Internet Traffic Analysis and Operational Security: Passive DNS Methods As Powerful Tools to Investigate and Corroborate

Cybersecurity: Technology and the Law
Portland Marriott Downtown Waterfront
3:00-4:00 PM, Thursday, August 13, 2015

Joe St Sauver, Ph.D. (stsauver@fsi.io)
Distributed System Scientist, Farsight Security, Inc.

https://www.stsauver.com/joe/cybersec-tech-and-law/

1. Introduction

Thanks

- I'd like to begin by thanking you for attending, and thanking Sean Hoar for the opportunity to speak with you today.

- Sean and I go back a ways – he was an Assistant US Attorney for the US Department of Justice, and DOJ's lead cyber attorney in Oregon; he was also an adjunct faculty member at the University of Oregon School of Law, teaching cyber crime and related courses.

- I know Sean from those roles, and it has always been a pleasure and an honor to engage with him on cyber security-related projects such as today's seminar.

- I'd also like to thank Ms. Nici Dawber from Law Seminars for her patience with me when it comes to logistics, etc.

A Little About My Background

- I'm a scientist for Paul Vixie's new company, **Farsight Security, Inc. (FSI).** Farsight operates **DNSDB,** the world's most comprehensive and trusted source of passive DNS data. See https://www.farsightsecurity.com/ for more information.
- I previously worked for nearly 28 years for the **University of Oregon**, including working for over eight years under a UO contract with **Internet2** as their Nationwide Security Programs Manager. (Internet2 is higher ed's high speed nationwide backbone, with most connections running at 10 to 100 Gbps).
- Among other things, I'm also one of half a dozen Senior Technical Advisor for the Messaging, Malware and Mobile Anti-Abuse Working Group (**M3AAWG**). M3AAWG's a global industry group representing over 1 billion mailboxes worldwide
- My Ph.D. is in Production and Operations Management from UO.
- If you're bored, lots more at https://www.stsauver.com/joe/

Today's Audience

- When putting together a session like today's, I always try to keep my audience in mind.
- My understanding is that many of you will likely be attorneys, or people actively supporting the work of those who are members of the Bar.
- As such, I'm going to try to hit a technical level that will meet your needs.
- If I provide too much backfill for some of you, sorry about that. If I dive into something that's totally alien to you without laying proper foundation, please speak up, do <u>not</u> just suffer in silence! Feel free to ask questions!
- Towards the end of this talk we will "geek out" a little. By that point, if your head is full, feel free to tune out (I wanted to include at least a little in the way of geeky content for any tech folks in the room).

The Format of My Talks

- Traditionally, PowerPoint talks have a limited amount of text, which then gets "amplified" during delivery. **That's fine for non-technical material, but a poor model for tech content, where there's often a lot of detail.** That's one reason I use my more verbose slide format (don't worry, I won't read my slides to you).
- While it takes time to build detailed slides, I do so so that **you don't need to take notes**, and so you can **share these slides** with colleagues who aren't here.
- Having detailed slides gives me a chance of covering what I want to cover, not getting sidetracked, and finishing on time. If not, you'll at least have a copy of what I was *going to* ***try*** to cover.
- Finally, I'm also committed to making my material accessible to <u>everyone</u>, including the deaf and hard-of-hearing. Thus, think of these slides as providing **"closed captioning"** for my comments.

Defanged Domain Representation

- In some areas of this talk I may show selected domains in the format: example[dot]com

  I do this to ensure that those domains aren't accidentally visited, and to ensure they don't get "noticed" when this file gets emailed or otherwise transfered.

- Mentally read the "[dot]" as being "decimal point"

- The [dot] will NOT actually show up in output from commands.

- If you try putting the [dot] (written as such) into commands you enter, it WON'T work (any [dot] needs to be written as a regular "." if you intentionally want to visit that domain).

2. Why Has Cybercrime Become Such A Problem?

Criminals Really <u>Like</u> Doing Business Online

- Opportunities are **everywhere**
- Startup is **easy** (and entry costs are minimal)
- They have access to **worldwide** markets full of potential victims/ customers
- Likelihood of a new criminal enterprise succeeding is **high**
- Payoff for many online schemes is **potentially substantial**
- Risks to the criminal? Sadly, all-too-often, those are **MINIMAL:**
  - Low risk of personal injury for a cyber criminal (unlike muggings or armed robberies, where victims may resist and fight back)
  - Low risk of arrest (unless you become truly notorious) -- so many cyber criminals, so little time
  - Even if a cyber criminal is arrested and convicted, like most white collar crimes, they normally wouldn't be facing a long prison term
- **Is anyone here actually surprised that online crime is thriving?**

The Fundamental Challenge: Attributability

- "On the Internet, no one knows you're a dog." Many actions, including many illegal actions, may be anonymous, or nearly so.

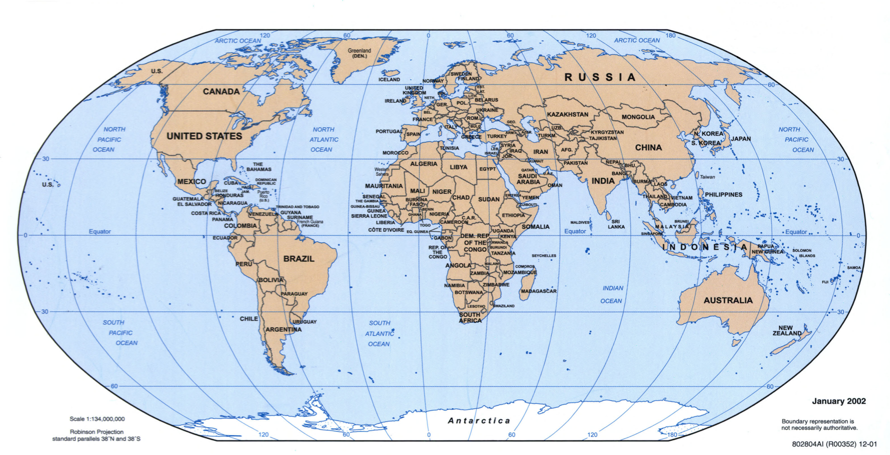
- Cyber criminals try to commit their online crimes **anonymously, leaving few (if any) leads,** thereby avoiding **being identified, and arrested or sued.**

- Law enforcement officers (LEOs), civil investigators, and others need to **pierce that veil** and **bring offenders to justice**. Doing so normally means (a) documenting illegal online behaviors,
  (b) tying that unlawful activity to an online identity, and
  (c) connecting that online ID to a real world identity.

- This can be hard. There may be many investigative and prosecutorial challenges that need to be overcome.

An Investigative Challenge: Diverse Jurisdictions

- A US victim may be attacked
  -- by a Russian citizen,
  -- working from Germany,
  -- using Brazilian malware,
  -- with their servers in China,
  -- and their proceeds sent to
  banks in the Cook Islands.



- "No reason" ***that*** might be hard to investigate/prosecute, right?
- U.S. LEOs or other investigators will typically not have direct jurisdiction in any of those countries, and may need to use the relatively slow and cumbersome MLAT process, instead.
- Now add in lagging legal frameworks, language issues, time zone challenges, corruption, differing enforcement priorities, travel budgets, etc. -- it can be very hard to prosecute online criminals.

(image: http://commons.wikimedia.org/wiki/File:CIA_Political_World_Map_2002.jpg)

A 2nd Investigative/Prosecutorial Challenge: Scale

- A cyber criminal might drop malware on literally hundreds of thousands or even millions of vulnerable systems. This is a scale of victimization that's rarely seen in non-cyber crimes.
  – Because of that scale, <u>per-victim</u> losses may be small, even though <u>aggregate</u> losses may total tens of millions of dollars.

- Coping with evidentiary issues for crimes of this breadth can also be overwhelming, even for investigators and prosecutors who leverage the latest technological options. You may find yourself tackling tasks that require automation, not mere due diligence.

- Infrastructure can be at mass scale, too. A cyber criminal might have thousands – or tens of thousands – of sites online. Obviously it might be hard to find and arrange to take down all those sites at the same time you arrest the bad guys.

A Final Example of An Investigative/Prosecutorial Challenge: Technical Sophistication

- Many cyber crimes are technically challenging, exploiting subtle vulnerabilities or requiring extensive background to fully understand. These flaws can be challenging even for experts to 'grok,' and we shouldn't (and can't!) expect most investigators, prosecutors, defense attorneys, judges, and juries to be expert.
- Many may (at least initially) lack the technical background required to assess technically complex attacks.
- Expert witnesses can help provide some badly-needed backfill, but expert witnesses do not represent a total solution.
- Being prepared to competently prosecute (or defend) a complex technical cyber crime case requires a long term commitment to acquiring and maintaining needed technical knowledge and skills. We hope today's session is a step in the right direction.

