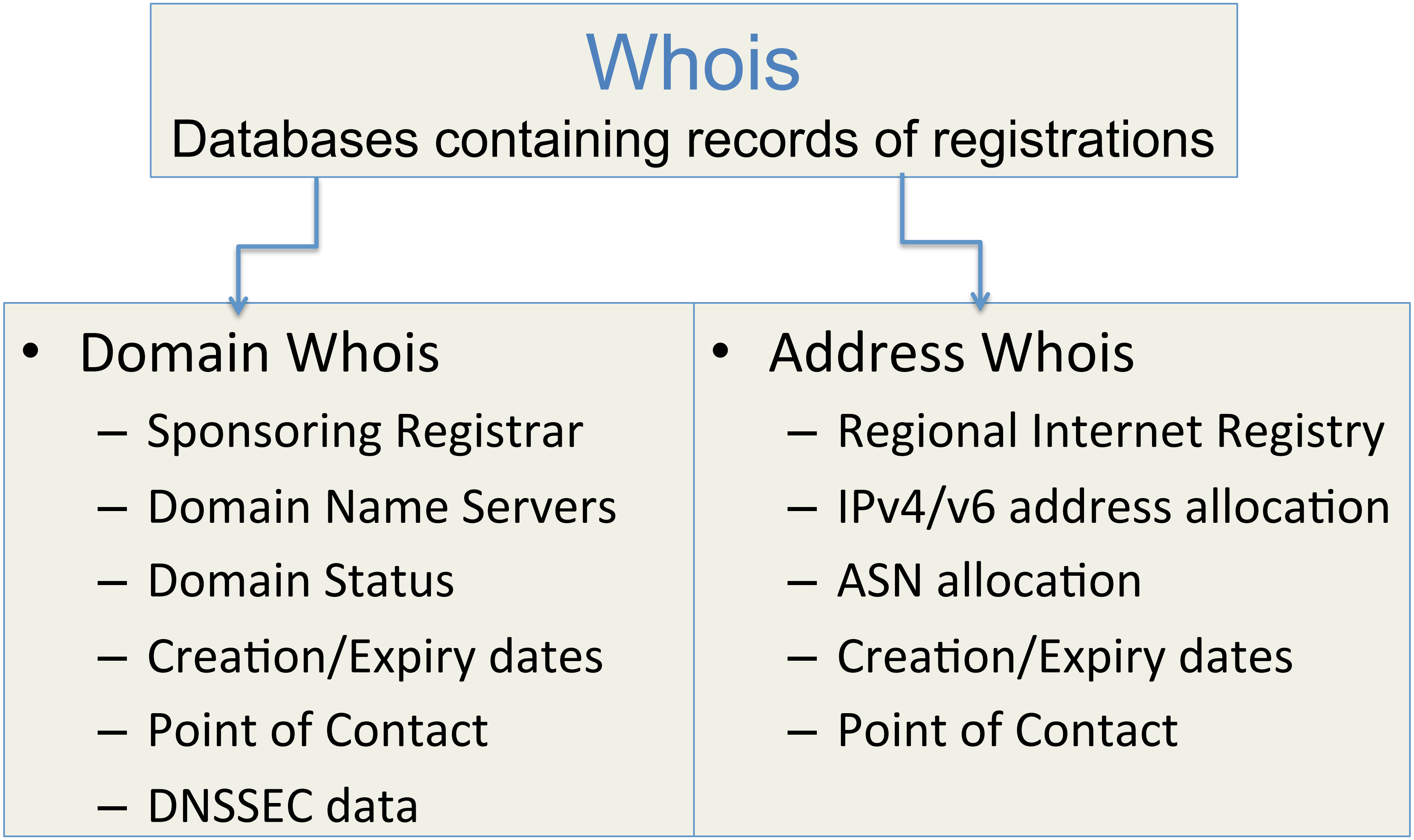
- *www (world wide web)*
- *IN (Internet)*
- *A (IPv4)   * AAAA is IPv6*

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"*

Registration Data Directory Service



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

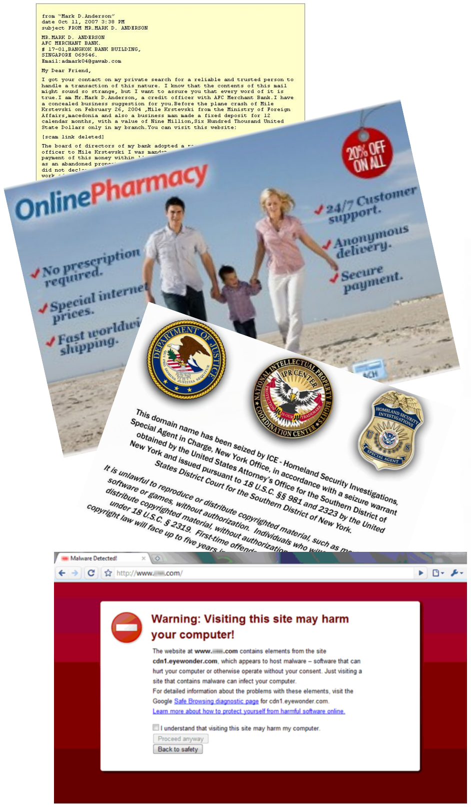
Why Identifiers Are Relevant to Investigators?

Online crime or abuse investigations typically require that you collect 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
officer to Mile Krstevski I was mand
payment of this money within
as an abandoned prop
did not decl
work

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 m
software or games, without authorization. Individuals who wi
distribute copyrighted material, without authorization
under 18 U.S.C. § 2319. First-time offend
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

Domains registered by criminals for

- 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…)

Common Uses for Misused or Abused Domain Registrations

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

Domains compromised or hijacked by criminals or state-sponsored actors

- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Tunneling (covert communications)
- Data Exfiltration

Methods

- Infection (Malware)
- Configuration change (DNSChanger)
- Poisoning (resolver/ISP)
- Man in the Middle attacks (insertion, capture)

How criminals acquire DNS resources

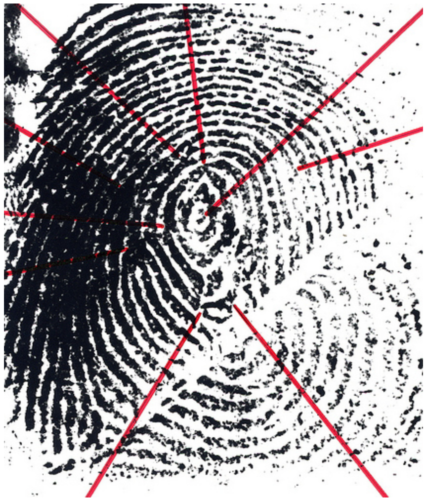
https://www.flickr.com/photos/danielfoster/
https://www.flickr.com/photos/23905174@N00/

- 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 data or buy domains

Is this an Abuse (Malicious) Domain or a Misused (Exploited) Domain?

Not always easy to differentiate

Collecting Evidence of DNS Abuse/Misuse



Analogs:

- *Number of matching minutiae*
- *Body of evidence*

- 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

http://www.flickr.com/photos/vincealongi/

Not always easy to identify badness

- Criminals 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
  - Whois Point of Contact information culled from obituaries
- Criminals use ACLs
  - Prevent registrars, Google, LE, investigators from seeing sites
- “Criminal” behaviors can emulate legitimate behavior
  - EXAMPLE: Fast flux versus adaptive networking (e.g., CDNs)

Taking Action Against Domains, Hosts, or Content

Who? What? When? Where? How?

- Who is the target of your action?
  - Registrant, Registry, Registrar, Hosting operator
- What is the goal of the action?
- When will you act? In synchrony with others?
- Where in the world are the people or things you're targeting?
- How will you take action?
  - Court order, acceptable use, compliance violation

Chainsaw, scalpel or laser?

- Domain name "takedown"
  - Contact Registry, registrar, or DNS hosting provider
  - DNS will not resolve name
  - DNS will resolve name to sinkhole
  - Try AUP violation, may require court order
- This action is *broadly disruptive*
  - All subdomains will become unreachable
  - All content is taken offline
  - All users of all services

Chainsaw, scalpel or laser?

- Take (malicious) content offline
  - Contact content hosting provider
  - Minimizes harm, not always easy
  - Try AUP violation, may require court order
- This action affects targeted content only
  - No assurance that content is removed (forever)

Chainsaw, scalpel or laser?

- Blocking content (or traffic)
  - Contact reputation service provider (blocklisting org)
  - Most granular action
    - Can be applied to TLD, ASN, domain, IP, or URL
  - Done independently from AUP, court order

- Minimally intrusive but highly localized,
  - Only protects parties protected by blocklist(s)
  - Content may remain online
  - May be temporary/stop gap only
  - Names will continue to resolve

What Hinders Mitigation or Prosecution?

JURISDICTION	**What is the prevailing jurisdiction of content hosting, DNS hosting, domain registration, alleged perpetrators?**
LAW	Is this a criminal activity in all relevant jurisdictions?
CONTRACT, INTERPRETATION	Is a contracted party in breach of an obligation? According to whose interpretation?

Steps to investigate & suspend domains

1. Collect evidence of abuse

   The purpose of this course is to show ways to do this

2. Determine hosting provider or registrar
   - A. Is a reseller of that registrar involved?
3. Contact hosting provider or 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. Whois Data Problem Reporting System
   - D. ICANN compliance

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

Collect Evidence of Identifier Abuse,Misuse

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

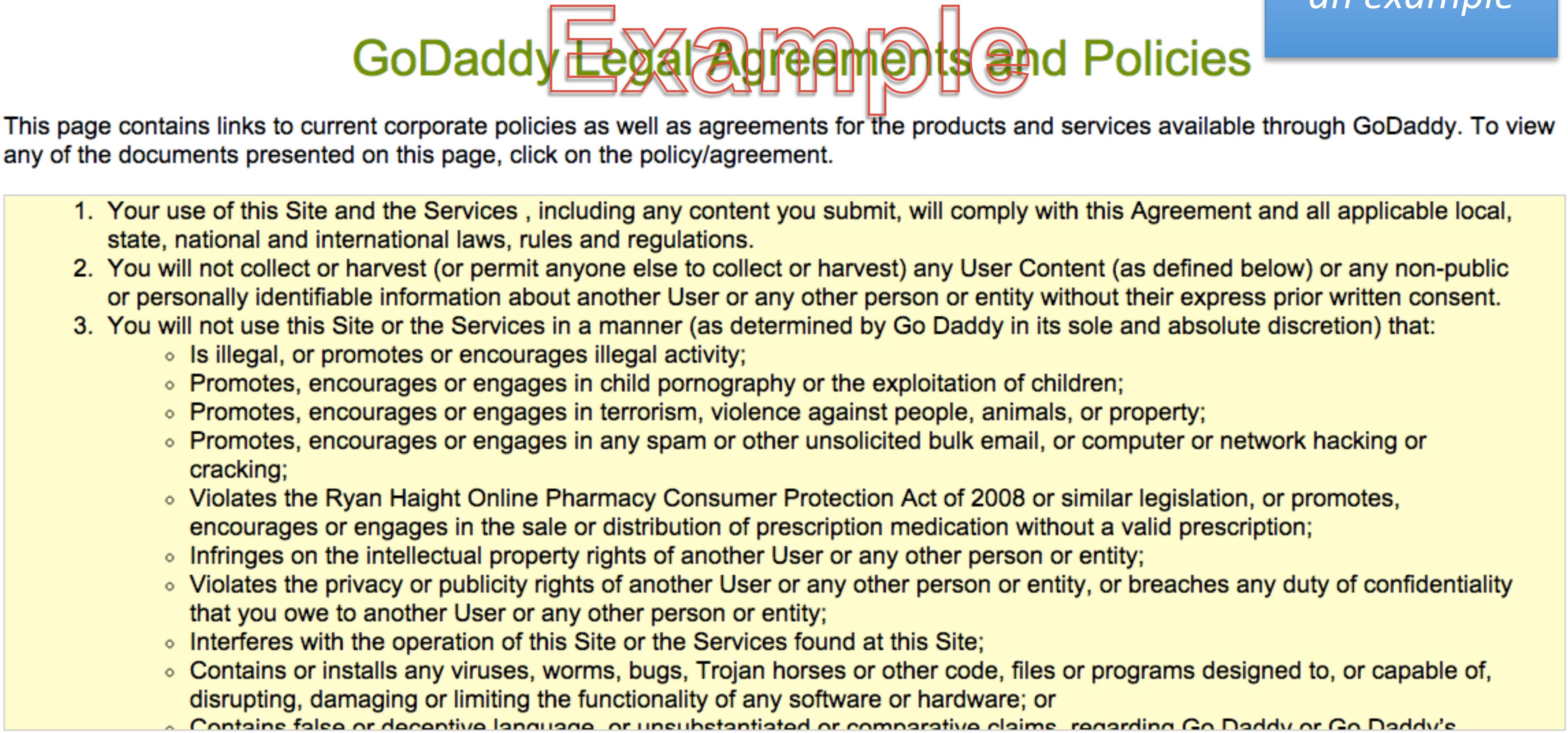
- Host IP addresses
- IP networks
- Address registration data
- Autonomous systems
- Service providers
- Hosting providers
- Content

Reputation

ToS? Contract Violation? Court order?

- Does the registration violate Terms of Service, Acceptable use?
- Can you demonstrate a contract violation to ICANN Compliance?
- Do you have sufficient evidence to procure a court order?

Never hurts to ask or *provide an example*



Example

GoDaddy Legal Agreements and Policies

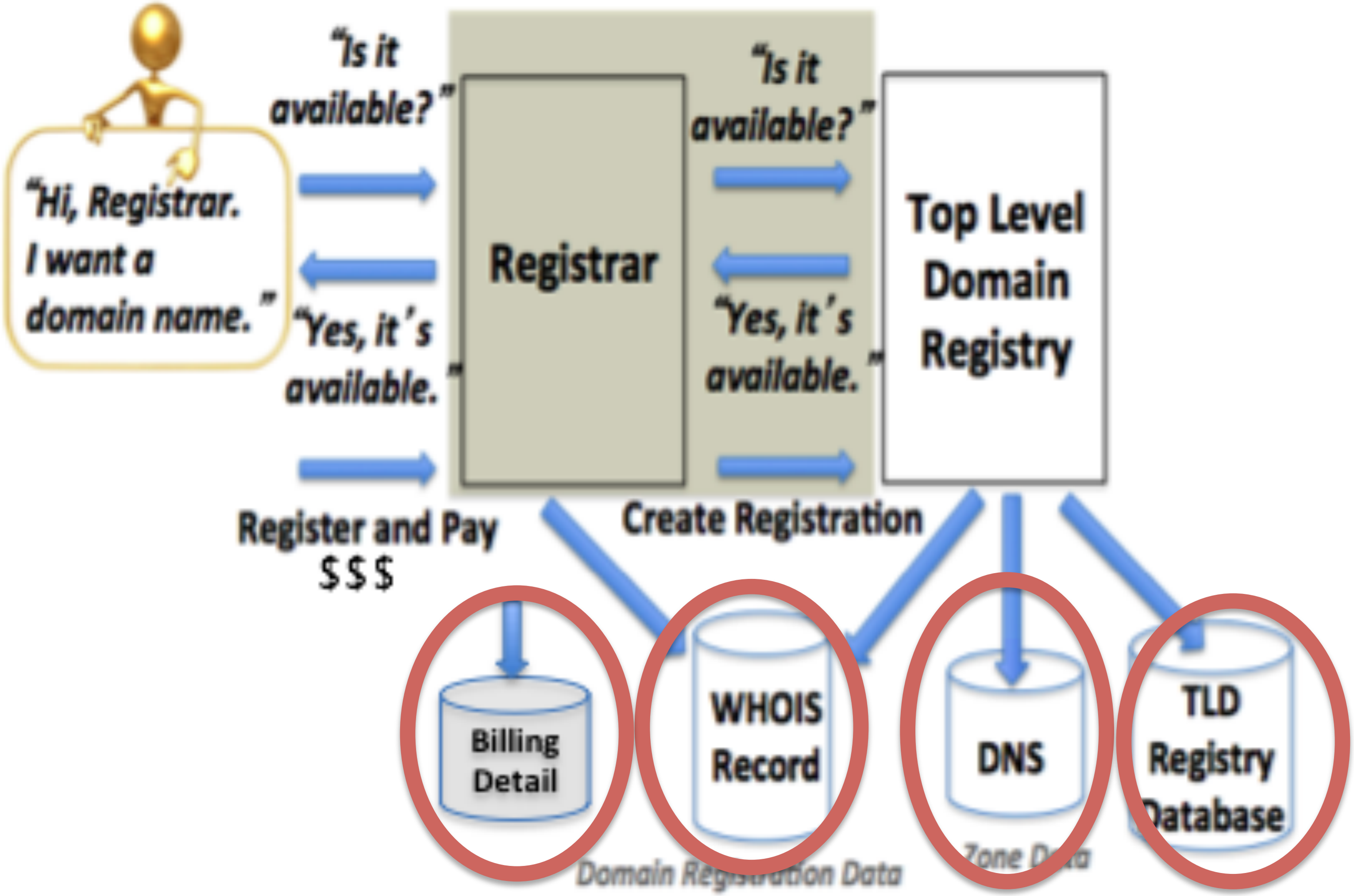
This page contains links to current corporate policies as well as agreements for the products and services available through GoDaddy. To view any of the documents presented on this page, click on the policy/agreement.

1. Your use of this Site and the Services , including any content you submit, will comply with this Agreement and all applicable local, state, national and international laws, rules and regulations.
2. You will not collect or harvest (or permit anyone else to collect or harvest) any User Content (as defined below) or any non-public or personally identifiable information about another User or any other person or entity without their express prior written consent.
3. You will not use this Site or the Services in a manner (as determined by Go Daddy in its sole and absolute discretion) that:
   - Is illegal, or promotes or encourages illegal activity;
   - Promotes, encourages or engages in child pornography or the exploitation of children;
   - Promotes, encourages or engages in terrorism, violence against people, animals, or property;
   - Promotes, encourages or engages in any spam or other unsolicited bulk email, or computer or network hacking or cracking;
   - Violates the Ryan Haight Online Pharmacy Consumer Protection Act of 2008 or similar legislation, or promotes, encourages or engages in the sale or distribution of prescription medication without a valid prescription;
   - Infringes on the intellectual property rights of another User or any other person or entity;
   - Violates the privacy or publicity rights of another User or any other person or entity, or breaches any duty of confidentiality that you owe to another User or any other person or entity;
   - Interferes with the operation of this Site or the Services found at this Site;
   - Contains or installs any viruses, worms, bugs, Trojan horses or other code, files or programs designed to, or capable of, disrupting, damaging or limiting the functionality of any software or hardware; or
   - Contains false or deceptive language, or unsubstantiated or comparative claims, regarding Go Daddy or Go Daddy's

If you're going to seize the domain…

The right documentation makes a big difference

Seizures affect several Internet name databases and operations



Relevance to order or warrant

- (List of) domain name(s) identifies
  - Registries that are obliged to act on the order
  - The name(s) associated with the (criminal) act
- Registration data ("Whois") identifies
  - Sponsoring registrar
  - Party alleged to "own" the domain
  - Servers that provide DNS (name resolution)
  - "Status" of the domain

Served parties must have context

- Who is making the request?
  - Plaintiff, defendant, court of record
  - Who are the primary points of contact?
  - Can registry/registrar readily verify the request?
- What kind of request is this?
  - Court order or 3rd party request for action?
- What is the expected response time?

Set expectations for served parties

- Is there a desire to obtain records?
- Is the domain name to be transferred to a different sponsoring registrar?
- Are you transferring the registration? To whom?
- What status should the registry set for the domain?
  - E.g., prevent transfer, update, or delete?
- What should WHOIS for the domain name display?

What do you want the DNS to do?

- How should DNS respond to queries for seized domains?
  - Is name resolution service (DNS) to be suspended?
  - Is redirection to a text of notice page required?
  - Is redirection of Internet hosting required?
- Who will operate DNS for seized domains?
  - Is the party that provides name resolution service (DNS) to be changed?

Have you minimized collateral harm?

Examples of questions to ask before you file:

- Will your action disrupt
  - Name service for other (reputable) domains?
  - Hosting services for parties other than those named in your order?
- What services other than web are affected by your action on the domain name?
- What do you expect as the “long term disposition” of the domain name?
- Could your actions interfere with other active investigations, monitoring, surveillance… ?

Read Is Jotform a Poster Child for Domain Takedown Overkill?
http://www.securityskeptic.com/2012/02/is-jotform-a-poster-child-for-domain-shutdown-overkill.html

Preparation

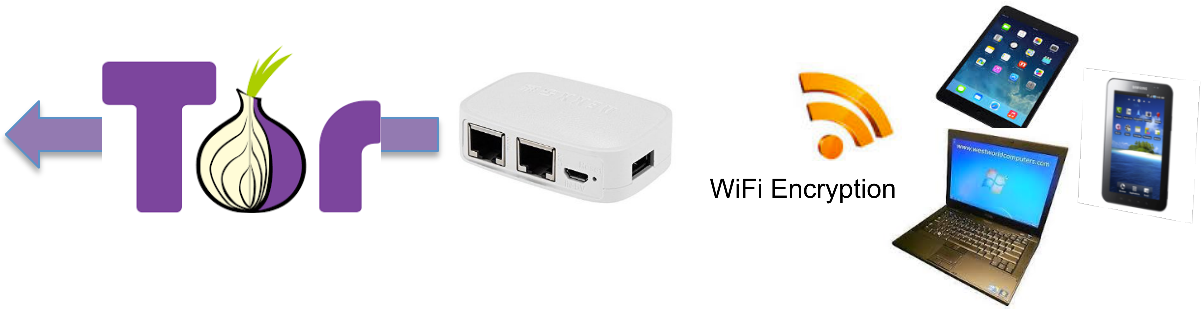
There’s no hiding in plain sight…

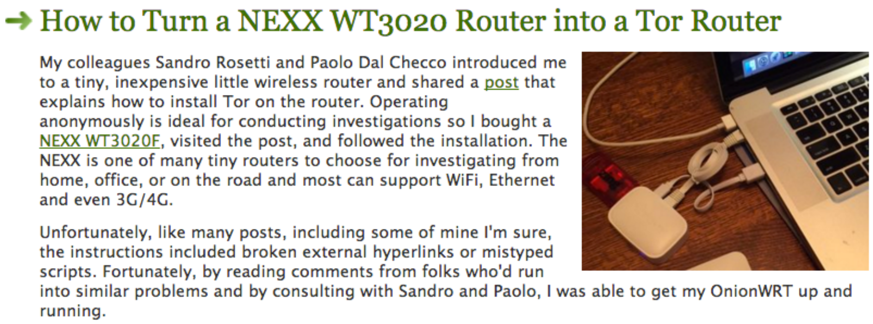
Before you begin an investigation, ask

- Should you hide your activities from bad actors?
  - Criminals may block IPs of known investigators
  - They may also monitor activity
- Do you want to leave crumbs associated with investigations that are traceable back to you?
  - Log records, metadata at third party intel sources
- Do you want resources you use to leave crumbs on your devices
  - Cookies, plug-ins, or worse…

OnionWRT: Tor router

1. Buy a micro router or Raspberry Pi (inexpensive!!)
2. Install OpenWRT and OnionWRT
3. Investigate over TOR from behind router
4. Put all your devices behind your router





➜ How to Turn a NEXX WT3020 Router into a Tor Router

My colleagues Sandro Rosetti and Paolo Dal Checco introduced me to a tiny, inexpensive little wireless router and shared a post that explains how to install Tor on the router. Operating anonymously is ideal for conducting investigations so I bought a NEXX WT3020F, visited the post, and followed the installation. The NEXX is one of many tiny routers to choose for investigating from home, office, or on the road and most can support WiFi, Ethernet and even 3G/4G.

Unfortunately, like many posts, including some of mine I'm sure, the instructions included broken external hyperlinks or mistyped scripts. Fortunately, by reading comments from folks who'd run into similar problems and by consulting with Sandro and Paolo, I was able to get my OnionWRT up and running.

http://www.securityskeptic.com/2016/01/how-to-turn-a-nexx-wt3020-router-into-a-tor-router.html

Software to Anonymize Traffic

- Tor https://www.torproject.org/projects/projects.html.en
  - The Amnesic Incognito Live System (TAILS), Tor browser
- Disposable, anonymous inboxes
  - Mailinator https://mailinator.com/
  - HIDE MY ASS! https://securemail.hidemyass.com/
- Browser tricks
  - Incognito/private mode can still be tracked
  - User agent changes (can do with cURL as well)

Tools for Investigating Badness

DNS… domain registrations… name servers… hosting… content… reputation.

Tools for Investigators

- Tools to identify abused or malicious resource
  - Domain names, host names, IP addresses, ASNs
  - Hosting location (web, DNS, mail) or origin
  - Content (URL, file, email, attachment)
- 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

Tools for Investigating DNS

- nslookup (Windows, BSD) or host

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

- dig (Linux, BSD, MacOS),

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

- DNS query sniffer

  http://www.nirsoft.net/utils/dns_query_sniffer.html

- Passive DNS

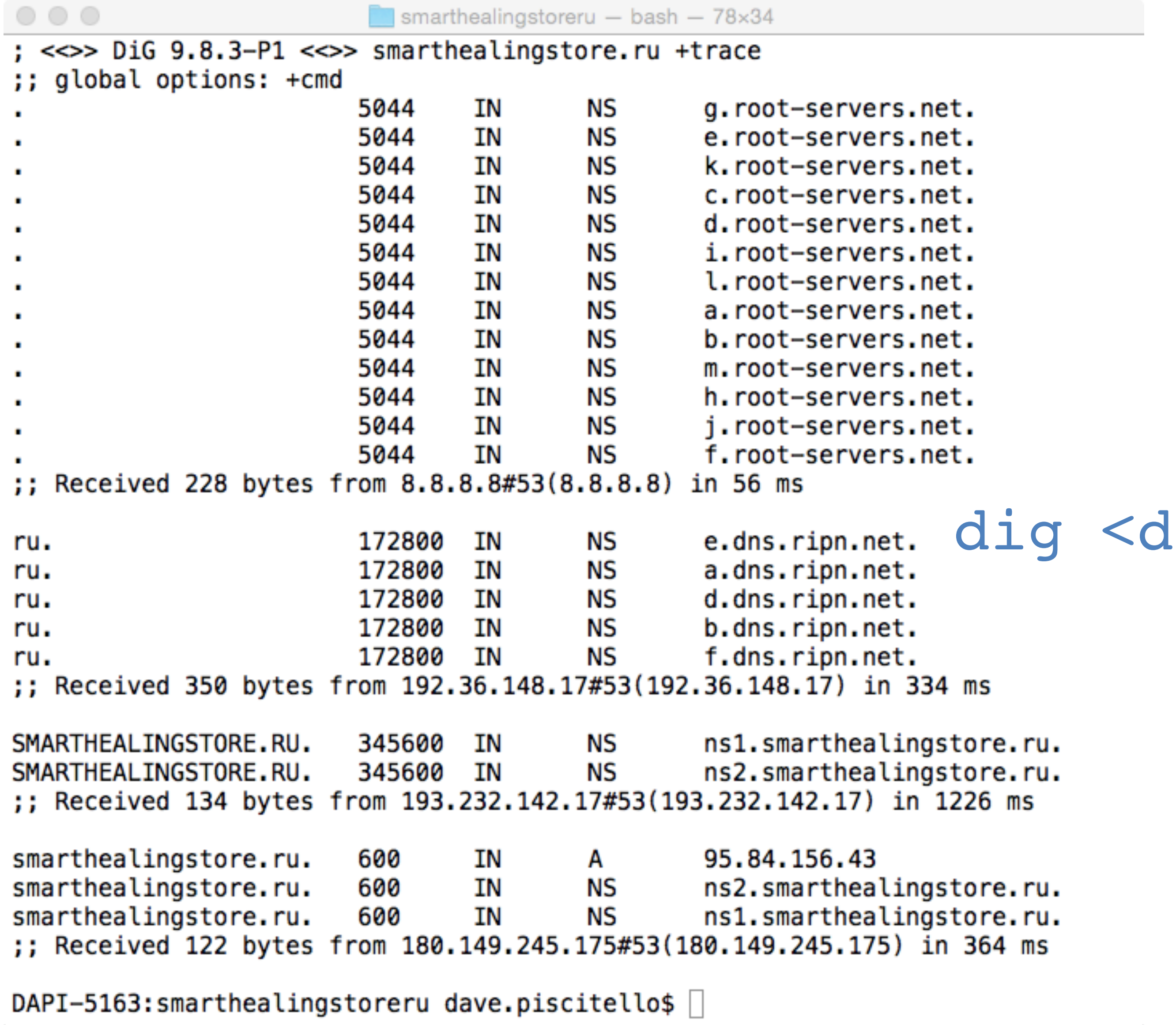
  BFK: http://www.bfk.de/bfk_dnslogger.html

  DNSDB: https://www.dnsdb.info/

- DNS history

  http://dnshistory.org

You Can Trace DNS Queries Using dig



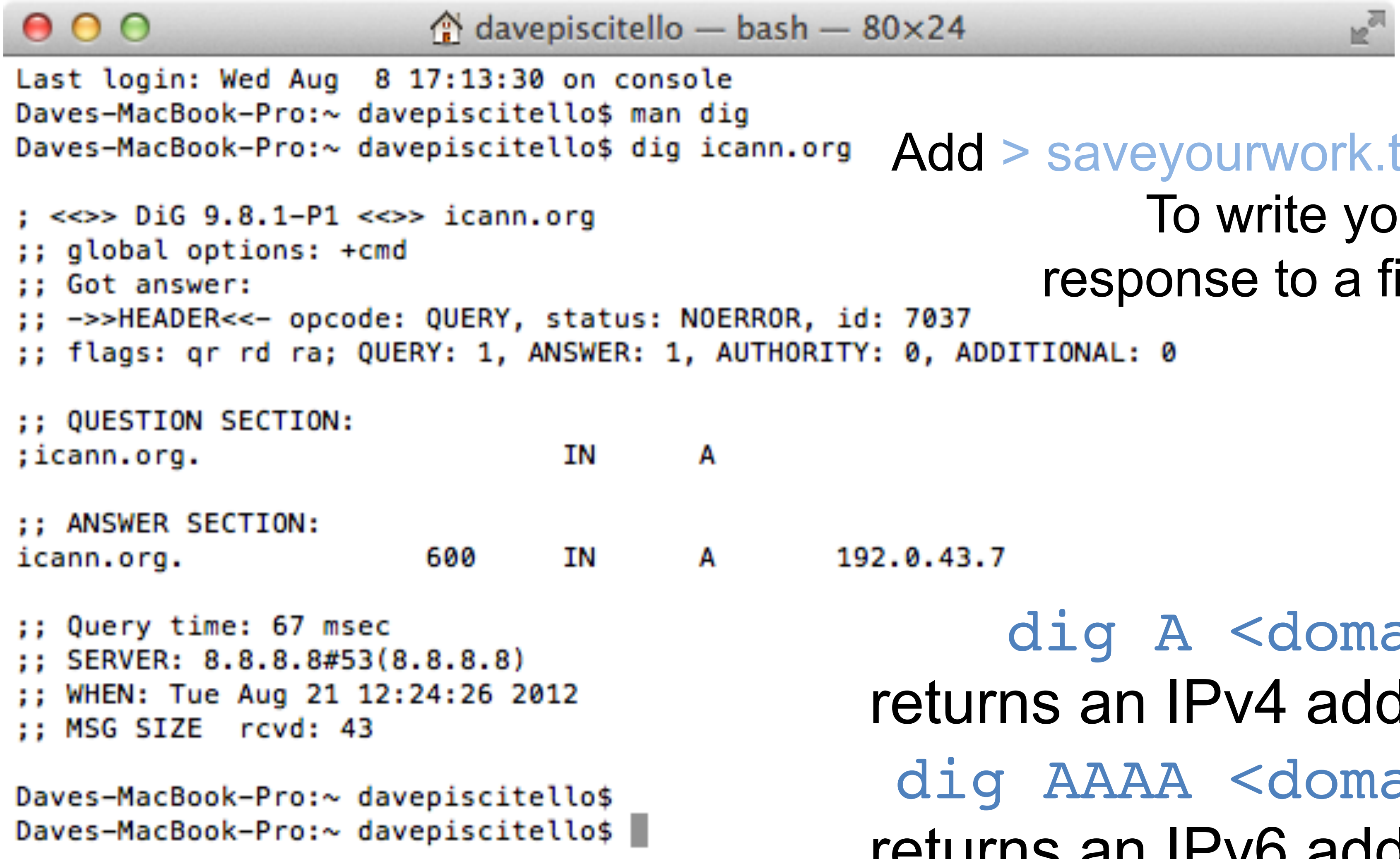
```
; <<>> DiG 9.8.3-P1 <<>> smarthealingstore.ru +trace
;; global options: +cmd
.                       5044    IN      NS      g.root-servers.net.
.                       5044    IN      NS      e.root-servers.net.
.                       5044    IN      NS      k.root-servers.net.
.                       5044    IN      NS      c.root-servers.net.
.                       5044    IN      NS      d.root-servers.net.
.                       5044    IN      NS      i.root-servers.net.
.                       5044    IN      NS      l.root-servers.net.
.                       5044    IN      NS      a.root-servers.net.
.                       5044    IN      NS      b.root-servers.net.
.                       5044    IN      NS      m.root-servers.net.
.                       5044    IN      NS      h.root-servers.net.
.                       5044    IN      NS      j.root-servers.net.
.                       5044    IN      NS      f.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 56 ms

ru.                     172800  IN      NS      e.dns.ripn.net.
ru.                     172800  IN      NS      a.dns.ripn.net.
ru.                     172800  IN      NS      d.dns.ripn.net.
ru.                     172800  IN      NS      b.dns.ripn.net.
ru.                     172800  IN      NS      f.dns.ripn.net.
;; Received 350 bytes from 192.36.148.17#53(192.36.148.17) in 334 ms

SMARTHEALINGSTORE.RU.   345600  IN      NS      ns1.smarthealingstore.ru.
SMARTHEALINGSTORE.RU.   345600  IN      NS      ns2.smarthealingstore.ru.
;; Received 134 bytes from 193.232.142.17#53(193.232.142.17) in 1226 ms

smarthealingstore.ru.   600     IN      A       95.84.156.43
smarthealingstore.ru.   600     IN      NS      ns2.smarthealingstore.ru.
smarthealingstore.ru.   600     IN      NS      ns1.smarthealingstore.ru.
;; Received 122 bytes from 180.149.245.175#53(180.149.245.175) in 364 ms

DAPI-5163:smarthealingstoreru dave.piscitello$ 
```

`dig <domain> +trace`

Returns iterative name resolution results

Using dig (Linux, BSD)

Domain internet groper



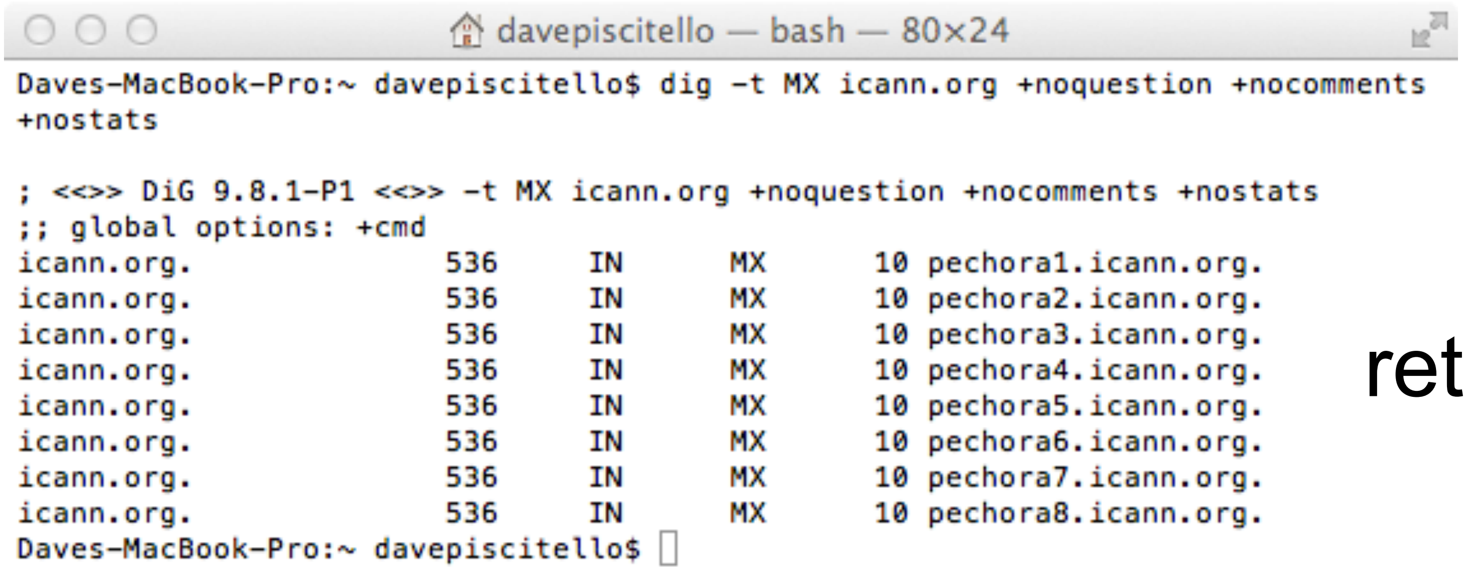
```
Last login: Wed Aug  8 17:13:30 on console
Daves-MacBook-Pro:~ davepiscitello$ man dig
Daves-MacBook-Pro:~ davepiscitello$ dig icann.org

; <<>> 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$ 
```

Add `> saveyourwork.txt`
To write your response to a file

`dig A <domain>`
returns an IPv4 address

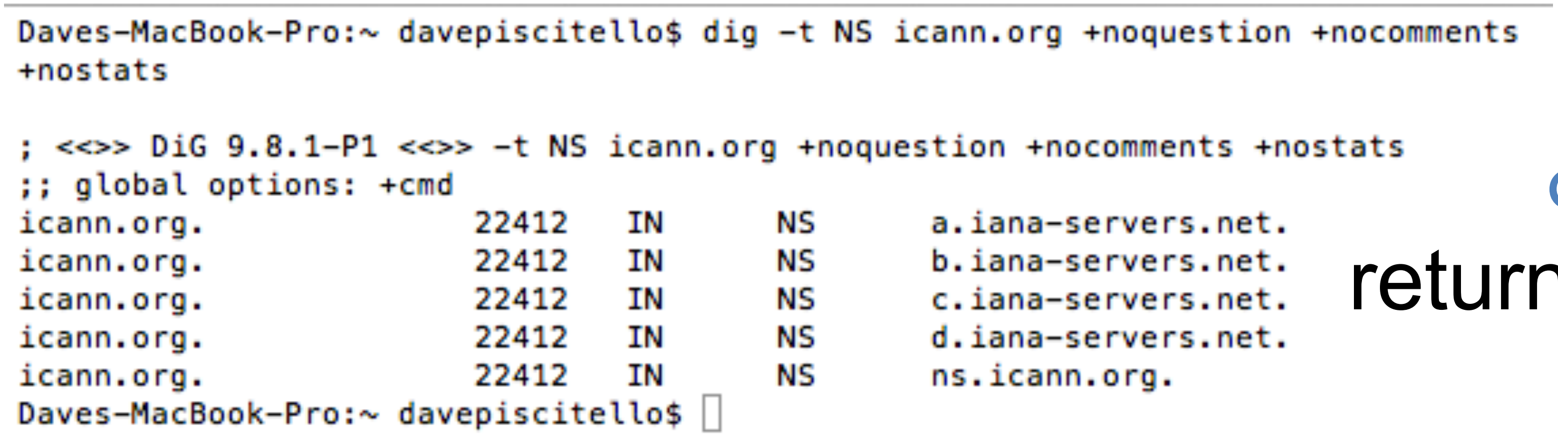
`dig AAAA <domain>`
returns an IPv6 address

Using dig (Linux, BSD, MSDOS)



```
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$ 
```