3. Finding Initial Leads

An Initial Lead

- Many investigations begin with a report or "complaint" documenting a criminal offense: "I've been ripped off online..." [There's an annual cybercrime summary from IC3 at https://www.ic3.gov/media/annualreport/2014_IC3Report.pdf summarizing over **<u>269,000</u> complaints for 2014**]
- In other cases, investigators may simply use tools such as **Google, Bing or others search engines** to find "starting points" relevant to their subject matter area of jurisdiction, typically a URL (or web address)
- Why can LEOs easily use search engines to find bad sites?
  - Ironically, while most criminals want to **avoid** attention from law enforcement, bad guys also **need to be easily found in search engines** in order to sell their stuff to their targeted customer base (this assumes that they're not using spam email or other "targeted" marketing techniques).
  - Hard to advertise to "customers," while not <u>also</u> being discoverable by investigators, eh?

What's Often Easily Found In Search Engines?

- **Knock-off merchandise sites (shoes, watches, jewelry, etc.)**
- Pirated software, music, videos, and games
- Scheduled controlled substances (illegal narcotics and other dangerous drugs), sold online without a valid prescription
- Prescription drugs that may not be controlled substances, but which need be tightly controlled due to known side effects (e.g., Accutane, a known teratogen)
- Some of the preceding sites may actually have been set up to rip off attempted purchasers, but there are many other scams, too (4-1-9, "HYIP", pump-and-dump, reshipping scams, etc.)
- Phishing and carding sites ("fullz", etc.)
- Extremist sites, etc.
- This is all on the "regular" Internet... other badness may be on anonymity network-only networks such as I2P or the equivalent.

4. Whois: Basic Investigative Tool #1

Registering a Domain Name

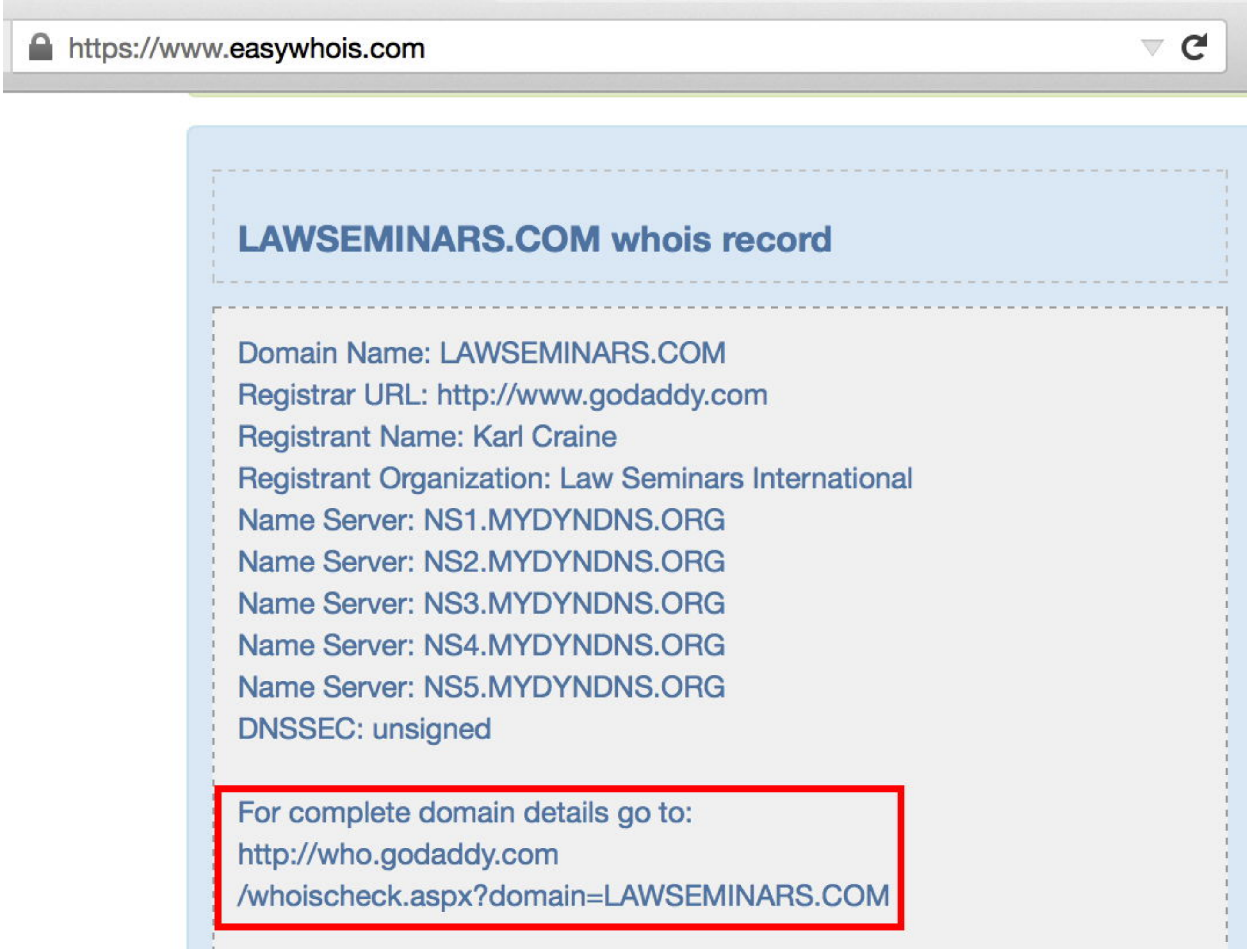
- Services (such as the web) use domain names. Domain names get created ("registered") via registrars. Registrars are commercial companies such as Godaddy, Tucows, etc. There are many registrars you can pick from, depending on the features they offer, their pricing, your personal preferences, etc.
- When you want to create a new domain name, you:
  -- specify the domain name you want to register,
  -- provide (supposedly accurate) point of contact (POC) details,
  -- decide if you want to have those POC details "unlisted" through use of a privacy/proxy registration service
  -- define the authoritative name servers that know how to map your domains to the IP address(es) of your server
  -- pay an annual fee to the registrar (often ~$10/year)
- **Point of contact information and related details about most domains get added to an online database known as "Whois"**

Whois For Domains

- Domain whois tells you "who is" the owner of a domain name, their street address, their email address, phone numbers, etc.
- This is a mission critical service that every investigator routinely uses.
- To do a whois query on a Mac, in a Terminal window enter:

  $ whois *domainname*

- On Windows? See https://technet.microsoft.com/en-us/sysinternals/bb897435.aspx
- There are also domain whois web sites such as https://www.easywhois.com/

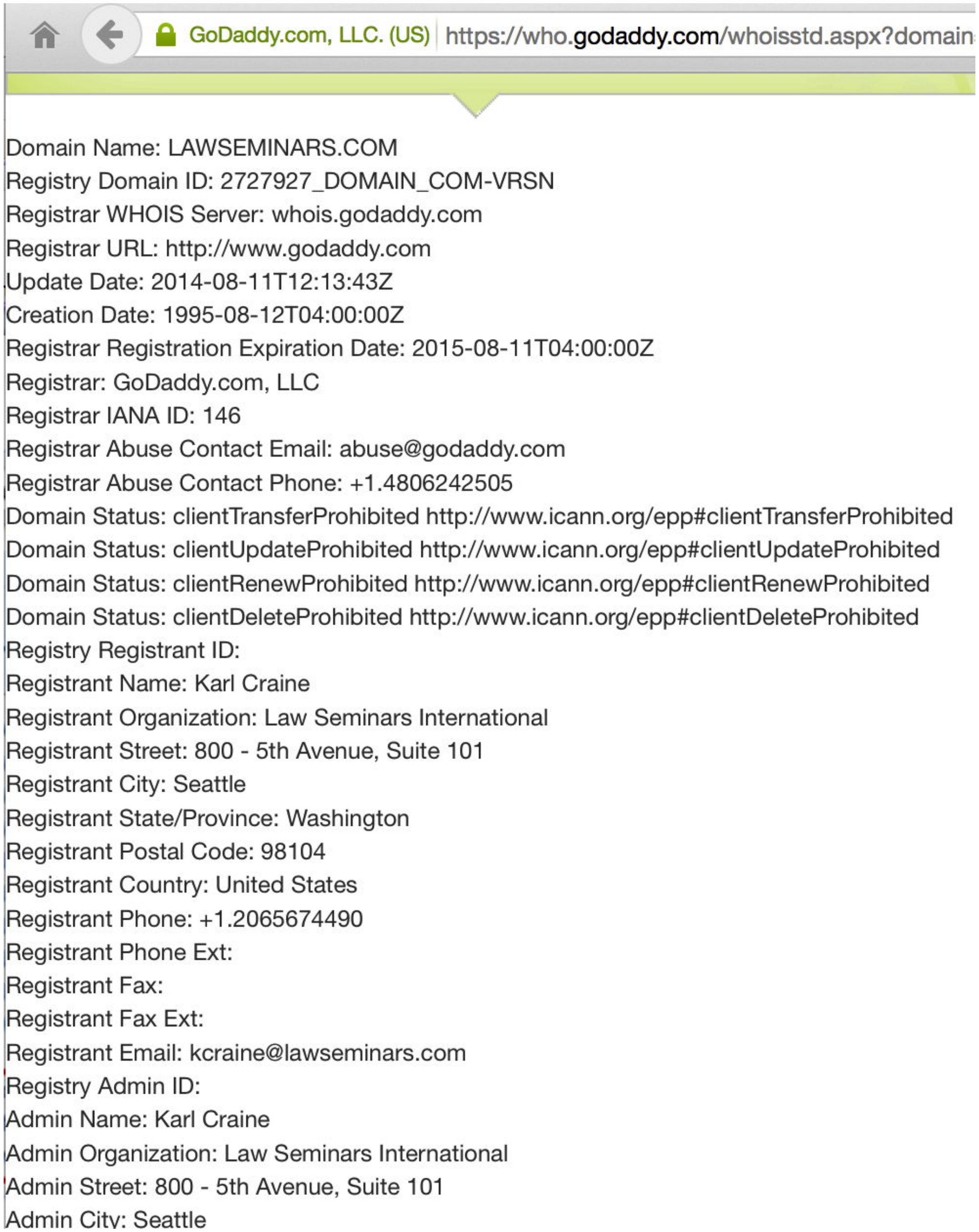


https://www.easywhois.com

LAWSEMINARS.COM whois record

Domain Name: LAWSEMINARS.COM
Registrar URL: http://www.godaddy.com
Registrant Name: Karl Craine
Registrant Organization: Law Seminars International
Name Server: NS1.MYDYNDNS.ORG
Name Server: NS2.MYDYNDNS.ORG
Name Server: NS3.MYDYNDNS.ORG
Name Server: NS4.MYDYNDNS.ORG
Name Server: NS5.MYDYNDNS.ORG
DNSSEC: unsigned

For complete domain details go to:
http://who.godaddy.com
/whoischeck.aspx?domain=LAWSEMINARS.COM



Domain Name: LAWSEMINARS.COM
Registry Domain ID: 2727927_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2014-08-11T12:13:43Z
Creation Date: 1995-08-12T04:00:00Z
Registrar Registration Expiration Date: 2015-08-11T04:00:00Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar 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
Registry Registrant ID:
Registrant Name: Karl Craine
Registrant Organization: Law Seminars International
Registrant Street: 800 - 5th Avenue, Suite 101
Registrant City: Seattle
Registrant State/Province: Washington
Registrant Postal Code: 98104
Registrant Country: United States
Registrant Phone: +1.2065674490
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kcraine@lawseminars.com
Registry Admin ID:
Admin Name: Karl Craine
Admin Organization: Law Seminars International
Admin Street: 800 - 5th Avenue, Suite 101
Admin City: Seattle

Whois and Real World Identities?

- Registering a domain may result in the domain registrant leaving clues to their "real world"/"meat space" identity in whois:

  -- their **name** (but the claimed name may be a totally bogus one, or someone else's name used without authorization)

  -- a **street address** (but is that address a 3rd party mail drop? incomplete? totally fictitious? etc.)

  -- a **phone number** (but it may be a prepaid "burner" phone)

  -- an **email address** (but that may be a throw away email address from a free provider, used once and then never touched again)

- If you have the ability to get a court order, you can also get:

  -- their **credit card number** (but that may be a stolen card, or a prepaid card, or maybe they paid using Bitcoin),

  -- an **IP address** from which they placed their order, etc.

Some Info (Such As Addresses) May Be Inaccurate

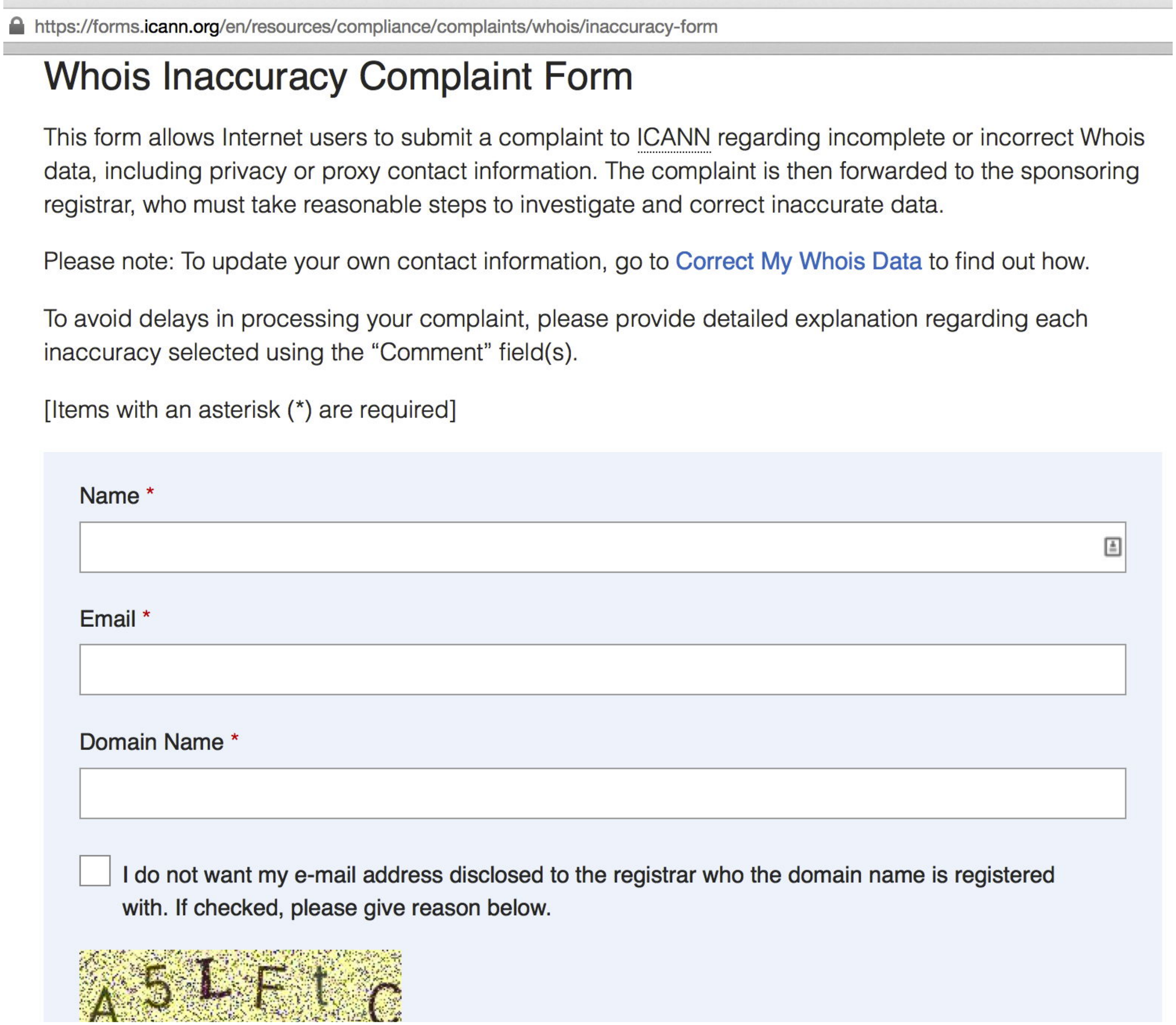
- If contact details are demonstrably inaccurate in a domain's whois data, that inaccuracy can be used as a basis for suspending the domain unless those inaccuracies get corrected.

- Note the "bind" this creates – criminals have a choice between:

  -- having **accurate** contact information (tying a resource to them, which means that they can be identified and potentially held accountable), or

  -- using a **bogus** identity for things like registering their domains (which means that they may lose access to their domains if anyone bothers to investigate and complain)

Complaining About Inaccurate gTLD Whois Info



https://forms.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form

Whois Inaccuracy Complaint Form

This form allows Internet users to submit a complaint to ICANN regarding incomplete or incorrect Whois data, including privacy or proxy contact information. The complaint is then forwarded to the sponsoring registrar, who must take reasonable steps to investigate and correct inaccurate data.

Please note: To update your own contact information, go to Correct My Whois Data to find out how.

To avoid delays in processing your complaint, please provide detailed explanation regarding each inaccuracy selected using the "Comment" field(s).

[Items with an asterisk (*) are required]

Name *

Email *

Domain Name *

□ I do not want my e-mail address disclosed to the registrar who the domain name is registered with. If checked, please give reason below.