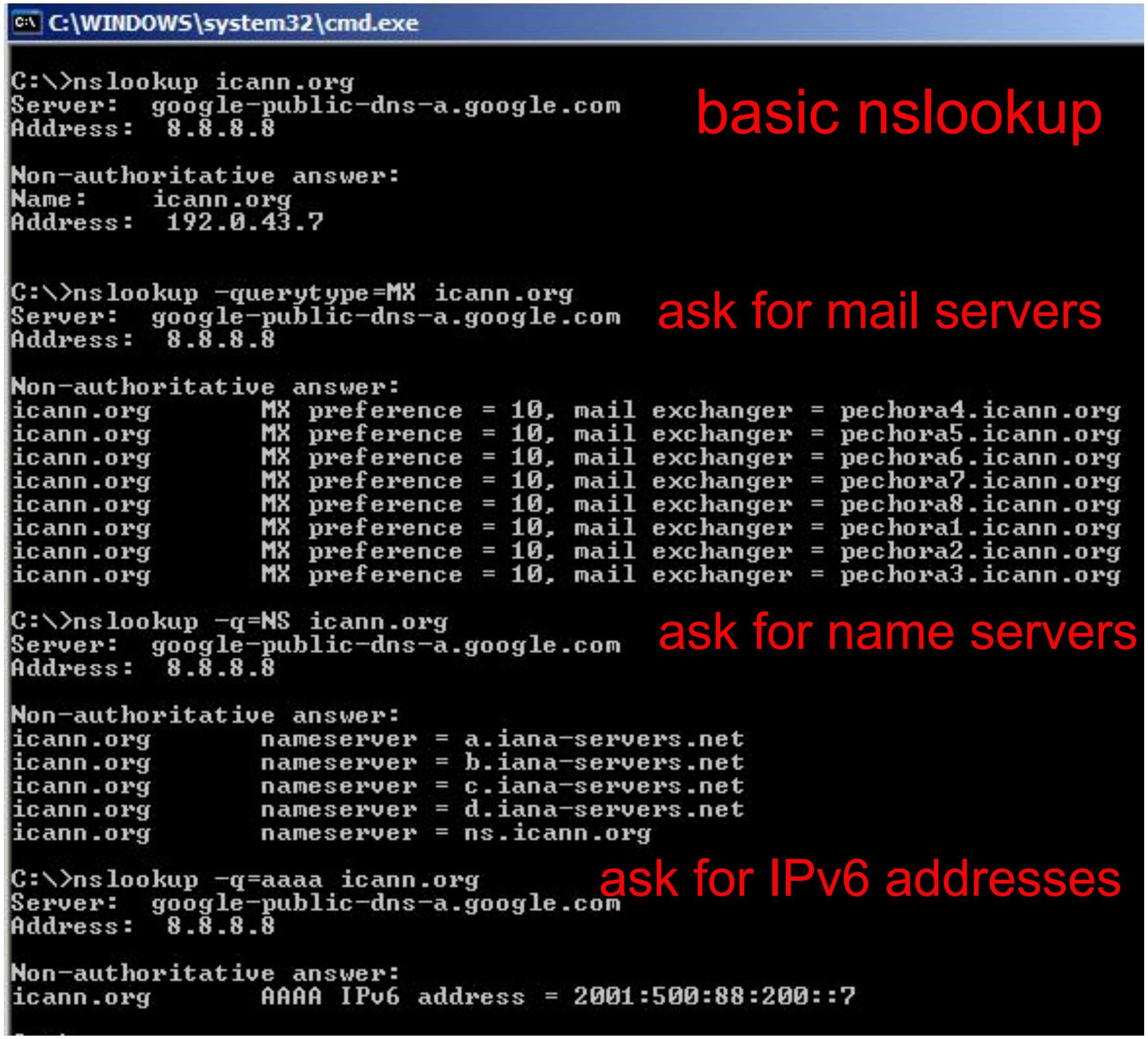
`dig MX` returns mail relay



```
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$ 
```

`dig NS` returns name server

Using nslookup (MSDOS)



basic nslookup

```
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
```

ask for mail servers

```
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
```

ask for name servers

```
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
```

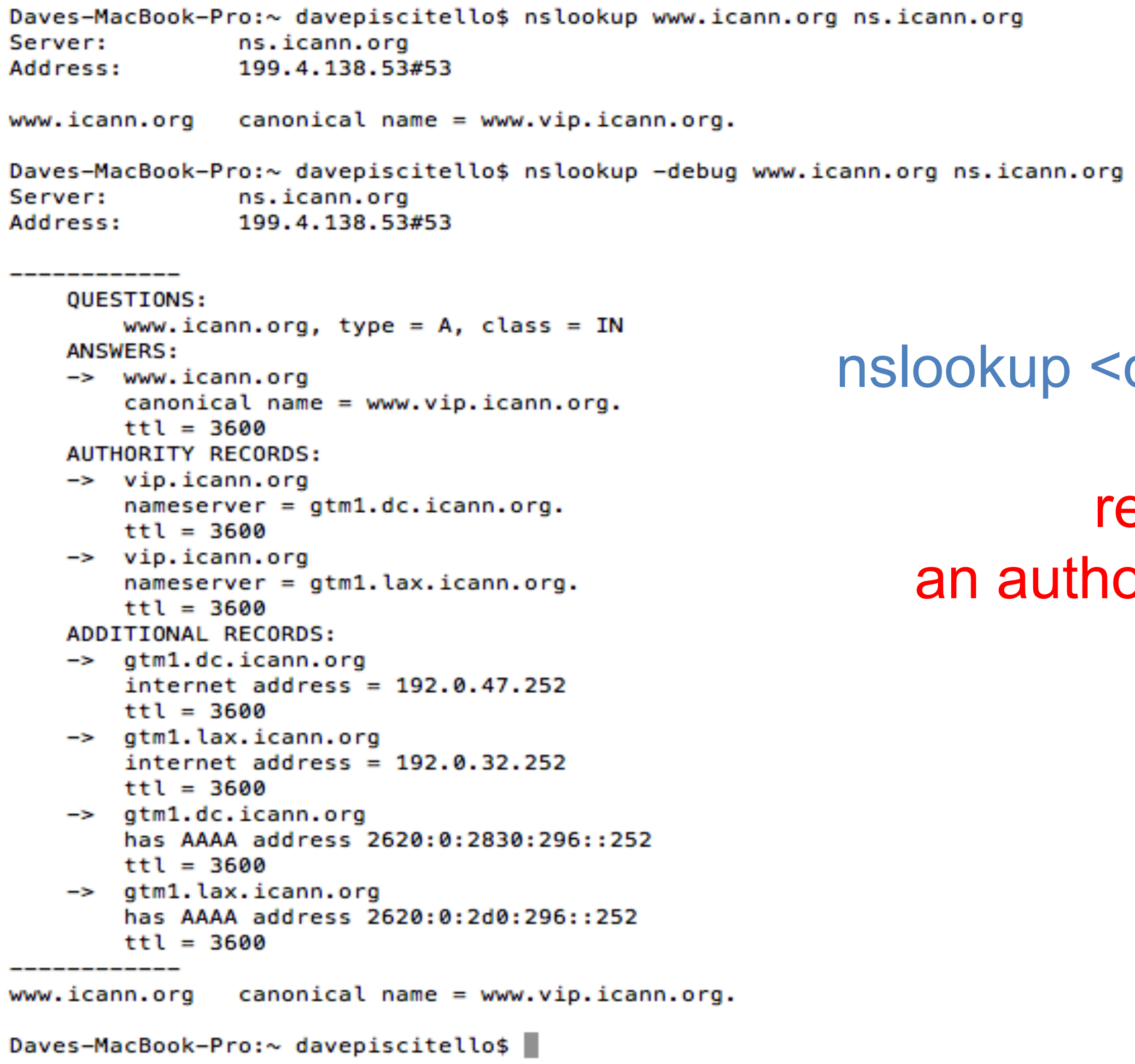
ask for IPv6 addresses

```
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
```

`nslookup` commands use an explicit `-querytype=` or `-q=`

For detailed/verbose answers add -debug

Using nslookup (Linux, BSD)

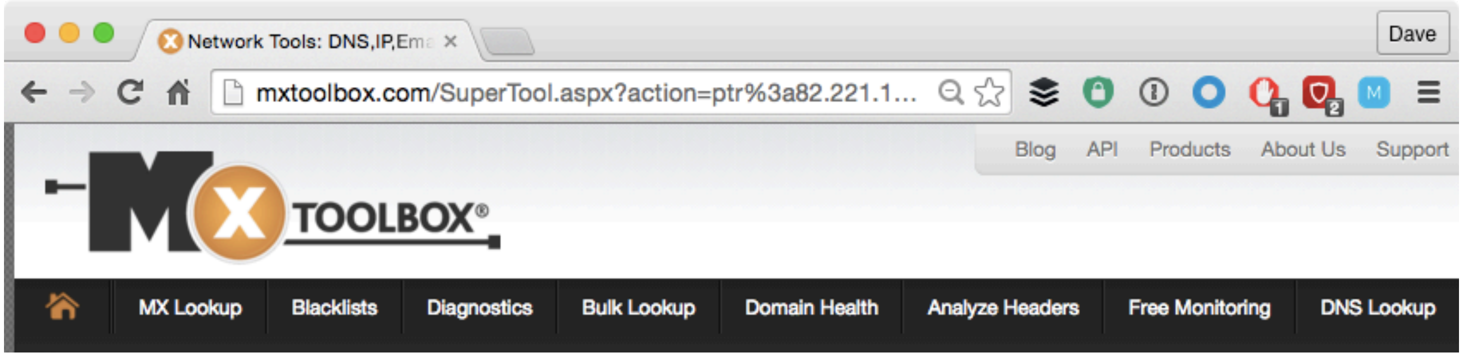


```
Daves-MacBook-Pro:~ davepiscitello$ nslookup www.icann.org ns.icann.org
Server:         ns.icann.org
Address:        199.4.138.53#53

www.icann.org   canonical name = www.vip.icann.org.

Daves-MacBook-Pro:~ davepiscitello$ nslookup -debug www.icann.org ns.icann.org
Server:         ns.icann.org
Address:        199.4.138.53#53

------------
    QUESTIONS:
        www.icann.org, type = A, class = IN
    ANSWERS:
    ->  www.icann.org
        canonical name = www.vip.icann.org.
        ttl = 3600
    AUTHORITY RECORDS:
    ->  vip.icann.org
        nameserver = gtm1.dc.icann.org.
        ttl = 3600
    ->  vip.icann.org
        nameserver = gtm1.lax.icann.org.
        ttl = 3600
    ADDITIONAL RECORDS:
    ->  gtm1.dc.icann.org
        internet address = 192.0.47.252
        ttl = 3600
    ->  gtm1.lax.icann.org
        internet address = 192.0.32.252
        ttl = 3600
    ->  gtm1.dc.icann.org
        has AAAA address 2620:0:2830:296::252
        ttl = 3600
    ->  gtm1.lax.icann.org
        has AAAA address 2620:0:2d0:296::252
        ttl = 3600
------------
www.icann.org   canonical name = www.vip.icann.org.

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

nslookup <domain> <authority>

If you don’t trust a resolver’s answer ask an authoritative name server

Query Zone Data Using Web Tools

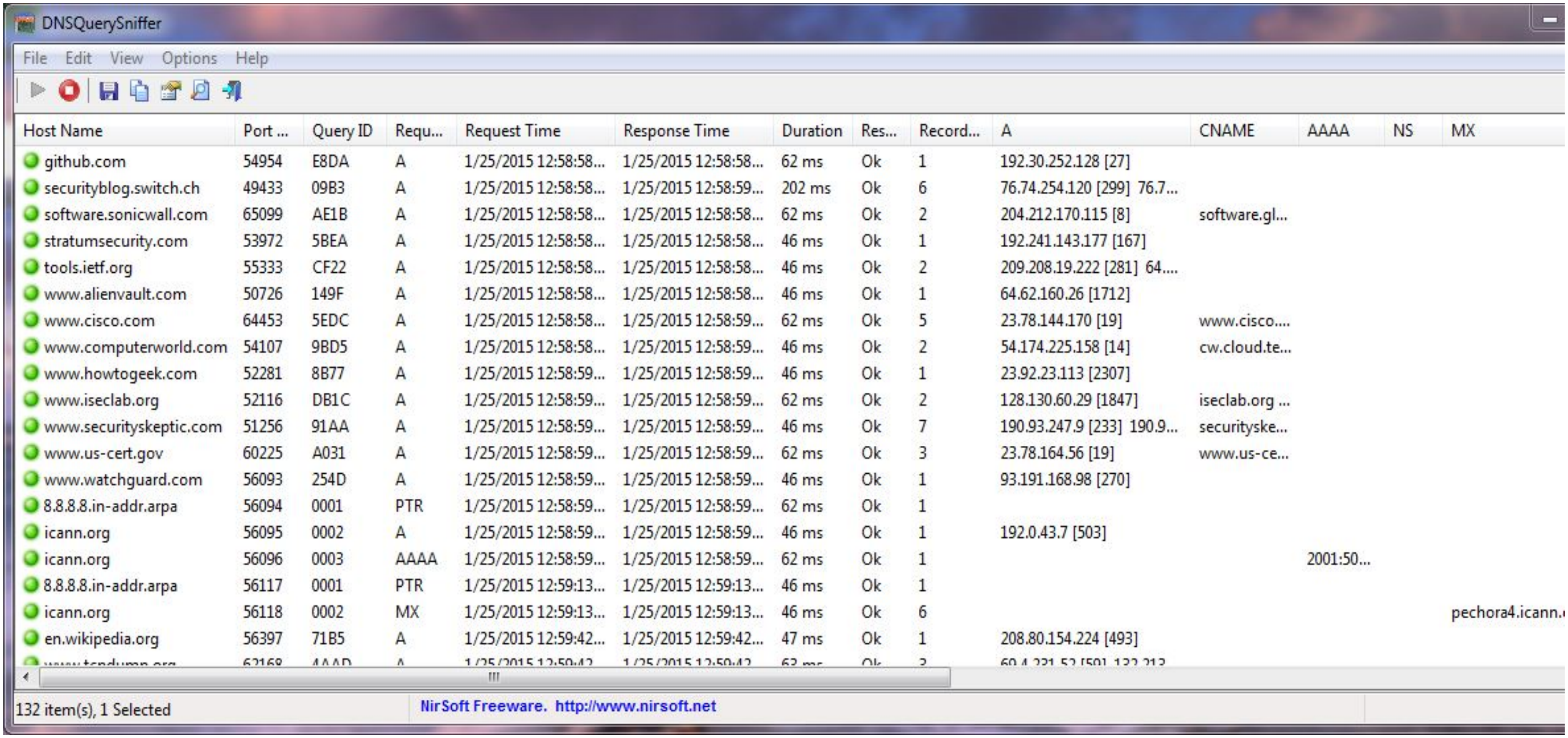


- Commands available:
- For DNS
  - soa, ns, mx, a, cname, txt, spf, ptr
- Other tools:
  - scan: a port scan on the host
  - whois: domain registration information
  - arin: IP address block registration information
  - tcp: Verify an IP Address allows tcp connections
  - http: Verify a URL allows http connections
  - https: Verify a URL allows secure http connections
  - ping: Perform a standard ICMP ping
  - trace: Perform a standard ICMP trace route
  - Blacklist: reputation checks
  - Smtp: test mail server
  - dns:Check DNS Servers for problems

http://mxtoolbox.comSuperTool.aspx

Free to use,
No account required

Observe DNS In Action, In Real Time



Host Name	Port ...	Query ID	Requ...	Request Time	Response Time	Duration	Res...	Record...	A	CNAME	AAAA	NS	MX
github.com	54954	E8DA	A	1/25/2015 12:58:58...	1/25/2015 12:58:58...	62 ms	Ok	1	192.30.252.128 [27]				
securityblog.switch.ch	49433	09B3	A	1/25/2015 12:58:58...	1/25/2015 12:58:59...	202 ms	Ok	6	76.74.254.120 [299] 76.7...				
software.sonicwall.com	65099	AE1B	A	1/25/2015 12:58:58...	1/25/2015 12:58:58...	62 ms	Ok	2	204.212.170.115 [8]	software.gl...			
stratumsecurity.com	53972	5BEA	A	1/25/2015 12:58:58...	1/25/2015 12:58:58...	46 ms	Ok	1	192.241.143.177 [167]				
tools.ietf.org	55333	CF22	A	1/25/2015 12:58:58...	1/25/2015 12:58:58...	46 ms	Ok	2	209.208.19.222 [281] 64....				
www.alienvault.com	50726	149F	A	1/25/2015 12:58:58...	1/25/2015 12:58:58...	46 ms	Ok	1	64.62.160.26 [1712]				
www.cisco.com	64453	5EDC	A	1/25/2015 12:58:58...	1/25/2015 12:58:59...	62 ms	Ok	5	23.78.144.170 [19]	www.cisco....			
www.computerworld.com	54107	9BD5	A	1/25/2015 12:58:58...	1/25/2015 12:58:59...	46 ms	Ok	2	54.174.225.158 [14]	cw.cloud.te...			
www.howtogeek.com	52281	8B77	A	1/25/2015 12:58:59...	1/25/2015 12:58:59...	46 ms	Ok	1	23.92.23.113 [2307]				
www.iseclab.org	52116	DB1C	A	1/25/2015 12:58:59...	1/25/2015 12:58:59...	62 ms	Ok	2	128.130.60.29 [1847]	iseclab.org ...			
www.securityskeptic.com	51256	91AA	A	1/25/2015 12:58:59...	1/25/2015 12:58:59...	46 ms	Ok	7	190.93.247.9 [233] 190.9...	securityske...			
www.us-cert.gov	60225	A031	A	1/25/2015 12:58:59...	1/25/2015 12:58:59...	62 ms	Ok	3	23.78.164.56 [19]	www.us-ce...			
www.watchguard.com	56093	254D	A	1/25/2015 12:58:59...	1/25/2015 12:58:59...	46 ms	Ok	1	93.191.168.98 [270]				
8.8.8.8.in-addr.arpa	56094	0001	PTR	1/25/2015 12:58:59...	1/25/2015 12:58:59...	62 ms	Ok	1					
icann.org	56095	0002	A	1/25/2015 12:58:59...	1/25/2015 12:58:59...	46 ms	Ok	1	192.0.43.7 [503]				
icann.org	56096	0003	AAAA	1/25/2015 12:58:59...	1/25/2015 12:58:59...	62 ms	Ok	1			2001:50...		
8.8.8.8.in-addr.arpa	56117	0001	PTR	1/25/2015 12:59:13...	1/25/2015 12:59:13...	46 ms	Ok	1					
icann.org	56118	0002	MX	1/25/2015 12:59:13...	1/25/2015 12:59:13...	46 ms	Ok	6					pechora4.icann.
en.wikipedia.org	56397	71B5	A	1/25/2015 12:59:42...	1/25/2015 12:59:42...	47 ms	Ok	1	208.80.154.224 [493]				
www.tcpdump.org	62168	4AAD	A	1/25/2015 12:59:42	1/25/2015 12:59:42	62 ms	Ok	3	69.4.231.52 [50] 132.213				

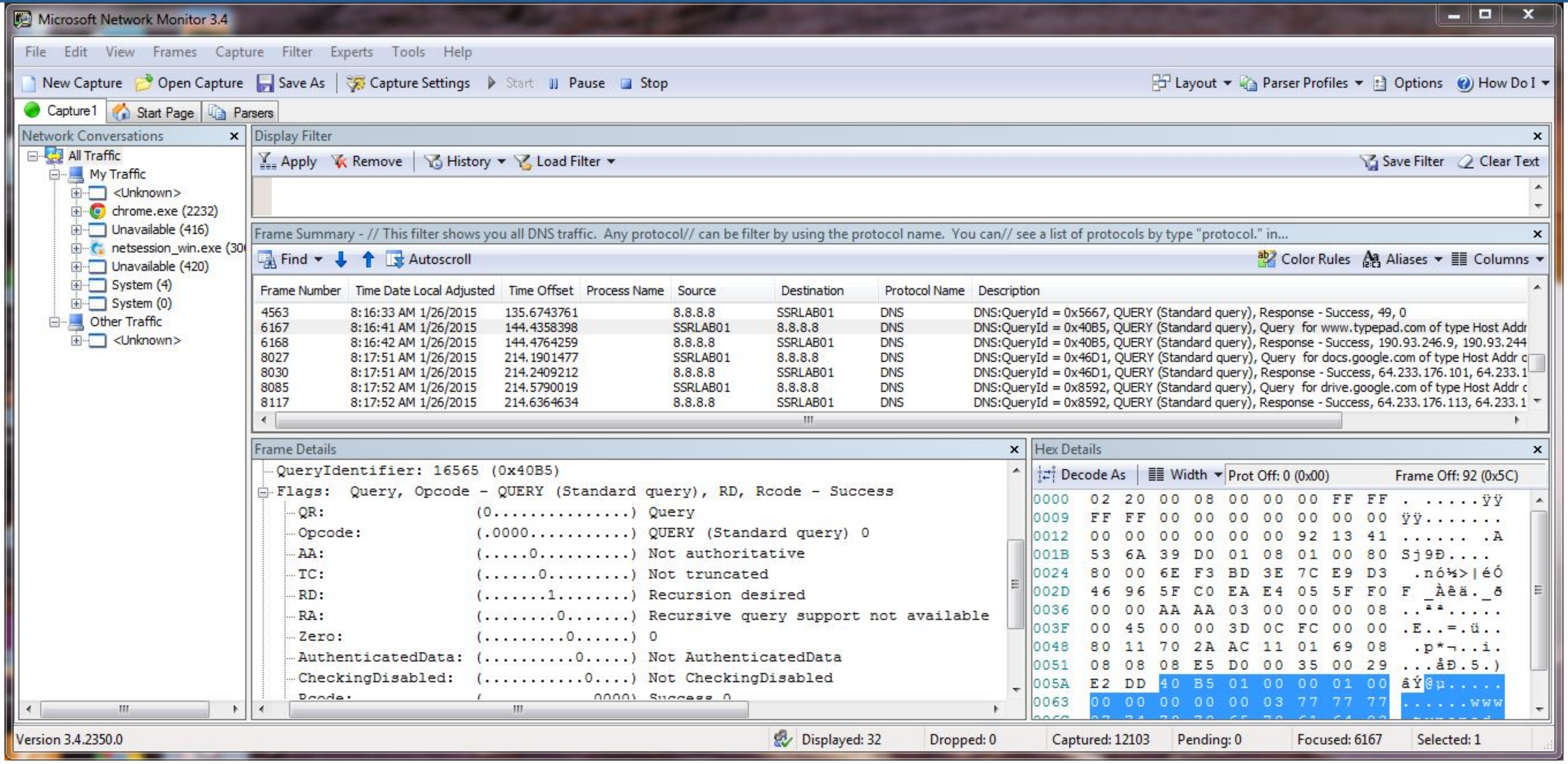
132 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

DNS Query Sniffer (Windows, freeware)

http://www.nirsoft.net/utils/dns_query_sniffer.html

Observe DNS using a LAN Analysis Tool



Frame Summary - // This filter shows you all DNS traffic. Any protocol// can be filter by using the protocol name. You can// see a list of protocols by type "protocol." in...

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
4563	8:16:33 AM 1/26/2015	135.6743761		8.8.8.8	SSRLAB01	DNS	DNS:QueryId = 0x5667, QUERY (Standard query), Response - Success, 49, 0
6167	8:16:41 AM 1/26/2015	144.4358398		SSRLAB01	8.8.8.8	DNS	DNS:QueryId = 0x40B5, QUERY (Standard query), Query for www.typepad.com of type Host Addr
6168	8:16:42 AM 1/26/2015	144.4764259		8.8.8.8	SSRLAB01	DNS	DNS:QueryId = 0x40B5, QUERY (Standard query), Response - Success, 190.93.246.9, 190.93.244
8027	8:17:51 AM 1/26/2015	214.1901477		SSRLAB01	8.8.8.8	DNS	DNS:QueryId = 0x46D1, QUERY (Standard query), Query for docs.google.com of type Host Addr c
8030	8:17:51 AM 1/26/2015	214.2409212		8.8.8.8	SSRLAB01	DNS	DNS:QueryId = 0x46D1, QUERY (Standard query), Response - Success, 64.233.176.101, 64.233.1
8085	8:17:52 AM 1/26/2015	214.5790019		SSRLAB01	8.8.8.8	DNS	DNS:QueryId = 0x8592, QUERY (Standard query), Query for drive.google.com of type Host Addr c
8117	8:17:52 AM 1/26/2015	214.6364634		8.8.8.8	SSRLAB01	DNS	DNS:QueryId = 0x8592, QUERY (Standard query), Response - Success, 64.233.176.113, 64.233.1

```
QueryIdentifier: 16565 (0x40B5)
Flags:  Query, Opcode - QUERY (Standard query), RD, Rcode - Success
   QR:                 (0...............) Query
   Opcode:             (.0000...........) QUERY (Standard query) 0
   AA:                 (.....0..........) Not authoritative
   TC:                 (......0.........) Not truncated
   RD:                 (.......1........) Recursion desired
   RA:                 (........0.......) Recursive query support not available
   Zero:               (.........0......) 0
   AuthenticatedData:  (..........0.....) Not AuthenticatedData
   CheckingDisabled:   (...........0....) Not CheckingDisabled
   Rcode:              (............0000) Success 0
```

Prot Off: 0 (0x00) Frame Off: 92 (0x5C)

```
0000  02 20 00 08 00 00 00 FF FF  . .....ÿÿ
0009  FF FF 00 00 00 00 00 00 00  ÿÿ.......
0012  00 00 00 00 00 00 92 13 41  ...... .A
001B  53 6A 39 D0 01 08 01 00 80  Sj9Ð....
0024  80 00 6E F3 BD 3E 7C E9 D3   .nó½>|éÓ
002D  46 96 5F C0 EA E4 05 5F F0  F _Àêä._ð
0036  00 00 AA AA 03 00 00 00 08  ..ªª.....
003F  00 45 00 00 3D 0C FC 00 00  .E..=.ü..
0048  80 11 70 2A AC 11 01 69 08   .p*¬..i.
0051  08 08 08 E5 D0 00 35 00 29  ...åÐ.5.)
005A  E2 DD 40 B5 01 00 00 01 00  âÝ@µ.....
0063  00 00 00 00 00 03 77 77 77  ......www
```

Version 3.4.2350.0 | Displayed: 32 | Dropped: 0 | Captured: 12103 | Pending: 0 | Focused: 6167 | Selected: 1

Free LAN analyzers with a “DNS” filter to capture DNS traffic:

- WireShark (BSD, Linux, Windows)
- Tcpdump (BSD, Linux, DOS)
- DNS Analyzer (BSD, Linux)
- nmcap3 (Windows) http://support.microsoft.com/kb/933741

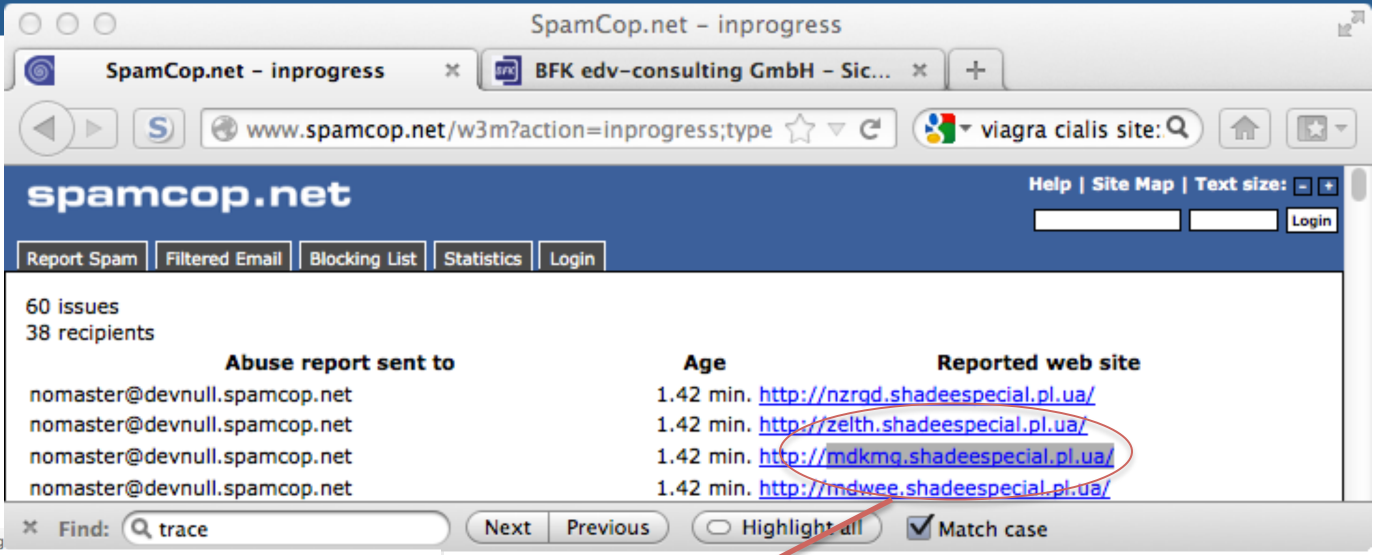
Passive DNS Replication (PDNS)

City of Westminster
METROPOLITAN POLICE
Working together for a safer London
THIEVES BEWARE
PASSIVE DNS
Advanced Forensic Marking
is used in this area
Secured by Design
You are entering an area where premises are forensically protected by SelectaDNA
www.selectadna.co.uk

- Passive DNS
  - Monitors DNS queries & responses near recursive resolvers
  - Puts DNS data you monitor into database
- Passive DNS databases shows query and response traffic, i.e.,
  - DNS records that clients ask to resolve
  - DNS responses that resolvers receive from authoritative servers
- Query database to extract behavior

Passive DNS Replication: DNSlogger

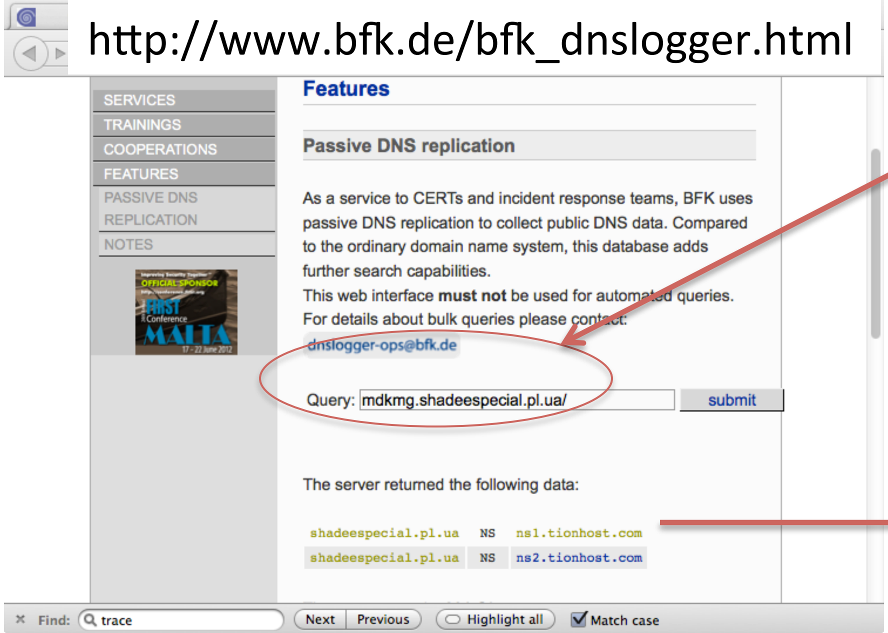
1) Ask
“What name server hosts the zone for the reported abuse domain?”



60 issues
38 recipients

Abuse report sent to	Age	Reported web site
nomaster@devnull.spamcop.net	1.42 min.	http://nzrgd.shadeespecial.pl.ua/
nomaster@devnull.spamcop.net	1.42 min.	http://zelth.shadeespecial.pl.ua/
nomaster@devnull.spamcop.net	1.42 min.	http://mdkmg.shadeespecial.pl.ua/
nomaster@devnull.spamcop.net	1.42 min.	http://mdwee.shadeespecial.pl.ua/

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



Features

Passive DNS replication

As a service to CERTs and incident response teams, BFK uses passive DNS replication to collect public DNS data. Compared to the ordinary domain name system, this database adds further search capabilities.

This web interface **must not** be used for automated queries. For details about bulk queries please contact: dnslogger-ops@bfk.de

Query: mdkmg.shadeespecial.pl.ua/

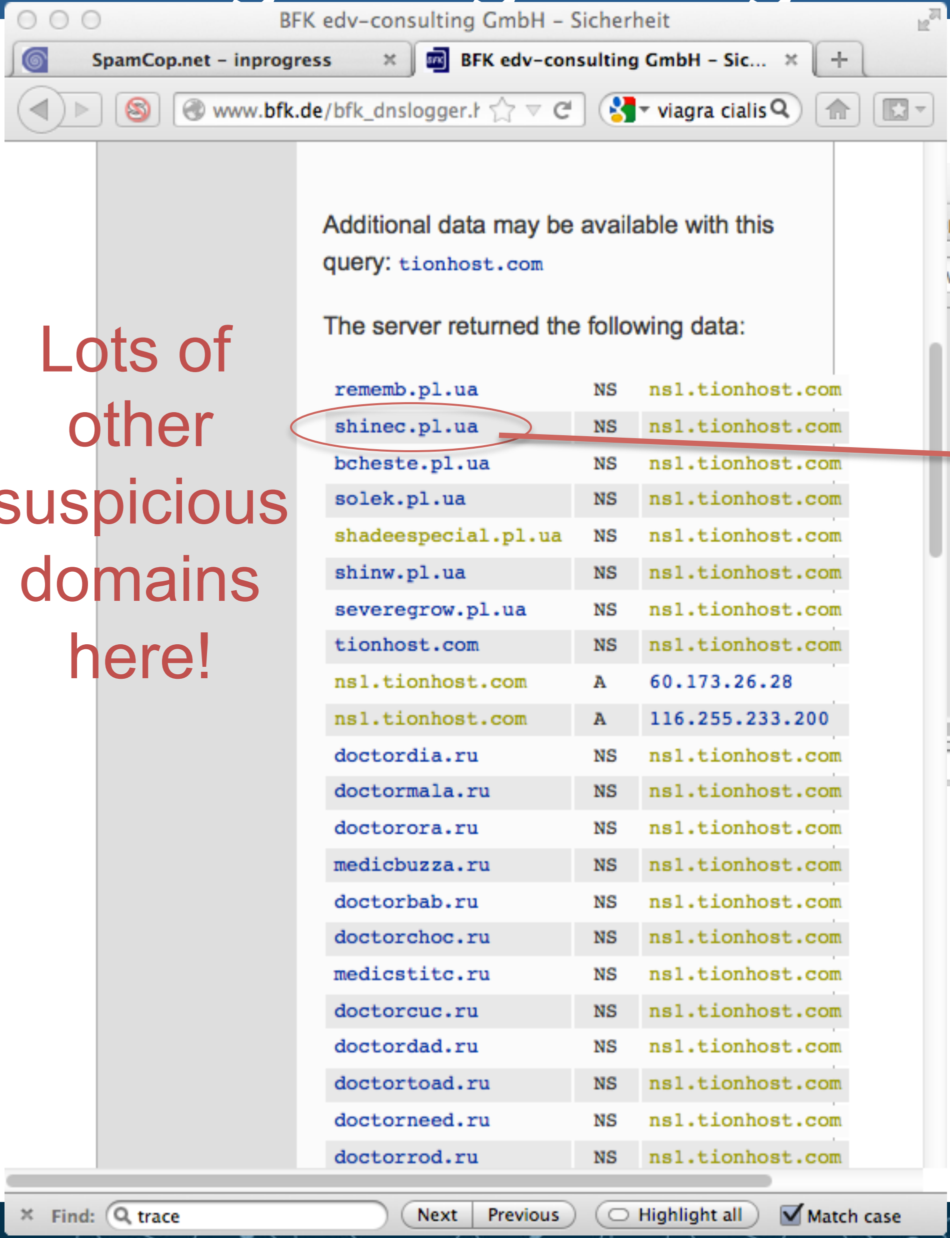
The server returned the following data:

```
shadeespecial.pl.ua   NS   ns1.tionhost.com
shadeespecial.pl.ua   NS   ns2.tionhost.com
```

2) Next ask
“What has been collected about this name at BFK’s monitored resolvers?”

And PDNS says…

Investigating using DNSlogger

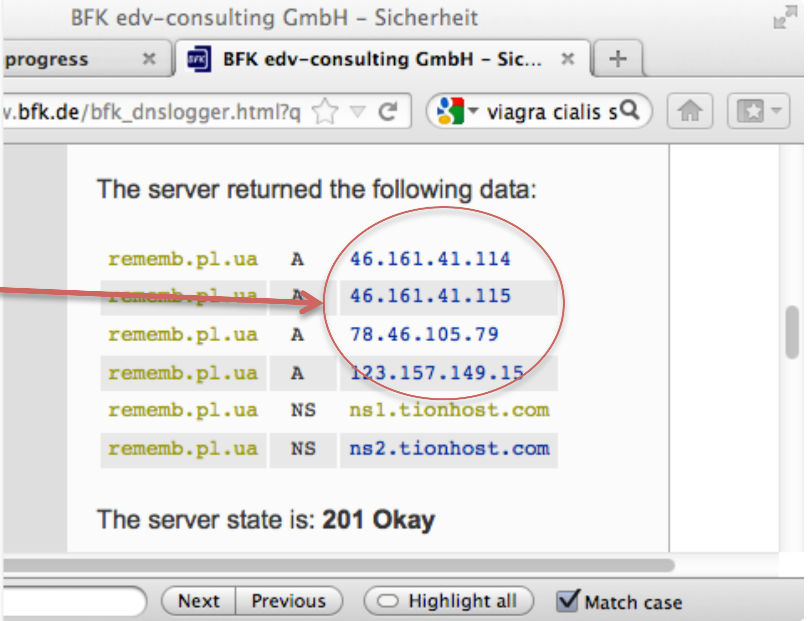


BFK edv-consulting GmbH – Sicherheit
SpamCop.net – inprogress
BFK edv-consulting GmbH – Sic...
www.bfk.de/bfk_dnslogger.h
viagra cialis

Additional data may be available with this query: tionhost.com

The server returned the following data:

rememb.pl.ua	NS	ns1.tionhost.com
shinec.pl.ua	NS	ns1.tionhost.com
bcheste.pl.ua	NS	ns1.tionhost.com
solek.pl.ua	NS	ns1.tionhost.com
shadeespecial.pl.ua	NS	ns1.tionhost.com
shinw.pl.ua	NS	ns1.tionhost.com
severegrow.pl.ua	NS	ns1.tionhost.com
tionhost.com	NS	ns1.tionhost.com
ns1.tionhost.com	A	60.173.26.28
ns1.tionhost.com	A	116.255.233.200
doctordia.ru	NS	ns1.tionhost.com
doctormala.ru	NS	ns1.tionhost.com
doctorora.ru	NS	ns1.tionhost.com
medicbuzza.ru	NS	ns1.tionhost.com
doctorbab.ru	NS	ns1.tionhost.com
doctorchoc.ru	NS	ns1.tionhost.com
medicstitc.ru	NS	ns1.tionhost.com
doctorcuc.ru	NS	ns1.tionhost.com
doctordad.ru	NS	ns1.tionhost.com
doctortoad.ru	NS	ns1.tionhost.com
doctorneed.ru	NS	ns1.tionhost.com
doctorrod.ru	NS	ns1.tionhost.com



BFK edv-consulting GmbH – Sicherheit
progress
BFK edv-consulting GmbH – Sic...
v.bfk.de/bfk_dnslogger.html?q
viagra cialis s

The server returned the following data:

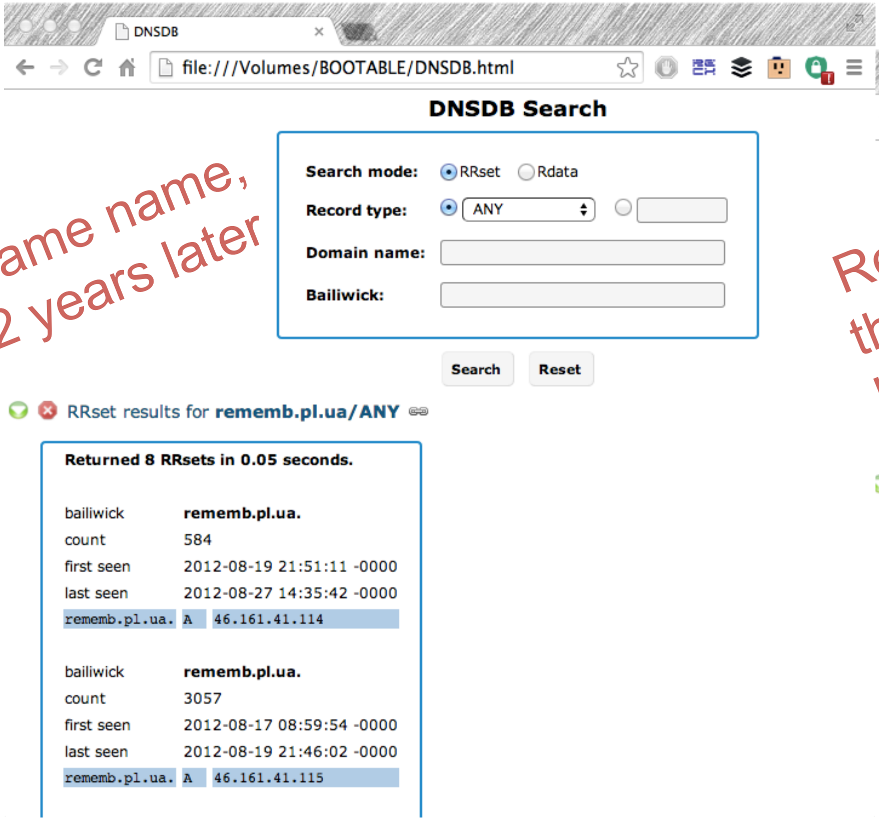
rememb.pl.ua	A	46.161.41.114
rememb.pl.ua	A	46.161.41.115
rememb.pl.ua	A	78.46.105.79
rememb.pl.ua	A	123.157.149.15
rememb.pl.ua	NS	ns1.tionhost.com
rememb.pl.ua	NS	ns2.tionhost.com

The server state is: **201 Okay**

Lots of other suspicious domains here!

Next…
Start looking at:
Domain Whois
IP and ASN Whois

Passive DNS Replication Using DNSDB



Same name, 2 years later

DNSDB Search

Search mode: ● RRset ○ Rdata

Record type: ● ANY ○

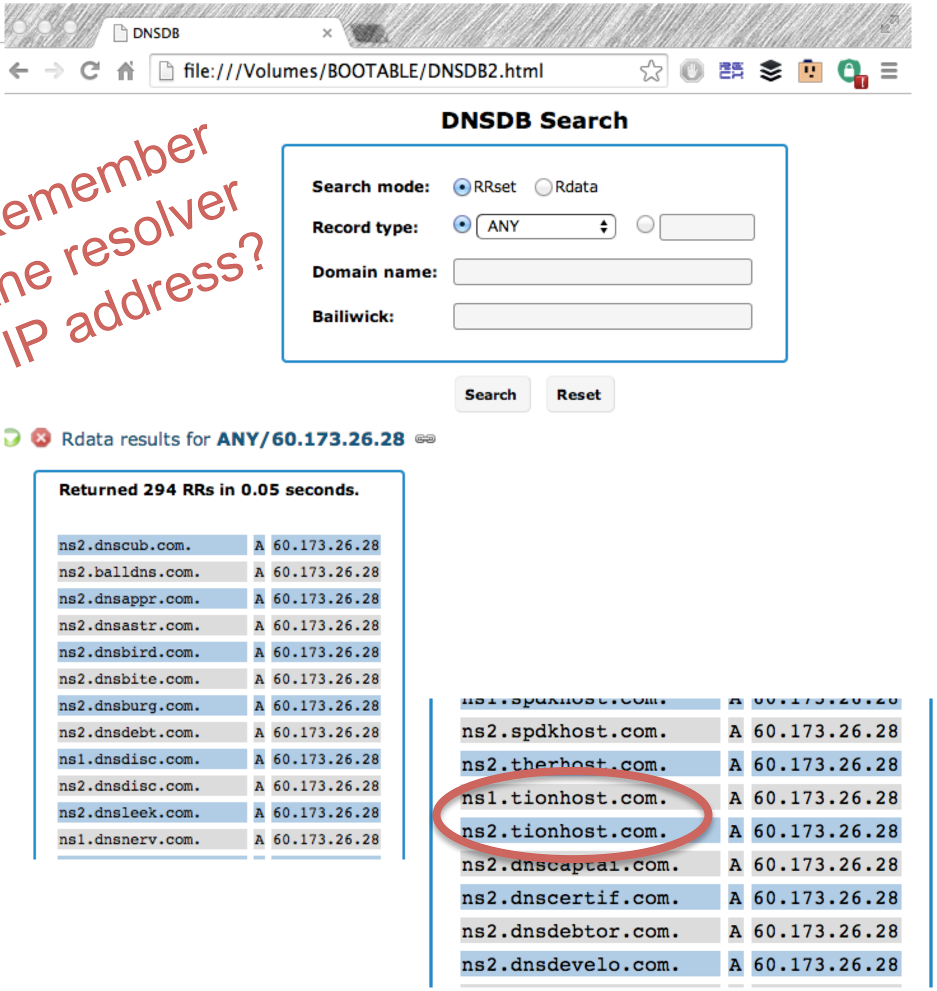
Domain name:

Bailiwick:

RRset results for **rememb.pl.ua/ANY**

Returned 8 RRsets in 0.05 seconds.