Proxy/Privacy Services

- Or people can try to hide behind a domain proxy/privacy service
- Proxy/privacy protection may be free (bundled with a domain's registration), or offered as an extra cost service.
- Proxy/privacy services allow registrants to conceal their contact details from public display
- Even if used, LEOs can still seek a court order to strip a domain's proxy/privacy status or to directly obtain underlying details (but this can be a pain & underlying details may still be bogus or require additional deobfuscation (see (www.securityskeptic.com/2015/07/how-to-register-a-gtld-domain-name-without-disclosing-personal-data.html)
- Some proxy/privacy service providers may have TOS which allow them to unilaterally remove protections for a domain (if a domain is obviously being misused, e.g. for phishing or CSAMs)

ccTLDs

- ICANN administers "global top level domains" ("gTLDs") such as dot com, dot net, dot org, dot biz, dot info, etc.). ICANN requires whois service (although they permit privacy/proxy registrations)
- There are also "country code" TLDs, or "ccTLDs". **ccTLDs are run according to their own rules.** Some of them have polices which limit public access to the whois data for any/all of their domains:
  -- whois information may only be available via a web form, perhaps only usable by registered users. In other cases, users may need to decode a hard-to-read CAPTCHA for each domain
  -- some whois information may be displayed in graphical format to hinder automated "scraping"/cut-n-pasting of whois data
  -- whois access may be strictly rate limited, with access slowed or blocked altogether after just a handful of domains are checked from the same IP address.
  -- in other cases, whois information may not exist at all.

Example of a ccTLD With Limited Public Information

```
$ whois canadianmedsprogram[dot]ru
```

```
domain:         CANADIANMEDSPROGRAM[dot]RU
nserver:        ns1.canadianmedsprogram[dot]ru. 93.189.41.138
nserver:        ns2.canadianmedsprogram[dot]ru. 202.78.227.138
state:          REGISTERED, DELEGATED, VERIFIED
person:         Private Person
registrar:      R01-RU
admin-contact:      https://partner.r01.ru/contact_admin.khtml
created:        2015.07.03
paid-till:      2016.07.03
free-date:      2016.08.03
source:         TCI
```

Commercial Bulk Whois Service Providers

- High volume whois usage becomes easier if you use a commercial bulk domain whois service
- Commercial bulk whois service providers specialize in acting as whois "data brokers," collecting and parsing whois data into a **searchable** and **consistently-formatted** resource, eliminating rate limits and other impediments to at-scale use of whois.
- Commercial domain whois service providers may also offer "who-was" data, allowing you to "warp backwards" in time to see what whois data looked like at some earlier date.
- Farsight partners with one provider of commercial bulk whois services, but there are others with offerings in this space, too.

5. IP Addresses and Web Hosting

Web Hosting

- Once a domain has been registered, most people, including most cyber criminals, promptly proceed to bring up a web site.

- Legitimate users have their pick of web hosting providers, with many web hosting providers offering a basic virtual web hosting environment for just a few bucks a month.

Mapping Domain Names To IP Addresses

- When users go to web sites in a web browser such as Firefox or Chrome, the domain names of the web sites they visit are actually symbolic "short cuts" for underlying IP address. Systems normally do that translation automatically in the background.
- **You can also perform the name resolution process explicitly.** There are several commands you can use; we normally use and recommend the "dig" command:

  ```
  $ dig www.lawseminars.com +short
  67.228.94.89
  ```

- IP addresses (such as 67.228.94.89, as found in this case) provide another bit of data you can also explore via whois (just like domain names, IP addresses also have whois)

Sample IP whois

```
$ whois 67.228.94.89
[snip]
NetRange:       67.228.0.0 - 67.228.255.255
CIDR:           67.228.0.0/16
[snip]
OrgName:        SoftLayer Technologies Inc.
OrgId:          SOFTL
Address:        4849 Alpha Rd.
City:           Dallas
StateProv:      TX
[snip]
ReferralServer:  rwhois://rwhois.softlayer.com:4321
[snip]
```

Following the Rwhois Referral

```
$ telnet rwhois.softlayer.com 4321        ← my improvised rwhois "client"
[snip]
67.228.94.89
[snip]
network:IP-Network-Block:67.228.94.88-67.228.94.91
network:Organization;I:Law Seminars International
network:Street-Address:800 Fifth Avenue
network:City:Seattle
network:State:WA
network:Postal-Code:98104
network:Country-Code:US
network:Tech-Contact;I:sysadmins@softlayer.com
network:Abuse-Contact;I:abuse@lawseminars.org
[snip]
```

Obviously, That's A Legitimate IP Address Block

- And not surprisingly, that the IP address whois for that IP address block is well defined.

- Sadly, the IP whois information for abused address blocks will often be incomplete, out-of-date, or missing altogether.

- Bad IP whois data can and should be flagged for attention:

  – https://www.apnic.net/apnic-info/whois_search/using-whois/abuse-and-spamming/invalid-contact-form
  – https://www.arin.net/public/whoisinaccuracy/index.xhtml
  – http://www.lacnic.net/en/web/lacnic/faq
  – https://www.ripe.net/manage-ips-and-asns/resource-management/assisted-registry-check

What About Less-Legitimate Customers?

- Most web hosters aren't interested in iffy customers. "Grey-hat" (or worse "black-hat") customers often represent:
  -- **Lost revenue** (shady customer may pay with a stolen card; chargebacks occurs; provider gets $0 for services provided)
  -- **Damaged reputation** for provider IP addresses (and once your address space gets block listed, it can be very hard to get it 'rehabilitated' or even to figure out WHERE it is being blocked)
  -- **The hoster may becoming a target for DDoS attack traffic**
  -- Hosting companies can even go into a ***"death spiral:"***
  – **MORE shady customers may** arrive as the bad guy "grapevine" says "hey, provider X doesn't care, they're a great place to misbehave"
  – **Collateral damage** takes place when innocent customers end up getting blocked, too (➔ they may "move to a better online neighborhood")
  – At some point, the **provider may have nobody left but the bad guys**, and by then the provider has lost control (kicking out the bad guys probably means going out of business)

So-Called "Bulletproof" Hosting

- So-called "bulletproof" hosting services specifically target those who are engaged in online abusive/illegal activities that wouldn't be tolerated by a legitimate hosting company.
- Bad guys pay these companies a premium, perhaps ~10-100X normal prices, and in exchange for doing so, the provider ignores complaints received about them.
- Sometimes they may even actively help bad guy customers. For example: a so-called bulletproof hoster may:
  -- "Forget" to document abusive customer address ranges
  -- Claim to terminate a customer (while simply moving them to a new address range and allowing them to continue)
  -- Some so-called bulletproof hoster have even been known to demand extensive and un-redacted proof of abusive behavior, sharing that data directly with the abusive customers.
- That said, some providers DO end up getting taken down...

Media Reports and A Recently-Released White Paper

- **"Accused of tolerating scammers, an ISP [Intercage] goes dark,"** www.computerworld.com/article/2533287/networking/accused-of-tolerating-scammers--an-isp-goes-dark.html
  [Sep 23, 2008]
- "**Malware, mayhem, and the McColo takedown,"** http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/ [November 13th, 2008]
- **"Esthost Taken Down – Biggest Cybercriminal Takedown in History,"** blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/ [November 9th, 2011]

- **"Criminal Hideouts for Lease: Bulletproof Hosting Services,"** www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-criminal-hideouts-for-lease.pdf
  [July 15, 2015]

Impact of One Takedown: Dramatic (For ~45 Days)

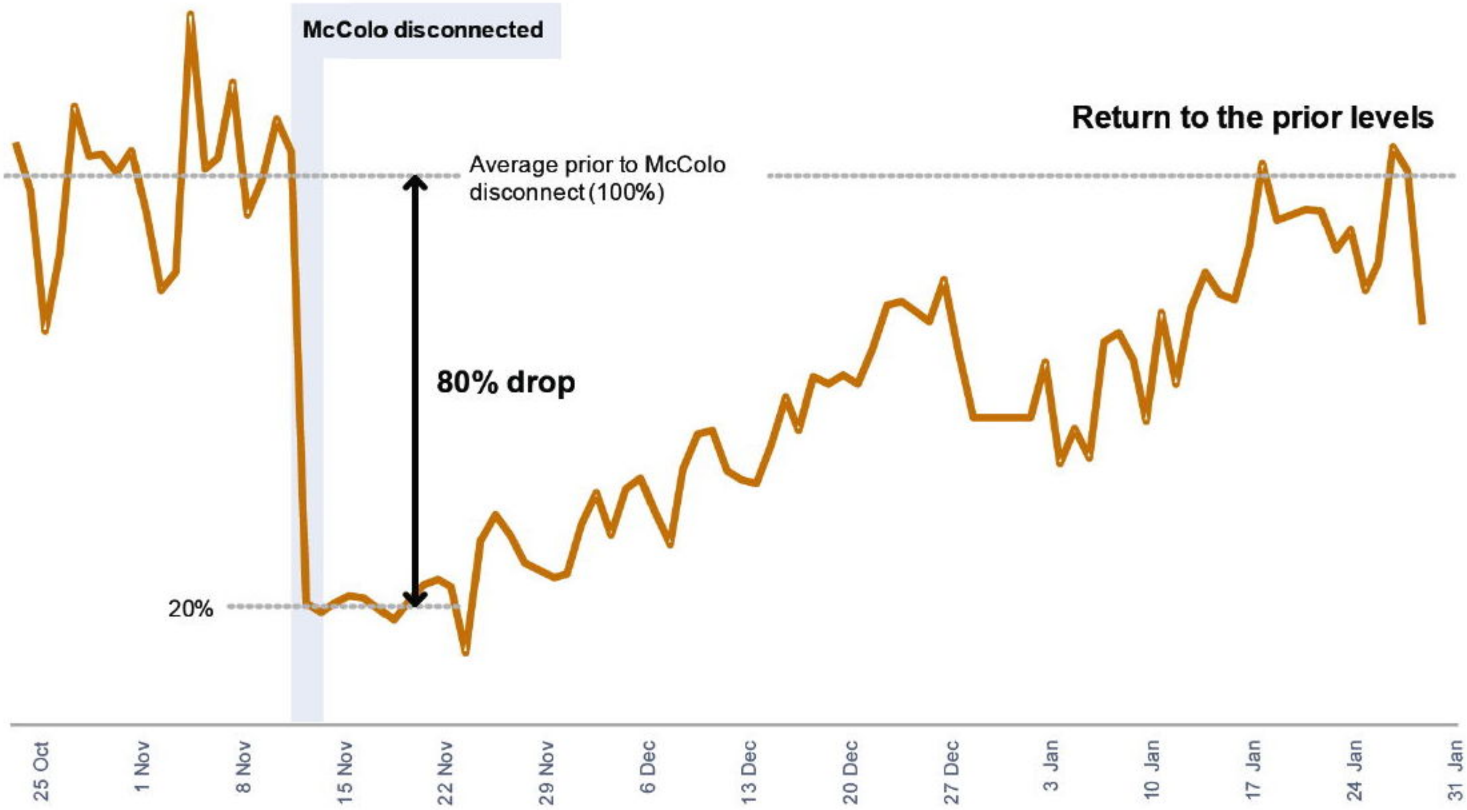


Figure 13: Temporary impact of the shutdown of hosting provider McColo on spam e-mail (Diagram by MessageLabs, Symantec Hosted Services). [209]

Source: "Botnets: Measurement, Detection, Disinfection and Defence, ENISA, PDF page 109.

A Focused, At-Scale, ONGOING Effort Is Needed

- Cyber criminals are like an insect infestation in a house.
- There's no single takedown that will make a targeted problem area go away forever.
- You need to have an ongoing effort, AT SCALE and FOCUSED, to keep any particular targeted cyber crime problem area at tolerable levels.
- This means finding ALL related domains, or at least as many as reasonably possible.

6. Finding Related Domains Using Passive DNS

Following Leads To Related Sites

- Once you've identified an initial site of interest, investigators will normally want to ensure they get **ALL** the related sites associated with an online criminal scheme.

- Doing so avoids an **"incomplete"** or **"ineffective" takedown.**

- In an incomplete or ineffective takedown scenario, perhaps a few of the best-known associated sites get identified and taken down. The rest, however, remain up and usable.

- This means that the "takedown" (which have taken a lot of effort to perform) is really just a "minor bump in the road," and it's basically "business as usual" for the cyber criminals. It would obviously be embarrassing and unfortunate to have that happen.

Additional Reasons To Find ALL Related Sites

- Even if a cybercriminal is careful not to leave any leads when it comes to <u>one</u> site, they may be careless with <u>others.</u>
- Finding the full extent of a criminal enterprise helps justify focusing on one entity rather than some other one. If you've only got limited investigative/prosecutorial resources, you need to get maximum "bang" for your limited "bucks."
- Finding the full extent of a criminal enterprise helps you to meet or exceeded any prosecutorial minimum-badness thresholds
- Finding the full extent of a criminal enterprise helps you to maximize PR impact when action is taken, *"pour les encouragement des les autres."*
- There will virtually **ALWAYS** be more than just one site. If you've only found one, you've only just begun. Keep going! (This is just like a cop finding a weapon – if you find ONE during a pat down, keep looking, there WILL be more)

HOW Can An Investigator Find Related Domains?

- If you found the first bad site in Google, Bing or another search engine, you may be able to use the same search engine to find additional related sites, perhaps by searching for unique bits of text included on the initial web site (many bad guys will clone web sites, including copying spelling errors and atypical grammar and usage)

- You can also **use the relationships inherent in DNS transactions** to easily find related sites.

Cyber Criminals "Reduce, Reuse, Recycle"

- Bad guys *could* make each domain totally unique. For example, when registering domains, they could use:
  - A different registrant name for each domain
  - A unique point of contact address for each domain
  - A unique email for each domain, and
  - A different phone number for each domain they create... **but they don't.**
- In reality, a cyber criminal may host hundreds or even thousands of websites on a single IP address, making it easy to find related domains by checking to see what domains have been seen "living" on a suspect IP.
- Or, as another example, they may share a single pair of name servers across thousands of websites.
- This commonality provides linkages that let us take *one* suspect domain and parlay it into many, many more.

Virtually Everything You Do On The Internet Begins With The Domain Name System

- Visit a web page? The web uses the Domain Name System (DNS) to figure out what server you're trying to access
- Send an email? Email uses DNS to find the server to which your email should be delivered
- And the list goes on... virtually everything you do on the Internet begins with DNS, whether you know it or not.
- This reality makes DNS a terrific indirect tool for understanding phenomena that we may not be able to directly measure – including things like malware infections, spam, phishing, etc.
- DNS is like a trail of breadcrumbs that everyone silently leaves online, including criminals, whether they mean to or not.
- The problem? Regular DNS can't answer the sort of questions investigators would like to have answered. **Passive DNS can.**

Queries That Only Passive DNS Can Answer

- "Given one domain as a starting point, tell me all the other domains that share the same IP address"
- "Given one domain as a starting point, tell me all the other domains that use the same name servers"
- "Show me all the IP addresses that foo.example.com used for the past week (or month, or three months, or year)..."
- "What are all the fully qualified domain names (hostnames) that are known to exist under a domain of interest?"
- "Given the IP address range 128.223.0.0/16, what hosts are known to have used IP addresses from that range?"
- "Show me domains that include the word 'rolex' "
- Those are obviously very powerful capabilities, particularly if you're working on cyber criminal enterprises that use a lot of different domains

How Passive DNS Works

- Passive DNS synthesizes DNS relationships based on **actually-observed Internet DNS queries.**

- Sensors get deployed above recursive resolvers, collecting DNS query and response data. Farsight has sensors of this sort deployed at over 500 participating sites all around the world.

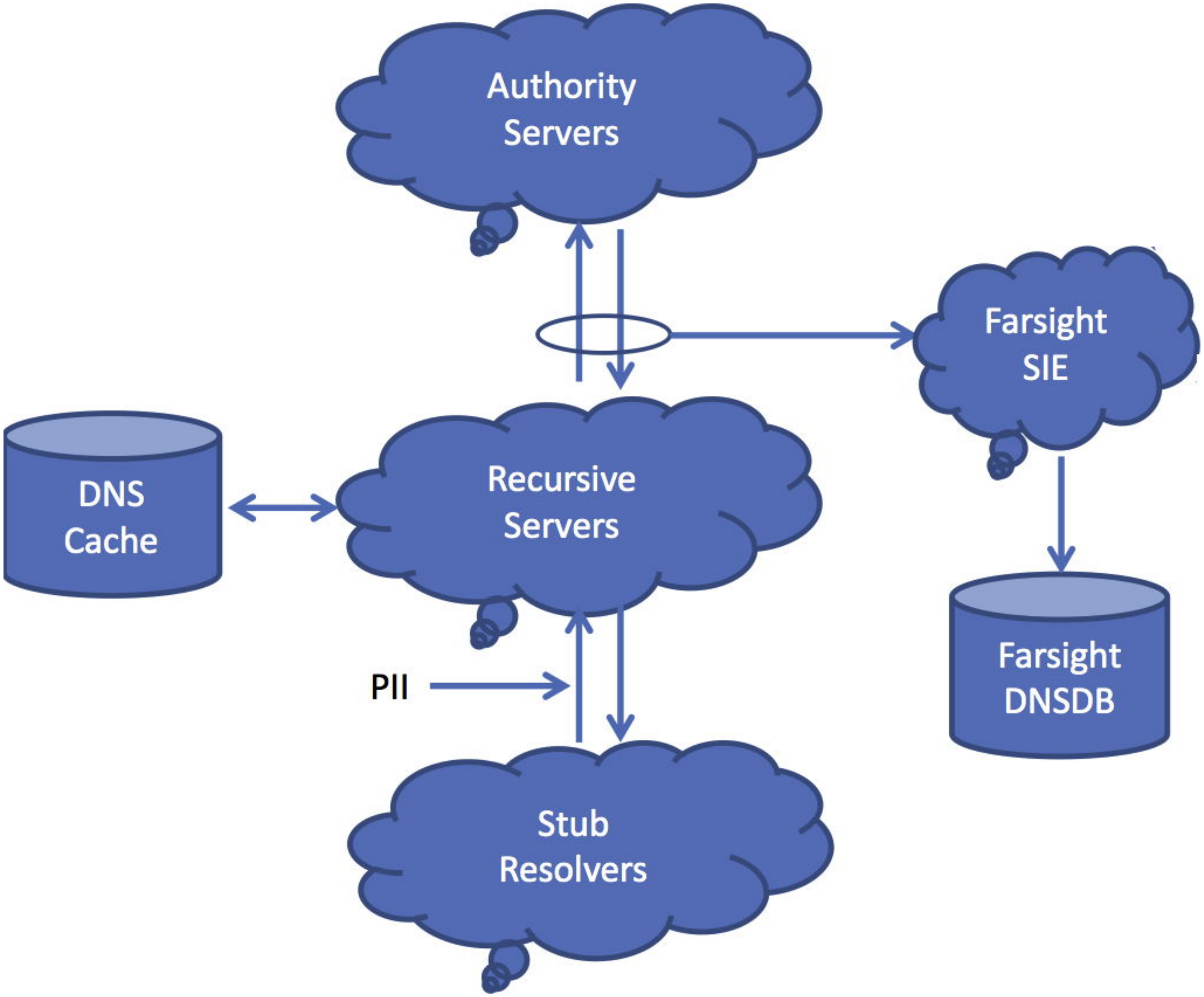
- That data gets sent back to Farsight,and put into a database that can then be easily queried by authorized researchers, cybercrime analysts, LEOs, etc.