```
bailiwick    rememb.pl.ua.
count        584
first seen   2012-08-19 21:51:11 -0000
last seen    2012-08-27 14:35:42 -0000
rememb.pl.ua. A 46.161.41.114

bailiwick    rememb.pl.ua.
count        3057
first seen   2012-08-17 08:59:54 -0000
last seen    2012-08-19 21:46:02 -0000
rememb.pl.ua. A 46.161.41.115
```



Remember the resolver IP address?

DNSDB Search

Search mode: ● RRset ○ Rdata

Record type: ● ANY ○

Domain name:

Bailiwick:

Rdata results for **ANY/60.173.26.28**

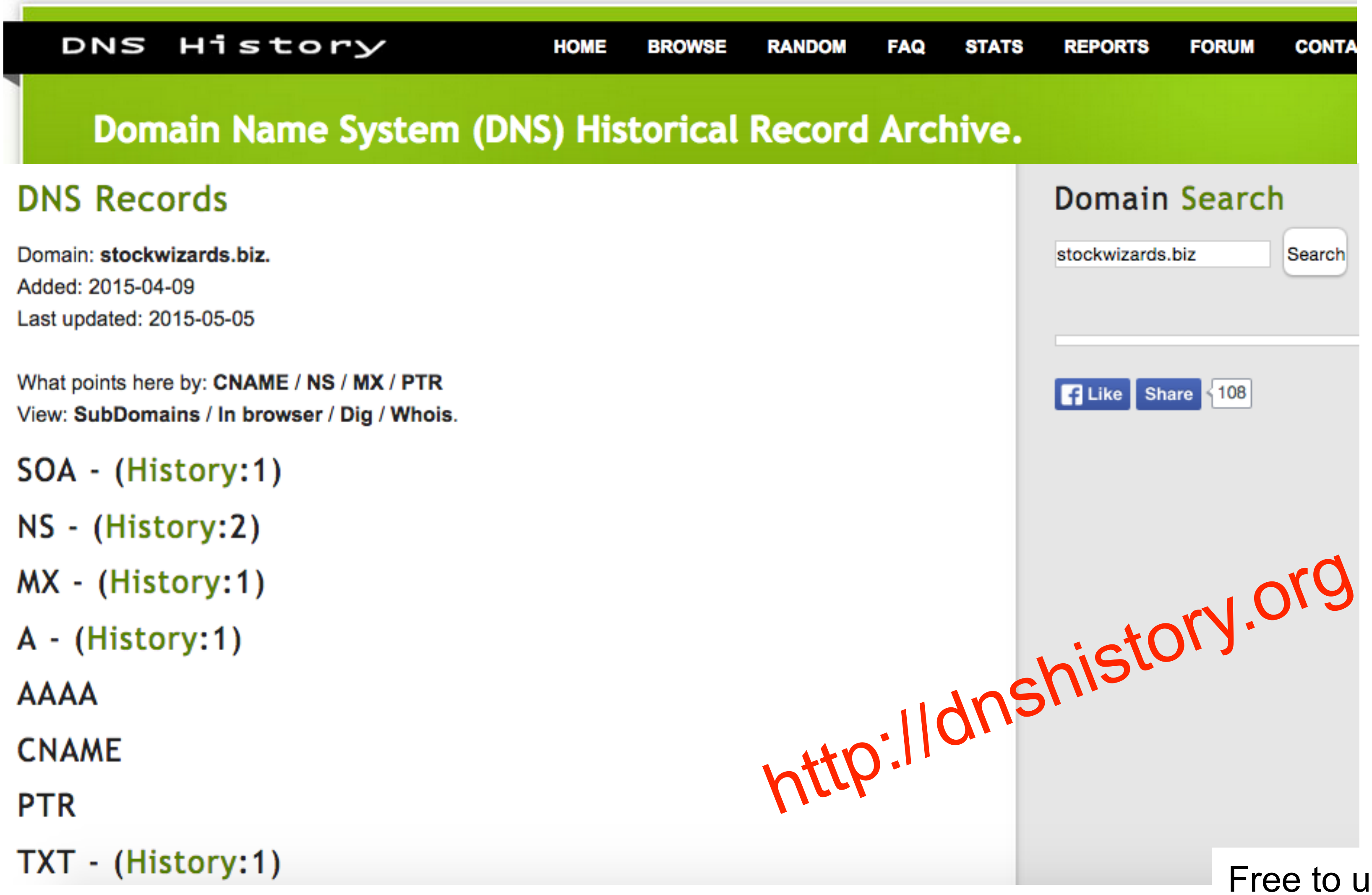
Returned 294 RRs in 0.05 seconds.

```
ns2.dnscub.com.   A 60.173.26.28
ns2.balldns.com.  A 60.173.26.28
ns2.dnsappr.com.  A 60.173.26.28
ns2.dnsastr.com.  A 60.173.26.28
ns2.dnsbird.com.  A 60.173.26.28
ns2.dnsbite.com.  A 60.173.26.28
ns2.dnsburg.com.  A 60.173.26.28
ns2.dnsdebt.com.  A 60.173.26.28
ns1.dnsdisc.com.  A 60.173.26.28
ns2.dnsdisc.com.  A 60.173.26.28
ns2.dnsleek.com.  A 60.173.26.28
ns1.dnsnerv.com.  A 60.173.26.28
```

```
ns1.spdkhost.com.   A 60.173.26.28
ns2.spdkhost.com.   A 60.173.26.28
ns2.therhost.com.   A 60.173.26.28
ns1.tionhost.com.   A 60.173.26.28
ns2.tionhost.com.   A 60.173.26.28
ns2.dnscaptal.com.  A 60.173.26.28
ns2.dnscertif.com.  A 60.173.26.28
ns2.dnsdebtor.com.  A 60.173.26.28
ns2.dnsdevelo.com.  A 60.173.26.28
```

https://www.dnsdb.info/#search
(requires account)

DNSHistory.org: Historical DNS Data



DNS Records

Domain: **stockwizards.biz.**
Added: 2015-04-09
Last updated: 2015-05-05

What points here by: **CNAME** / **NS** / **MX** / **PTR**
View: **SubDomains** / **In browser** / **Dig** / **Whois**.

SOA - (History:1)

NS - (History:2)

MX - (History:1)

A - (History:1)

AAAA

CNAME

PTR

TXT - (History:1)

http://dnshistory.org

Free to use,
No account required

Whois: Registration Data Directory

- Decentralized sets of registration databases
  - Domain registrations managed by registries and registrars
  - Address registrations managed by regional Internet registries
- Two basic models for domain registration data
- *Thin whois*
  - Registrar keeps points of contact, name servers
  - Registry keeps sponsoring registrar, name servers, domain status, domain creation/expiry
- *Thick* whois
  - Registry keeps sponsoring registrar, name servers, domain status, domain creation/expiry, points of contact, name servers

Who Manages The Whois Database?

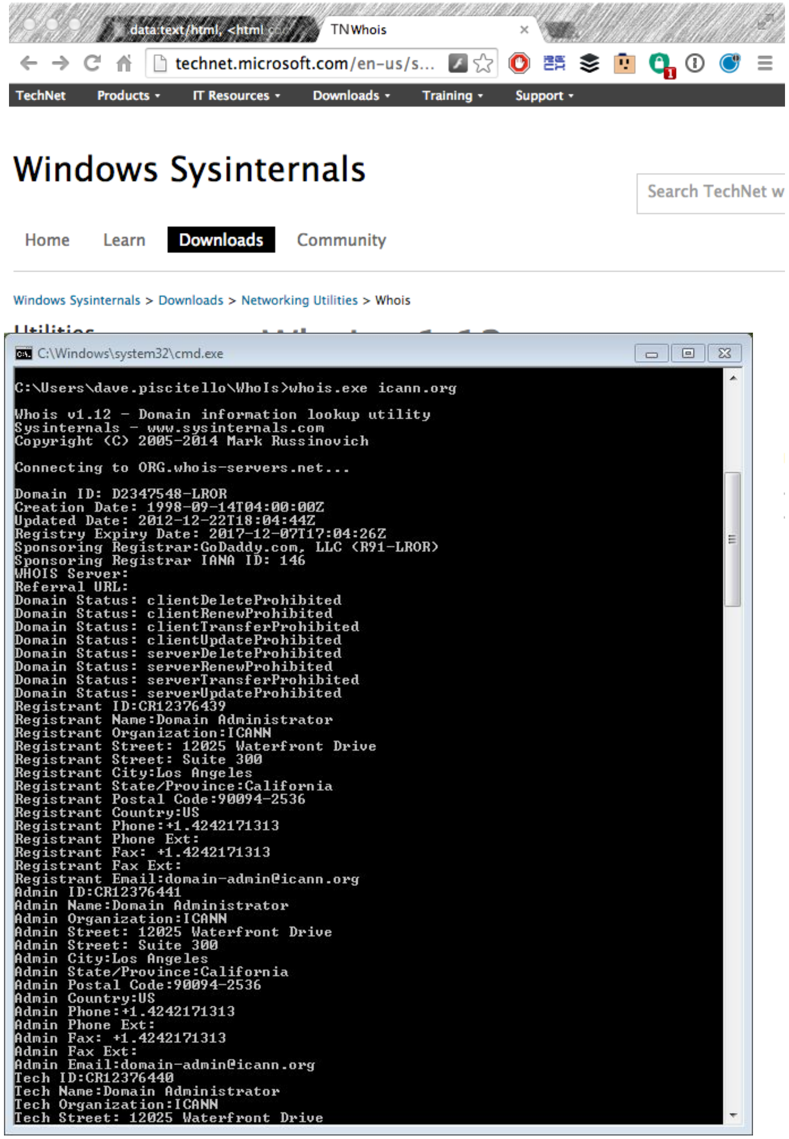
- No single entity manages Domain Whois
  - Domain Whois is highly distributed and privately replicated
    - Registrant is responsible for accuracy
    - ICANN gTLDs and registrars must display Whois data
    - ccTLDs are under no obligation to display Whois data
    - NewTLDs are all to use “Thick whois”
- Address Whois has fewer administrative entities
  - Historically more accurate contact information than Domain Whois

2013 Registrar Accreditation Agreement

2013 “RAA”

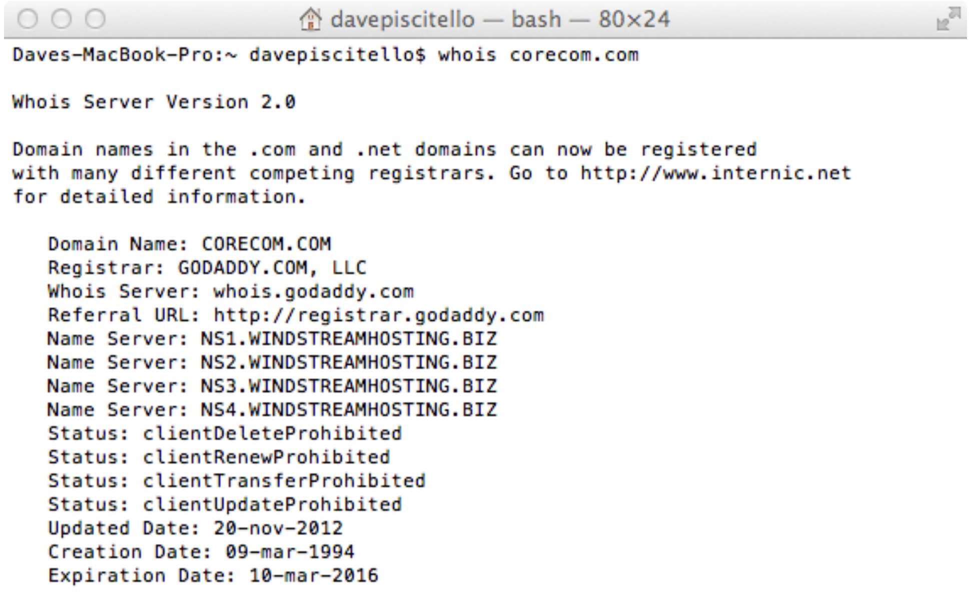
- LE and public Abuse Points of Contact
- Privacy/Proxy specification
- Judicial finding on cybersquatting is cause to terminate domain registration
- Registrars must support DNSSEC & IPv6 data
- Mandatory whois inaccuracy checks (validation, verification, format)
- Enhanced compliance enforcement tools

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 client in default installs:



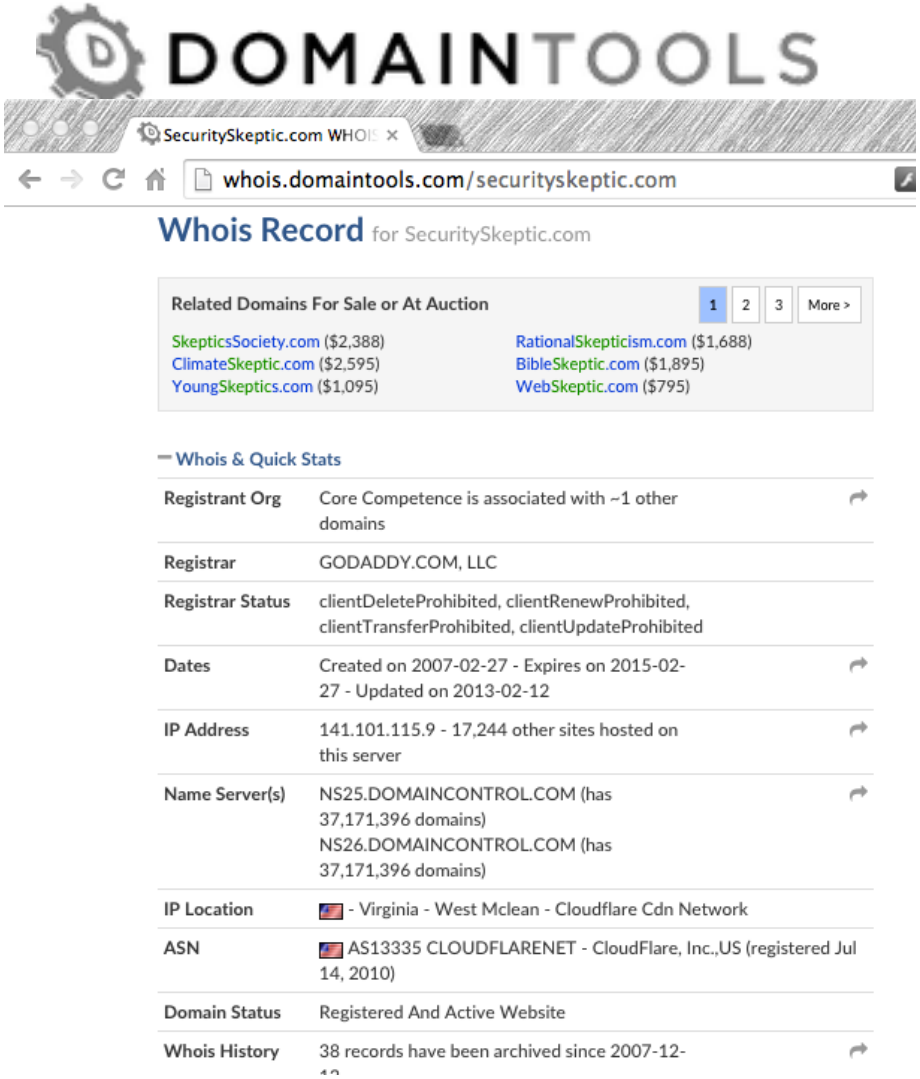
```
Daves-MacBook-Pro:~ davepiscitello$ whois corecom.com

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

Free download for DOS here:

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

Web Based Whois Services



whois.domaintools.com/securityskeptic.com

Whois Record for SecuritySkeptic.com

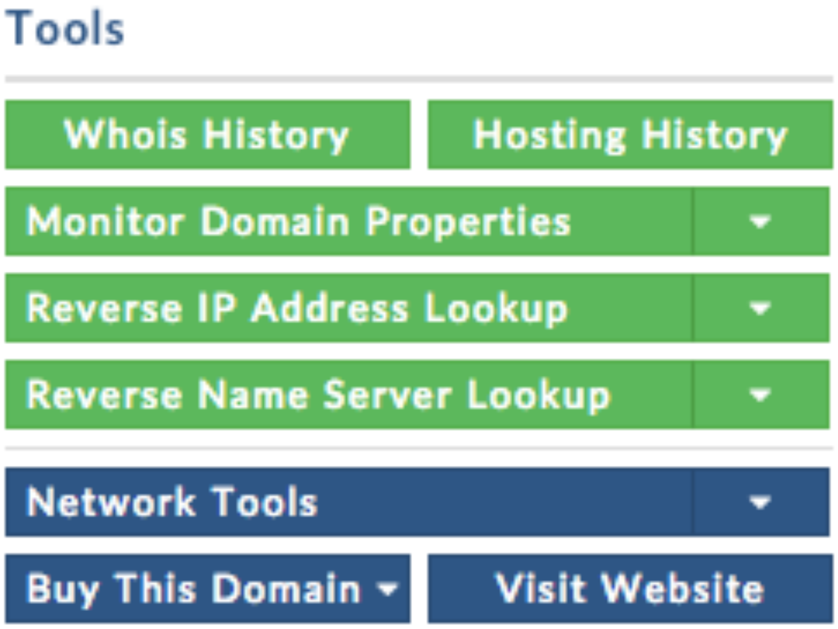
Related Domains For Sale or At Auction

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

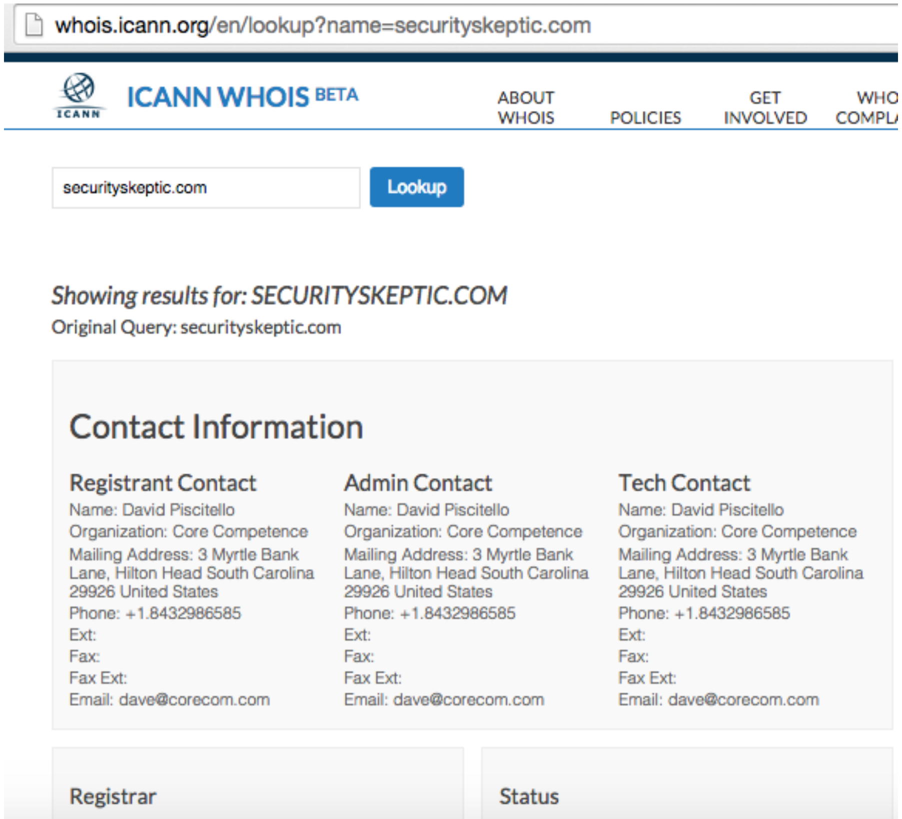
– Whois & Quick Stats

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) 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
Whois History	38 records have been archived since 2007-12-

- Domain Tools (http://domaintools.com)
  - Subscription service offers investigators many tools


Tools
Whois History
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Reverse Name Server Lookup
Network Tools
Buy This Domain
Visit Website

Web Based Whois Services



whois.icann.org/en/lookup?name=securityskeptic.com

Showing results for: SECURITYSKEPTIC.COM

Original Query: securityskeptic.com

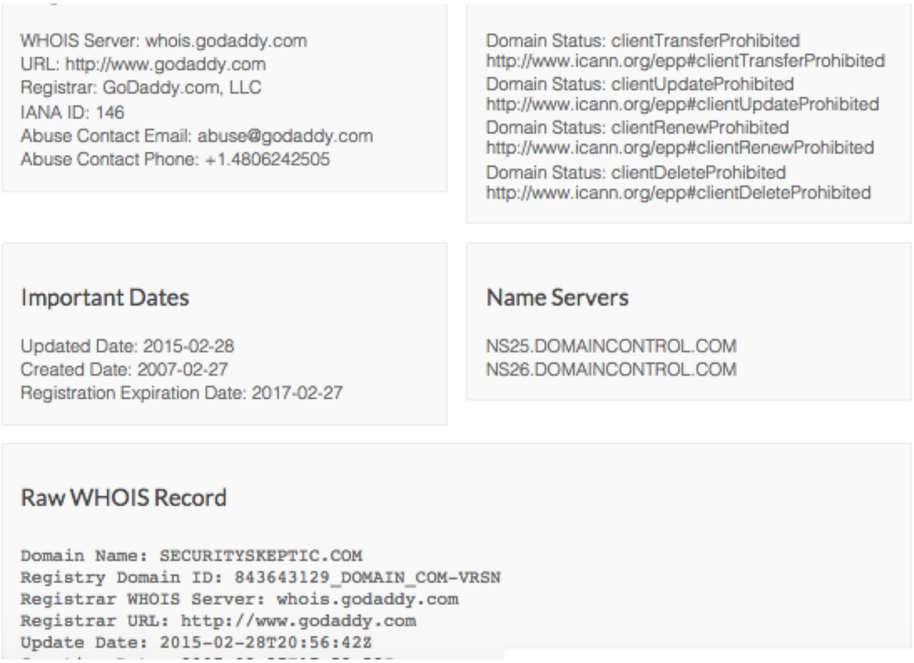
Contact Information

Registrant Contact	Admin Contact	Tech Contact
Name: David Piscitello	Name: David Piscitello	Name: David Piscitello
Organization: Core Competence	Organization: Core Competence	Organization: Core Competence
Mailing Address: 3 Myrtle Bank Lane, Hilton Head South Carolina 29926 United States	Mailing Address: 3 Myrtle Bank Lane, Hilton Head South Carolina 29926 United States	Mailing Address: 3 Myrtle Bank Lane, Hilton Head South Carolina 29926 United States
Phone: +1.8432986585	Phone: +1.8432986585	Phone: +1.8432986585
Ext:	Ext:	Ext:
Fax:	Fax:	Fax:
Fax Ext:	Fax Ext:	Fax Ext:
Email: dave@corecom.com	Email: dave@corecom.com	Email: dave@corecom.com

Registrar

Status

- ICANN (http://whois.icann.org)



WHOIS Server: whois.godaddy.com
URL: http://www.godaddy.com
Registrar: GoDaddy.com, LLC
IANA ID: 146
Abuse Contact Email: abuse@godaddy.com
Abuse Contact Phone: +1.4806242505

Domain Status: clientTransferProhibited
http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited
http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited
http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited
http://www.icann.org/epp#clientDeleteProhibited

Important Dates

Updated Date: 2015-02-28
Created Date: 2007-02-27
Registration Expiration Date: 2017-02-27

Name Servers

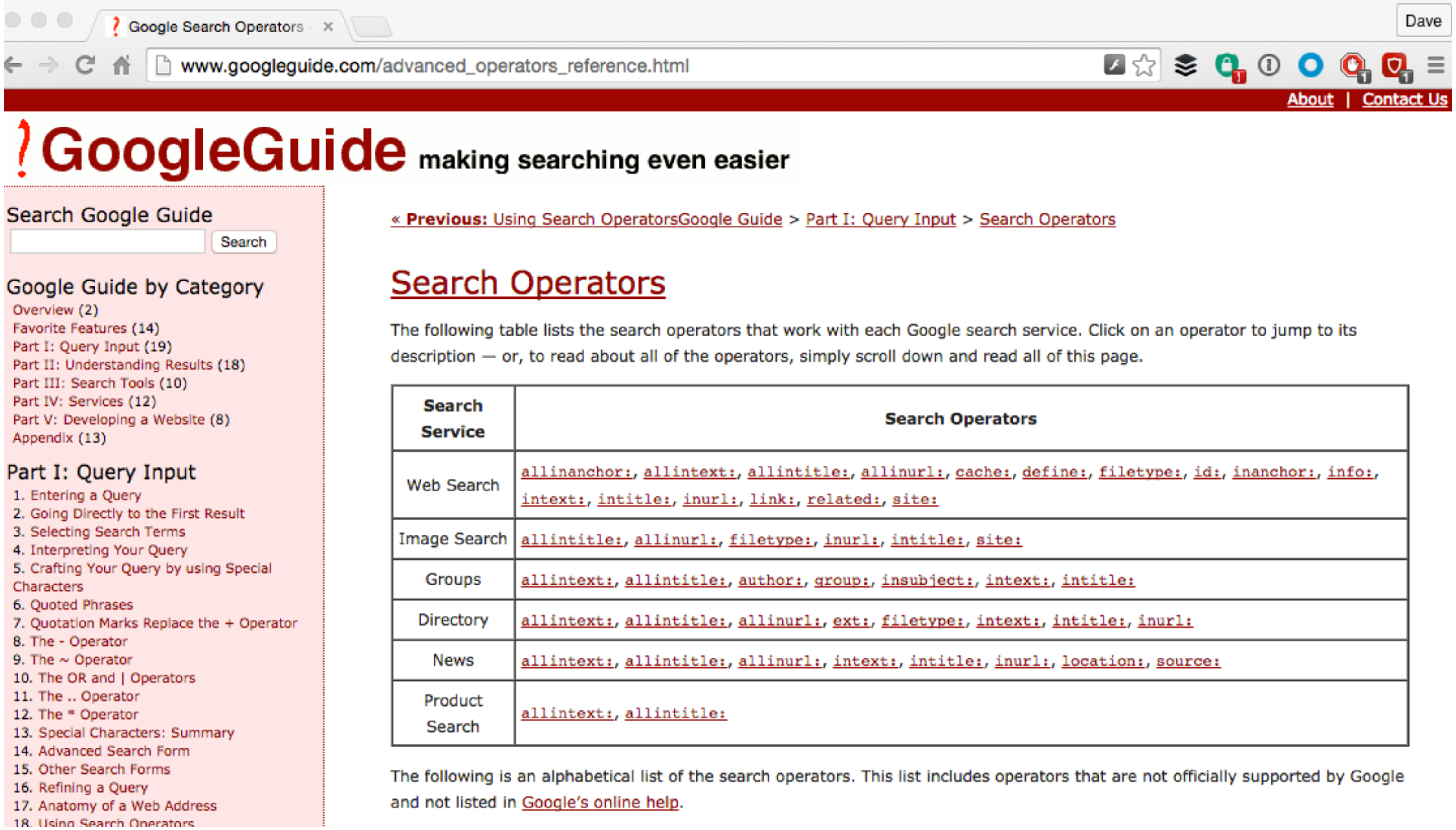
NS25.DOMAINCONTROL.COM
NS26.DOMAINCONTROL.COM

Raw WHOIS Record

```
Domain Name: SECURITYSKEPTIC.COM
Registry Domain ID: 843643129_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2015-02-28T20:56:42Z
```

Free to use,
No account required

Advanced Search Operators



GoogleGuide making searching even easier

Search Google Guide

Search

Google Guide by Category

Overview (2)
Favorite Features (14)
Part I: Query Input (19)
Part II: Understanding Results (18)
Part III: Search Tools (10)
Part IV: Services (12)
Part V: Developing a Website (8)
Appendix (13)

Part I: Query Input

1. Entering a Query
2. Going Directly to the First Result
3. Selecting Search Terms
4. Interpreting Your Query
5. Crafting Your Query by using Special Characters
6. Quoted Phrases
7. Quotation Marks Replace the + Operator
8. The - Operator
9. The ~ Operator
10. The OR and | Operators
11. The .. Operator
12. The * Operator
13. Special Characters: Summary
14. Advanced Search Form
15. Other Search Forms
16. Refining a Query
17. Anatomy of a Web Address
18. Using Search Operators

« **Previous:** Using Search OperatorsGoogle Guide > Part I: Query Input > Search Operators

Search Operators

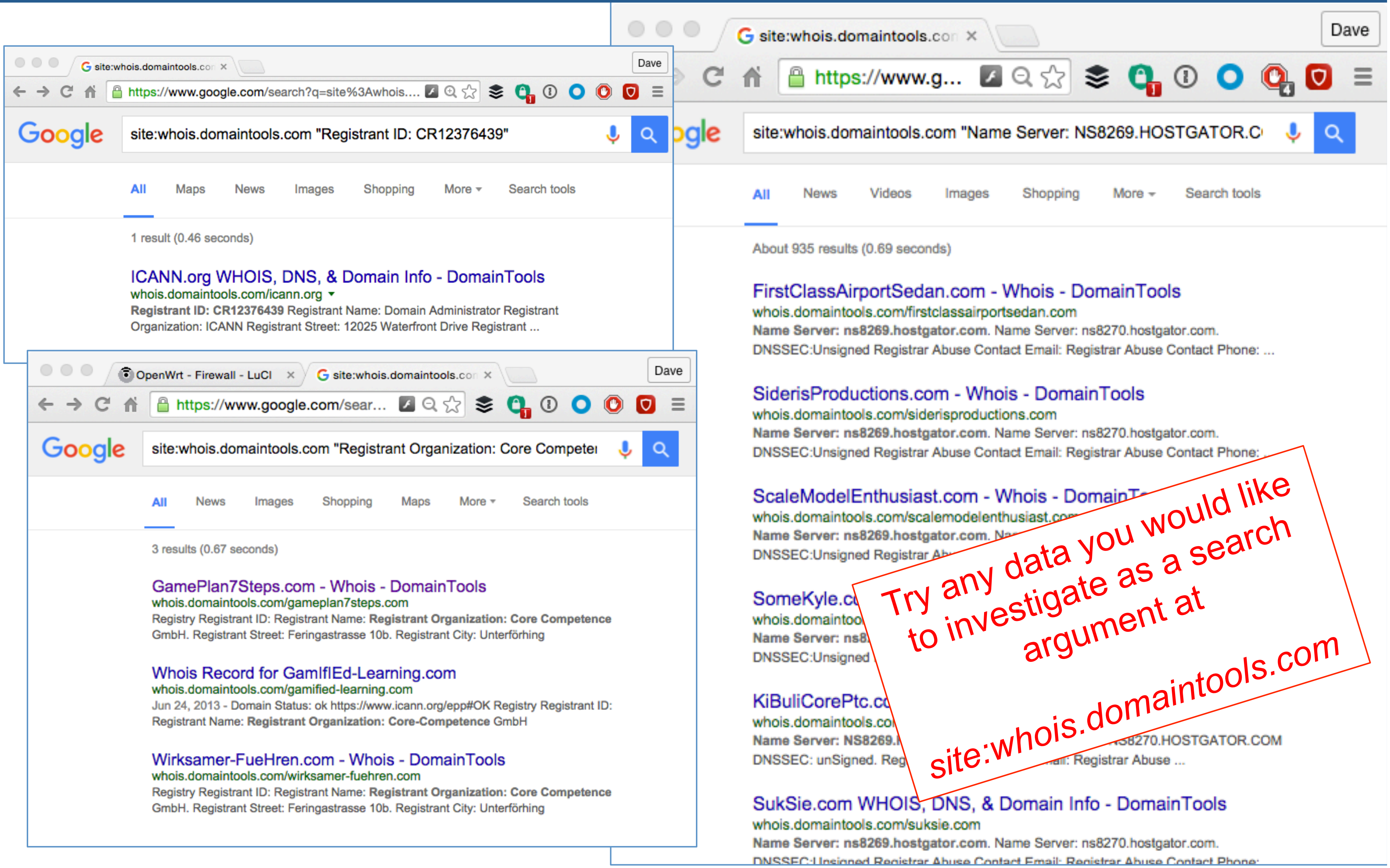
The following table lists the search operators that work with each Google search service. Click on an operator to jump to its description — or, to read about all of the operators, simply scroll down and read all of this page.

Search Service	Search Operators
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Product Search	allintext:, allintitle:

The following is an alphabetical list of the search operators. This list includes operators that are not officially supported by Google and not listed in Google's online help.

Google: http://www.googleguide.com/advanced_operators_reference.html
Bing: http://vlaurie.com/computers2/Articles/bing_advanced_search.htm
Duck Duck Go: https://duck.co/help/results/syntax

Google Hacking Whois



site:whois.domaintools.co ×
Dave
https://www.google.com/search?q=site%3Awhois....
Google
All
Maps
News
Images
Shopping
More ▾
Search tools

site:whois.domaintools.com "Registrant ID: CR12376439"

1 result (0.46 seconds)

ICANN.org WHOIS, DNS, & Domain Info - DomainTools
whois.domaintools.com/icann.org ▾
Registrant ID: CR12376439 Registrant Name: Domain Administrator Registrant Organization: ICANN Registrant Street: 12025 Waterfront Drive Registrant ...

OpenWrt - Firewall - LuCI ×
site:whois.domaintools.co ×
Dave
https://www.google.com/sear...
Google
All
News
Images
Shopping
Maps
More ▾
Search tools

site:whois.domaintools.com "Registrant Organization: Core Compete

3 results (0.67 seconds)

GamePlan7Steps.com - Whois - DomainTools
whois.domaintools.com/gameplan7steps.com
Registry Registrant ID: Registrant Name: **Registrant Organization: Core Competence** GmbH. Registrant Street: Feringastrasse 10b. Registrant City: Unterförhing

Whois Record for GamIflEd-Learning.com
whois.domaintools.com/gamified-learning.com
Jun 24, 2013 - Domain Status: ok https://www.icann.org/epp#OK Registry Registrant ID: Registrant Name: **Registrant Organization: Core-Competence** GmbH

Wirksamer-FueHren.com - Whois - DomainTools
whois.domaintools.com/wirksamer-fuehren.com
Registry Registrant ID: Registrant Name: **Registrant Organization: Core Competence** GmbH. Registrant Street: Feringastrasse 10b. Registrant City: Unterförhing

site:whois.domaintools.com "Name Server: NS8269.HOSTGATOR.C

About 935 results (0.69 seconds)

FirstClassAirportSedan.com - Whois - DomainTools
whois.domaintools.com/firstclassairportsedan.com
Name Server: ns8269.hostgator.com. Name Server: ns8270.hostgator.com. DNSSEC:Unsigned Registrar Abuse Contact Email: Registrar Abuse Contact Phone: ...

SiderisProductions.com - Whois - DomainTools
whois.domaintools.com/siderisproductions.com
Name Server: ns8269.hostgator.com. Name Server: ns8270.hostgator.com. DNSSEC:Unsigned Registrar Abuse Contact Email: Registrar Abuse Contact Phone: ...

ScaleModelEnthusiast.com - Whois - DomainT
whois.domaintools.com/scalemodelenthusiast.com
Name Server: ns8269.hostgator.com. Na
DNSSEC:Unsigned Registrar Ab

SomeKyle.c
whois.domaintoo
Name Server: ns8
DNSSEC:Unsigned

KiBuliCorePtc.c
whois.domaintools.co
Name Server: NS8269. 8270.HOSTGATOR.COM
DNSSEC: unSigned. Reg ail: Registrar Abuse ...

SukSie.com WHOIS, DNS, & Domain Info - DomainTools
whois.domaintools.com/suksie.com
Name Server: ns8269.hostgator.com. Name Server: ns8270.hostgator.com.
DNSSEC:Unsigned Registrar Abuse Contact Email: Registrar Abuse Contact Phone:

Try any data you would like to investigate as a search argument at

site:whois.domaintools.com

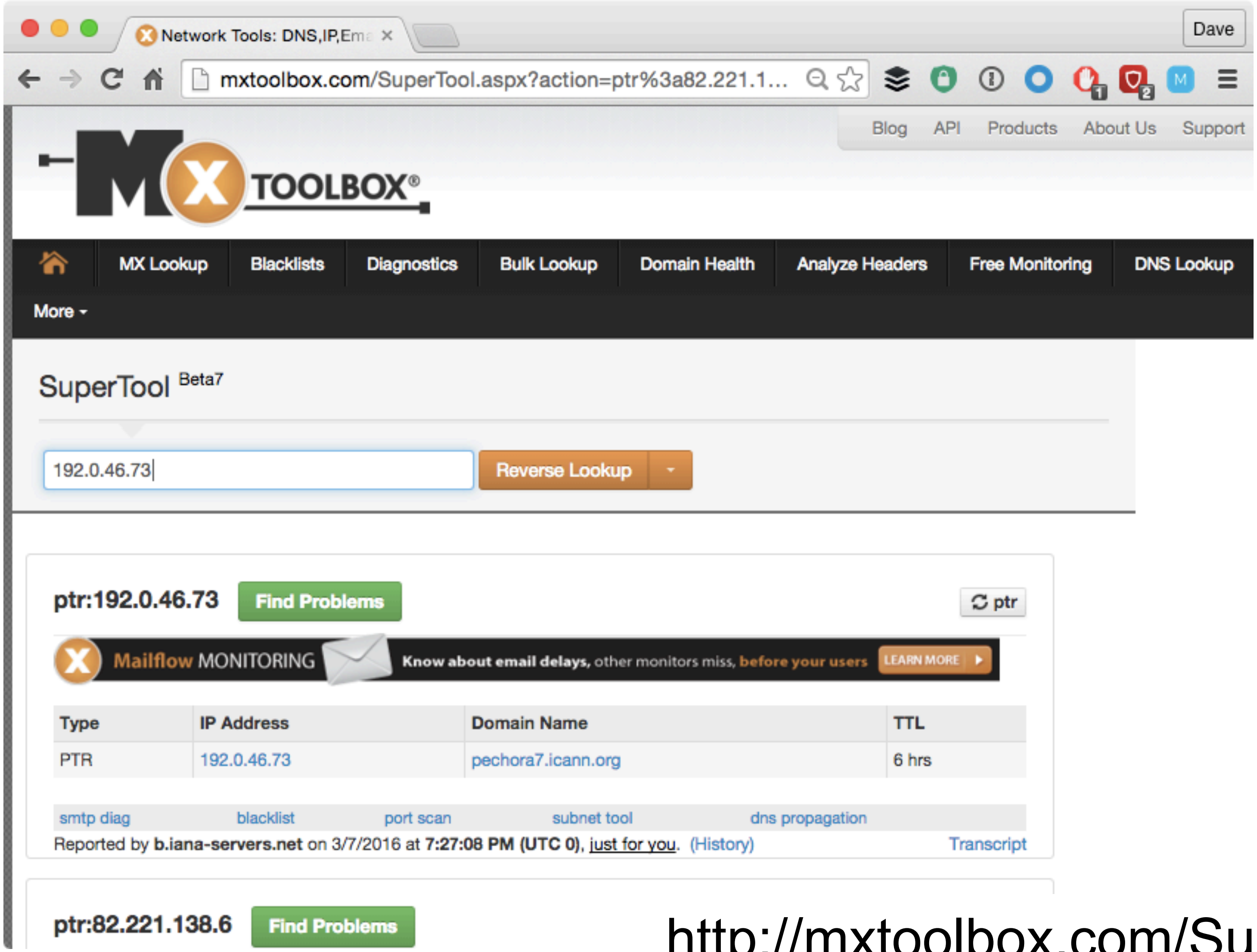
Investigating IP Addresses And ASNs

Address Whois:

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

- Shadowserver Whois
  - http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP
- Ripe Stats
  - http://stat.ripe.net
- Team Cymru
  - https://asn.cymru.com/
- Mxtoolbox
  - http://mxtoolbox.com/SuperTool.aspx
- YouGetSignal
  - http://www.yougetsignal.com

Reverse IP Lookup



192.0.46.73

ptr:192.0.46.73

Type	IP Address	Domain Name	TTL
PTR	192.0.46.73	pechora7.icann.org	6 hrs

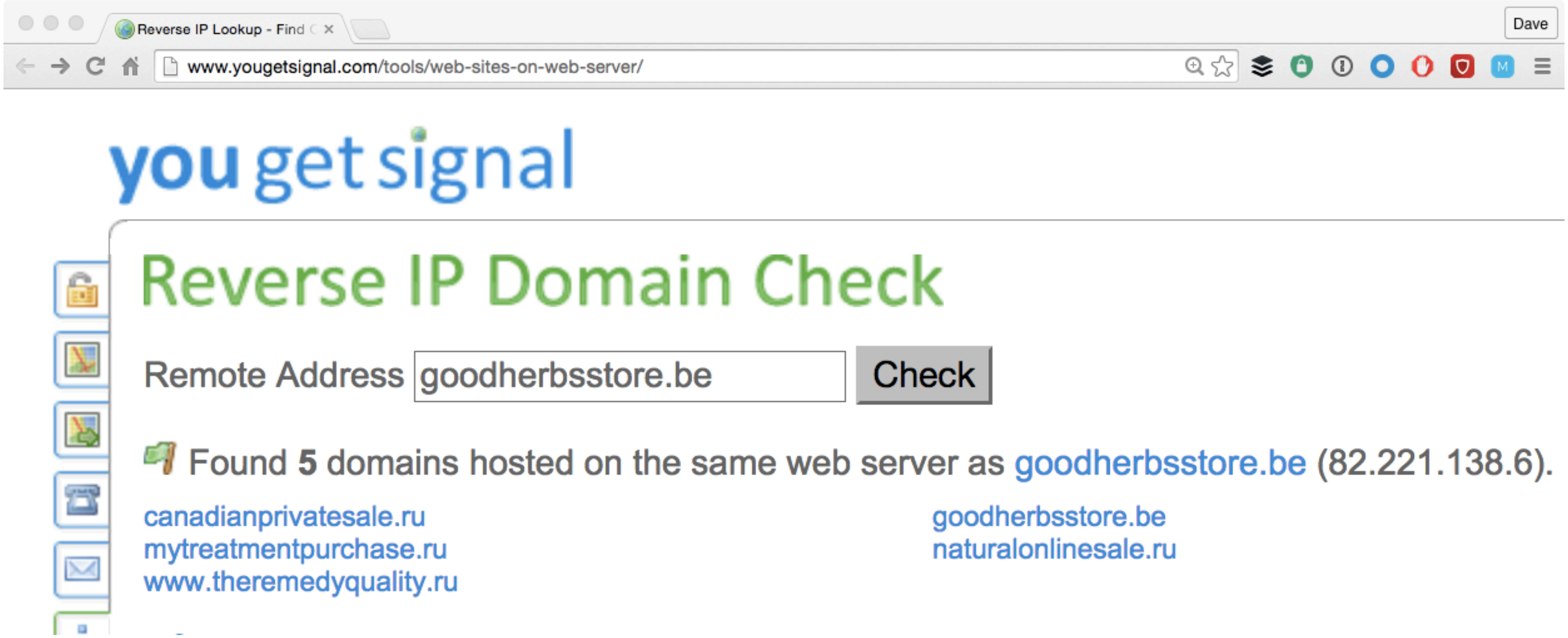
Reported by **b.iana-servers.net** on 3/7/2016 at **7:27:08 PM (UTC 0)**, just for you. (History)

ptr:82.221.138.6

http://mxtoolbox.com/SuperTool.aspx

Reverse IP Domain Check

What other domains are hosted on same web server?



Reverse IP Lookup - Find C ×
Dave
www.yougetsignal.com/tools/web-sites-on-web-server/
you get signal

Reverse IP Domain Check

Remote Address goodherbsstore.be Check

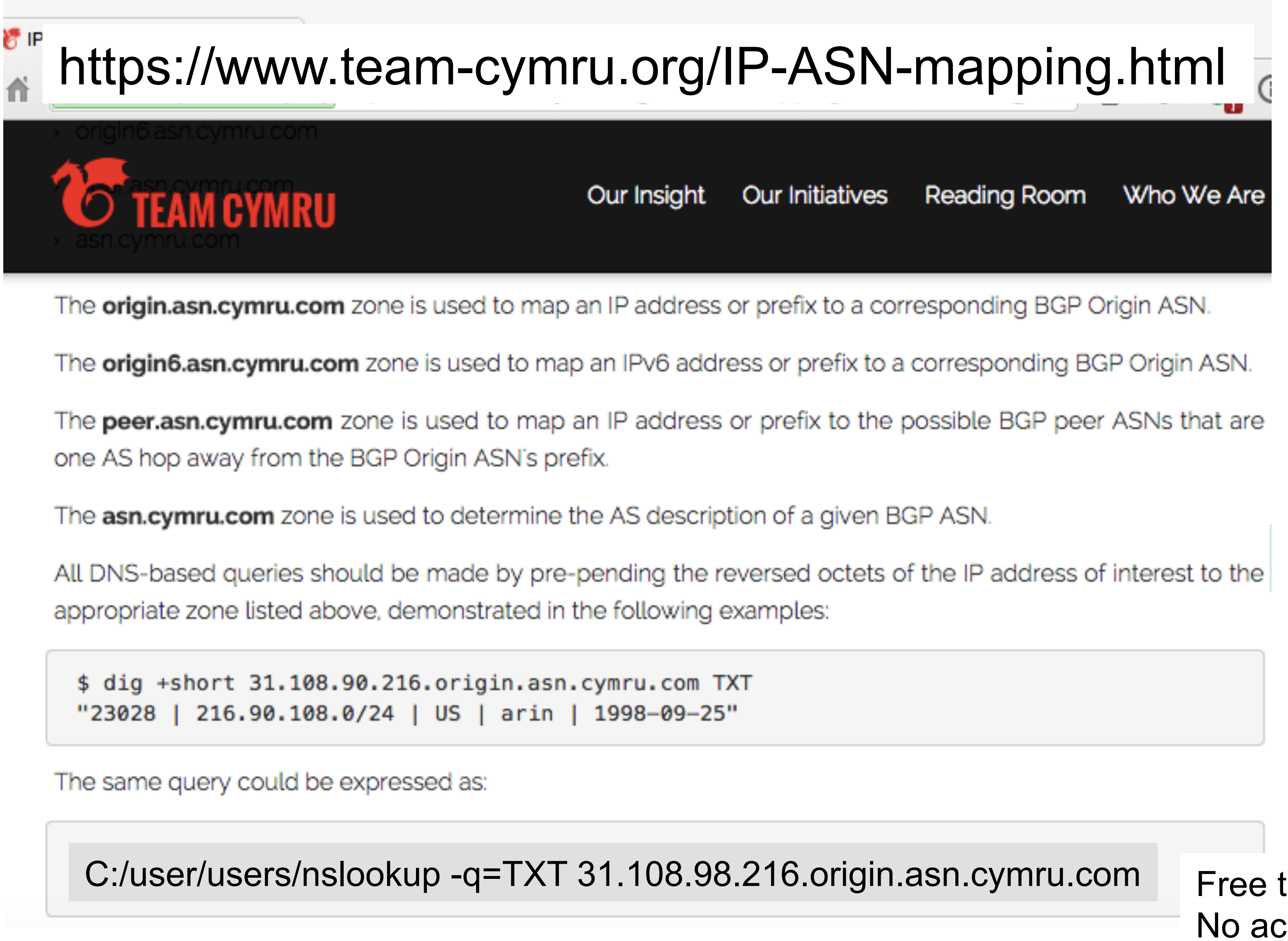
Found **5** domains hosted on the same web server as goodherbsstore.be (82.221.138.6).

canadianprivatesale.ru
mytreatmentpurchase.ru
www.theremedyquality.ru
goodherbsstore.be
naturalonlinesale.ru

http://www.yougetsignal.com

Free to use,
No account required

Mapping IP To BGP Prefixes And ASNs



https://www.team-cymru.org/IP-ASN-mapping.html

The **origin.asn.cymru.com** zone is used to map an IP address or prefix to a corresponding BGP Origin ASN.

The **origin6.asn.cymru.com** zone is used to map an IPv6 address or prefix to a corresponding BGP Origin ASN.

The **peer.asn.cymru.com** zone is used to map an IP address or prefix to the possible BGP peer ASNs that are one AS hop away from the BGP Origin ASN's prefix.

The **asn.cymru.com** zone is used to determine the AS description of a given BGP ASN.

All DNS-based queries should be made by pre-pending the reversed octets of the IP address of interest to the appropriate zone listed above, demonstrated in the following examples:

```
$ dig +short 31.108.90.216.origin.asn.cymru.com TXT
"23028 | 216.90.108.0/24 | US | arin | 1998-09-25"
```

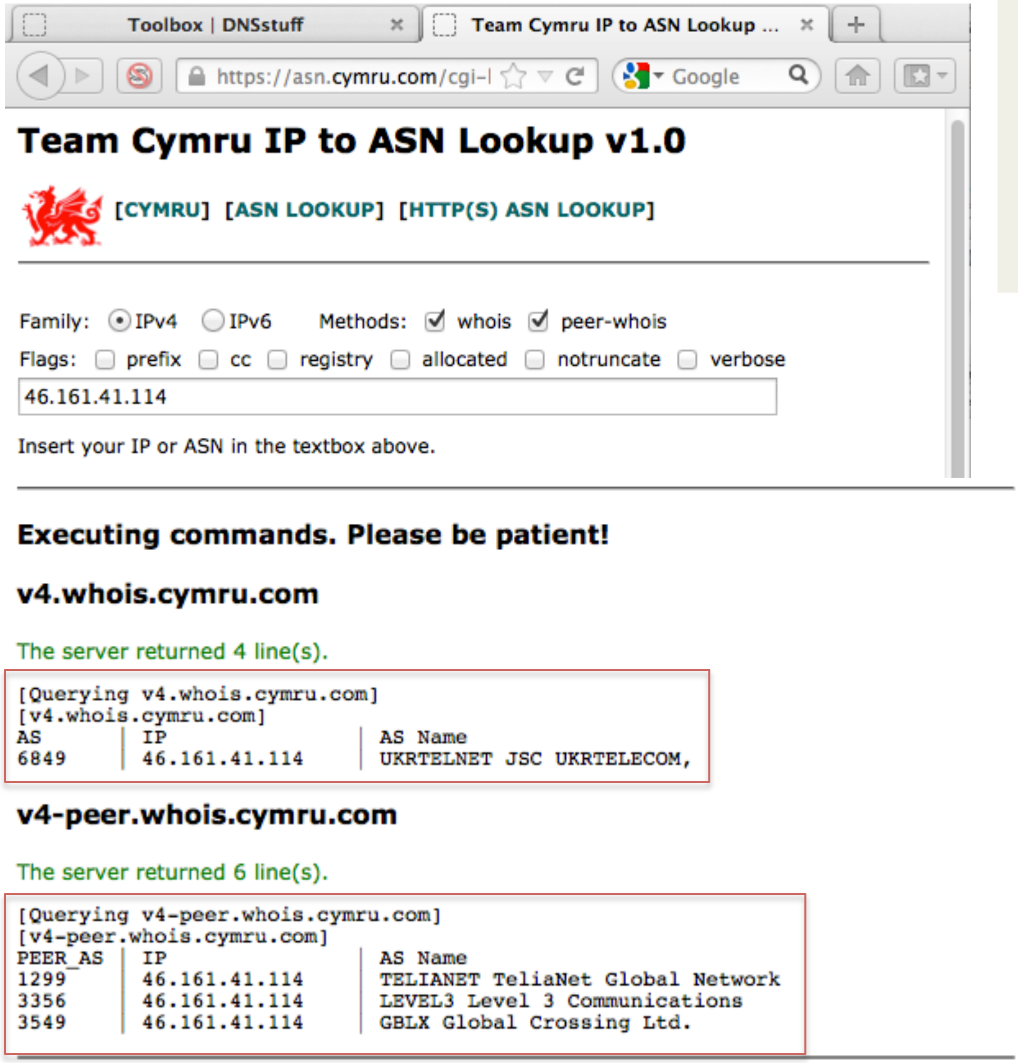
The same query could be expressed as:

```
C:/user/users/nslookup -q=TXT 31.108.98.216.origin.asn.cymru.com
```

Free to use,
No account required

Investigating Autonomous Systems

1) Get ASN that advertises IP network of abuse domain
2) Get ASNs of providers that peer…
3) Get PoCs from IP whois



Team Cymru IP to ASN Lookup v1.0

[CYMRU] [ASN LOOKUP] [HTTP(S) ASN LOOKUP]

Family: ● IPv4 ○ IPv6 Methods: ☑ whois ☑ peer-whois

Flags: □ prefix □ cc □ registry □ allocated □ notruncate □ verbose

46.161.41.114

Insert your IP or ASN in the textbox above.

Executing commands. Please be patient!

v4.whois.cymru.com

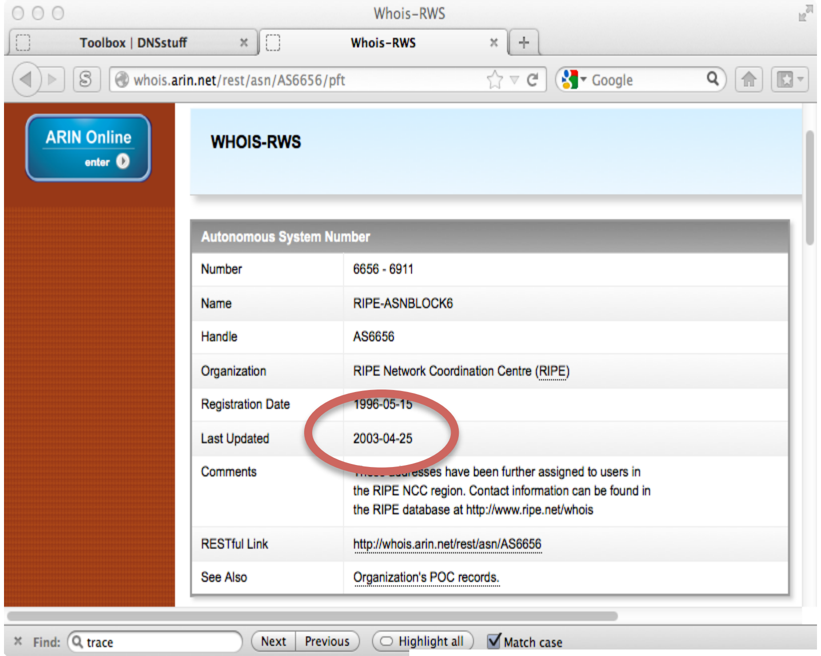
The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
AS      | IP               | AS Name
6849    | 46.161.41.114    | UKRTELNET JSC UKRTELECOM,
```

v4-peer.whois.cymru.com

The server returned 6 line(s).

```
[Querying v4-peer.whois.cymru.com]
[v4-peer.whois.cymru.com]
PEER_AS | IP               | AS Name
1299    | 46.161.41.114    | TELIANET TeliaNet Global Network
3356    | 46.161.41.114    | LEVEL3 Level 3 Communications
3549    | 46.161.41.114    | GBLX Global Crossing Ltd.
```



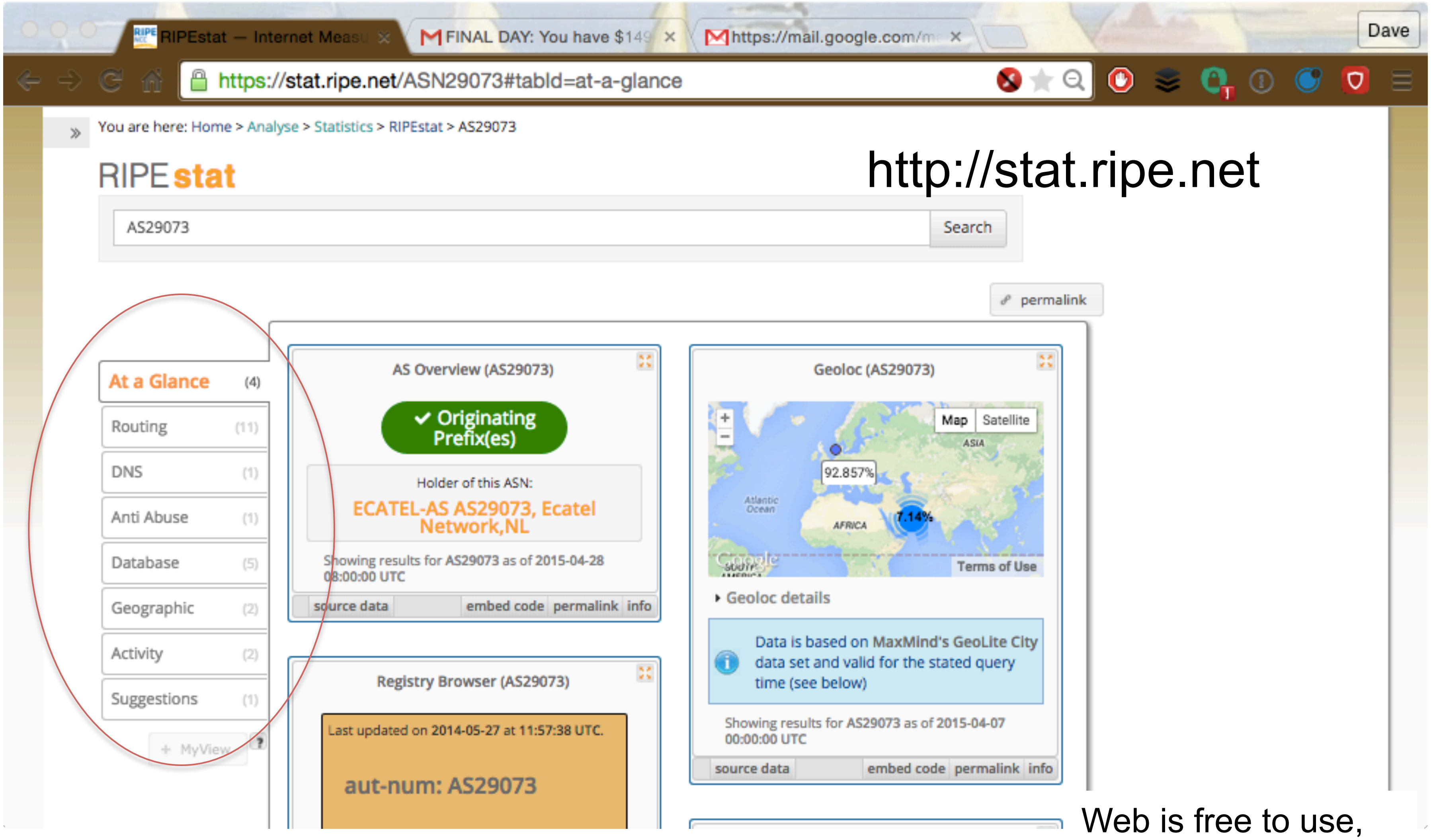
WHOIS-RWS

Autonomous System Number	
Number	6656 - 6911
Name	RIPE-ASNBLOCK6
Handle	AS6656
Organization	RIPE Network Coordination Centre (RIPE)
Registration Date	1996-05-15
Last Updated	2003-04-25
Comments	These addresses have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at http://www.ripe.net/whois
RESTful Link	http://whois.arin.net/rest/asn/AS6656
See Also	Organization's POC records.

Free to use,
No account required

https://asn.cymru.com/

Addressing Intelligence



RIPEstat — Internet Measu ×
FINAL DAY: You have $149 ×
https://mail.google.com/m ×

Dave

https://stat.ripe.net/ASN29073#tabId=at-a-glance

You are here: Home > Analyse > Statistics > RIPEstat > AS29073

RIPE stat

AS29073 Search

permalink

At a Glance	(4)
Routing	(11)
DNS	(1)
Anti Abuse	(1)
Database	(5)
Geographic	(2)
Activity	(2)
Suggestions	(1)

+ MyView ?

AS Overview (AS29073)

✓ Originating Prefix(es)

Holder of this ASN:

ECATEL-AS AS29073, Ecatel Network,NL

Showing results for AS29073 as of 2015-04-28 08:00:00 UTC

source data | embed code | permalink | info

Geoloc (AS29073)

▸ Geoloc details

Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for AS29073 as of 2015-04-07 00:00:00 UTC

source data | embed code | permalink | info

Registry Browser (AS29073)

Last updated on 2014-05-27 at 11:57:38 UTC.

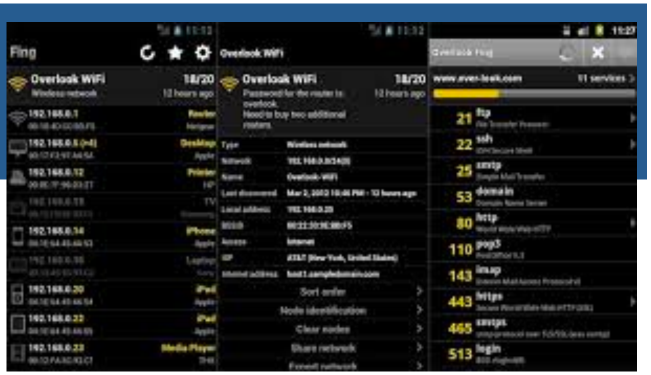
aut-num: AS29073

http://stat.ripe.net

Web is free to use,
API account required

DNS And IP Tools For Mobile Devices (Android, iOS)

Android



Whois and DNS query clients

- DYN Whois
  https://play.google.com/store/apps/details?id=com.dyn.dynwhois.app&hl=en
- DNS Lookup
  https://play.google.com/store/apps/details?id=com.kodholken.dnslookup&hl=en

Tor

- Orfox Tor browser
  https://play.google.com/store/apps/details?id=info.guardianproject.orfox&hl=en

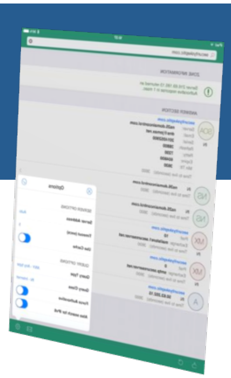
DNS intelligence

- UltraTools Mobile (Domain Health Check)
  https://play.google.com/store/apps/details?id=com.ultra.mobile&hl=en

Pen testing

- FING
  https://play.google.com/store/search?q=fing&c=apps&hl=en

iOS



Whois and DNS query clients

- Deep Whois
  https://itunes.apple.com/us/app/deep-whois/id328895000?mt=8
- NS Lookup Plus
  https://itunes.apple.com/us/app/nslookup/id423175511?mt=8i

Tor

- Red OnionTor browser
  https://itunes.apple.com/us/app/red-onion-tor-powered-web/id829739720?mt=8

RBL intelligence

- RBL Status
  https://itunes.apple.com/us/app/rbl-status/id328354770?mt=8

Pen testing and DNS intelligence

- SCANY
  https://itunes.apple.com/us/app/scany-network-scanner/id328077901?mt=8

Reputation

Tools for Investigating Reputation

Reputation services, Block lists, Malware Analysis

Spamhaus

SURBL, URIBL

ZeusTracker

Team Cymru

Alexa

Clean MX

CBL

Stopbadware

Barracuda Central

Fspamlist

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

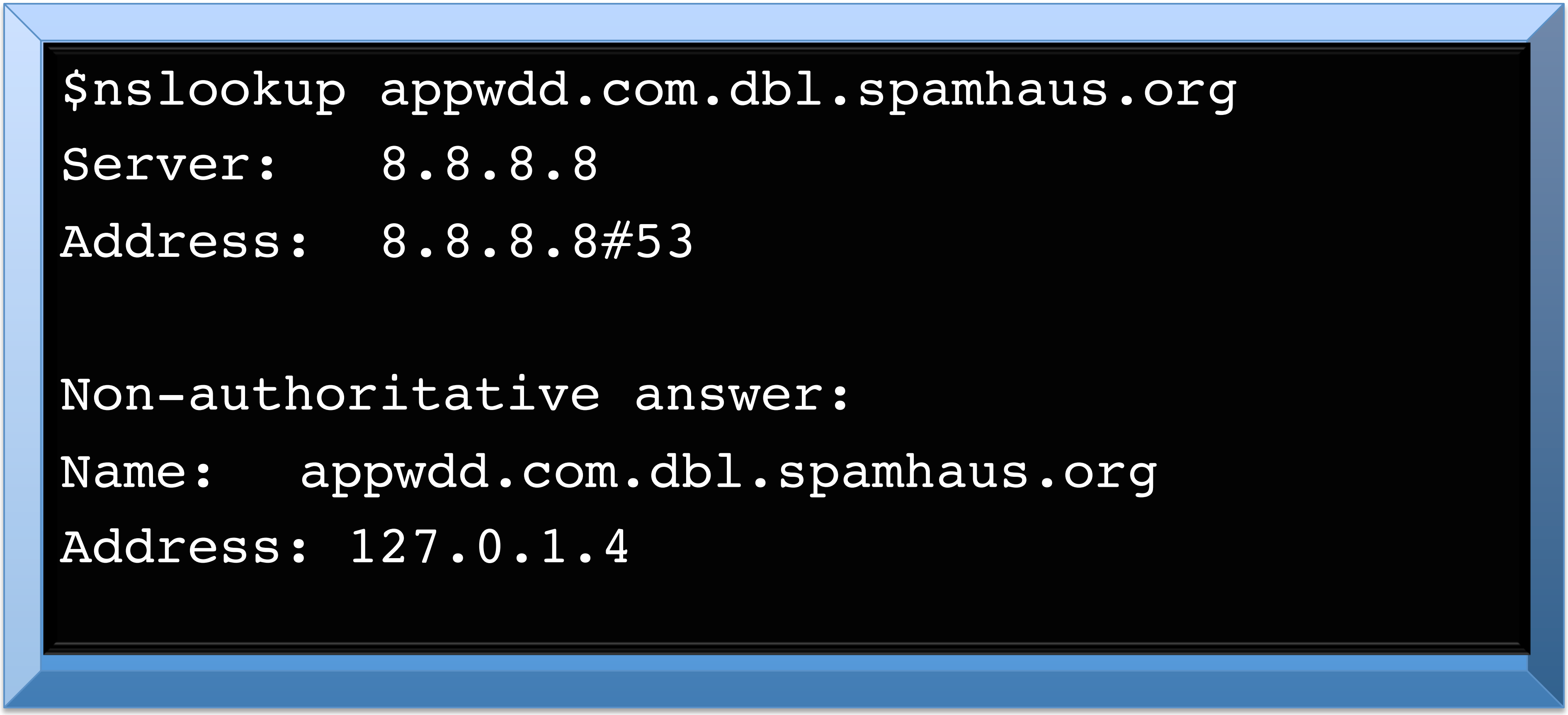
Checking Blocklists Using The DNS

Reverse the octets of the IP and query DNS:

```
$nslookup save1.allonline-newpointshere.us

Non-authoritative answer:
Name:   save1.allonline-newpointshere.us
Address: 162.255.119.254



$nslookup 254.119.255.162.zen.spamhaus.org
$nslookup 254.119.255.162.b.barracudacentral.org
$nslookup 254.119.255.162.cbl.abuseat.org
```

Checking Blocklists Using the DNS

Prepend the domain to the blocklist service:

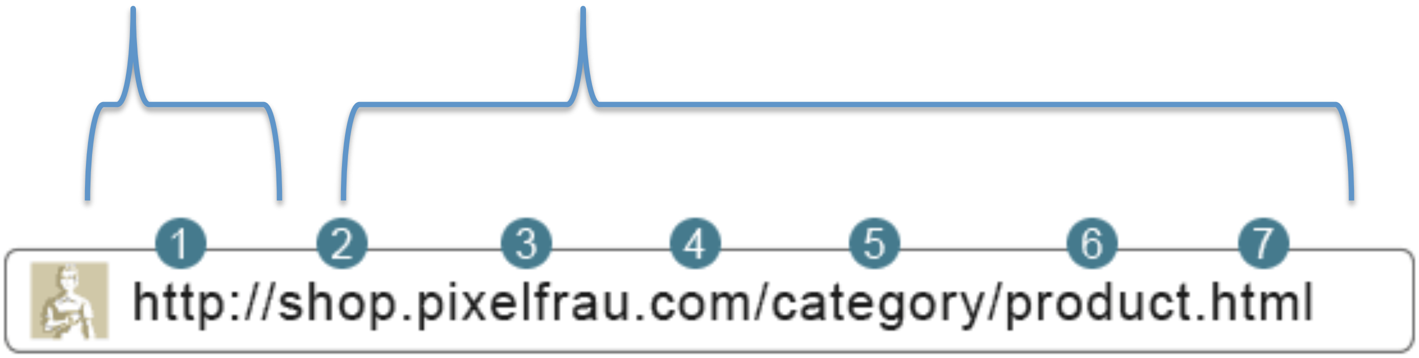


```
$nslookup appwdd.com.dbl.spamhaus.org
Server:    8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
Name:   appwdd.com.dbl.spamhaus.org
Address: 127.0.1.4
```

Tools for Investigating URLs (Hyperlinks)

URL (URI) Composition