- Our passive database, **DNSDB**, created by ISC in June 2010, is now the largest such database in the world.

Passive DNS And Privacy

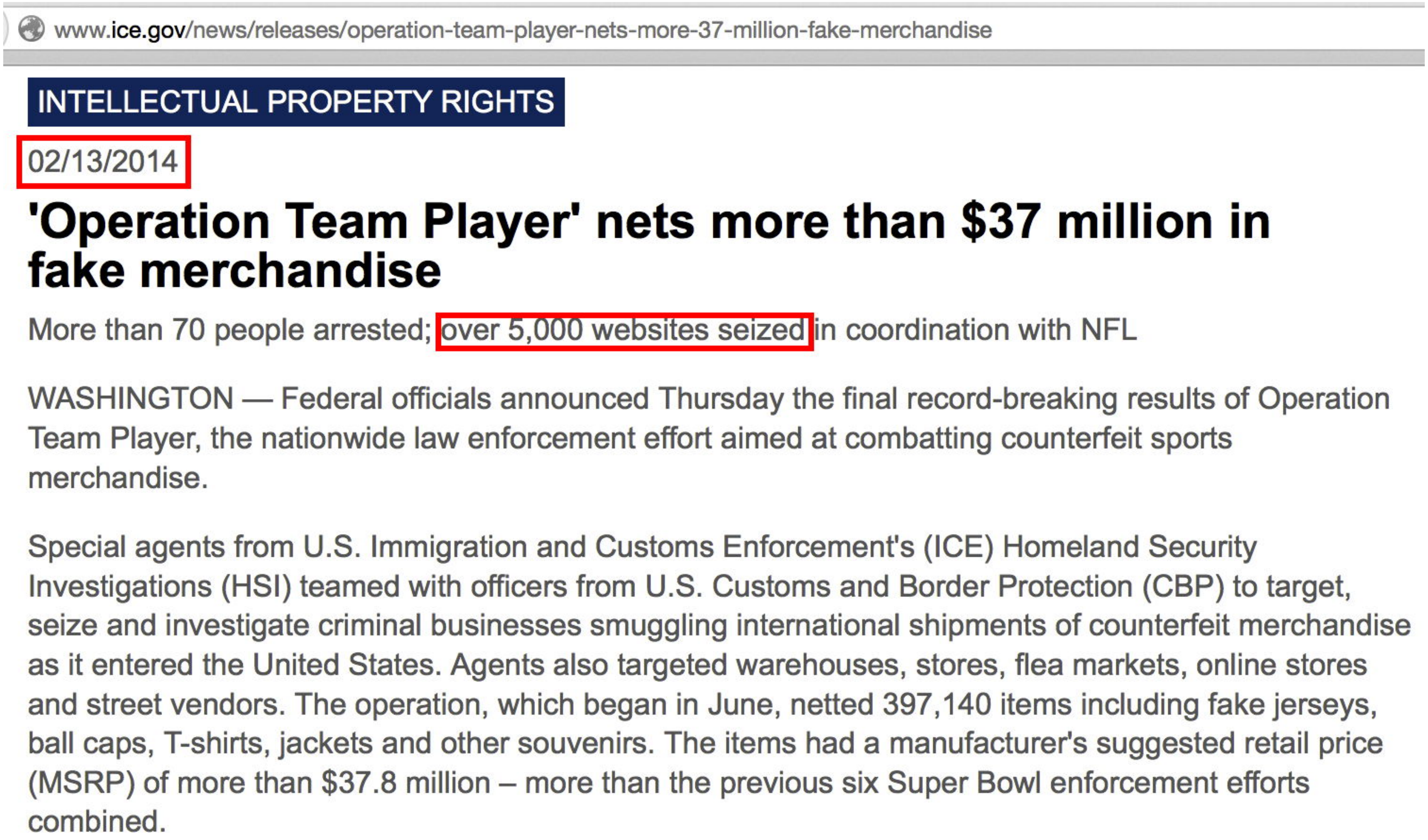
- Any time we talk about passive monitoring of Internet traffic, the issue of end-user privacy must be considered. I take end-user privacy very seriously, and so does Farsight Security, Inc., just as I'm sure many of the rest of you do.
- I can't speak for all passive DNS efforts, but at least in Farsight's case, we intentionally collect passive DNS **above recursive resolvers** specifically in order to **avoid** collecting PII.
- This means that the queries and responses that our collectors gather all appear to come from the recursive resolver itself (which is typically shared by tens of thousands of users or more) rather than from any individually-attributable user.
- See the diagram on the next slide.

Privacy-Protecting Passive DNS Collection



7. An Example: Brand Protection

An Example From The Brand Protection Area



www.ice.gov/news/releases/operation-team-player-nets-more-37-million-fake-merchandise

INTELLECTUAL PROPERTY RIGHTS

02/13/2014

'Operation Team Player' nets more than $37 million in fake merchandise

More than 70 people arrested; over 5,000 websites seized in coordination with NFL

WASHINGTON — Federal officials announced Thursday the final record-breaking results of Operation Team Player, the nationwide law enforcement effort aimed at combatting counterfeit sports merchandise.

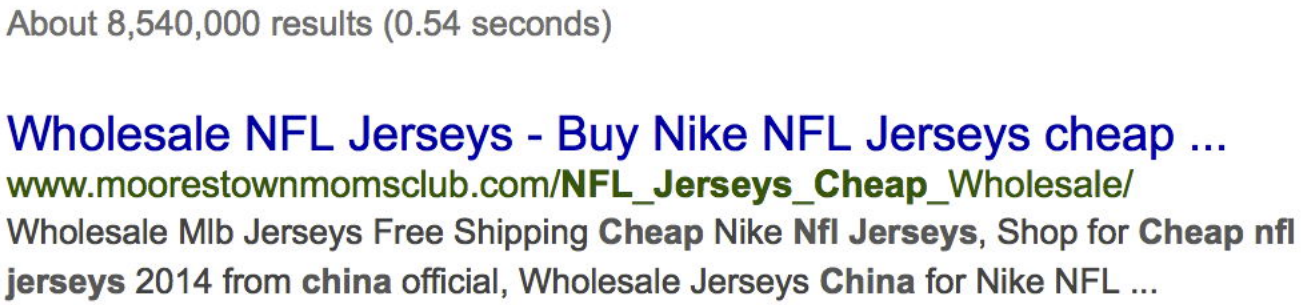
Special agents from U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) teamed with officers from U.S. Customs and Border Protection (CBP) to target, seize and investigate criminal businesses smuggling international shipments of counterfeit merchandise as it entered the United States. Agents also targeted warehouses, stores, flea markets, online stores and street vendors. The operation, which began in June, netted 397,140 items including fake jerseys, ball caps, T-shirts, jackets and other souvenirs. The items had a manufacturer's suggested retail price (MSRP) of more than $37.8 million – more than the previous six Super Bowl enforcement efforts combined.

Working A Brand Protection Example

- Perhaps your work day as a brand infringement person begins with a simple Google search:

  cheap NFL jerseys china

- First hit when we tried this:



About 8,540,000 results (0.54 seconds)

Wholesale NFL Jerseys - Buy Nike NFL Jerseys cheap ...
www.moorestownmomsclub.com/**NFL_Jerseys_Cheap**_Wholesale/
Wholesale Mlb Jerseys Free Shipping **Cheap** Nike **Nfl Jerseys**, Shop for **Cheap nfl jerseys** 2014 from **china** official, Wholesale Jerseys **China** for Nike NFL ...