```
<scheme name> : <hierarchical part> [ ? <query> ] [ # <fragment> ]
```

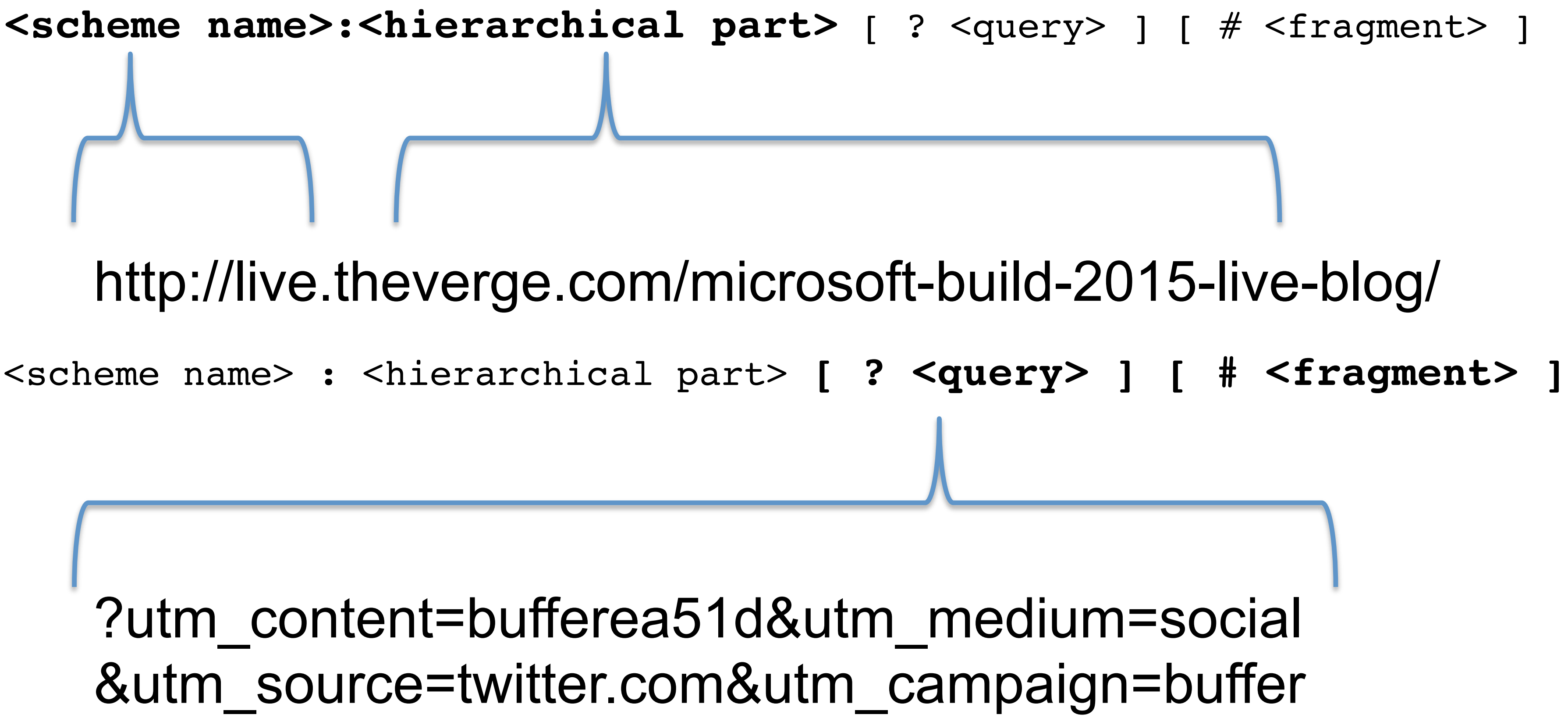


1. URI Scheme or Protocol
2. Subdomain
3. Domain name
4. Top-Level Domain (TLD)
5. Folder / Path
6. Page
7. File Extension

Can also be an IP address

https://www.pixelfrau.com/anatomy-of-a-url/

URL (URI) Composition



<scheme name>:<hierarchical part> [? <query>] [# <fragment>]

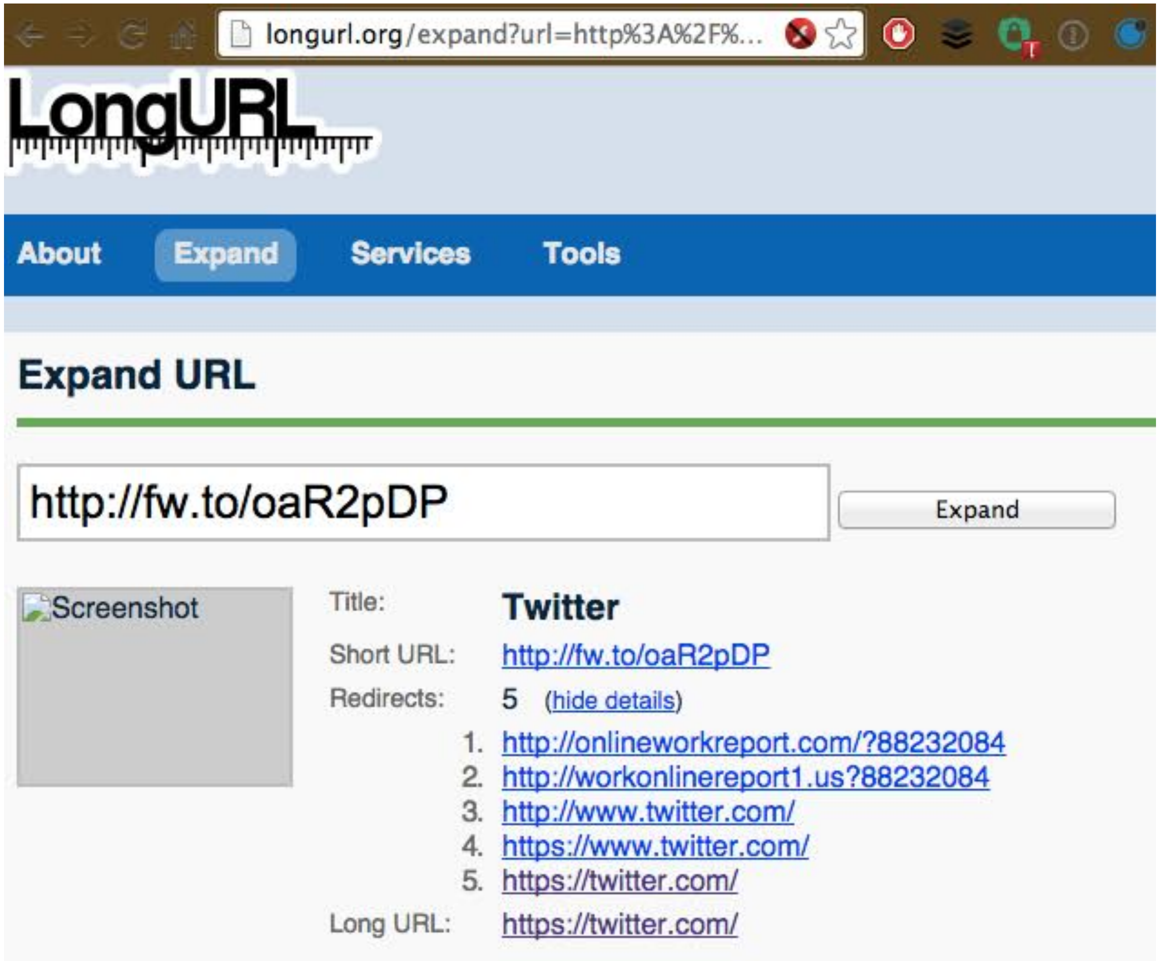
http://live.theverge.com/microsoft-build-2015-live-blog/

<scheme name> : <hierarchical part> **[? <query>] [# <fragment>]**

?utm_content=bufferea51d&utm_medium=social
&utm_source=twitter.com&utm_campaign=buffer

How To Expand Shortened URLs

- Twitter or text spam or phishing use shortened URLs
- Visit http://longurl.org to expand before you
  - Recognizes 300+ shorteners
  - Expands recursively shortened URLs



Expand URL

http://fw.to/oaR2pDP

Title: Twitter

Short URL: http://fw.to/oaR2pDP

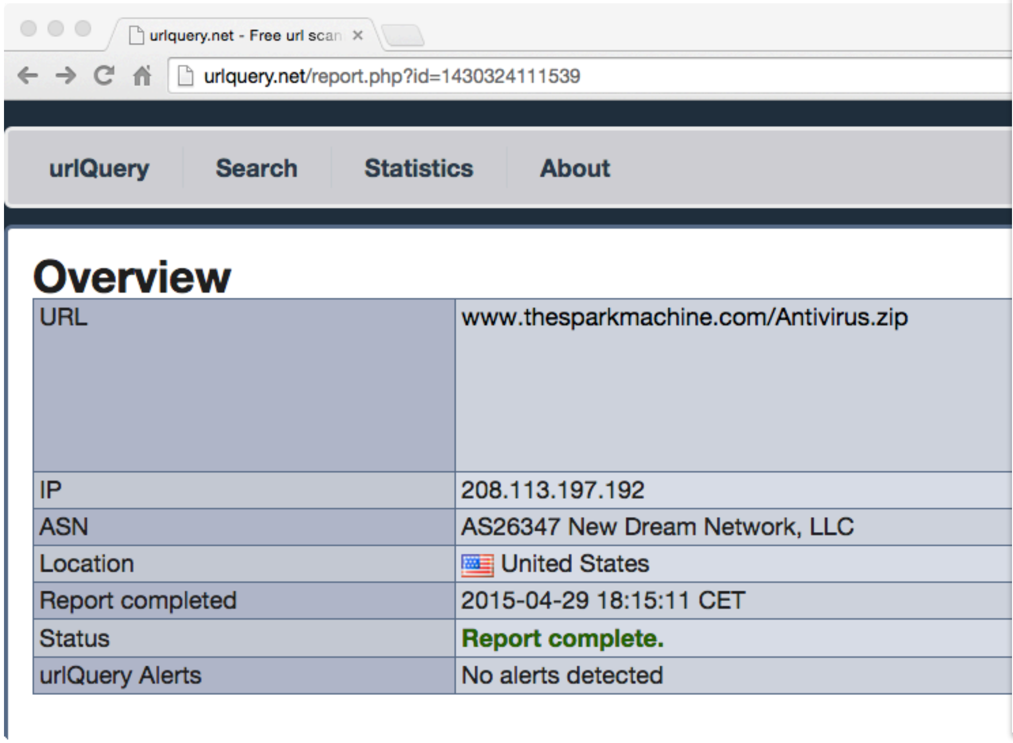
Redirects: 5 (hide details)

1. http://onlineworkreport.com/?88232084
2. http://workonlinereport1.us?88232084
3. http://www.twitter.com/
4. https://www.twitter.com/
5. https://twitter.com/

Long URL: https://twitter.com/

Free to use,
No account required

Use Case: Using URLQuery.net


urlquery.net - Free url scan
urlquery.net/report.php?id=1430324111539
urlQuery
Search
Statistics
About

Overview

URL	www.thesparkmachine.com/Antivirus.zip
IP	208.113.197.192
ASN	AS26347 New Dream Network, LLC
Location	🇺🇸 United States
Report completed	2015-04-29 18:15:11 CET
Status	**Report complete.**
urlQuery Alerts	No alerts detected

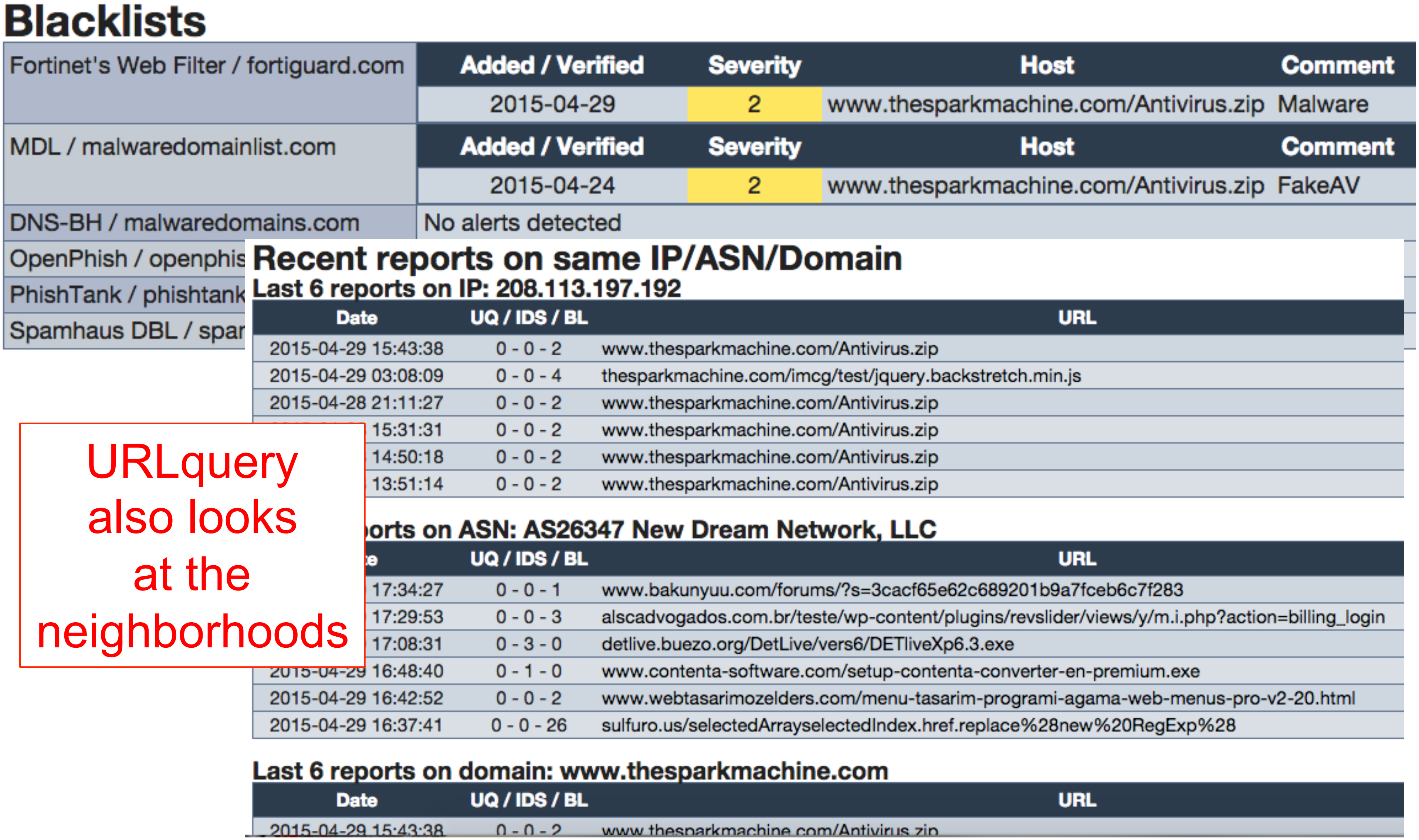
Use http://urlquery.net for

- Malware scans, blacklist notifications
- Recent reports on same IP/ ASN/domain
- Executes scripts
- Enumerates HTTP transactions

Is http://www.thesparkmachine.com/Antivirus.zip a malicious URL?

Free to use,
No account required

URLQuery Results



Blacklists

	Added / Verified	Severity	Host	Comment
Fortinet's Web Filter / fortiguard.com	2015-04-29	2	www.thesparkmachine.com/Antivirus.zip	Malware
MDL / malwaredomainlist.com	2015-04-24	2	www.thesparkmachine.com/Antivirus.zip	FakeAV
DNS-BH / malwaredomains.com	No alerts detected			
OpenPhish / openphis				
PhishTank / phishtank				
Spamhaus DBL / spar				

Recent reports on same IP/ASN/Domain

Last 6 reports on IP: 208.113.197.192

Date	UQ / IDS / BL	URL
2015-04-29 15:43:38	0 - 0 - 2	www.thesparkmachine.com/Antivirus.zip
2015-04-29 03:08:09	0 - 0 - 4	thesparkmachine.com/imcg/test/jquery.backstretch.min.js
2015-04-28 21:11:27	0 - 0 - 2	www.thesparkmachine.com/Antivirus.zip
15:31:31	0 - 0 - 2	www.thesparkmachine.com/Antivirus.zip
14:50:18	0 - 0 - 2	www.thesparkmachine.com/Antivirus.zip
13:51:14	0 - 0 - 2	www.thesparkmachine.com/Antivirus.zip

orts on ASN: AS26347 New Dream Network, LLC

e	UQ / IDS / BL	URL
17:34:27	0 - 0 - 1	www.bakunyuu.com/forums/?s=3cacf65e62c689201b9a7fceb6c7f283
17:29:53	0 - 0 - 3	alscadvogados.com.br/teste/wp-content/plugins/revslider/views/y/m.i.php?action=billing_login
17:08:31	0 - 3 - 0	detlive.buezo.org/DetLive/vers6/DETliveXp6.3.exe
2015-04-29 16:48:40	0 - 1 - 0	www.contenta-software.com/setup-contenta-converter-en-premium.exe
2015-04-29 16:42:52	0 - 0 - 2	www.webtasarimozelders.com/menu-tasarim-programi-agama-web-menus-pro-v2-20.html
2015-04-29 16:37:41	0 - 0 - 26	sulfuro.us/selectedArrayselectedIndex.href.replace%28new%20RegExp%28

Last 6 reports on domain: www.thesparkmachine.com

Date	UQ / IDS / BL	URL
2015-04-29 15:43:38	0 - 0 - 2	www.thesparkmachine.com/Antivirus.zip

URLquery also looks at the neighborhoods

Checking Domains Or URLs for Malware

Confirm that you've found a malware sample

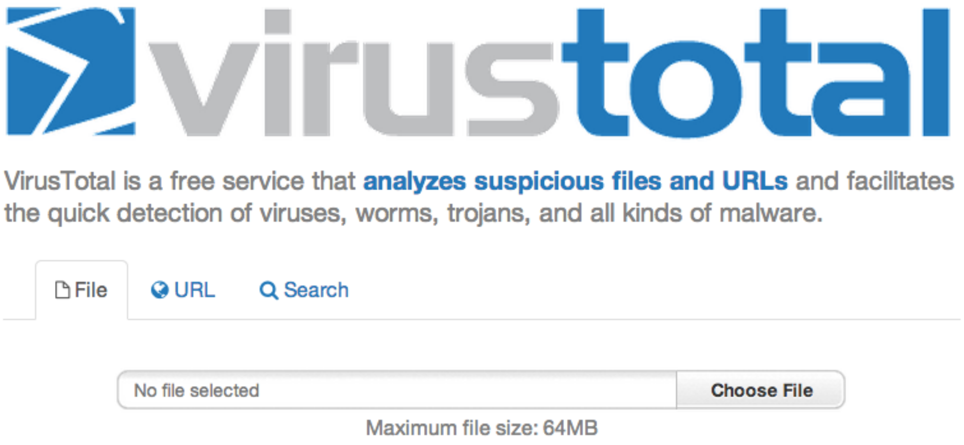
- Majority of malware are derivations of known malware
- These can typically be confirmed/analyzed via *cloud-based malware analysis services*
  - Anubis : http://anubis.iseclab.org
  - Comodo : http://camas.comodo.com
  - Malwr : https://malwr.com/submission
  - Vicheck : https://www.vicheck.ca
  - Threat Expert : http://www.threatexpert.com/submit.aspx
  - Threat Track : http://www.threattracksecurity.com

See also *Automated Malware Analysis in the Cloud*
http://resources.infosecinstitute.com/overview-automated-malware-analysis-cloud/

VirusTotal

Useful first stop for malware check

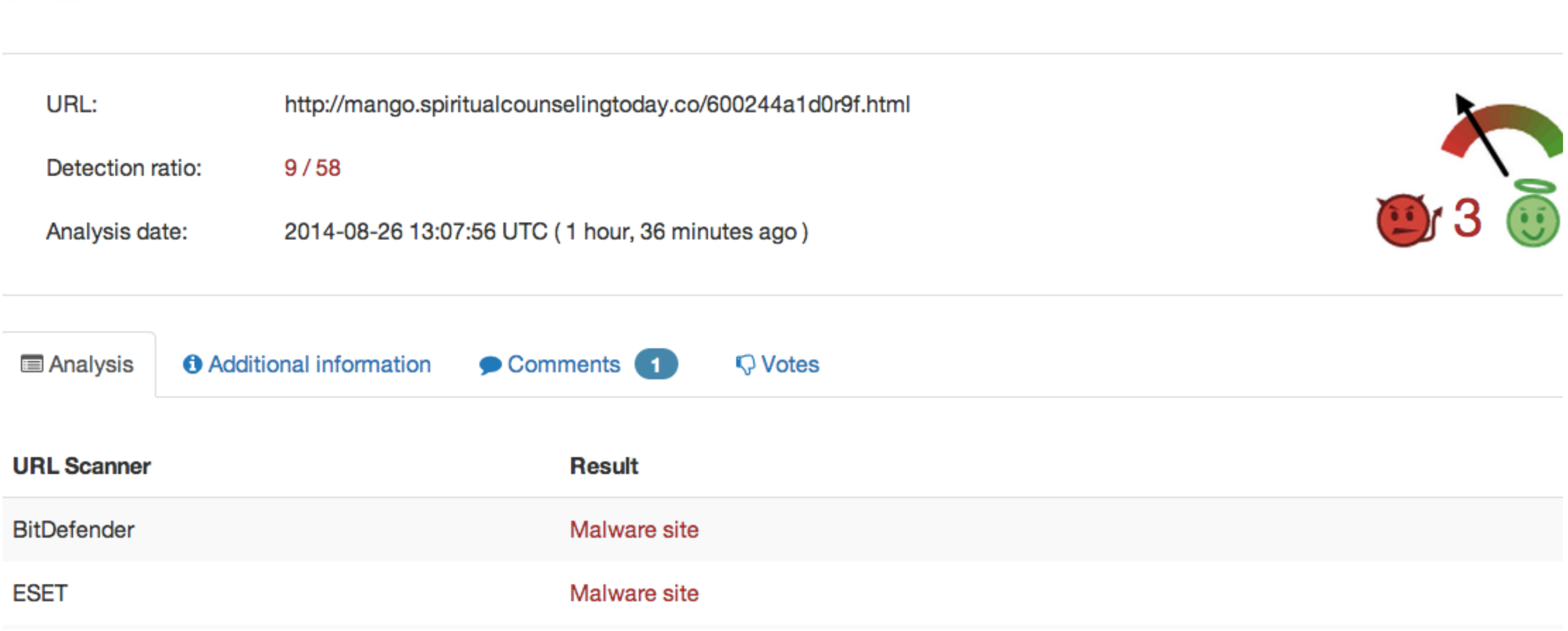
- Upload file for analysis
- Submit URL for analysis
- Search database using a hash, URL, domain or IP



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 64MB

virustotal



URL: http://mango.spiritualcounselingtoday.co/600244a1d0r9f.html

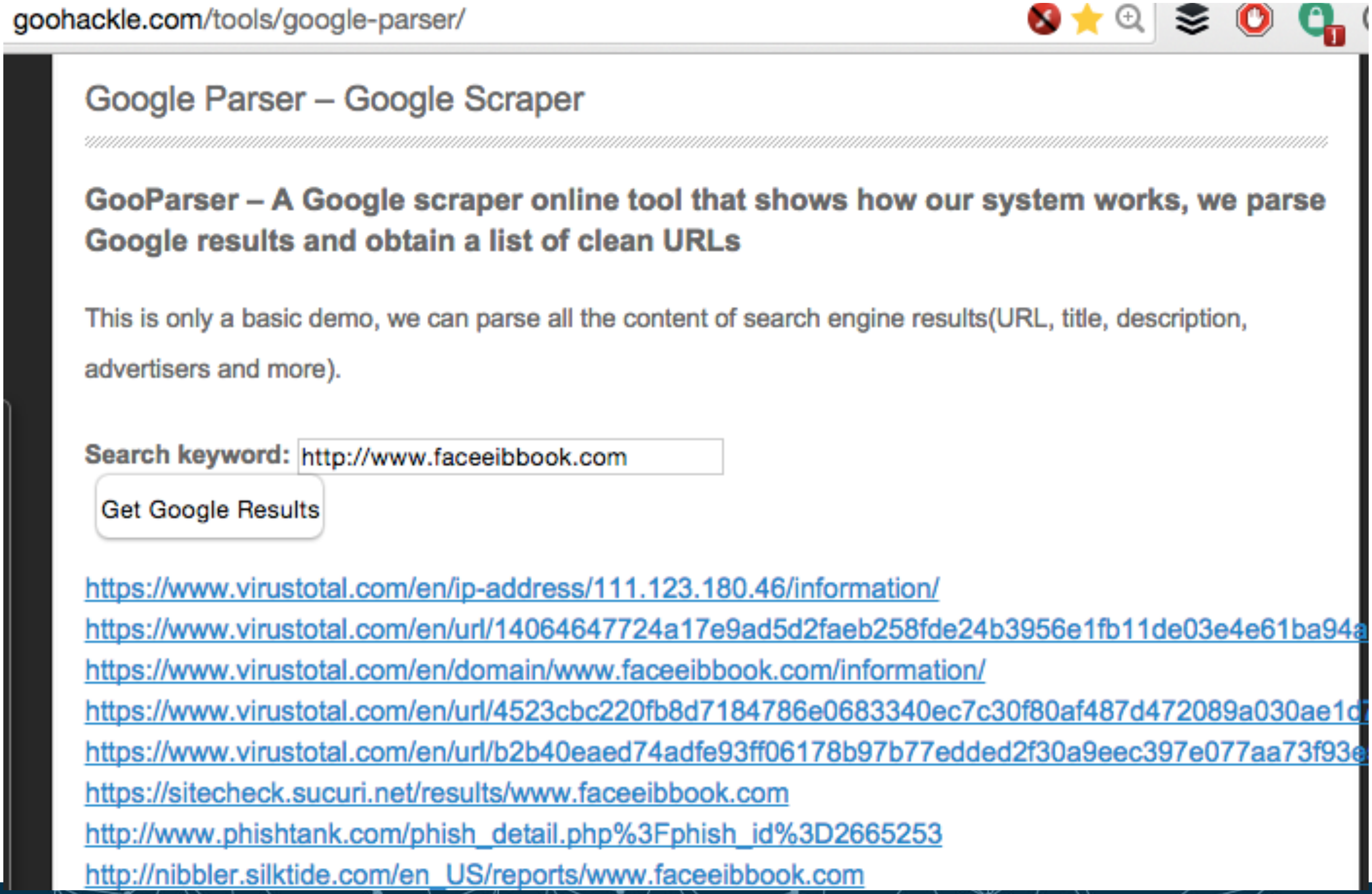
Detection ratio: 9 / 58

Analysis date: 2014-08-26 13:07:56 UTC (1 hour, 36 minutes ago)

URL Scanner	Result
BitDefender	Malware site
ESET	Malware site

Goohackle.com: A Google Parser/Scraper

Quickly check whether someone else is investigating this URL



goohackle.com/tools/google-parser/

Google Parser – Google Scraper

GooParser – A Google scraper online tool that shows how our system works, we parse Google results and obtain a list of clean URLs

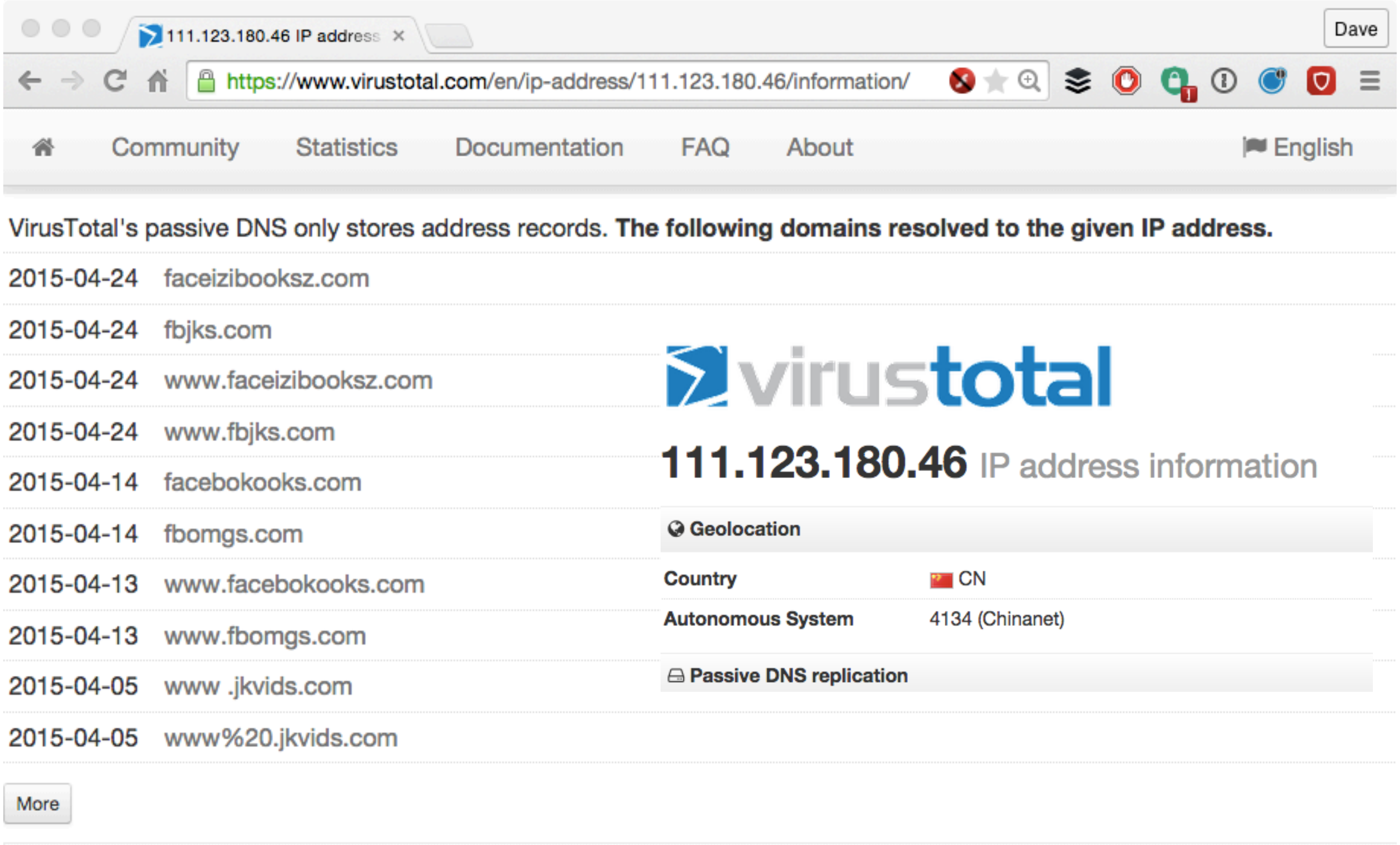
This is only a basic demo, we can parse all the content of search engine results(URL, title, description, advertisers and more).

Search keyword: http://www.faceeibbook.com

https://www.virustotal.com/en/ip-address/111.123.180.46/information/
https://www.virustotal.com/en/url/14064647724a17e9ad5d2faeb258fde24b3956e1fb11de03e4e61ba94a
https://www.virustotal.com/en/domain/www.faceeibbook.com/information/
https://www.virustotal.com/en/url/4523cbc220fb8d7184786e0683340ec7c30f80af487d472089a030ae1d
https://www.virustotal.com/en/url/b2b40eaed74adfe93ff06178b97b77edded2f30a9eec397e077aa73f93e
https://sitecheck.sucuri.net/results/www.faceeibbook.com
http://www.phishtank.com/phish_detail.php%3Fphish_id%3D2665253
http://nibbler.silktide.com/en_US/reports/www.faceeibbook.com

VirusTotal's IP Passive DNS

nslookup of www.faceeibbook.com returns 111.123.180.46



111.123.180.46 IP address
Dave
https://www.virustotal.com/en/ip-address/111.123.180.46/information/
Community
Statistics
Documentation
FAQ
About
English
virustotal
More

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2015-04-24	faceizibooksz.com
2015-04-24	fbjks.com
2015-04-24	www.faceizibooksz.com
2015-04-24	www.fbjks.com
2015-04-14	facebokooks.com
2015-04-14	fbomgs.com
2015-04-13	www.facebokooks.com
2015-04-13	www.fbomgs.com
2015-04-05	www .jkvids.com
2015-04-05	www%20.jkvids.com

111.123.180.46 IP address information

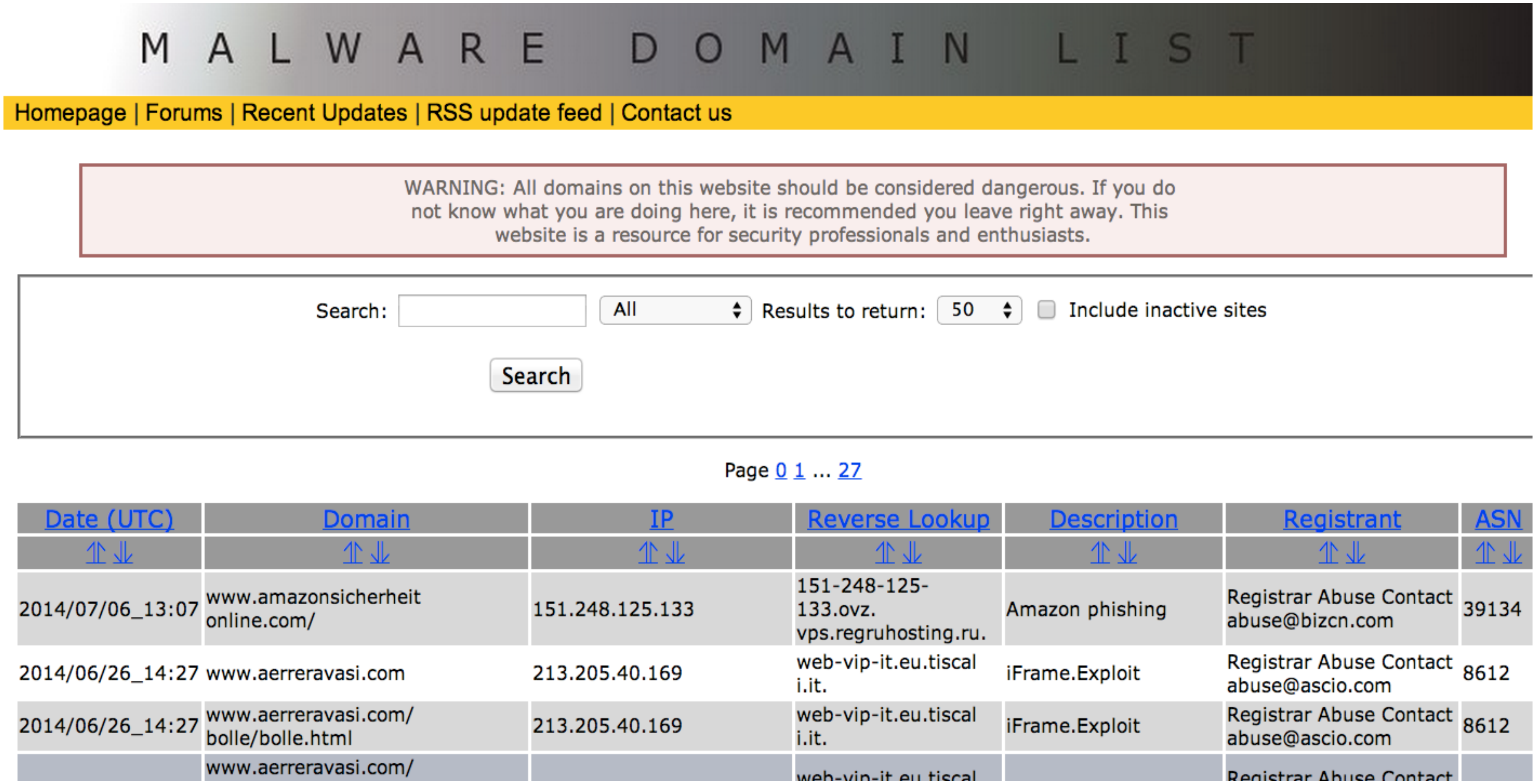
Geolocation

Country	CN
Autonomous System	4134 (Chinanet)

Passive DNS replication

Malware Domain List

Check whether someone else has reported the domain



M A L W A R E D O M A I N L I S T

Homepage | Forums | Recent Updates | RSS update feed | Contact us

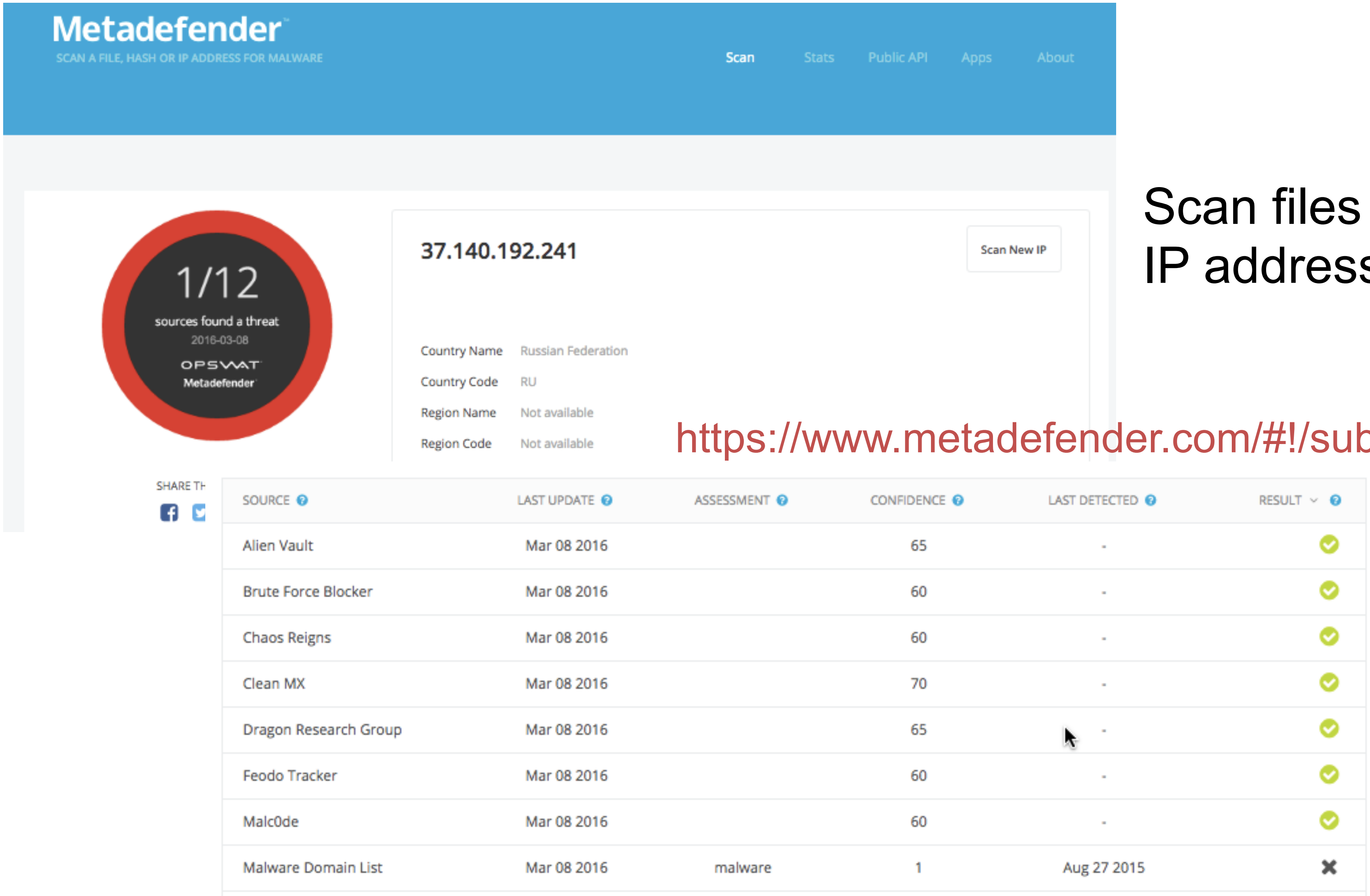
WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Page 0 1 ... 27

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
⇑ ⇓	⇑ ⇓	⇑ ⇓	⇑ ⇓	⇑ ⇓	⇑ ⇓	⇑ ⇓
2014/07/06_13:07	www.amazonsicherheitonline.com/	151.248.125.133	151-248-125-133.ovz.vps.regruhosting.ru.	Amazon phishing	Registrar Abuse Contact abuse@bizcn.com	39134
2014/06/26_14:27	www.aerreravasi.com	213.205.40.169	web-vip-it.eu.tiscali.it.	iFrame.Exploit	Registrar Abuse Contact abuse@ascio.com	8612
2014/06/26_14:27	www.aerreravasi.com/bolle/bolle.html	213.205.40.169	web-vip-it.eu.tiscali.it.	iFrame.Exploit	Registrar Abuse Contact abuse@ascio.com	8612
	www.aerreravasi.com/		web-vip-it.eu.tiscal		Registrar Abuse Contact	

http://malwaredomainlist.com

Metadefender



37.140.192.241

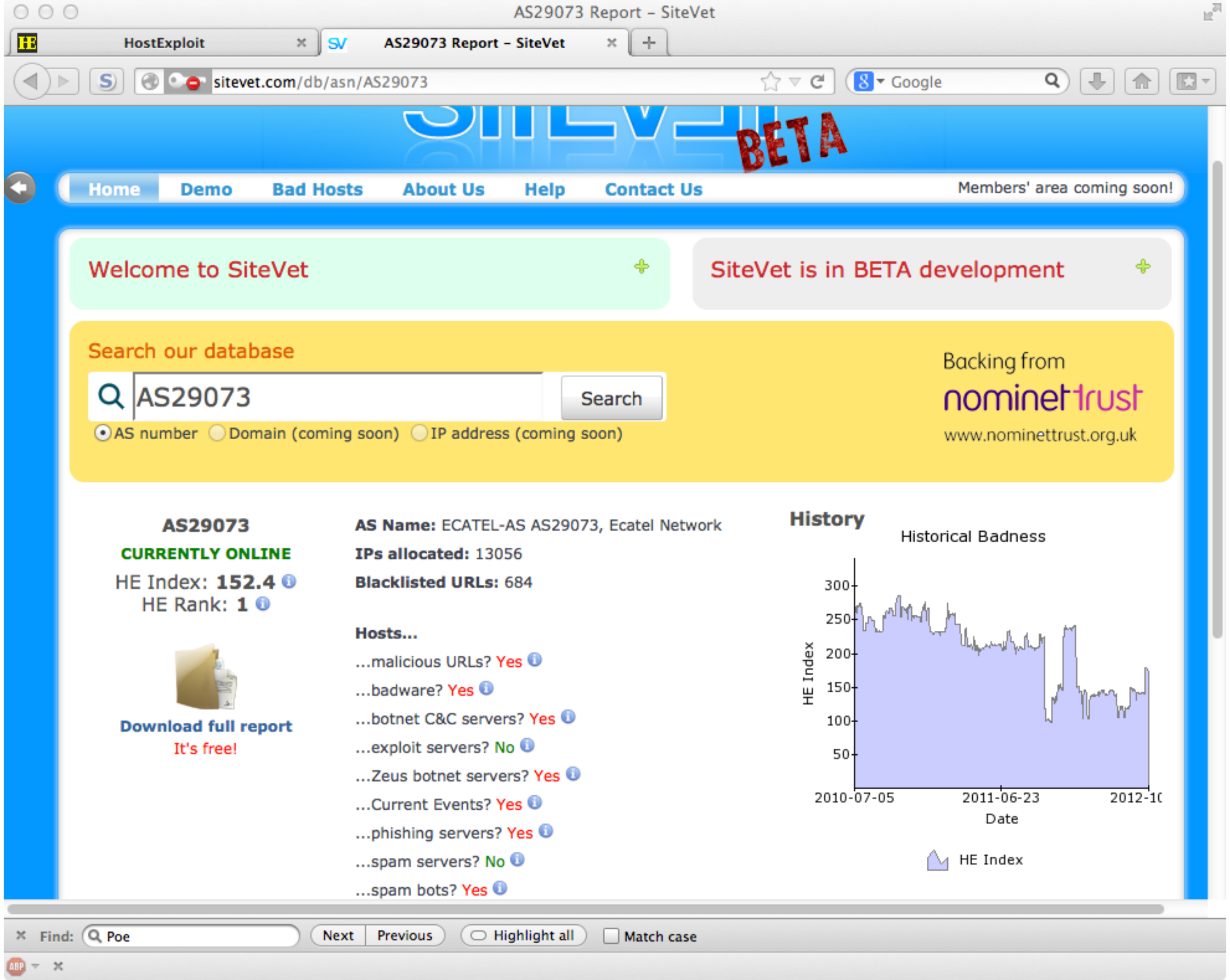
Country Name	Russian Federation
Country Code	RU
Region Name	Not available
Region Code	Not available

SOURCE	LAST UPDATE	ASSESSMENT	CONFIDENCE	LAST DETECTED	RESULT
Alien Vault	Mar 08 2016		65	-	✓
Brute Force Blocker	Mar 08 2016		60	-	✓
Chaos Reigns	Mar 08 2016		60	-	✓
Clean MX	Mar 08 2016		70	-	✓
Dragon Research Group	Mar 08 2016		65	-	✓
Feodo Tracker	Mar 08 2016		60	-	✓
Malc0de	Mar 08 2016		60	-	✓
Malware Domain List	Mar 08 2016	malware	1	Aug 27 2015	✗

Scan files or IP addresses

https://www.metadefender.com/#!/submit-ip

Checking ASN Reputation



AS29073 Report – SiteVet

HostExploit | AS29073 Report – SiteVet

sitevet.com/db/asn/AS29073

Home | Demo | Bad Hosts | About Us | Help | Contact Us

Members' area coming soon!

Welcome to SiteVet

SiteVet is in BETA development

Search our database

AS29073 | Search

● AS number ○ Domain (coming soon) ○ IP address (coming soon)

Backing from nominettrust www.nominettrust.org.uk

AS29073

CURRENTLY ONLINE

HE Index: **152.4**

HE Rank: **1**

Download full report

It's free!

AS Name: ECATEL-AS AS29073, Ecatel Network

IPs allocated: 13056

Blacklisted URLs: 684

Hosts...

...malicious URLs? Yes

...badware? Yes

...botnet C&C servers? Yes

...exploit servers? No

...Zeus botnet servers? Yes

...Current Events? Yes

...phishing servers? Yes

...spam servers? No

...spam bots? Yes

History

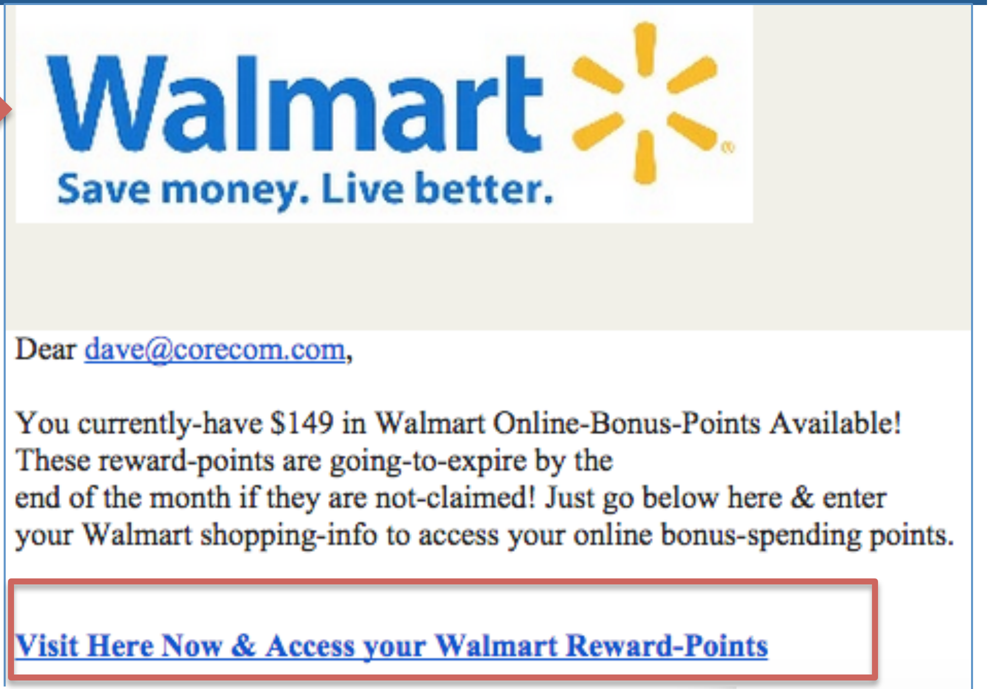
Find: Poe | Next | Previous | Highlight all | □ Match case

"A wretched nest of scum and villainy"

http://sitevet.com

Use Case: Phishing a Brand

1) Begin with a spam email



Walmart

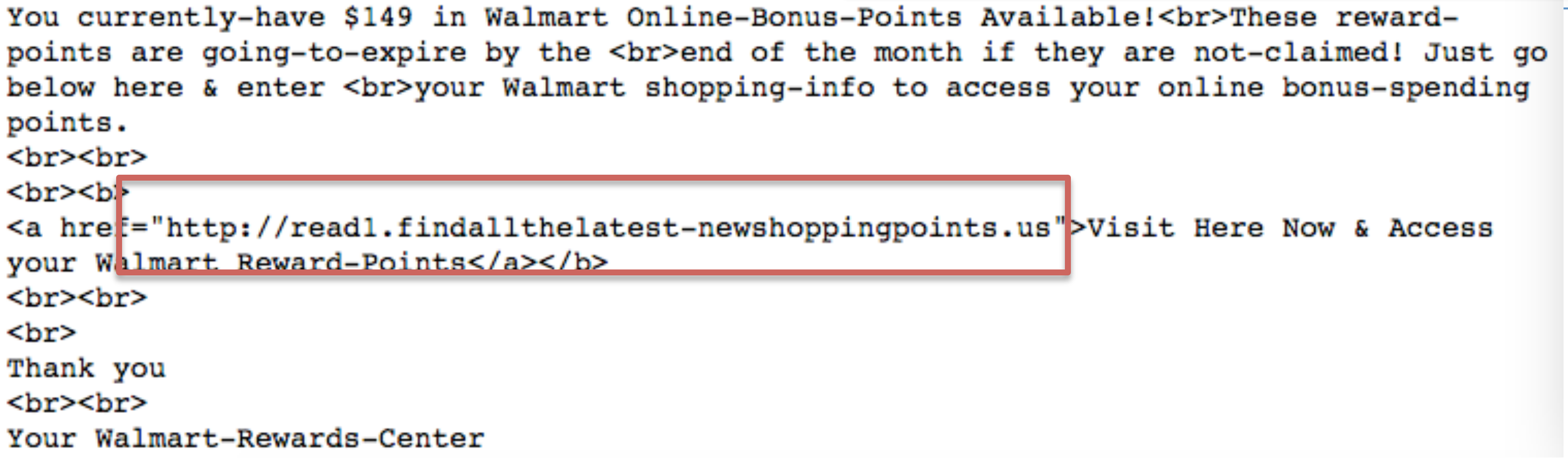
Save money. Live better.

Dear dave@corecom.com,

You currently-have $149 in Walmart Online-Bonus-Points Available!
These reward-points are going-to-expire by the
end of the month if they are not-claimed! Just go below here & enter
your Walmart shopping-info to access your online bonus-spending points.

Visit Here Now & Access your Walmart Reward-Points

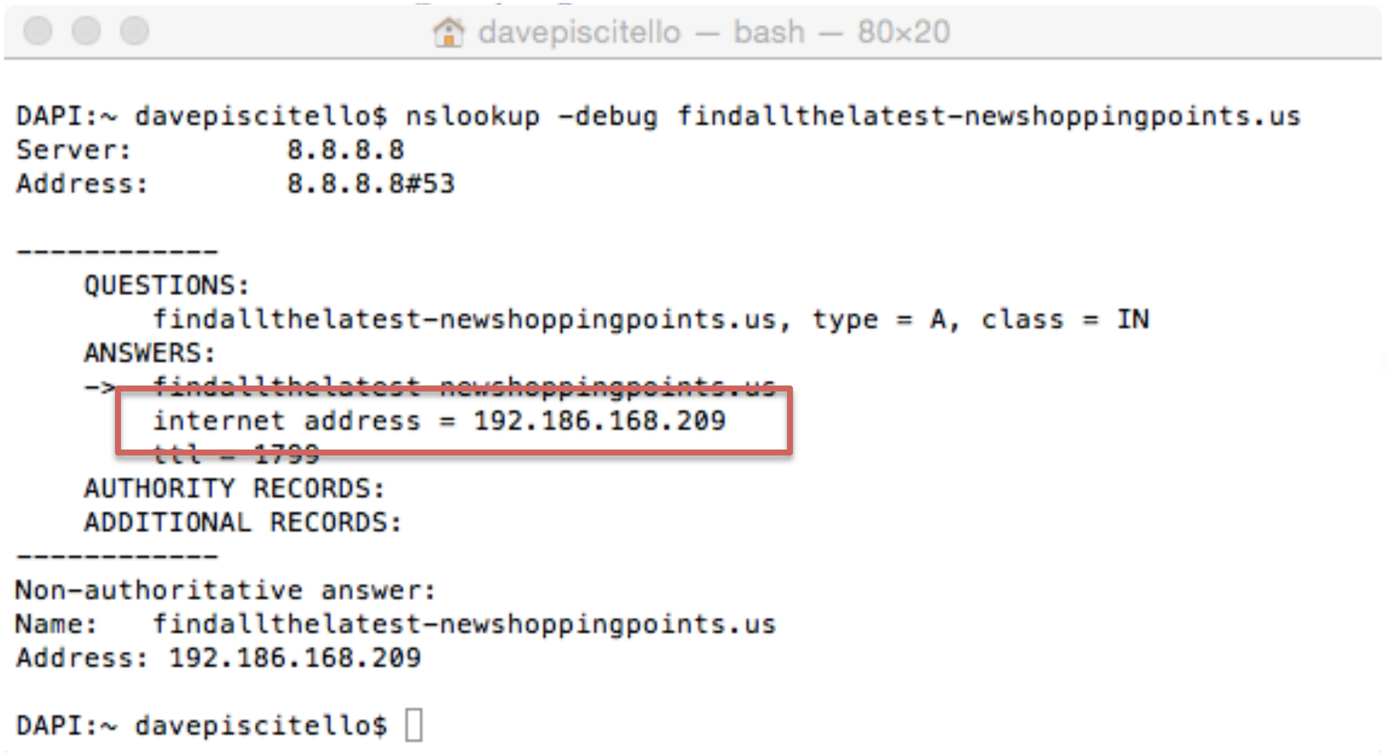
2) Grab the URL from the raw source of the html message body



```
You currently-have $149 in Walmart Online-Bonus-Points Available!<br>These reward-
points are going-to-expire by the <br>end of the month if they are not-claimed! Just go
below here & enter <br>your Walmart shopping-info to access your online bonus-spending
points.
<br><br>
<br><b>
<a href="http://read1.findallthelatest-newshoppingpoints.us">Visit Here Now & Access
your Walmart Reward-Points</a></b>
<br><br>
<br>
Thank you
<br><br>
Your Walmart-Rewards-Center
```

Use Case: Phishing a Brand

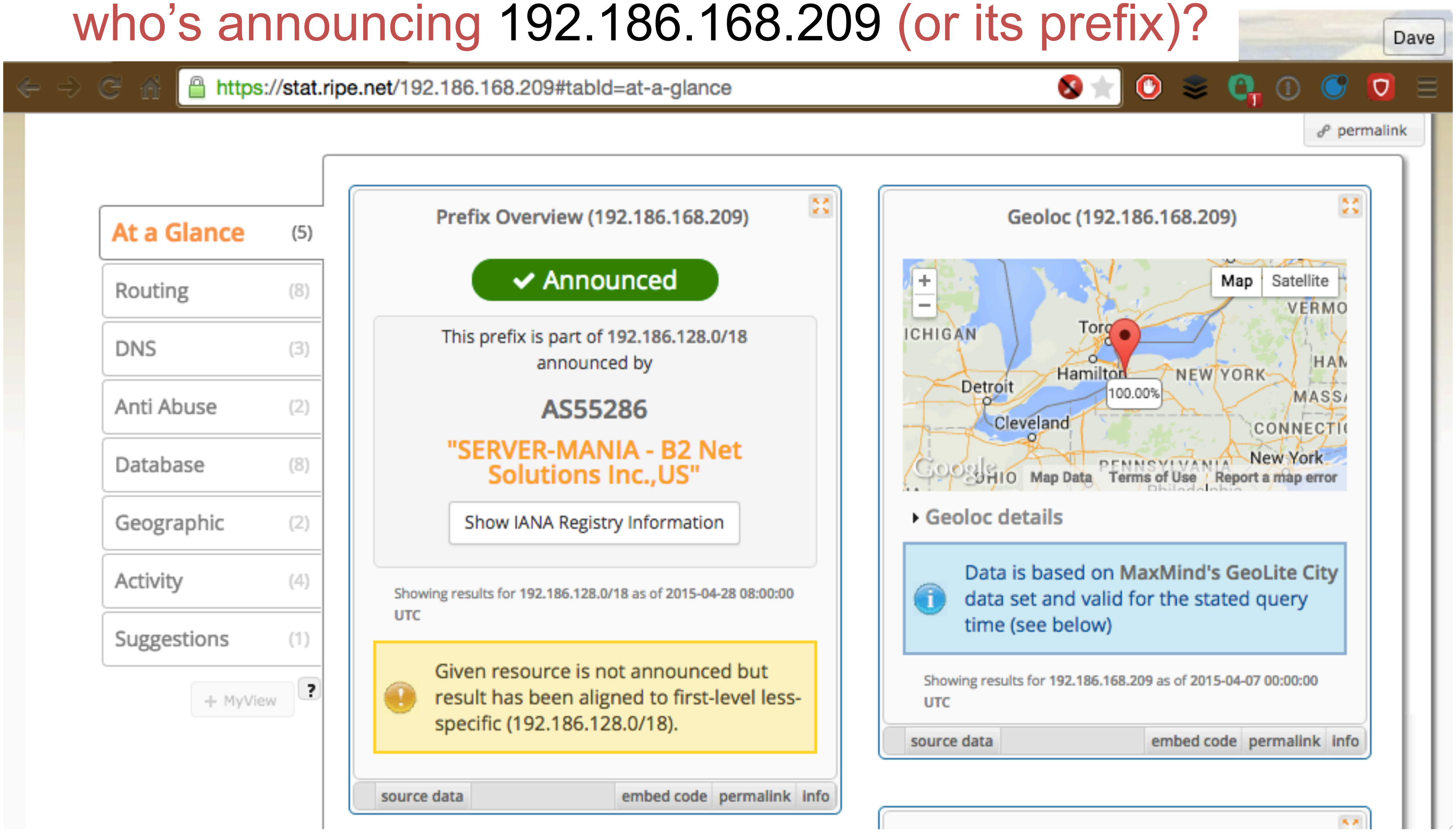
3) Strip the domain name from the URL and look up the address record



```
DAPI:~ davepiscitello$ nslookup -debug findallthelatest-newshoppingpoints.us
Server:         8.8.8.8
Address:        8.8.8.8#53

------------
    QUESTIONS:
        findallthelatest-newshoppingpoints.us, type = A, class = IN
    ANSWERS:
    ->  findallthelatest-newshoppingpoints.us
        internet address = 192.186.168.209
        ttl = 1799
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   findallthelatest-newshoppingpoints.us
Address: 192.186.168.209

DAPI:~ davepiscitello$ 
```

Use Case: Phishing a Brand

4) Check https://stats.ripe.net to see who's announcing 192.186.168.209 (or its prefix)?



https://stat.ripe.net/192.186.168.209#tabId=at-a-glance

Prefix Overview (192.186.168.209)

✓ Announced

This prefix is part of 192.186.128.0/18 announced by

AS55286

"SERVER-MANIA - B2 Net Solutions Inc.,US"

Show IANA Registry Information

Showing results for 192.186.128.0/18 as of 2015-04-28 08:00:00 UTC

Given resource is not announced but result has been aligned to first-level less-specific (192.186.128.0/18).

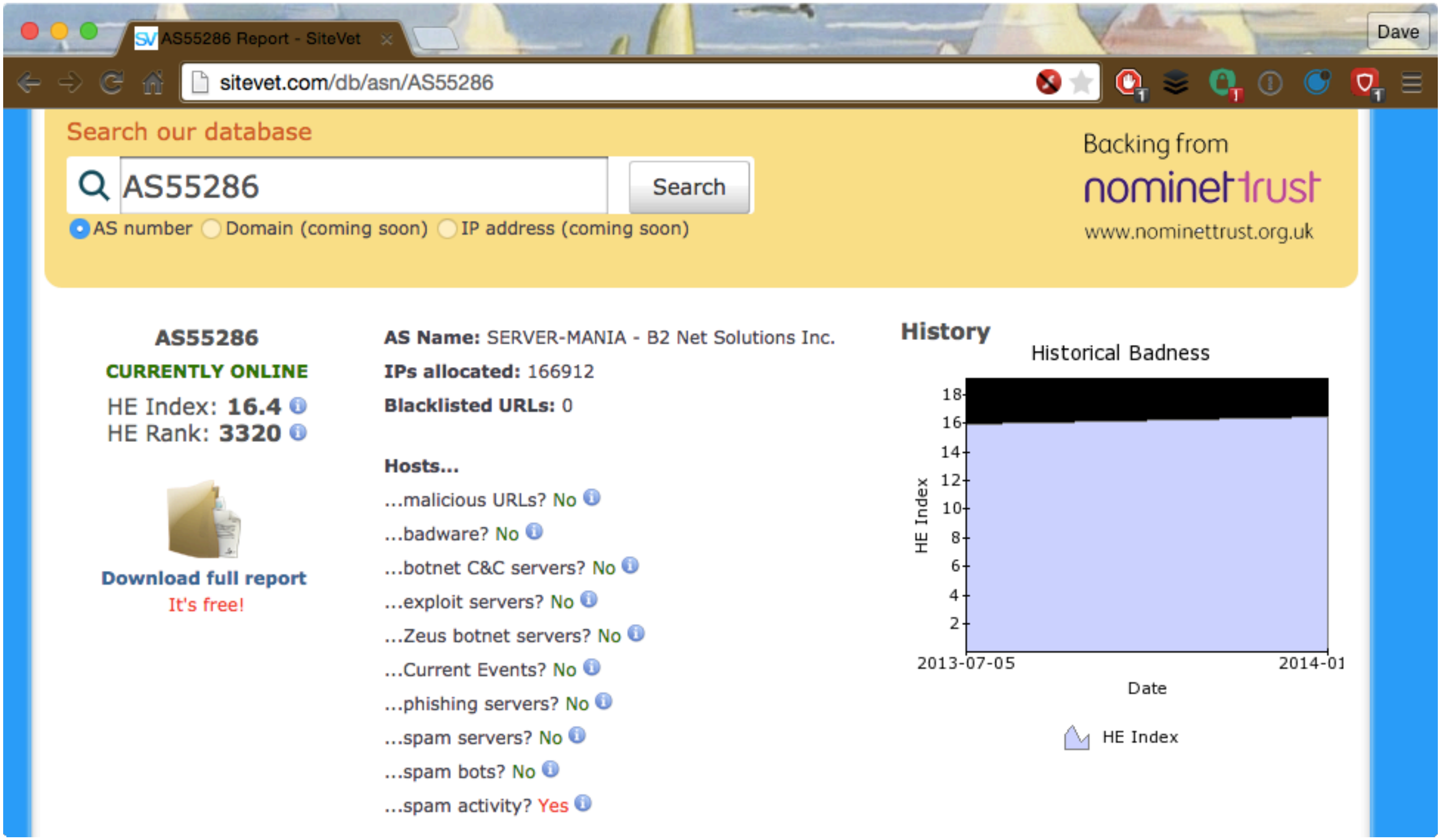
Geoloc (192.186.168.209)

Geoloc details

Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for 192.186.168.209 as of 2015-04-07 00:00:00 UTC

Use Case: Phishing a Brand



Search our database

AS55286 Search

● AS number ○ Domain (coming soon) ○ IP address (coming soon)

Backing from nominettrust www.nominettrust.org.uk

AS55286

CURRENTLY ONLINE

HE Index: **16.4**
HE Rank: **3320**

Download full report
It's free!

AS Name: SERVER-MANIA - B2 Net Solutions Inc.
IPs allocated: 166912
Blacklisted URLs: 0

Hosts...

...malicious URLs? No
...badware? No
...botnet C&C servers? No
...exploit servers? No
...Zeus botnet servers? No
...Current Events? No
...phishing servers? No
...spam servers? No
...spam bots? No
...spam activity? Yes

History

Analyzing Malicious Documents

Relevance to Identifier Systems: the documents may contain addresses or domains

Analyzing Malicious Documents

- Locate potentially malicious embedded code, such as shellcode, VBA macros, or JavaScript
- Not a malware analyst? Use publicly available tools to:
  - Execute in a sandbox for analysis
  - Extract suspicious code segments from the file
  - If relevant, disassemble and/or debug shellcode
  - If relevant, deobfuscate and examine JavaScript, ActionScript, or VB macro code.
  - Understand next steps in the infection chain

http://zeltser.com/reverse-malware/analyzing-malicious-documents.html - Lenny Zeltser

Tools For Analyzing MS Office Files

- OfficeMalScanner:
  - locates shellcode, VBA macros in MS Office files http://www.reconstructer.org/code/OfficeMalScanner.zip
- MalHost-Setup (Part of OfficeMalScanner)
  - extracts shellcode from a given offset in an MS Office file and embeds it an EXE file for further analysis.
  - shows raw contents and structure of an MS Office file, and identifies some common exploits http://go.microsoft.com/fwlink/?LinkId=158791
- Hachoir-urwid
  - Navigate structure of binary Office files,view stream contents https://bitbucket.org/haypo/hachoir/wiki/hachoir-urwid

From http://zeltser.com/reverse-malware/analyzing-malicious-documents.html - Lenny Zeltser

Tools For Analyzing MS Office Files

- Office Binary Translator
  - converts DOC, PPT, and XLS files into Open XML files (includes BiffView tool) - http://b2xtranslator.sourceforge.net/
- Document Analyzer (http://documentanalyzer.net)
  - Launch suspicious office, pdf files in sandbox for inspection, analysis
- FileHex (not free - http://www.heaventools.com/) and FileInsight (http://vil.nai.com/vil/averttools.aspx)
  - hex editors tpparse and edit OLE structures.
- MalwareTracker PDF examiner
  - https://www.malwaretracker.com/pdf.php

From http://zeltser.com/reverse-malware/analyzing-malicious-documents.html - Lenny Zeltser

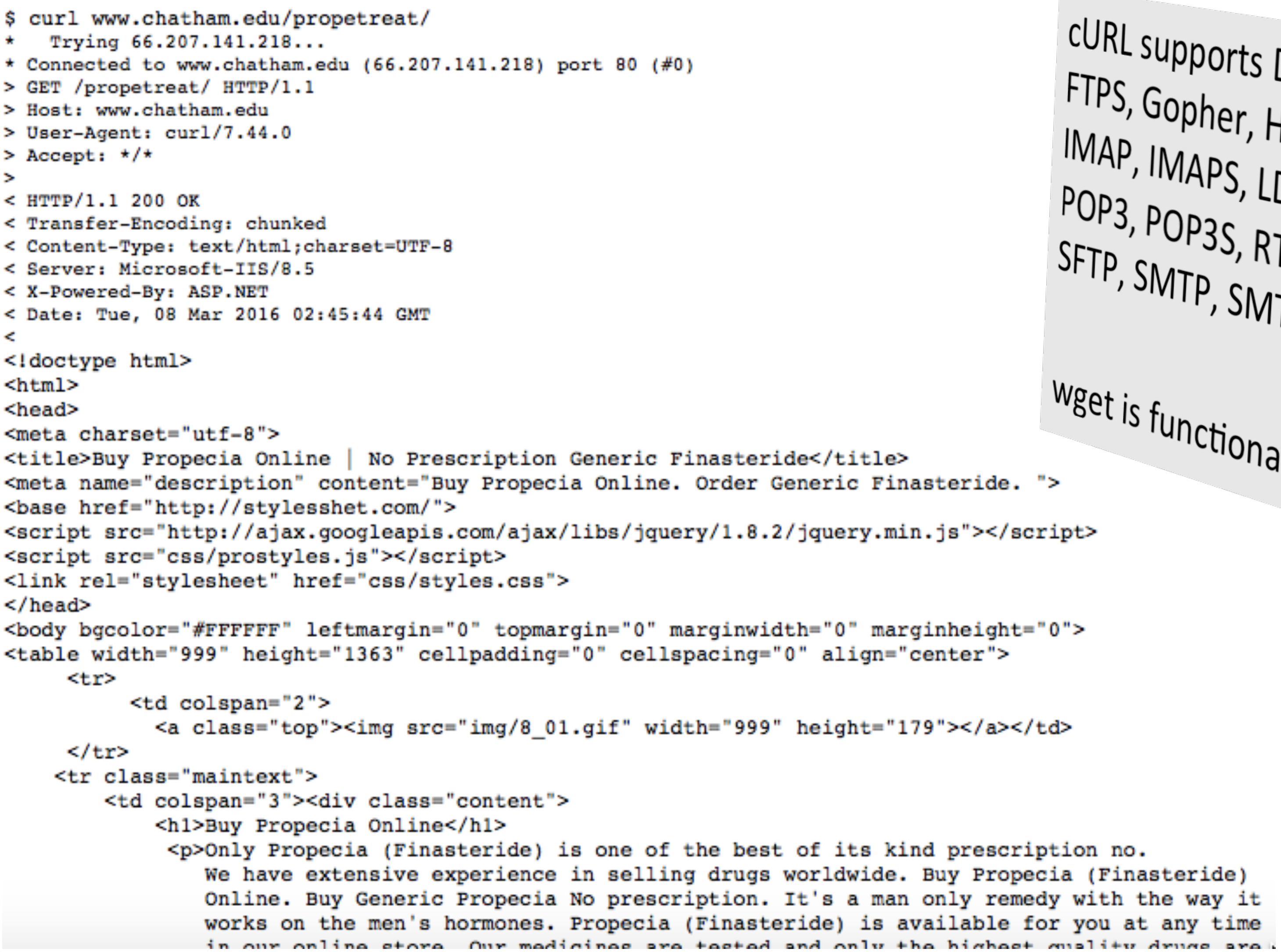
Investigating Web sites or Pages

Relevance to Identifier Systems: the pages may contain a crumb trail of addresses or domains

Investigating Web Sites Or Pages

- You may not want to visit a suspicious site using a browser
- If you want to *see* HTTP responses but don’t trust to *execute* use
  - cURL
    - http://curl.haxx.se/docs/manpage.html
    - http://www.thegeekstuff.com/2012/04/curl-examples/
    - Want to curl Gmail for new email? `curl -u username --silent "https://mail.google.com/mail/feed/atom" | perl -ne 'print "\t" if /<name>/; print "$2\n" if /<(title|name)>(.*)<\/\1>/;'`
  - Wget
    - http://www.gnu.org/software/wget/
    - http://gnuwin32.sourceforge.net/packages/wget.htm
  - Capture traffic with LAN traffic analyzers (wireshark)
- Want to see a site that’s no longer online?
  - try Wayback Machine at http://archive.org

Use curl Or wget On Web Pages



```
$ curl www.chatham.edu/propetreat/
*   Trying 66.207.141.218...
* Connected to www.chatham.edu (66.207.141.218) port 80 (#0)
> GET /propetreat/ HTTP/1.1
> Host: www.chatham.edu
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Transfer-Encoding: chunked
< Content-Type: text/html;charset=UTF-8
< Server: Microsoft-IIS/8.5
< X-Powered-By: ASP.NET
< Date: Tue, 08 Mar 2016 02:45:44 GMT
<
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>Buy Propecia Online | No Prescription Generic Finasteride</title>
<meta name="description" content="Buy Propecia Online. Order Generic Finasteride. ">
<base href="http://stylesshet.com/">
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.8.2/jquery.min.js"></script>
<script src="css/prostyles.js"></script>
<link rel="stylesheet" href="css/styles.css">
</head>
<body bgcolor="#FFFFFF" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
<table width="999" height="1363" cellpadding="0" cellspacing="0" align="center">
     <tr>
          <td colspan="2">
            <a class="top"><img src="img/8_01.gif" width="999" height="179"></a></td>
     </tr>
    <tr class="maintext">
        <td colspan="3"><div class="content">
            <h1>Buy Propecia Online</h1>
             <p>Only Propecia (Finasteride) is one of the best of its kind prescription no.
               We have extensive experience in selling drugs worldwide. Buy Propecia (Finasteride)
               Online. Buy Generic Propecia No prescription. It's a man only remedy with the way it
               works on the men's hormones. Propecia (Finasteride) is available for you at any time
               in our online store. Our medicines are tested and only the highest quality drugs are
```

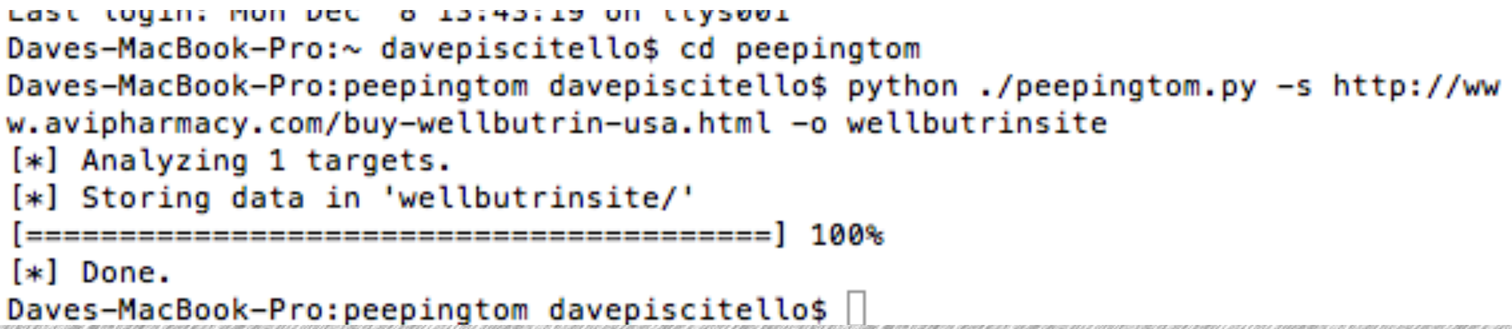
cURL supports DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet ,TFTP

wget is functionally the same

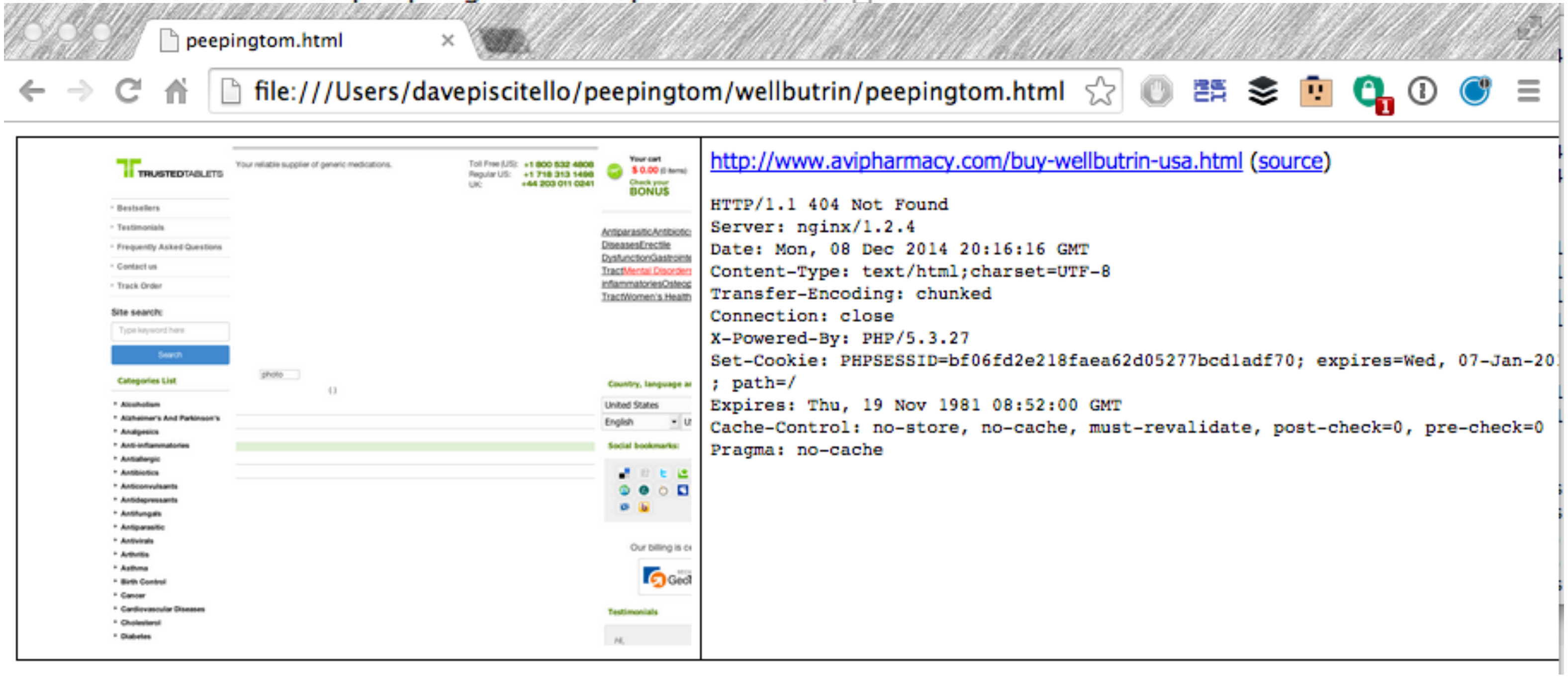
peepingtom

Python program to cURL and screenshot web pages

http://www.securityskeptic.com/2014/10/get-acquainted-with-a-peepingtom-you-bet.html



```
Last login: Mon Dec  8 13:43:19 on ttys001
Daves-MacBook-Pro:~ davepiscitello$ cd peepingtom
Daves-MacBook-Pro:peepingtom davepiscitello$ python ./peepingtom.py -s http://ww
w.avipharmacy.com/buy-wellbutrin-usa.html -o wellbutrinsite
[*] Analyzing 1 targets.
[*] Storing data in 'wellbutrinsite/'
[=======================================] 100%
[*] Done.
Daves-MacBook-Pro:peepingtom davepiscitello$ 
```



peepingtom.html
file:///Users/davepiscitello/peepingtom/wellbutrin/peepingtom.html
TRUSTEDTABLETS
Your reliable supplier of generic medications.
BONUS
Bestsellers
Testimonials
Frequently Asked Questions
Contact us
Track Order
Site search:
Search
Categories List

http://www.avipharmacy.com/buy-wellbutrin-usa.html (source)

```
HTTP/1.1 404 Not Found
Server: nginx/1.2.4
Date: Mon, 08 Dec 2014 20:16:16 GMT
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.3.27
Set-Cookie: PHPSESSID=bf06fd2e218faea62d05277bcd1adf70; expires=Wed, 07-Jan-20
; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
```

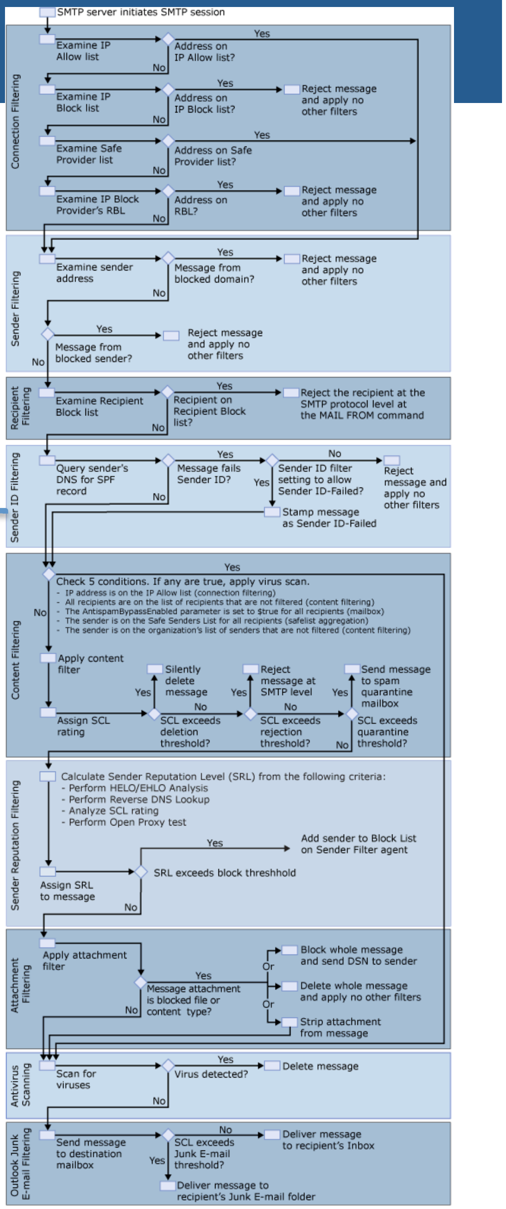
Internet Identifiers and SPAM

DNS… IP addresses…
Sender Policy Framework… Domain Key Identified Mail… reputation.

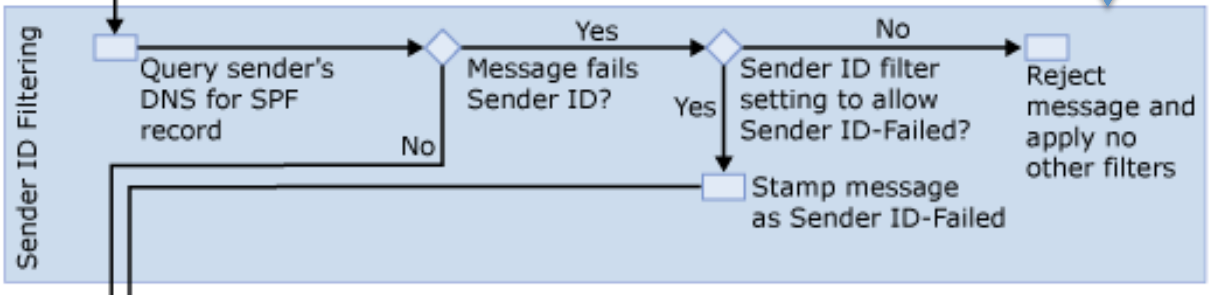
Identifiers in SPAM email

Typical spam checks include:

- Connection filtering (IP and safe provider lists)
- Sender and recipient filtering (mail address)
- Sender ID filtering (IPs from SPF records in DNS)
- Identity verification and message integrity (DKIM signature match using public key in DNS)
- DMARC policy (published in DNS)
- Content Filtering
- Sender Reputation Filtering
- Attachment filtering
- Antivirus scanning



SMTP server initiates SMTP session
Connection Filtering
Examine IP Allow list
Address on IP Allow list?
Yes
No
Examine IP Block list
Address on IP Block list?
Yes
No
Reject message and apply no other filters
Examine Safe Provider list
Address on Safe Provider list?
Yes
No
Examine IP Block Provider's RBL
Address on RBL?
Yes
No
Reject message and apply no other filters
Sender Filtering
Examine sender address
Message from blocked domain?
Yes
No
Reject message and apply no other filters
Message from blocked sender?
Yes
No
Reject message and apply no other filters
Recipient Filtering
Examine Recipient Block list
Recipient on Recipient Block list?
Yes
No
Reject the recipient at the SMTP protocol level at the MAIL FROM command
Sender ID Filtering
Query sender's DNS for SPF record
Message fails Sender ID?
Yes
No
Sender ID filter setting to allow Sender ID-Failed?
Yes
No
Reject message and apply no other filters
Stamp message as Sender ID-Failed
Content Filtering
Check 5 conditions. If any are true, apply virus scan.
- IP address is on the IP Allow list (connection filtering)
- All recipients are on the list of recipients that are not filtered (content filtering)
- The AntispamBypassEnabled parameter is set to $true for all recipients (mailbox)
- The sender is on the Safe Senders List for all recipients (safelist aggregation)
- The sender is on the organization's list of senders that are not filtered (content filtering)
Yes
No
Apply content filter
Assign SCL rating
SCL exceeds deletion threshold?
Yes
No
Silently delete message
SCL exceeds rejection threshold?
Yes
No
Reject message at SMTP level
SCL exceeds quarantine threshold?
Yes
No
Send message to spam quarantine mailbox
Sender Reputation Filtering
Calculate Sender Reputation Level (SRL) from the following criteria:
- Perform HELO/EHLO Analysis
- Perform Reverse DNS Lookup
- Analyze SCL rating
- Perform Open Proxy test
Assign SRL to message
SRL exceeds block threshhold
Yes
No
Add sender to Block List on Sender Filter agent
Attachment Filtering
Apply attachment filter
Message attachment is blocked file or content type?
Yes
No
Block whole message and send DSN to sender
Or
Delete whole message and apply no other filters
Or
Strip attachment from message
Antivirus Scanning
Scan for viruses
Virus detected?
Yes
No
Delete message
Outlook Junk E-mail Filtering
Send message to destination mailbox
SCL exceeds Junk E-mail threshold?
Yes
No
Deliver message to recipient's Inbox
Deliver message to recipient's Junk E-mail folder



Sender ID Filtering
Query sender's DNS for SPF record
No
Yes
Message fails Sender ID?
Yes
No
Sender ID filter setting to allow Sender ID-Failed?
Reject message and apply no other filters
Stamp message as Sender ID-Failed

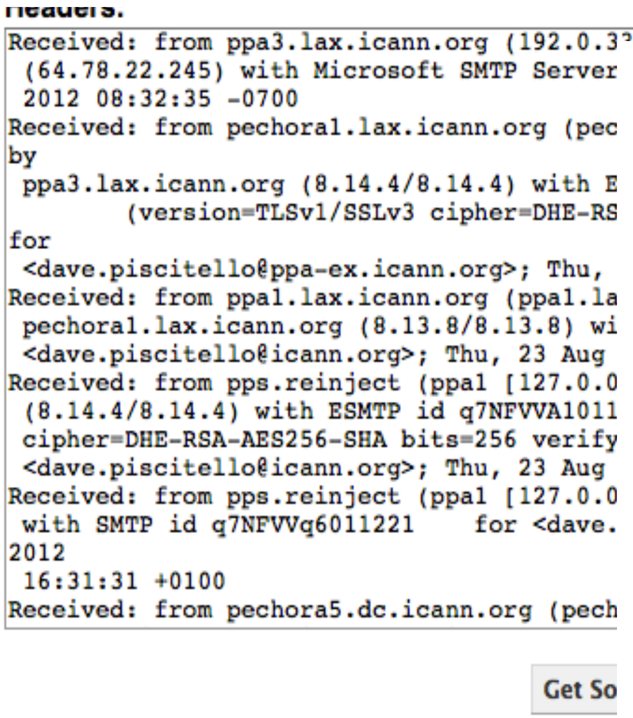
http://technet.microsoft.com/en-us/library/aa997242%28v=exchg.141%29.aspx

Investigating Identifiers in SPAM

- When you want DNS and IP addresses from SPAM email
  - Get the raw email source
    - Find a how to reveal full, unmodified email message in popular mail clients and web email at https://www.spamcop.net/fom-serve/cache/19.html
  - Examine sender and mail path in the headers
  - Get Sender Policy Framework (SPF) and Domain Keys (DKIM) from DNS
  - What do SPF or DKIM reveal?
  - Investigate domains, IPs, URLs in message body
- Sender reputation? Another minutiae

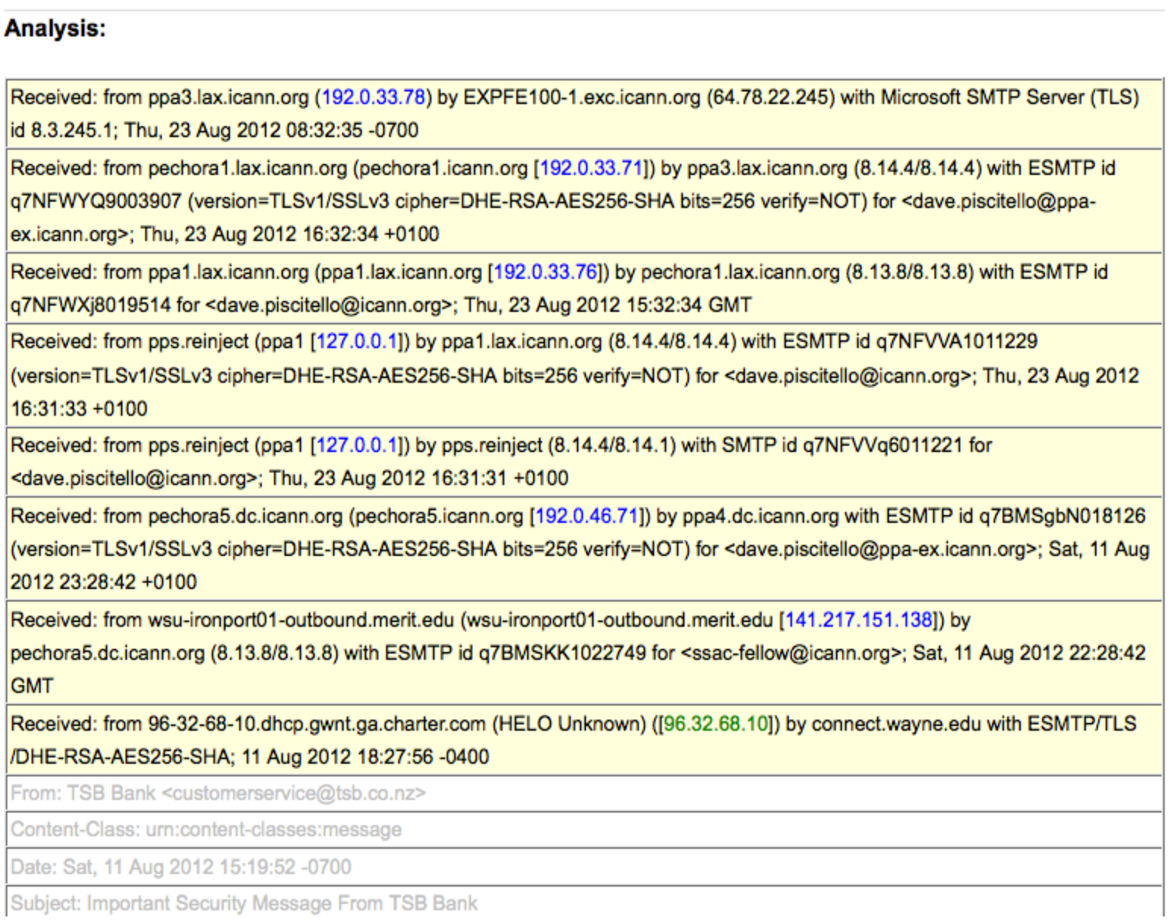
Examining Mail Headers

1) Copy-paste raw headers into http://whatismyipaddress.com/trace-email



Headers:

```
Received: from ppa3.lax.icann.org (192.0.33.78) by EXPFE100-1.exc.icann.org
 (64.78.22.245) with Microsoft SMTP Server
 2012 08:32:35 -0700
Received: from pechora1.lax.icann.org (pec
by
 ppa3.lax.icann.org (8.14.4/8.14.4) with E
        (version=TLSv1/SSLv3 cipher=DHE-RS
for
 <dave.piscitello@ppa-ex.icann.org>; Thu,
Received: from ppa1.lax.icann.org (ppa1.la
 pechora1.lax.icann.org (8.13.8/8.13.8) wi
 <dave.piscitello@icann.org>; Thu, 23 Aug
Received: from pps.reinject (ppa1 [127.0.0
 (8.14.4/8.14.4) with ESMTP id q7NFVVA1011
 cipher=DHE-RSA-AES256-SHA bits=256 verify
 <dave.piscitello@icann.org>; Thu, 23 Aug
Received: from pps.reinject (ppa1 [127.0.0
 with SMTP id q7NFVVq6011221    for <dave.
2012
 16:31:31 +0100
Received: from pechora5.dc.icann.org (pech
```



Analysis:

Received: from ppa3.lax.icann.org (192.0.33.78) by EXPFE100-1.exc.icann.org (64.78.22.245) with Microsoft SMTP Server (TLS) id 8.3.245.1; Thu, 23 Aug 2012 08:32:35 -0700

Received: from pechora1.lax.icann.org (pechora1.icann.org [192.0.33.71]) by ppa3.lax.icann.org (8.14.4/8.14.4) with ESMTP id q7NFWYQ9003907 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <dave.piscitello@ppa-ex.icann.org>; Thu, 23 Aug 2012 16:32:34 +0100

Received: from ppa1.lax.icann.org (ppa1.lax.icann.org [192.0.33.76]) by pechora1.lax.icann.org (8.13.8/8.13.8) with ESMTP id q7NFWXj8019514 for <dave.piscitello@icann.org>; Thu, 23 Aug 2012 15:32:34 GMT

Received: from pps.reinject (ppa1 [127.0.0.1]) by ppa1.lax.icann.org (8.14.4/8.14.4) with ESMTP id q7NFVVA1011229 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <dave.piscitello@icann.org>; Thu, 23 Aug 2012 16:31:33 +0100

Received: from pps.reinject (ppa1 [127.0.0.1]) by pps.reinject (8.14.4/8.14.1) with SMTP id q7NFVVq6011221 for <dave.piscitello@icann.org>; Thu, 23 Aug 2012 16:31:31 +0100

Received: from pechora5.dc.icann.org (pechora5.icann.org [192.0.46.71]) by ppa4.dc.icann.org with ESMTP id q7BMSgbN018126 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <dave.piscitello@ppa-ex.icann.org>; Sat, 11 Aug 2012 23:28:42 +0100

Received: from wsu-ironport01-outbound.merit.edu (wsu-ironport01-outbound.merit.edu [141.217.151.138]) by pechora5.dc.icann.org (8.13.8/8.13.8) with ESMTP id q7BMSKK1022749 for <ssac-fellow@icann.org>; Sat, 11 Aug 2012 22:28:42 GMT

Received: from 96-32-68-10.dhcp.gwnt.ga.charter.com (HELO Unknown) ([96.32.68.10]) by connect.wayne.edu with ESMTP/TLS /DHE-RSA-AES256-SHA; 11 Aug 2012 18:27:56 -0400

From: TSB Bank <customerservice@tsb.co.nz>

Content-Class: urn:content-classes:message

Date: Sat, 11 Aug 2012 15:19:52 -0700

Subject: Important Security Message From TSB Bank

2) Web page parses mail headers into readable format

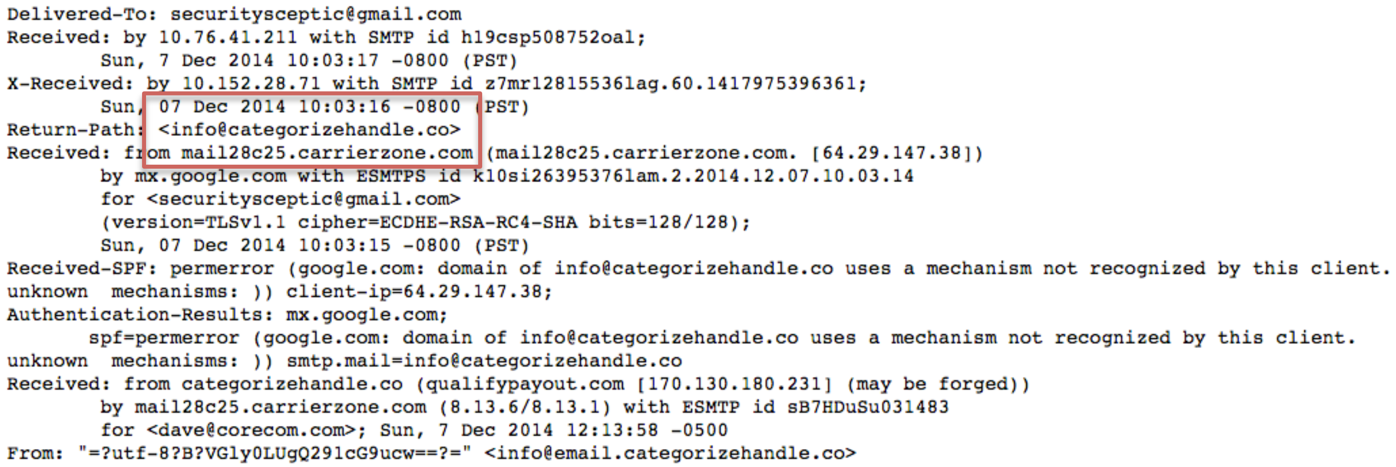
Sender Reputation checking

Need New Tires? Get The Best Deals On GoodYear, Michelin, Firestone & More Now!

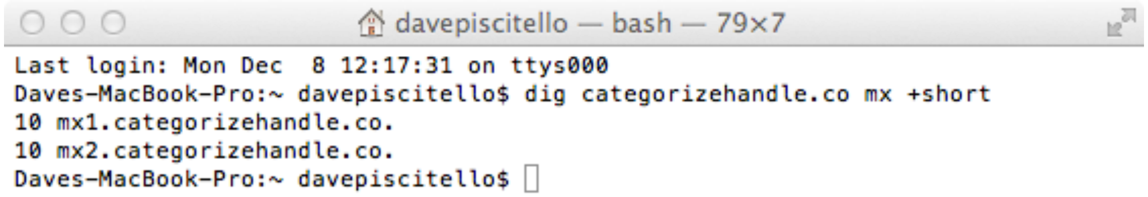
Visit Here for More Information About Tire Coupons

1) Grab your spample

2) Grab the domain from the headers

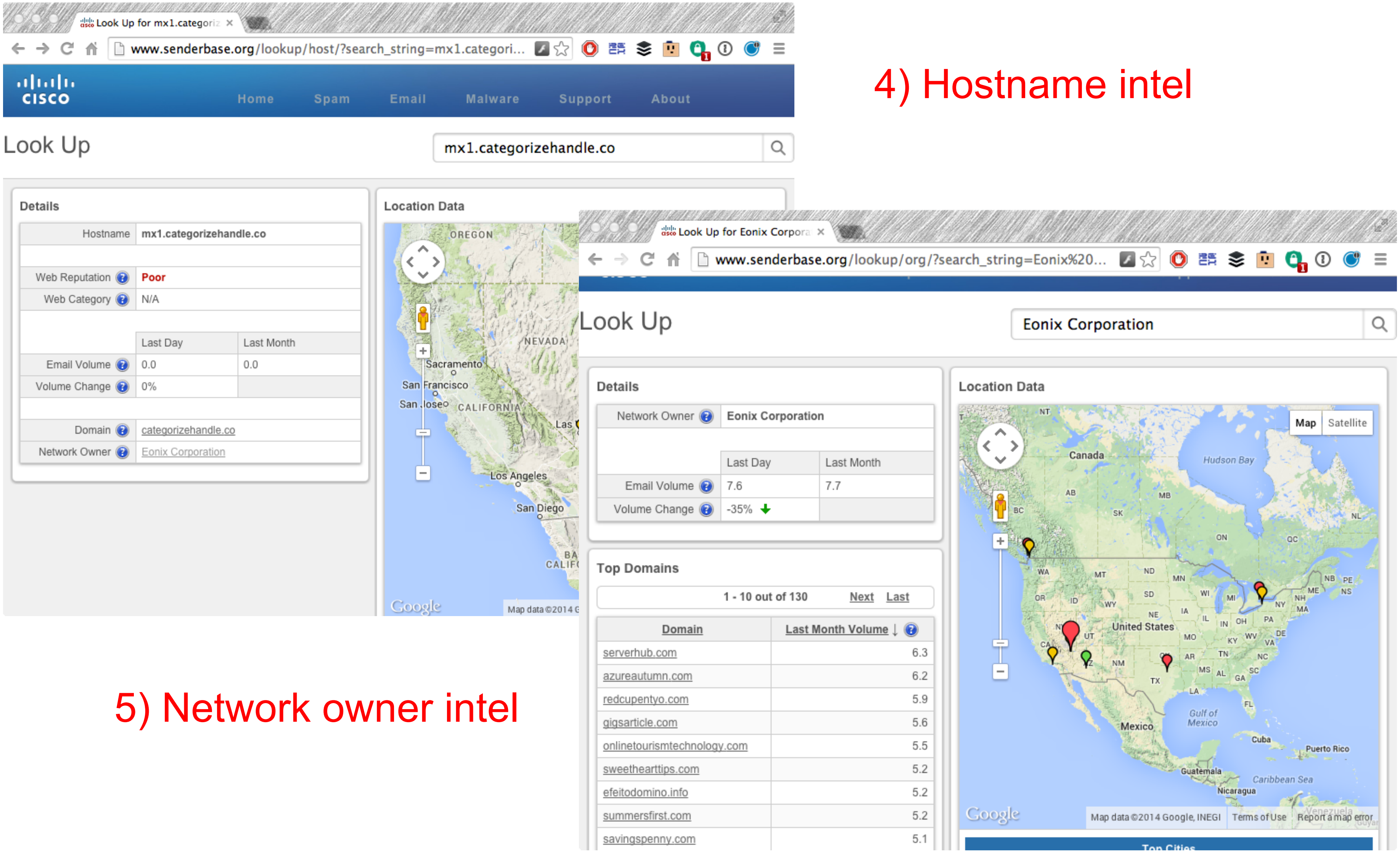

```
Delivered-To: securitysceptic@gmail.com
Received: by 10.76.41.211 with SMTP id h19csp508752oal;
        Sun, 7 Dec 2014 10:03:17 -0800 (PST)
X-Received: by 10.152.28.71 with SMTP id z7mr12815536lag.60.1417975396361;
        Sun, 07 Dec 2014 10:03:16 -0800 (PST)
Return-Path: <info@categorizehandle.co>
Received: from mail28c25.carrierzone.com (mail28c25.carrierzone.com. [64.29.147.38])
        by mx.google.com with ESMTPS id k10si26395376lam.2.2014.12.07.10.03.14
        for <securitysceptic@gmail.com>
        (version=TLSv1.1 cipher=ECDHE-RSA-RC4-SHA bits=128/128);
        Sun, 07 Dec 2014 10:03:15 -0800 (PST)
Received-SPF: permerror (google.com: domain of info@categorizehandle.co uses a mechanism not recognized by this client.
unknown  mechanisms: )) client-ip=64.29.147.38;
Authentication-Results: mx.google.com;
       spf=permerror (google.com: domain of info@categorizehandle.co uses a mechanism not recognized by this client.
unknown  mechanisms: )) smtp.mail=info@categorizehandle.co
Received: from categorizehandle.co (qualifypayout.com [170.130.180.231] (may be forged))
        by mail28c25.carrierzone.com (8.13.6/8.13.1) with ESMTP id sB7HDuSu031483
        for <dave@corecom.com>; Sun, 7 Dec 2014 12:13:58 -0500
From: "=?utf-8?B?VGly0LUgQ291cG9ucw==?=" <info@email.categorizehandle.co>
```

3) Get the MX record



```
Last login: Mon Dec  8 12:17:31 on ttys000
Daves-MacBook-Pro:~ davepiscitello$ dig categorizehandle.co mx +short
10 mx1.categorizehandle.co.
10 mx2.categorizehandle.co.
Daves-MacBook-Pro:~ davepiscitello$ 
```

Sender Reputation checking



Look Up for mx1.categoriz

www.senderbase.org/lookup/host/?search_string=mx1.categori…

Look Up

mx1.categorizehandle.co

Details

Hostname	mx1.categorizehandle.co	
Web Reputation	Poor	
Web Category	N/A	
	Last Day	Last Month
Email Volume	0.0	0.0
Volume Change	0%	
Domain	categorizehandle.co	
Network Owner	Eonix Corporation	

Location Data

4) Hostname intel

Look Up for Eonix Corpora

www.senderbase.org/lookup/org/?search_string=Eonix%20…

Look Up

Eonix Corporation

Details

Network Owner	Eonix Corporation	
	Last Day	Last Month
Email Volume	7.6	7.7
Volume Change	-35% ↓	

Top Domains

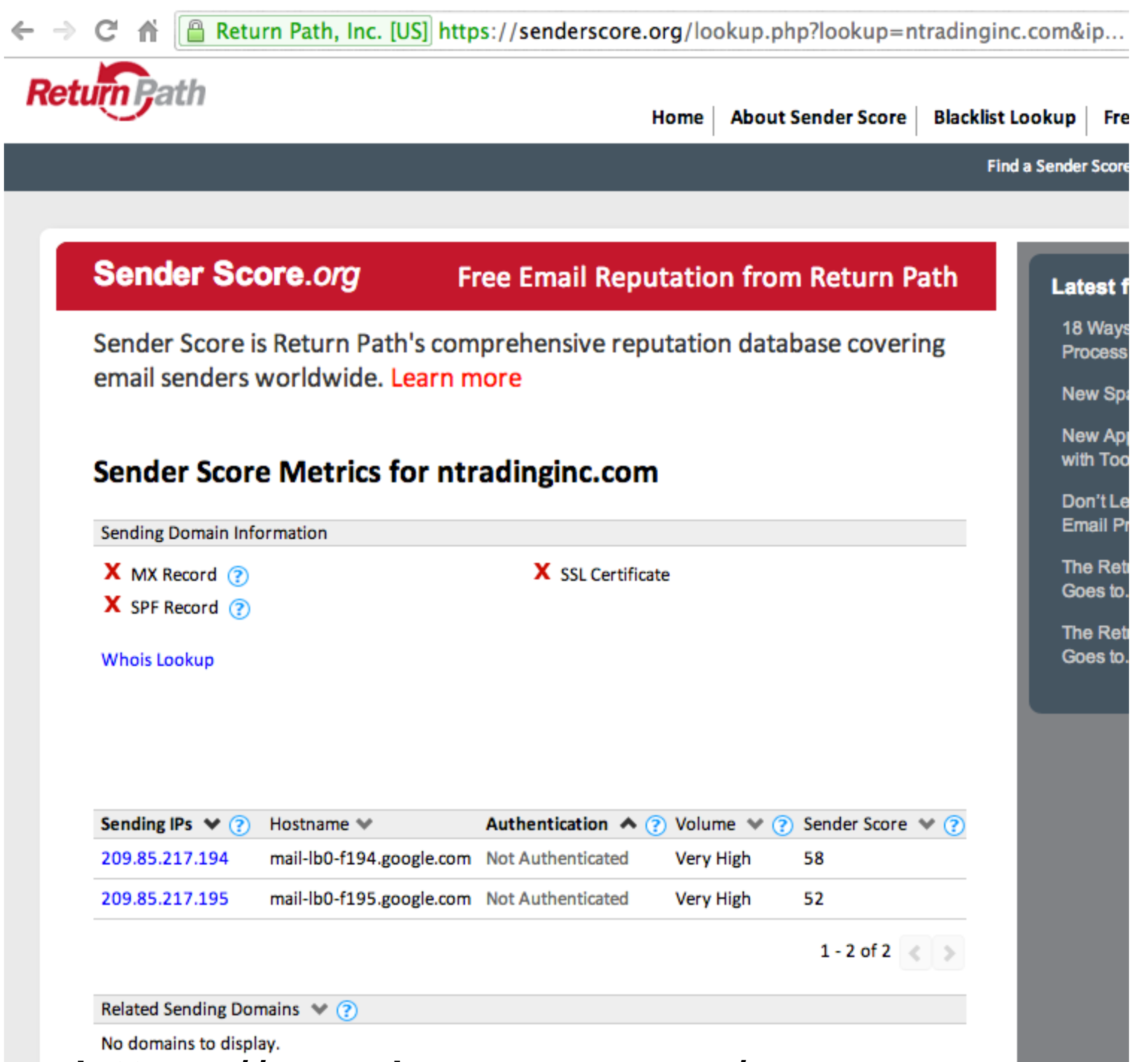
1 - 10 out of 130 Next Last

Domain	Last Month Volume ↓
serverhub.com	6.3
azureautumn.com	6.2
redcupentyo.com	5.9
gigsarticle.com	5.6
onlinetourismtechnology.com	5.5
sweethearttips.com	5.2
efeitodomino.info	5.2
summersfirst.com	5.2
savingspenny.com	5.1

Location Data

5) Network owner intel

Checking Sender Reputation



Return Path, Inc. [US] https://senderscore.org/lookup.php?lookup=ntradinginc.com&ip...
Return Path
Home | About Sender Score | Blacklist Lookup | Fre
Find a Sender Score
Latest f
18 Ways
Process
New Sp
New Ap
with Too
Don't Le
Email Pr
The Ret
Goes to.
The Ret
Goes to.

Sender Score.org Free Email Reputation from Return Path

Sender Score is Return Path's comprehensive reputation database covering email senders worldwide. Learn more

Sender Score Metrics for ntradinginc.com

Sending Domain Information

X MX Record ?
X SPF Record ?
X SSL Certificate

Whois Lookup

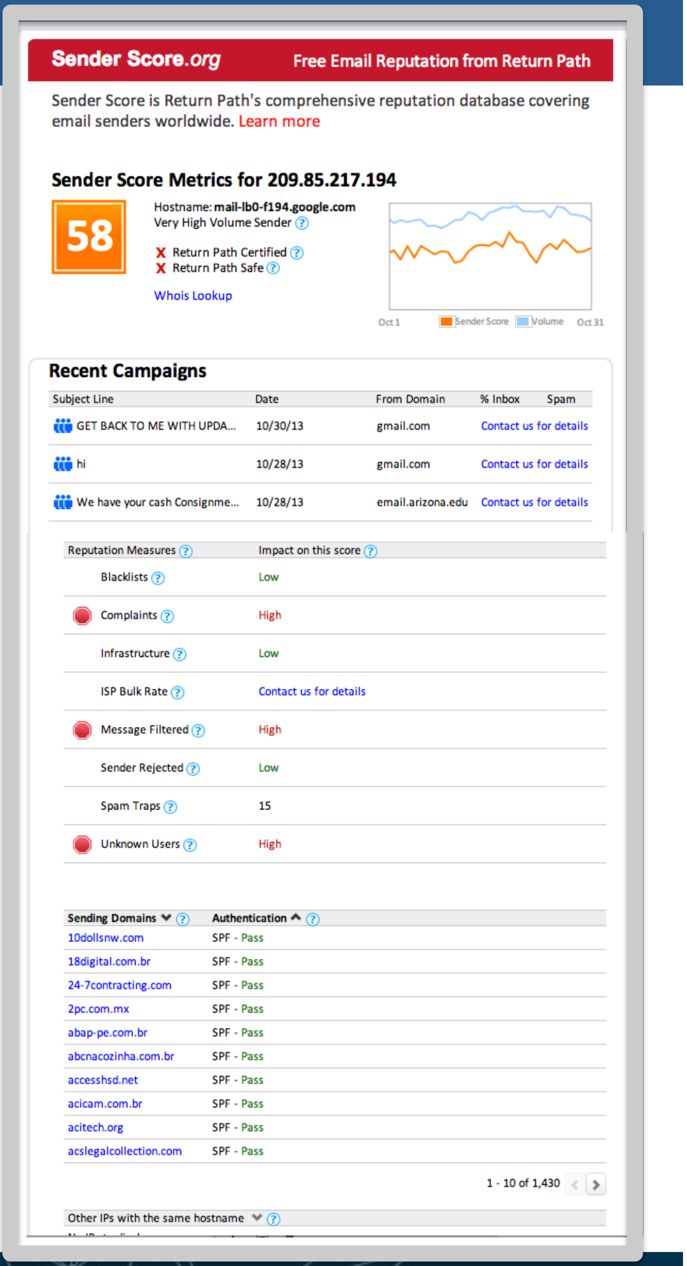
Sending IPs	Hostname	Authentication	Volume	Sender Score
209.85.217.194	mail-lb0-f194.google.com	Not Authenticated	Very High	58
209.85.217.195	mail-lb0-f195.google.com	Not Authenticated	Very High	52

1 - 2 of 2

Related Sending Domains ?

No domains to display.

https://senderscore.org/



Sender Score.org Free Email Reputation from Return Path

Sender Score is Return Path's comprehensive reputation database covering email senders worldwide. Learn more

Sender Score Metrics for 209.85.217.194

58

Hostname: **mail-lb0-f194.google.com**
Very High Volume Sender ?

X Return Path Certified ?
X Return Path Safe ?

Whois Lookup

Recent Campaigns

Subject Line	Date	From Domain	% Inbox	Spam
GET BACK TO ME WITH UPDA...	10/30/13	gmail.com	Contact us for details	
hi	10/28/13	gmail.com	Contact us for details	
We have your cash Consignme...	10/28/13	email.arizona.edu	Contact us for details	

Reputation Measures ?	Impact on this score ?
Blacklists ?	Low
● Complaints ?	High
Infrastructure ?	Low
ISP Bulk Rate ?	Contact us for details
● Message Filtered ?	High
Sender Rejected ?	Low
Spam Traps ?	15
● Unknown Users ?	High

Sending Domains ?	Authentication ?
10dollsnw.com	SPF - Pass
18digital.com.br	SPF - Pass
24-7contracting.com	SPF - Pass
2pc.com.mx	SPF - Pass
abap-pe.com.br	SPF - Pass
abcnacozinha.com.br	SPF - Pass
accesshsd.net	SPF - Pass
acicam.com.br	SPF - Pass
acitech.org	SPF - Pass
acslegalcollection.com	SPF - Pass

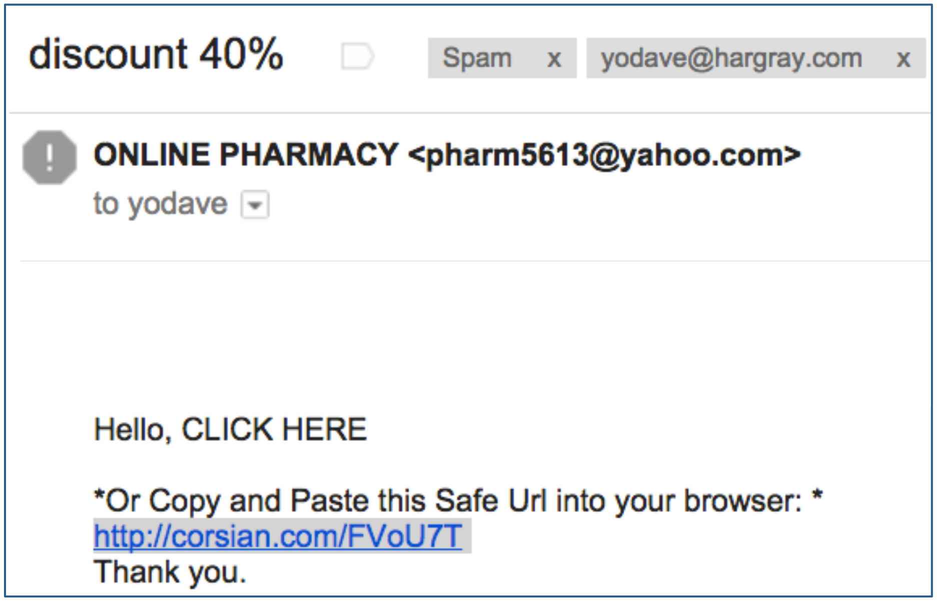
1 - 10 of 1,430

Other IPs with the same hostname ?

Final lap: Case Studies and Use Cases

Use Case: Your Crumb Trail Ends…

1) Grab URL from spam



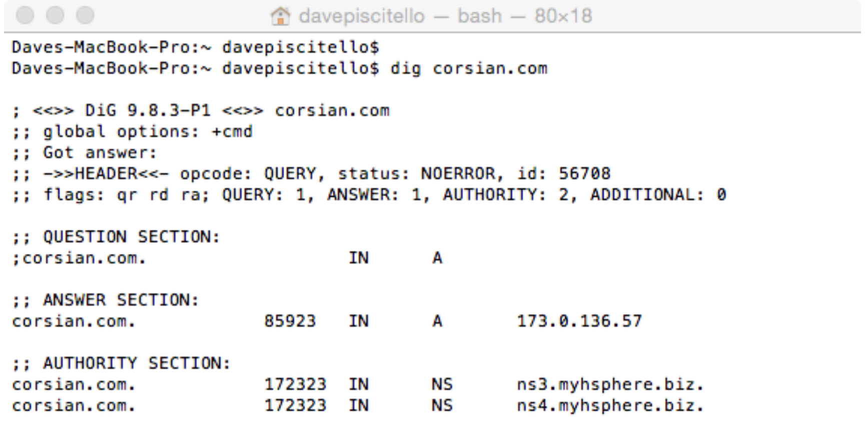
ONLINE PHARMACY <pharm5613@yahoo.com>

to yodave

Hello, CLICK HERE

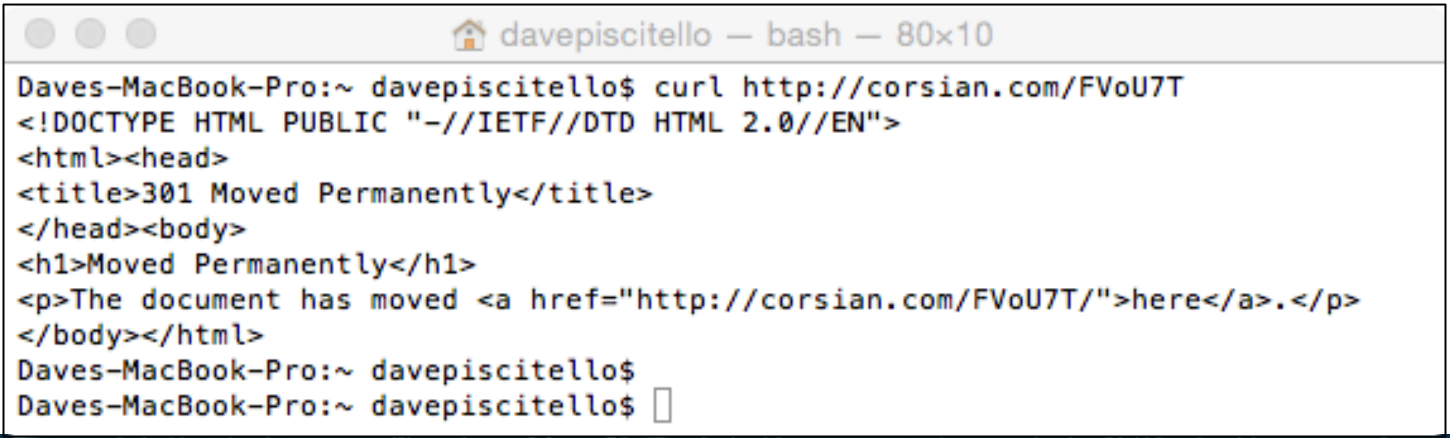
*Or Copy and Paste this Safe Url into your browser: *
http://corsian.com/FVoU7T
Thank you.

2) Find the host site IP



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

; <<>> DiG 9.8.3-P1 <<>> corsian.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56708
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;corsian.com.                   IN      A

;; ANSWER SECTION:
corsian.com.            85923   IN      A       173.0.136.57

;; AUTHORITY SECTION:
corsian.com.            172323  IN      NS      ns3.myhsphere.biz.
corsian.com.            172323  IN      NS      ns4.myhsphere.biz.
```

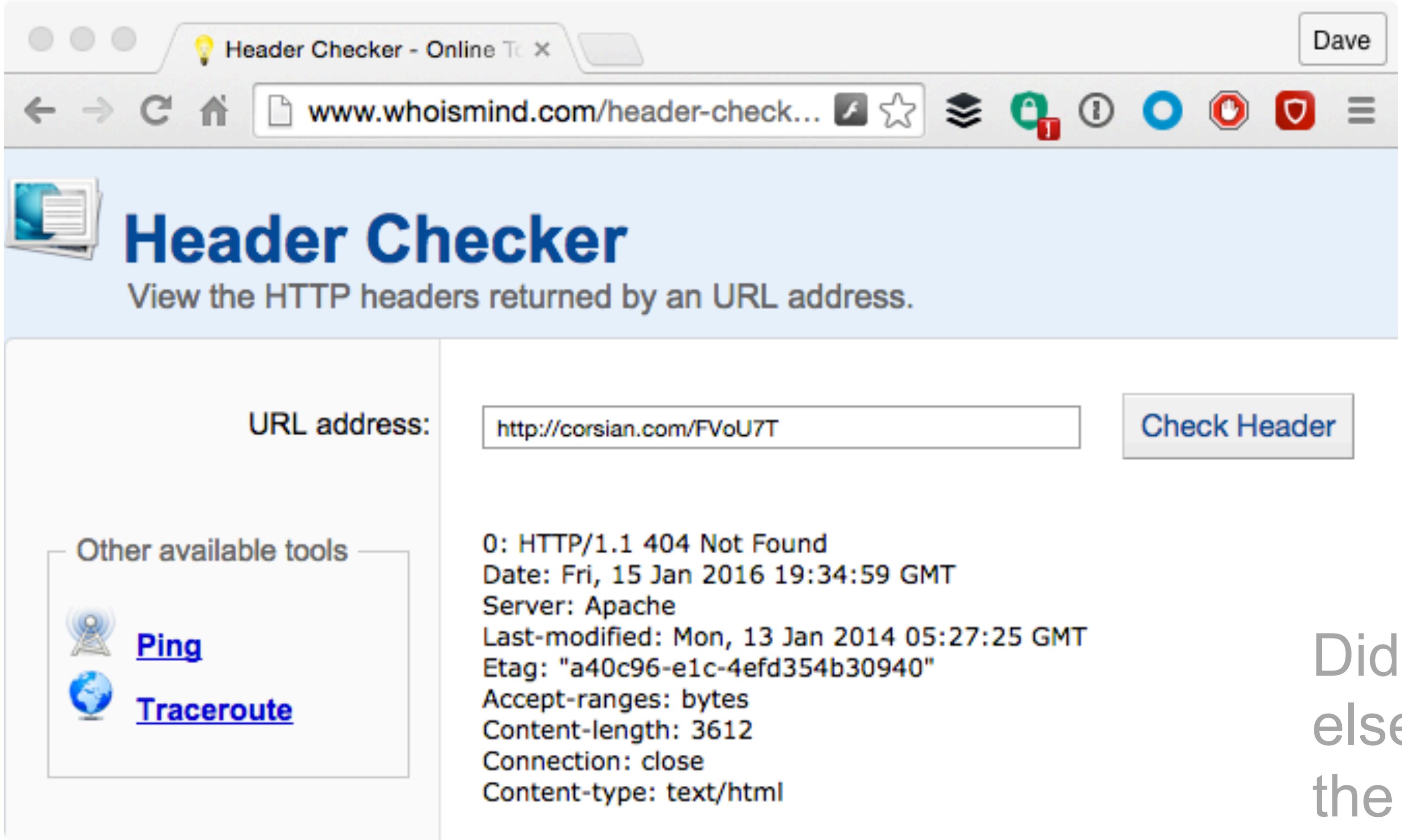
3) No content? Why?



```
Daves-MacBook-Pro:~ davepiscitello$ curl http://corsian.com/FVoU7T
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://corsian.com/FVoU7T/">here</a>.</p>
</body></html>
Daves-MacBook-Pro:~ davepiscitello$
Daves-MacBook-Pro:~ davepiscitello$ 
```

Use Case: Your Crumb Trail Ends…

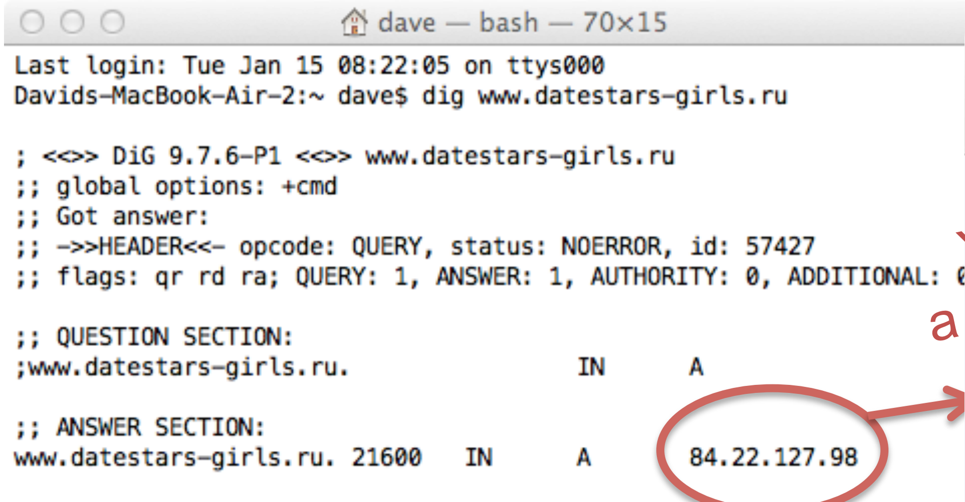
4) Try another tool, e.g., http://www.whoismind.com/header-checker.html


Header Checker - Online T
Dave
www.whoismind.com/header-check...
Header Checker
View the HTTP headers returned by an URL address.
URL address:
http://corsian.com/FVoU7T
Check Header
Other available tools
Ping
Traceroute

```
0: HTTP/1.1 404 Not Found
Date: Fri, 15 Jan 2016 19:34:59 GMT
Server: Apache
Last-modified: Mon, 13 Jan 2014 05:27:25 GMT
Etag: "a40c96-e1c-4efd354b30940"
Accept-ranges: bytes
Content-length: 3612
Connection: close
Content-type: text/html
```

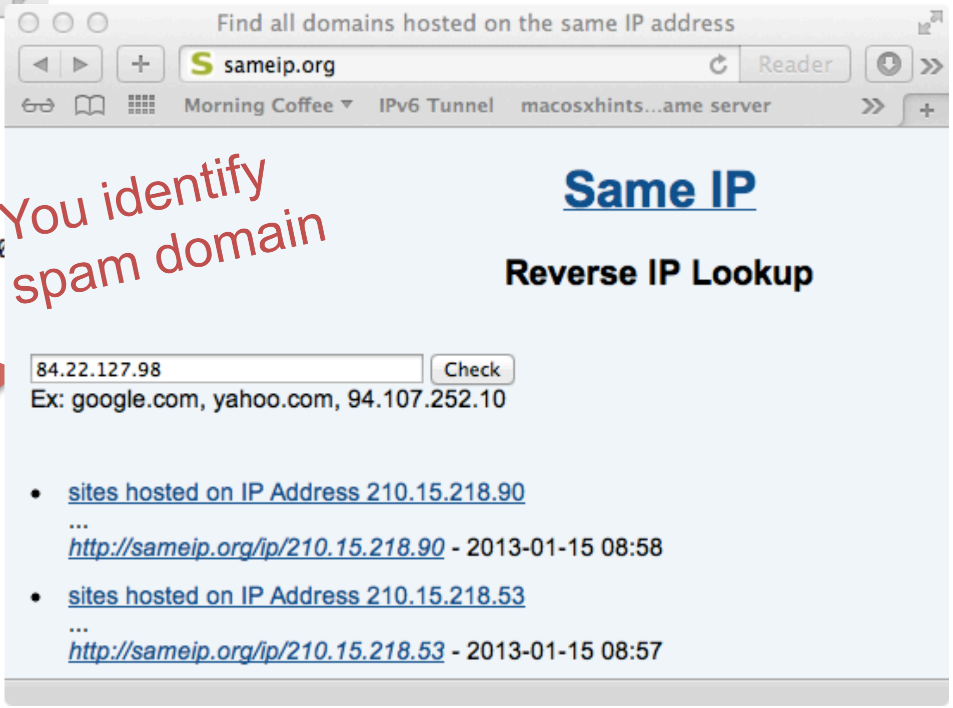
Did someone else report the site?

Case Study: Bad Neighborhood



```
Last login: Tue Jan 15 08:22:05 on ttys000
Davids-MacBook-Air-2:~ dave$ dig www.datestars-girls.ru

; <<>> DiG 9.7.6-P1 <<>> www.datestars-girls.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57427
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.datestars-girls.ru.             IN      A

;; ANSWER SECTION:
www.datestars-girls.ru. 21600   IN      A       84.22.127.98
```

You identify a spam domain



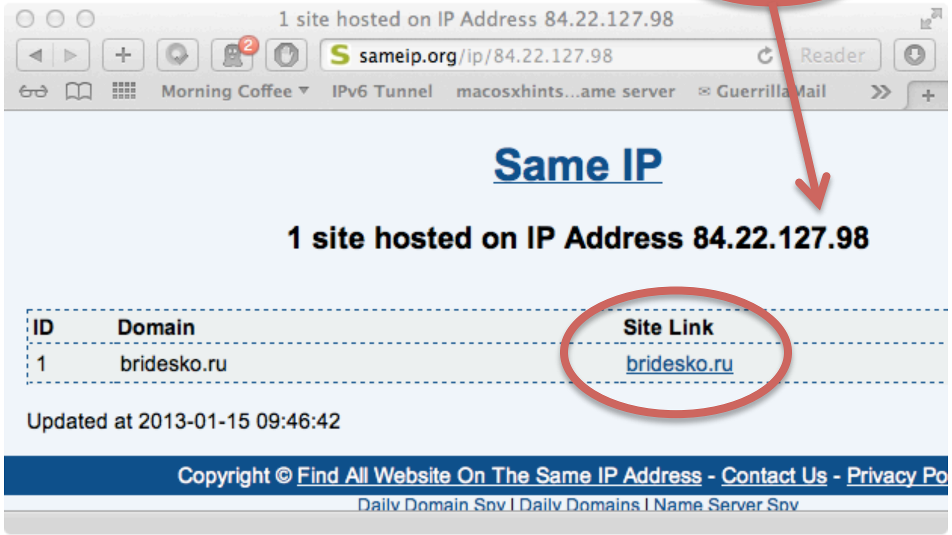
Same IP

Reverse IP Lookup

84.22.127.98 Check

Ex: google.com, yahoo.com, 94.107.252.10

- sites hosted on IP Address 210.15.218.90
  ...
  http://sameip.org/ip/210.15.218.90 - 2013-01-15 08:58
- sites hosted on IP Address 210.15.218.53
  ...
  http://sameip.org/ip/210.15.218.53 - 2013-01-15 08:57



Same IP

1 site hosted on IP Address 84.22.127.98

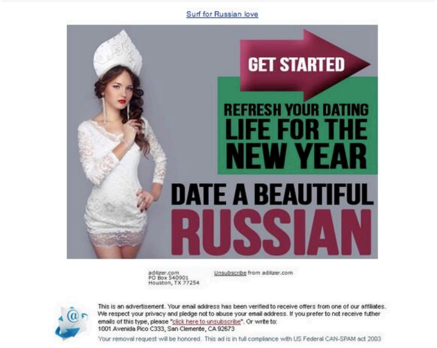
ID	Domain	Site Link
1	bridesko.ru	bridesko.ru

Updated at 2013-01-15 09:46:42

Copyright © Find All Website On The Same IP Address - Contact Us - Privacy Po

Daily Domain Spy | Daily Domains | Name Server Spy

And…
more
Russian brides

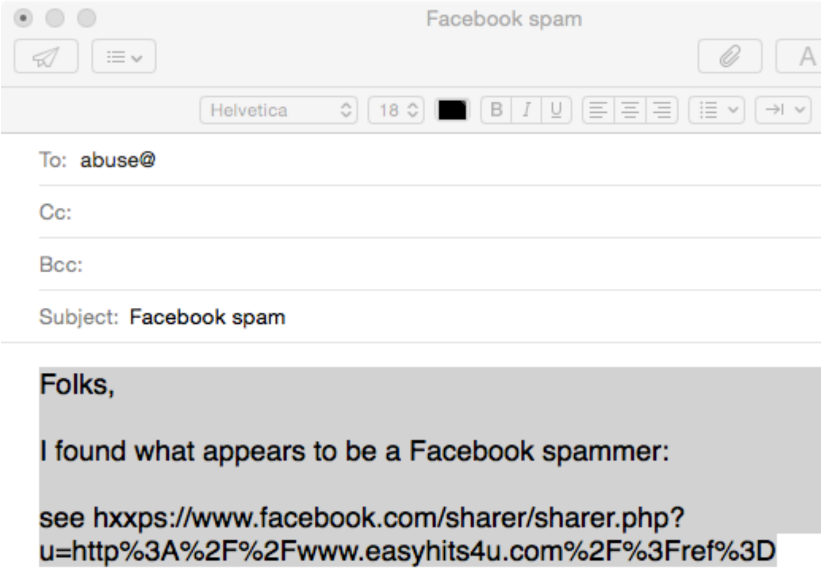

Surf for Russian love

adilzer.com
PO Box 540901
Houston, TX 77254

Unsubscribe from adilzer.com

This is an advertisement. Your email address has been verified to receive offers from one of our affiliates. We respect your privacy and pledge not to abuse your email address. If you prefer to not receive futher emails of this type, please "click here to unsubscribe". Or write to:
1001 Avenida Pico C333, San Clemente, CA 92673
Your removal request will be honored. This ad is in full compliance with US Federal CAN-SPAM act 2003

Use Case: Google hack Social Media for domain name intel



To: abuse@

Cc:

Bcc:

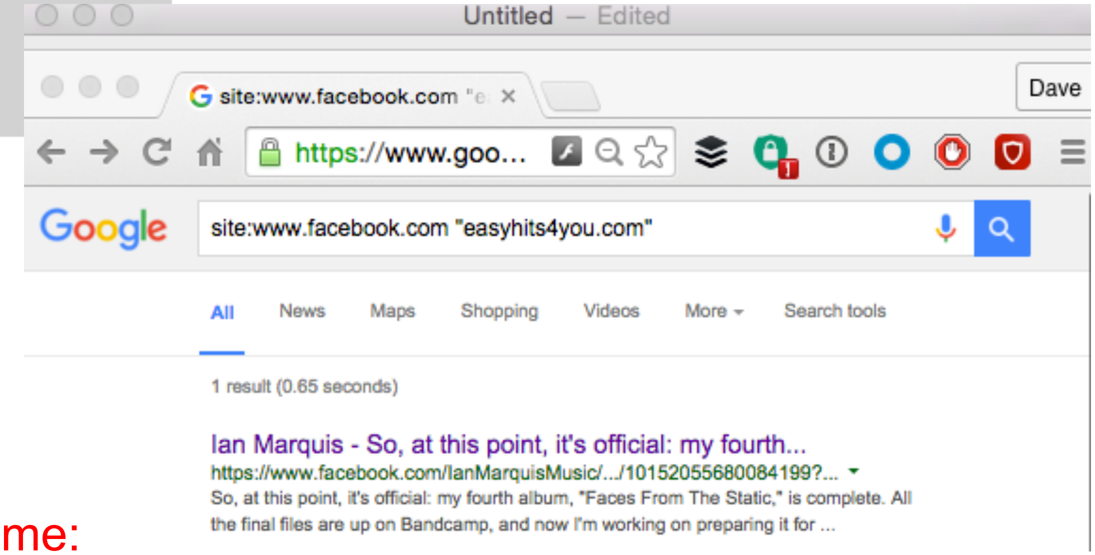
Subject: Facebook spam

Folks,

I found what appears to be a Facebook spammer:

see hxxps://www.facebook.com/sharer/sharer.php?u=http%3A%2F%2Fwww.easyhits4u.com%2F%3Fref%3D

Grab the domain easyhits4u.com from the abuse report,



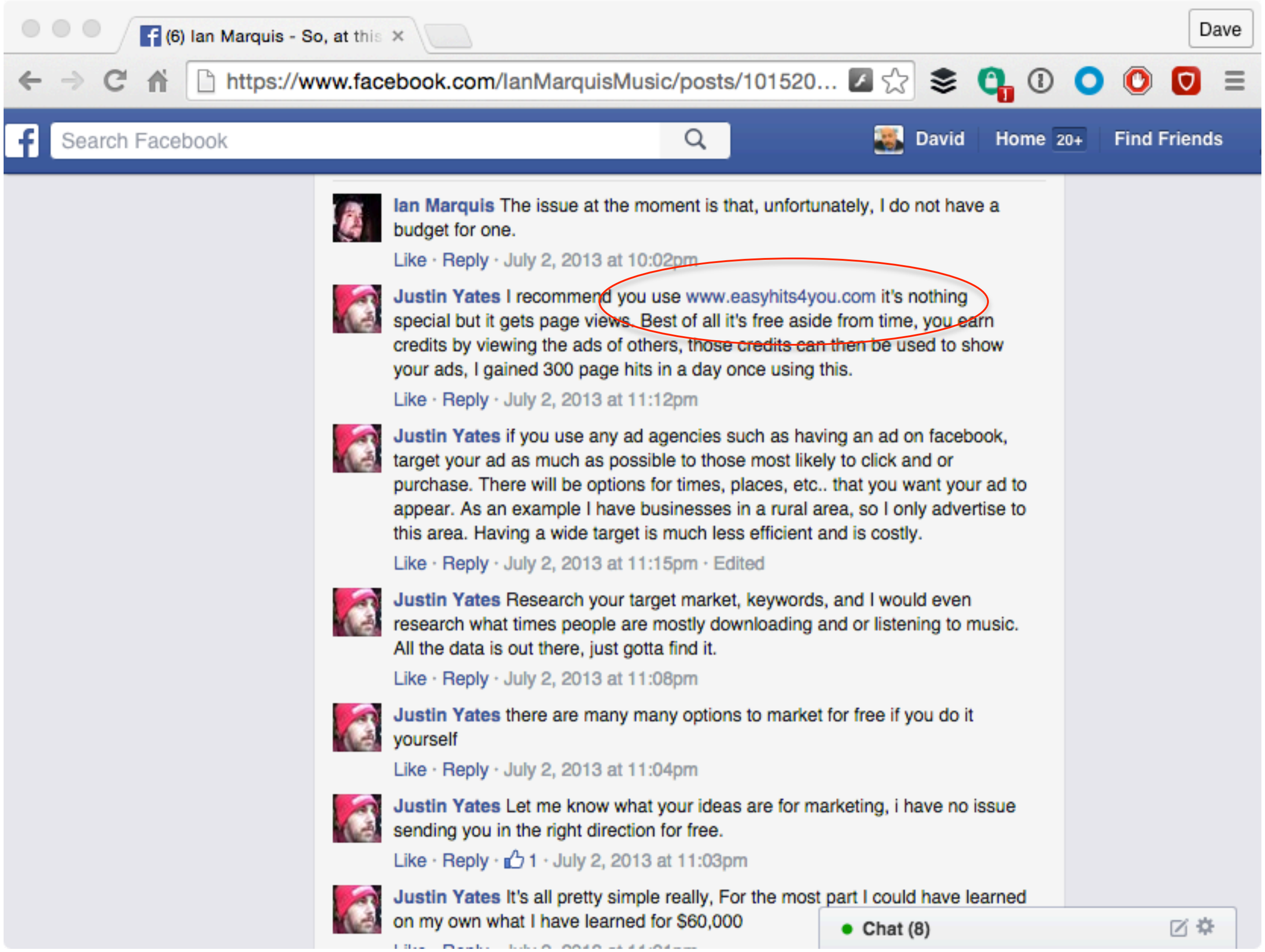
site:www.facebook.com "easyhits4you.com"

1 result (0.65 seconds)

Ian Marquis - So, at this point, it's official: my fourth...
https://www.facebook.com/IanMarquisMusic/.../10152055680084199?...
So, at this point, it's official: my fourth album, "Faces From The Static," is complete. All the final files are up on Bandcamp, and now I'm working on preparing it for ...