- What do we know about moorestownmomsclub[dot]com ? Let's check domain whois for the domain, to see who owns it.

moorestownmomsclub[dot]com domain whois info

```
$ whois moorestownmomsclub[dot]com
Domain Name: MOORESTOWNMOMSCLUB[dot]COM
[snip]
Update Date: 2015-06-05T00:26:15Z
Creation Date: 2008-07-18T12:45:32Z          ← Older domain, presumably expired
Registrar Registration Expiration Date: 2017-07-18T12:45:32Z    and reregistered
Registrar: GoDaddy.com, LLC
[snip]
Registrant Name: dong zhenbang
Registrant Street: fujian                      ← A little vague for a province of
Registrant City: fujian                               37.7 million in China...
Registrant State/Province: fujian
Registrant Postal Code: 754102
Registrant Country: China
Registrant Phone: +86.12233113
Registrant Fax:
Registrant Email: mlievhu@163.com
[etc]
```

The Next "Logical Step"

- The next "logical step" is probably to visit the site, to see what it is actually offering, and to confirm that it is still up and online, etc.

- **Important Note:** It can be dangerous to visit random web sites. Any site you visit has the potential to drop malware on your system, including malware that may NOT get detected and blocked by your anti-virus software.

- Use a system that you can "nuke and pave" (rebuild from scratch if necessary), or at least a sandboxed virtual machine, when investigating sites of unknown/dubious provenance.

- Always have a clean backup of your system, too!

What Do We See In This Case If We Visit That Site?

- In this case, the web site

  http://moorestownmomsclub[dot]com/

  immediately redirects to:

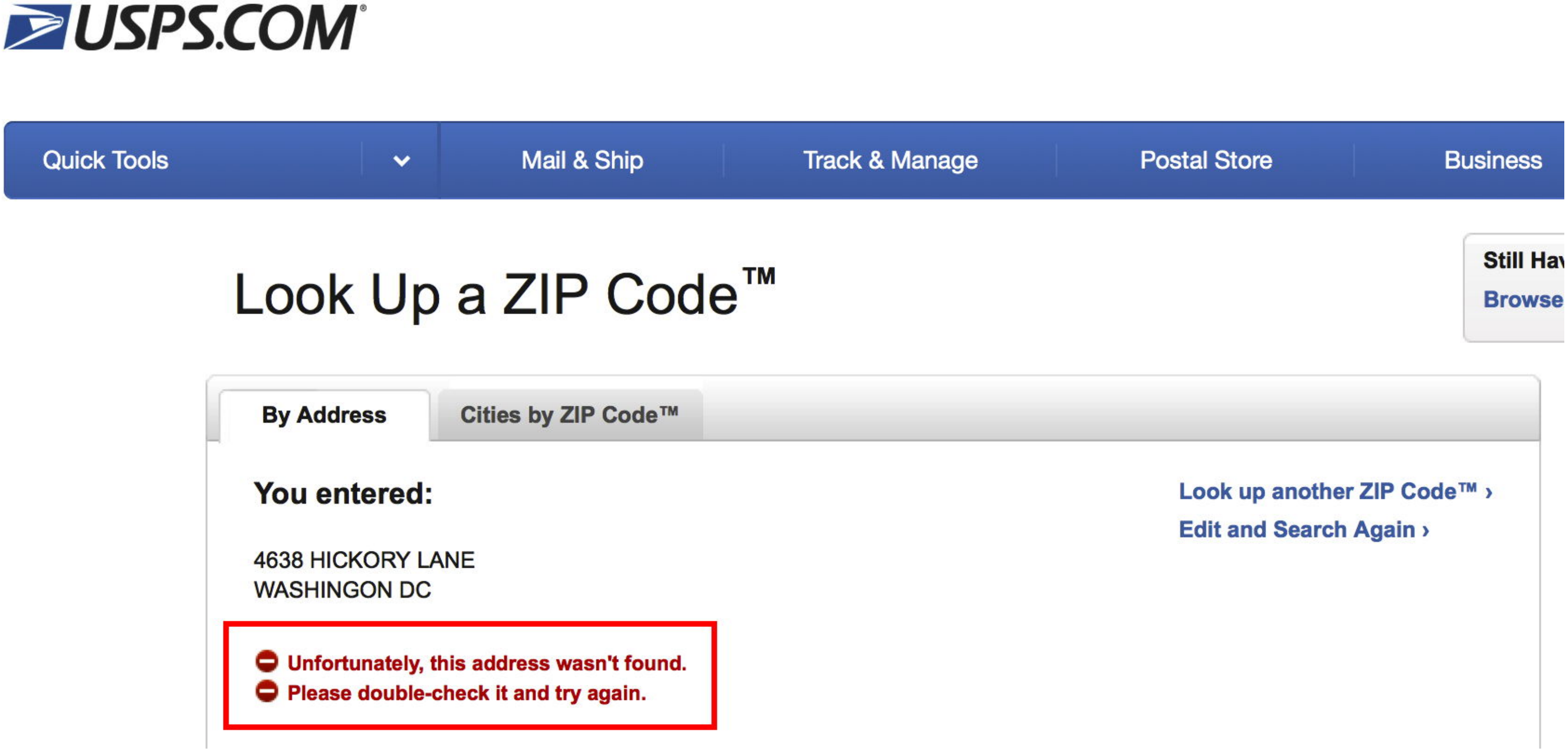
  http://www.chinacheapjerseys[dot]cc/

  [BTW, if you ever have trouble following the chain of sites that may rapidly be visited, check out the "Live HTTP Headers" extension that's available for Firefox]

Domain Whois

Domain Name: CHINACHEAPJERSEYS[dot]CC
[snip]
Updated Date: 2015-05-19T02:19:42Z ← *Freshly registered this May*
Creation Date: 2015-05-19T02:19:39Z
Registrar Registration Expiration Date: 2016-05-19T02:19:39Z ← *1 year only*
[snip]
Registrant Name: Gracie Garcia Gracie Garcia ← *Unusual name, eh?*
Registrant Organization: Gracie Garcia
Registrant Street: 4638 Hickory Lane ← *What about this address?*
Registrant City: Washington
Registrant State/Province: DC
Registrant Postal Code: 20200
Registrant Country: US
Registrant Phone: +1.2025316173
Registrant Fax:
Registrant Email: jerseys_2015@163.com
[snip]

The Post Office Says...



Look Up a ZIP Code™

You entered:

4638 HICKORY LANE
WASHINGON DC

⊖ Unfortunately, this address wasn't found.
⊖ Please double-check it and try again.

Where Does The Site We Found Live On The Network?

- **www.chinacheapjerseys[dot]cc** → 179.43.152.77

Checking the IP whois for that address:

```
inetnum:      179.43.128/18
status:       allocated
aut-num:      N/A
owner:        PRIVATE LAYER INC
ownerid:      PA-PLIN-LACNIC
responsible:  Ezequiel Pineda
address:      Torres De Las Americas, Torre C, 0, Piso 29 Suite 2901
address:      00000 - Panama -
country:      PA
phone:        +507  8365449 []
[etc]
```

Are There Other Sites On the Same IP?

We can checking passive DNS for other sites known to have been on 179.43.152.77 by saying:

```
$ dnsdb_query.py -i 179.43.152.77
```

We see:

```
chinacheapjerseys[dot]cc.              IN A 179.43.152.77
wholesalejerseysfrees[dot]com.         IN A 179.43.152.77
nflsteelersmall[dot]com.               IN A 179.43.152.77
```

plus a few other sites.

Let's check domain whois for those two other sites...

wholesalejerseysfrees[dot]com?

Domain Name: wholesalejerseysfrees[dot]com
[snip]
Updated Date: 2015-06-05T11:57:07Z
Creation Date: 2014-06-08T03:12:33Z
Registrar Registration Expiration Date: 2016-06-08T03:12:33Z
[snip]
Registrant Name: YinSi BaoHu Yi KaiQi **(Hidden by Whois Privacy Protection Service)**
Registrant Organization: YinSi BaoHu Yi KaiQi **(Hidden by Whois Privacy Protection Service)**
Registrant Street: 3/F.,HiChina Mansion,No.27 Gulouwai Avenue,Dongcheng District,Beijing 100120,China,
[snip]
Registrant Phone: +8610.65985888
Registrant Fax: +8610.65985438
Registrant Email: YuMing@YinSiBaoHu.AliYun.com
[snip]

nflsteelersmall[dot]com?

```
Domain Name: nflsteelersmall[dot]com
[snip]
Updated Date: 2015-06-25T14:17:08Z
Create Date: 2015-06-25T14:17:08Z
Registry Expiry Date: 2016-06-25T14:17:08Z
[snip]
Registrant Name: shao nian
Registrant Organization: shao nian
Registrant Street: Shang Hai Shi Qu
Registrant City: shanghaishi
Registrant State/Province: shanghai
Registrant Postal Code: 123123
Registrant Country: CN
Registrant Phone : +86.0211231231
Registrant Fax: +86.0211231231
Registrant Email: cj2015tit@126.com
[snip]
```