Search Facebook for more of same:
site:www.facebook.com "easyhits4you.com"

Use Case: Google hack Social Media for domain name intel


(6) Ian Marquis - So, at this
Dave
https://www.facebook.com/IanMarquisMusic/posts/101520...
Search Facebook
David
Home 20+
Find Friends
Chat (8)

Ian Marquis The issue at the moment is that, unfortunately, I do not have a budget for one.
Like · Reply · July 2, 2013 at 10:02pm

Justin Yates I recommend you use www.easyhits4you.com it's nothing special but it gets page views. Best of all it's free aside from time, you earn credits by viewing the ads of others, those credits can then be used to show your ads, I gained 300 page hits in a day once using this.
Like · Reply · July 2, 2013 at 11:12pm

Justin Yates if you use any ad agencies such as having an ad on facebook, target your ad as much as possible to those most likely to click and or purchase. There will be options for times, places, etc.. that you want your ad to appear. As an example I have businesses in a rural area, so I only advertise to this area. Having a wide target is much less efficient and is costly.
Like · Reply · July 2, 2013 at 11:15pm · Edited

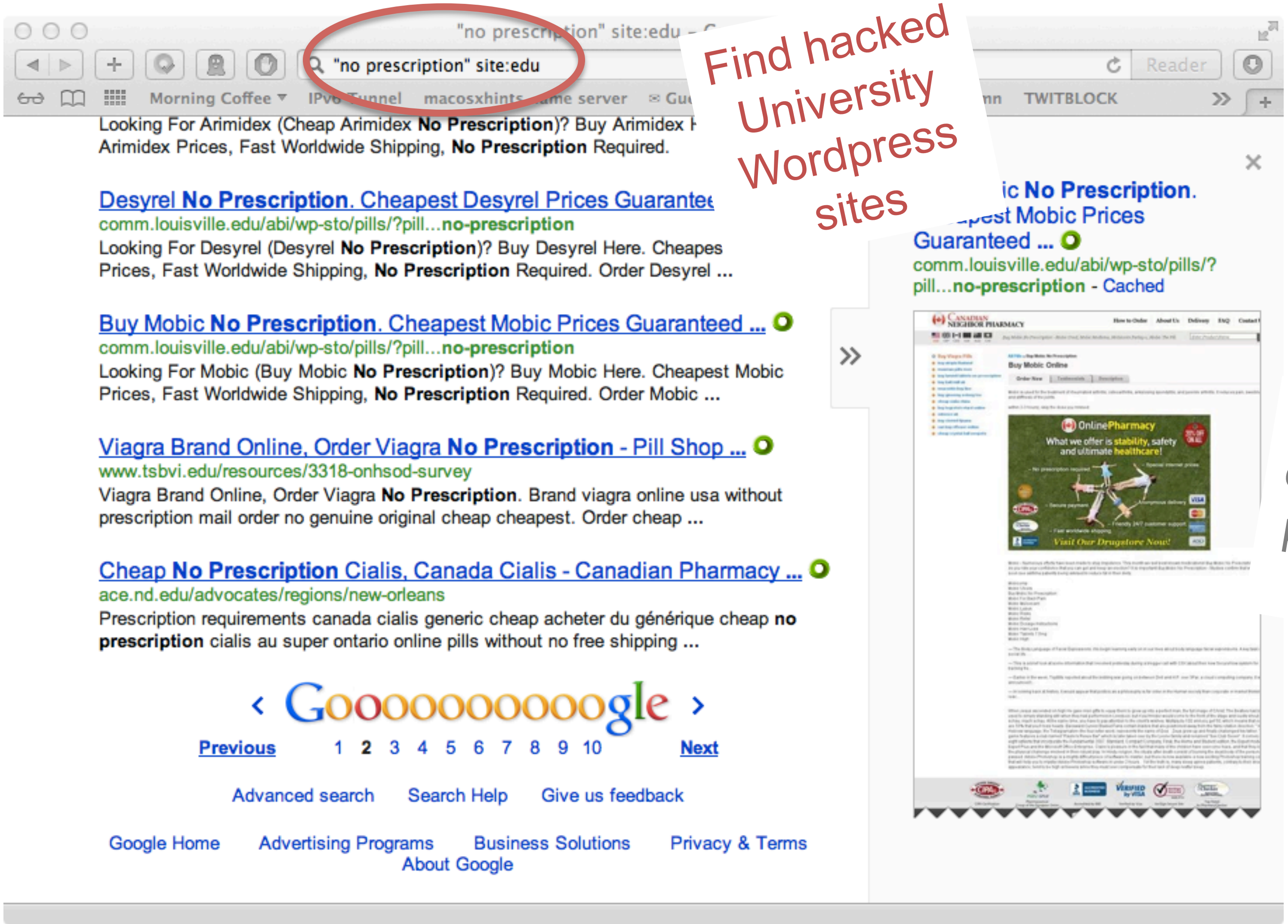
Justin Yates Research your target market, keywords, and I would even research what times people are mostly downloading and or listening to music. All the data is out there, just gotta find it.
Like · Reply · July 2, 2013 at 11:08pm

Justin Yates there are many many options to market for free if you do it yourself
Like · Reply · July 2, 2013 at 11:04pm

Justin Yates Let me know what your ideas are for marketing, i have no issue sending you in the right direction for free.
Like · Reply · 👍 1 · July 2, 2013 at 11:03pm

Justin Yates It's all pretty simple really, For the most part I could have learned on my own what I have learned for $60,000
Like · Reply · July 2, 2013 at 11:01pm

Case study: advanced search operators



Looking For Arimidex (Cheap Arimidex **No Prescription**)? Buy Arimidex H Arimidex Prices, Fast Worldwide Shipping, **No Prescription** Required.

Desyrel **No Prescription**. Cheapest Desyrel Prices Guarantee
comm.louisville.edu/abi/wp-sto/pills/?pill...**no-prescription**
Looking For Desyrel (Desyrel **No Prescription**)? Buy Desyrel Here. Cheapes Prices, Fast Worldwide Shipping, **No Prescription** Required. Order Desyrel ...

Buy Mobic **No Prescription**. Cheapest Mobic Prices Guaranteed ...
comm.louisville.edu/abi/wp-sto/pills/?pill...**no-prescription**
Looking For Mobic (Buy Mobic **No Prescription**)? Buy Mobic Here. Cheapest Mobic Prices, Fast Worldwide Shipping, **No Prescription** Required. Order Mobic ...

Viagra Brand Online, Order Viagra **No Prescription** - Pill Shop ...
www.tsbvi.edu/resources/3318-onhsod-survey
Viagra Brand Online, Order Viagra **No Prescription**. Brand viagra online usa without prescription mail order no genuine original cheap cheapest. Order cheap ...

Cheap **No Prescription** Cialis, Canada Cialis - Canadian Pharmacy ...
ace.nd.edu/advocates/regions/new-orleans
Prescription requirements canada cialis generic cheap acheter du générique cheap **no prescription** cialis au super ontario online pills without no free shipping ...

‹ Goooooooooogle ›
Previous 1 2 3 4 5 6 7 8 9 10 Next

Advanced search Search Help Give us feedback

Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

ic **No Prescription**. ...apest Mobic Prices Guaranteed ...
comm.louisville.edu/abi/wp-sto/pills/?pill...**no-prescription** - Cached

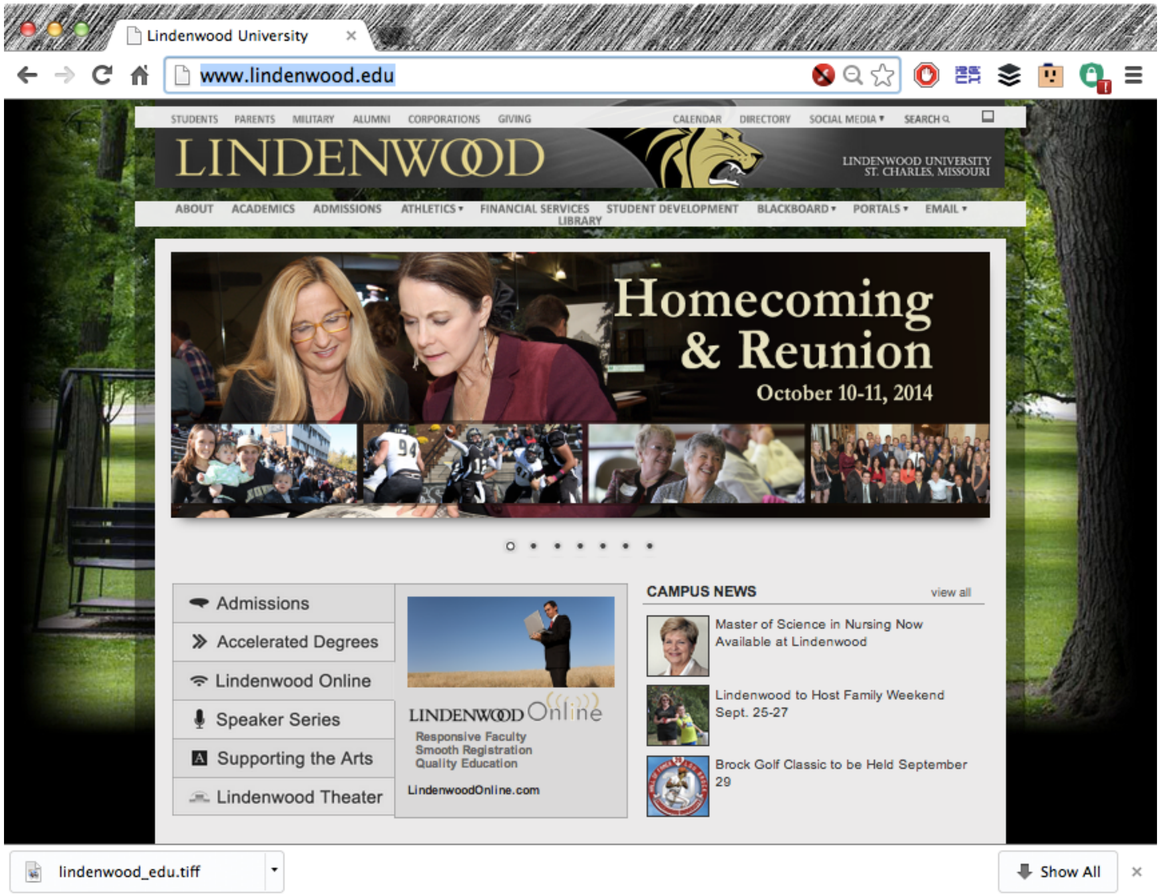
Find hacked University Wordpress sites

Also try the string *"Powered by Wordpress"*

The WOT extension previews page

Case Study: advanced search operators

(1) A search on “no prescription” site:edu returns
hxxp://www.lindenwood.edu/buynolvadexusa/



Master of Science in Nursing Now Available at Lindenwood

Lindenwood to Host Family Weekend Sept. 25-27

Brock Golf Classic to be Held September 29

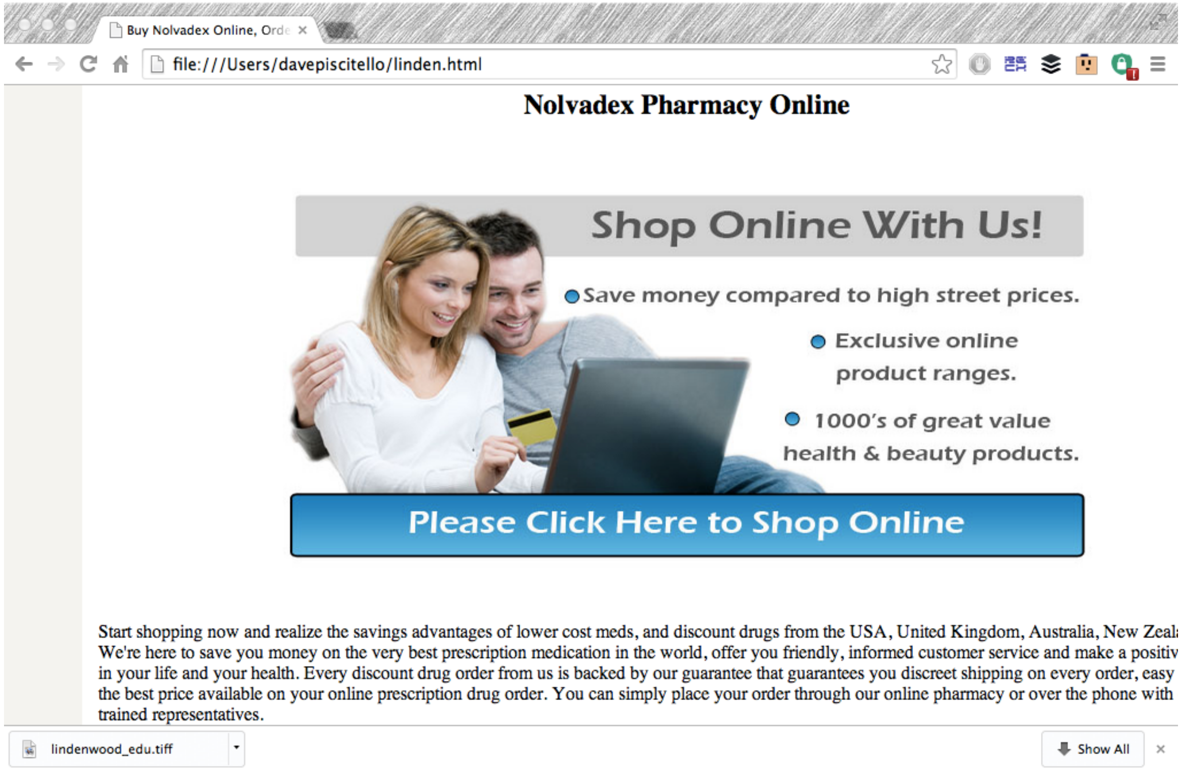
(2) Visit the home page and you see this..

But visit the URL..

Case Study: advanced search operators

(3) curl hxxp://www.lindenwood.edu/buynolvadexusa/ > linden.html

(4) cURL or peepingtom the URL, open the page, and you find:



file:///Users/davepiscitello/linden.html

Nolvadex Pharmacy Online

Shop Online With Us!

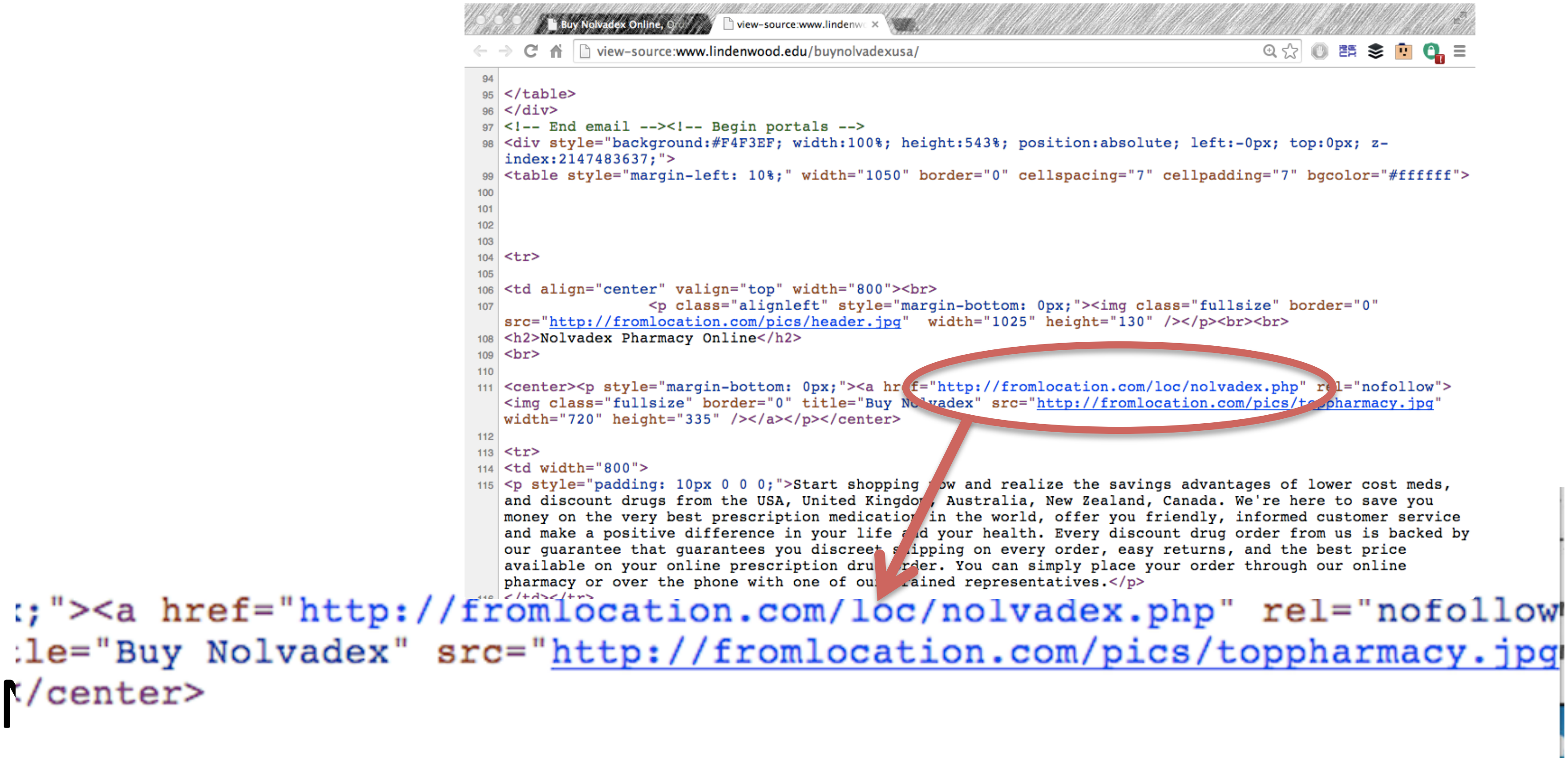
- Save money compared to high street prices.
- Exclusive online product ranges.
- 1000's of great value health & beauty products.

Please Click Here to Shop Online

Start shopping now and realize the savings advantages of lower cost meds, and discount drugs from the USA, United Kingdom, Australia, New Zeal
We're here to save you money on the very best prescription medication in the world, offer you friendly, informed customer service and make a positiv
in your life and your health. Every discount drug order from us is backed by our guarantee that guarantees you discreet shipping on every order, easy
the best price available on your online prescription drug order. You can simply place your order through our online pharmacy or over the phone with
trained representatives.

Case Study: advanced search operators

(5) Locate the link to the affiliate/merchant in the source



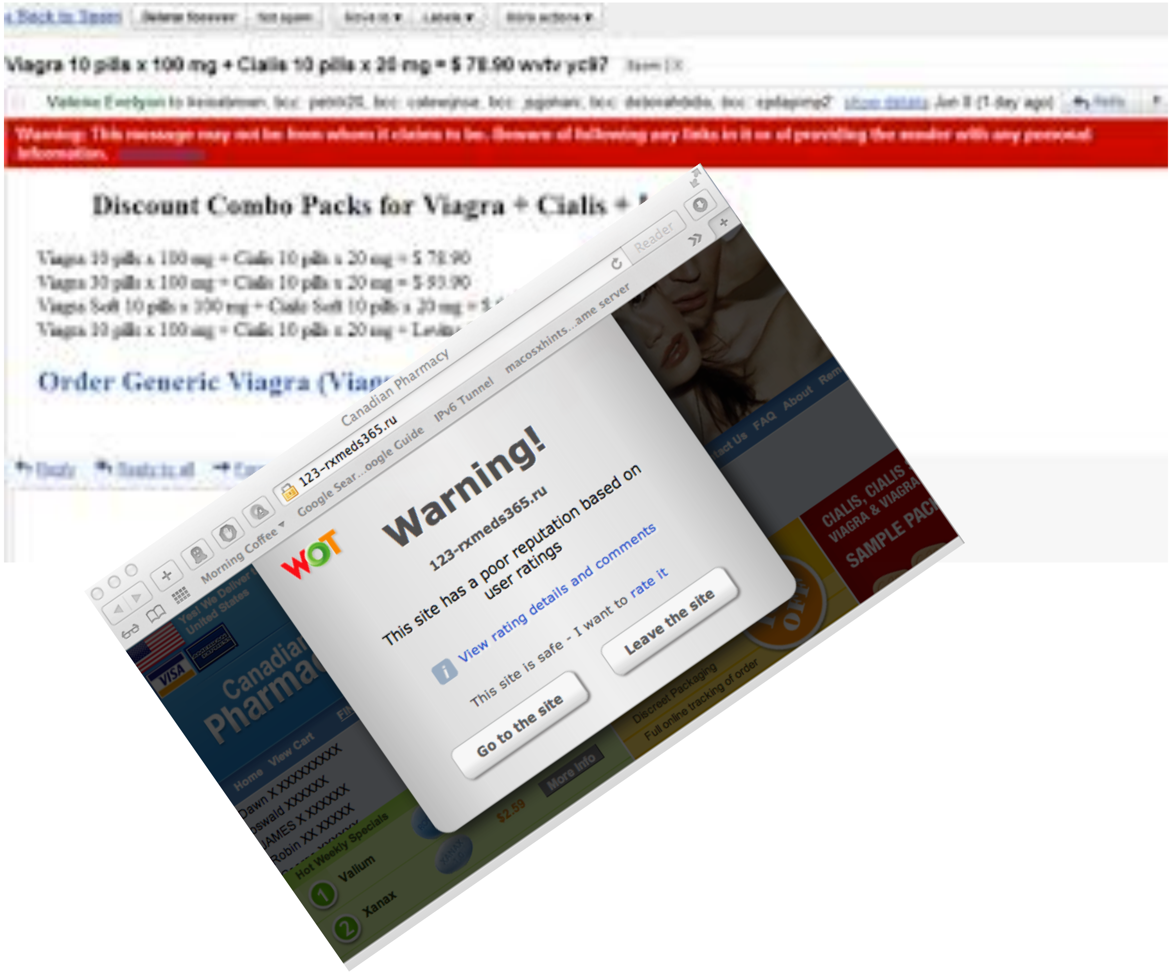
```
</table>
</div>
<!-- End email --><!-- Begin portals -->
<div style="background:#F4F3EF; width:100%; height:543%; position:absolute; left:-0px; top:0px; z-index:2147483637;">
<table style="margin-left: 10%;" width="1050" border="0" cellspacing="7" cellpadding="7" bgcolor="#ffffff">




<tr>

<td align="center" valign="top" width="800"><br>
                <p class="alignleft" style="margin-bottom: 0px;"><img class="fullsize" border="0" src="http://fromlocation.com/pics/header.jpg"  width="1025" height="130" /></p><br><br>
<h2>Nolvadex Pharmacy Online</h2>
<br>

<center><p style="margin-bottom: 0px;"><a href="http://fromlocation.com/loc/nolvadex.php" rel="nofollow"><img class="fullsize" border="0" title="Buy Nolvadex" src="http://fromlocation.com/pics/toppharmacy.jpg" width="720" height="335" /></a></p></center>

<tr>
<td width="800">
<p style="padding: 10px 0 0 0;">Start shopping now and realize the savings advantages of lower cost meds, and discount drugs from the USA, United Kingdom, Australia, New Zealand, Canada. We're here to save you money on the very best prescription medication in the world, offer you friendly, informed customer service and make a positive difference in your life and your health. Every discount drug order from us is backed by our guarantee that guarantees you discreet shipping on every order, easy returns, and the best price available on your online prescription drug order. You can simply place your order through our online pharmacy or over the phone with one of our trained representatives.</p>
</td></tr>
```

```
;"><a href="http://fromlocation.com/loc/nolvadex.php" rel="nofollow
le="Buy Nolvadex" src="http://fromlocation.com/pics/toppharmacy.jpg
/center>
```

Final lap

one last walk through the methodology

Use case: Is this an illegal pharma site?



Viagra 10 pills x 100 mg + Cialis 10 pills x 20 mg = $ 78.90 wvtv yc87

Jun 8 (1 day ago)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information.

Discount Combo Packs for Viagra + Cialis +

Viagra 10 pills x 100 mg + Cialis 10 pills x 20 mg = $ 78.90
Viagra 30 pills x 100 mg + Cialis 10 pills x 20 mg = $ 93.90
Viagra Soft 10 pills x 100 mg + Cialis Soft 10 pills x 20 mg = $
Viagra 10 pills x 100 mg + Cialis 10 pills x 20 mg + Levitra

Order Generic Viagra (Viagr

Warning!

123-rxmeds365.ru

This site has a poor reputation based on user ratings

View rating details and comments

This site is safe - I want to rate it

Recreational pharma spam leads to a site that's blocked by MyWOT

What can we use to confirm that 123-rxmeds365.ru is a malicious domain?

Use case: Is this an illegal pharma site?

dig (nslookup) the domain name from the URL

```
•   % dig 123-rxmeds365.ru
•   ;; QUESTION SECTION:
•   ;123-rxmeds365.ru.      IN   A

•   ;; ANSWER SECTION:
•   123-rxmeds365.ru.       300  IN   A    129.7.240.229
•   123-rxmeds365.ru.       300  IN   A    198.61.167.175
•   123-rxmeds365.ru.       300  IN   A    173.248.130.201
•   123-rxmeds365.ru.       300  IN   A    173.230.229.219

•   ;; AUTHORITY SECTION:
•   123-rxmeds365.ru. 345598   IN   NS
     ns4.bestrxfast365.ru.
•   123-rxmeds365.ru. 345598   IN   NS
     ns1.directrx724.com.
•   123-rxmeds365.ru. 345598   IN   NS   ns2.toprxbest.com.
•   123-rxmeds365.ru. 345598   IN   NS
     ns3.myfavoriterx724.ru.

•   ;; ADDITIONAL SECTION:
•   ns4.bestrxfast365.ru.  345598   IN   A    108.170.47.235
•   ns2.toprxbest.com. 172798   IN   A    63.143.54.116
•   ns3.myfavoriterx724.ru.    345598   IN   A
     68.73.80.135
•   ns1.directrx724.com.   172798   IN   A    64.31.37.232
```

Short TTLs
In A records
(*fast flux?*)

"Red flag" TLD,
"Pharma" label
Check Whois?
Dig SOA record?

Use case: Is this an illegal pharma site?

Even Incomplete Whois Tells
You Something – Nameservers!

```
[whois.ripn.net]
  domain:        123-RXMEDS365.RU
  nserver:       ns1.directrx724.com.
  nserver:       ns2.toprxbest.com.
  nserver:       ns3.myfavoriterx724.ru.
  nserver:       ns4.bestrxfast365.ru.
  state:         REGISTERED, DELEGATED, UNVERIFIED
  person:        Private Person
  registrar:     NAUNET-REG-RIPN
  admin-contact: https://client.naunet.ru/c/whoiscontact
  created:       2012.02.19
  paid-till:     2013.02.19
  free-date:     2013.03.22
  source:        TCI
```

What raises suspicion?

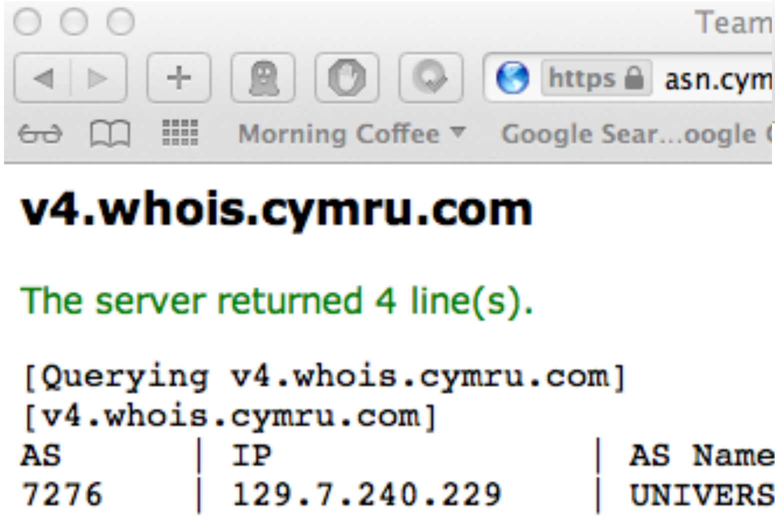
- Private registration?
- Registry reputation?
- Registrar reputation?
- Creation date (How recent?)
- Name servers?

Use case: Is this an illegal pharma site?

What can we learn from IP Whois?

```
% dig 123-rxmeds365.ru
;; QUESTION SECTION:
;123-rxmeds365.ru.          IN   A

;; ANSWER SECTION:
123-rxmeds365.ru.     300  IN   A     129.7.240.229
123-rxmeds365.ru.     300  IN   A     198.61.167.175
123-rxmeds365.ru.     300  IN   A     173.248.130.201
123-rxmeds365.ru.     300  IN   A     173.230.229.219
```

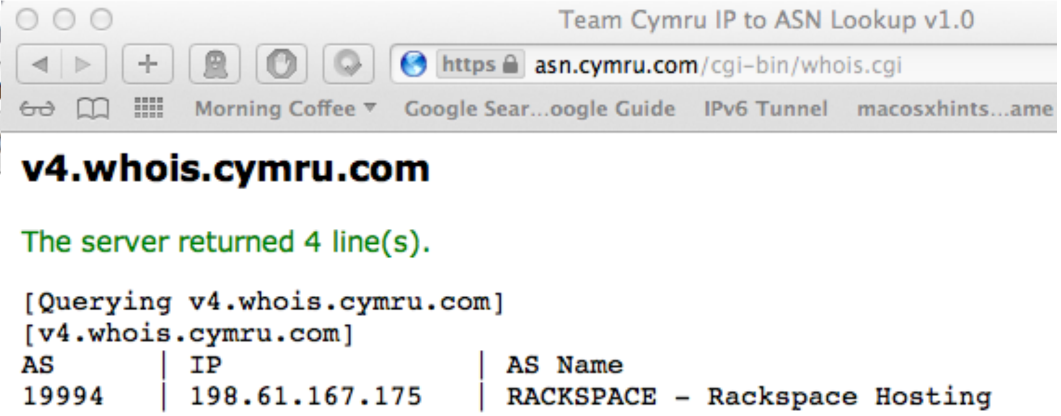
Domain is hosted on 4 different IPs in 4 different ASNs



v4.whois.cymru.com

The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
AS       | IP                | AS Name
7276     | 129.7.240.229     | UNIVERSITY-OF-HOUSTON - Univers
```


Team Cymru IP to ASN Lookup v1.0
https asn.cymru.com/cgi-bin/whois.cgi
Morning Coffee
Google Sear...oogle Guide
IPv6 Tunnel
macosxhints...ame

v4.whois.cymru.com

The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
AS       | IP                | AS Name
19994    | 198.61.167.175    | RACKSPACE - Rackspace Hosting
```

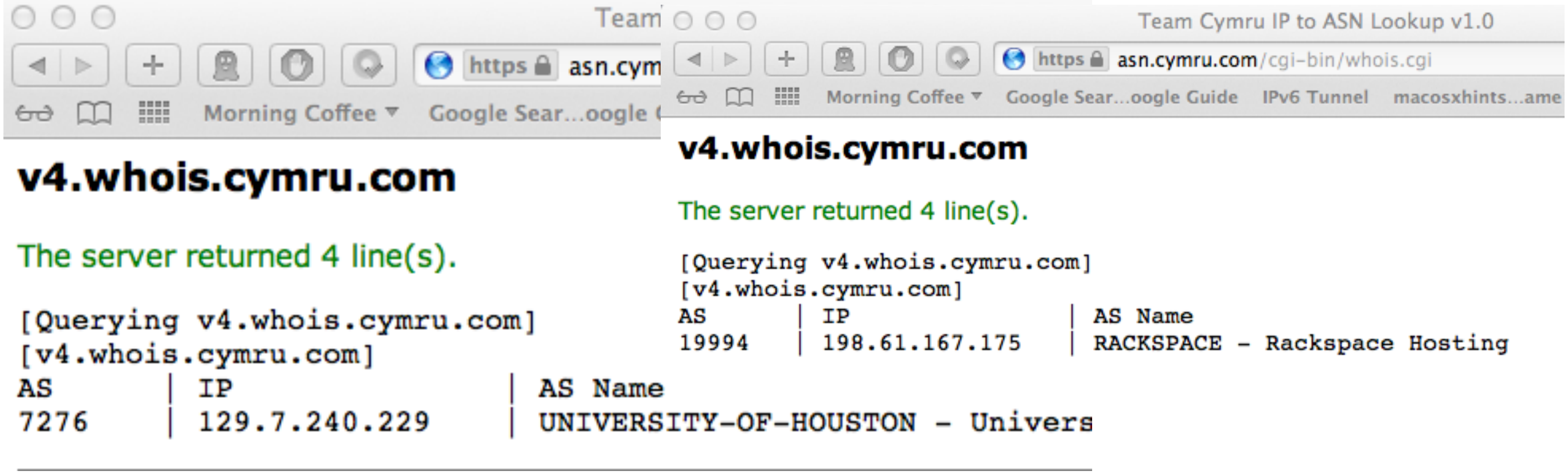
Other IPs are in Softsys Hosting, Baroda India via WeHostWebSites and Globalweb Outsourcing Corp, Aventura FL via

Use case: Is this an illegal pharma site?

What can we learn from IP Whois?

```
% dig 123-rxmeds365.ru
;; QUESTION SECTION:
;123-rxmeds365.ru.          IN   A

;; ANSWER SECTION:
123-rxmeds365.ru.     300   IN   A    129.7.240.229
123-rxmeds365.ru.     300   IN   A    198.61.167.175
123-rxmeds365.ru.     300   IN   A    173.248.130.201
123-rxmeds365.ru.     300   IN   A    173.230.229.219
```

Domain is hosted on 4 different IPs in 4 different ASNs


Team Cymru IP to ASN Lookup v1.0
https asn.cymru.com/cgi-bin/whois.cgi
Morning Coffee
Google Sear...oogle Guide
IPv6 Tunnel
macosxhints...ame

v4.whois.cymru.com

The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
AS      | IP               | AS Name
7276    | 129.7.240.229    | UNIVERSITY-OF-HOUSTON - Univers
```

v4.whois.cymru.com

The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
AS      | IP               | AS Name
19994   | 198.61.167.175   | RACKSPACE - Rackspace Hosting
```

Other IPs are in Softsys Hosting, Baroda India via WeHostWebSites and Globalweb Outsourcing Corp, Aventura FL via

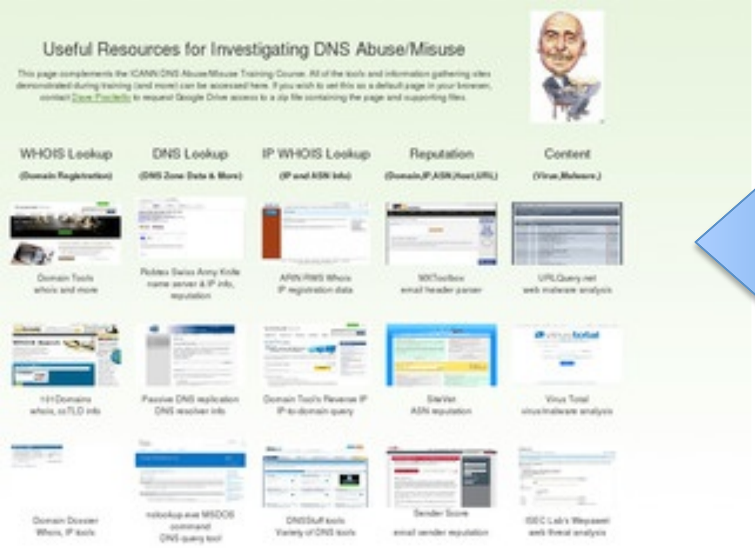
To get involved or get help

- Mailing lists
  - Regops (see Rod)
  - NX-Domains (ask around)
  - Various trust groups
- ICANN Compliance (RAA, Registry)
- ICANN Security Team (Coordination, Technical)
- ICANN working groups (PSWG
- FIRST and CERTs
- APWG, MAAWG, and other industry groups

Acknowledgements

These training materials are not the work of one but many. In particular, these individuals have contributed directly or by sharing their expertise or providing access to data feeds:		
Greg Aaron	Carlos Alvarez	Jeff Chan
Steve Conte	John Crain	Paolo Dal Checco
Susan Prosser	Rod Rasmussen	Sandro Rosetti
Joe St. Sauver	Gary Warner	Paul Vixie

You can’t possibly remember all these hyperlinks!



Useful Resources for Investigating DNS Abuse/Misuse

This page complements the ICANN DNS Abuse/Misuse Training Course. All of the tools and information gathering sites demonstrated during training (and more) can be accessed here. If you wish to set this as a default page in your browser, contact Dave Piscitello to request Google Drive access to a zip file containing the page and supporting files.

WHOIS Lookup (Domain Registration)	DNS Lookup (DNS Zone Data & More)	IP WHOIS Lookup (IP and ASN Info)	Reputation (Domain,IP,ASN,Host,URL)	Content (Virus,Malware,)
Domain Tools whois and more	Robtex Swiss Army Knife name server & IP info, reputation	ARIN RWS Whois IP registration data	MXToolbox email header parser	URLQuery.net web malware analysis
101Domains whois, ccTLD info	Passive DNS replication DNS resolver info	Domain Tool's Reverse IP IP-to-domain query	SiteVet ASN reputation	Virus Total virus/malware analysis
Domain Dossier Whois, IP tools	nslookup aka MSDOS command DNS query tool	DNSStuff tools Variety of DNS tools	Sender Score email sender reputation	ISEC Lab's Wepawet web threat analysis

So bookmark this page in your browser

http://securityskeptic.com/the-security-skeptic/investigatingdnsabusejs.html or

http://safe.mn/FknC

Questions?

Contacts:
email: dave.piscitello@icann.org
twitter: @securityskeptic

web: securityskeptic.com

company: icann.org

ICANN Security Team:
icann.org/resources/pages/security-2012-02-25-en