One Product For Sale At www.chinacheapjerseys[dot]cc

- "Nike Seahawks #54 Bobby Wagner Steel Blue Team Color Men's Stitched NFL Game Jersey," just $20.49

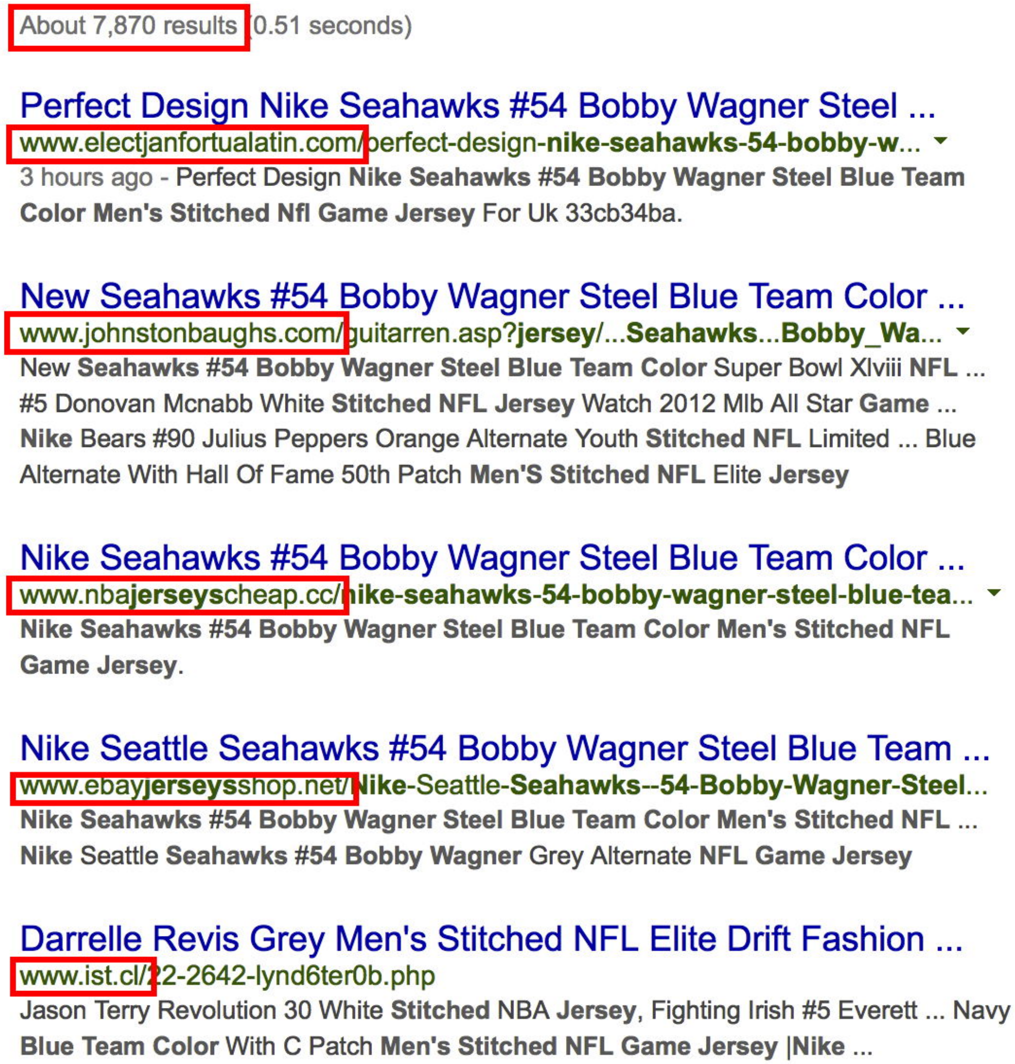
- For comparison,

  http://store.nike.com/us/en_us/pw/n/1j7?sl=seahawks+mens&ipp=70

  has NFL jerseys for select players for $295.00.

- Hmm. I wonder what else we can find that matches that set of keywords? Any other potentially related sites if we search for that product description?

Nike Seahawks #54 Bobby Wagner Steel Blue Team Color Men's Stitched NFL Game Jersey



About 7,870 results (0.51 seconds)

Perfect Design Nike Seahawks #54 Bobby Wagner Steel ...
www.electjanfortualatin.com/perfect-design-nike-seahawks-54-bobby-w...
3 hours ago - Perfect Design **Nike Seahawks #54 Bobby Wagner Steel Blue Team Color Men's Stitched Nfl Game Jersey** For Uk 33cb34ba.

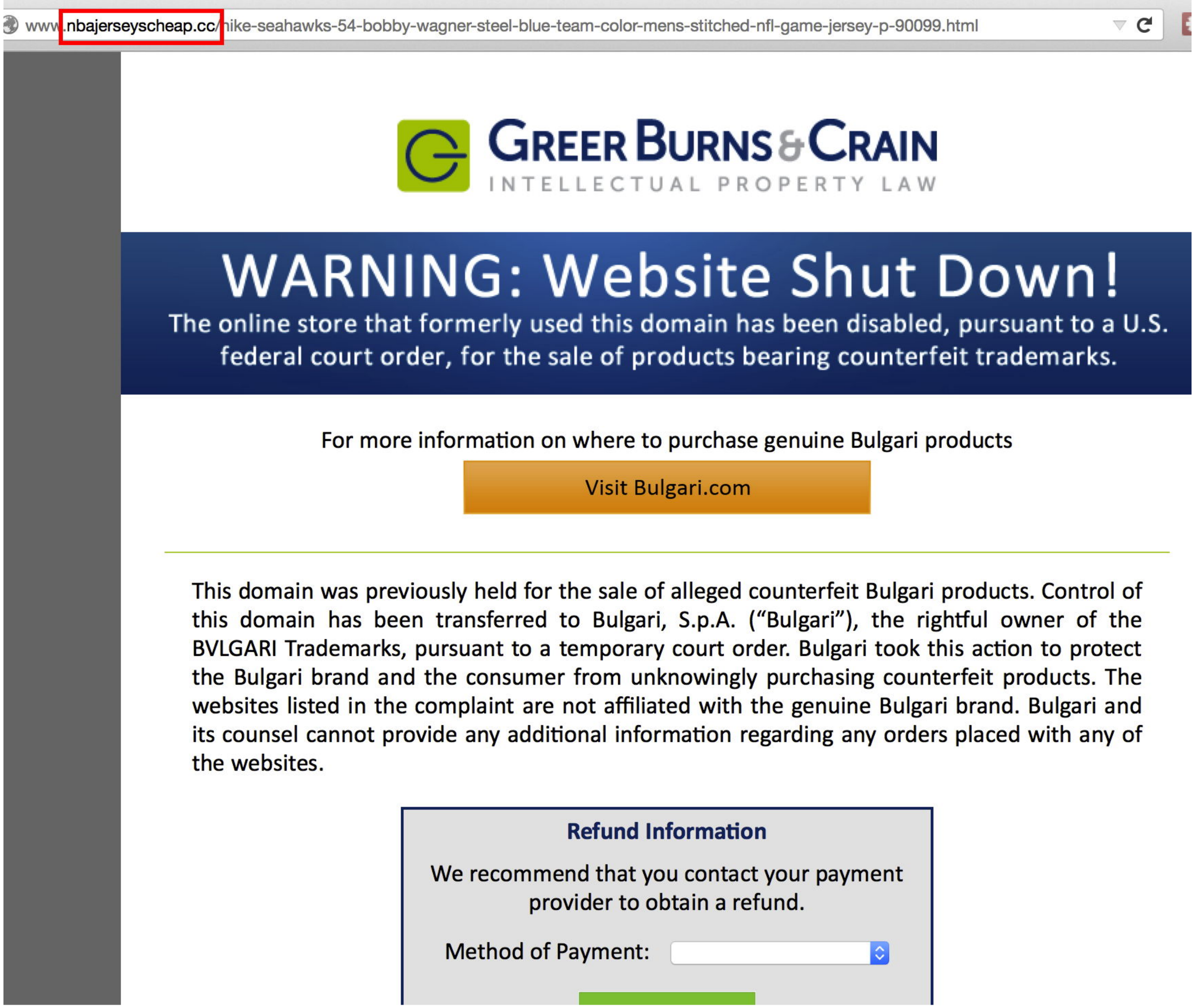
New Seahawks #54 Bobby Wagner Steel Blue Team Color ...
www.johnstonbaughs.com/guitarren.asp?jersey/...Seahawks...Bobby_Wa...
New **Seahawks #54 Bobby Wagner Steel Blue Team Color** Super Bowl Xlviii **NFL** ... #5 Donovan Mcnabb White **Stitched NFL Jersey** Watch 2012 Mlb All Star **Game** ... **Nike** Bears #90 Julius Peppers Orange Alternate Youth **Stitched NFL** Limited ... Blue Alternate With Hall Of Fame 50th Patch **Men'S Stitched NFL** Elite **Jersey**

Nike Seahawks #54 Bobby Wagner Steel Blue Team Color ...
www.nbajerseyscheap.cc/nike-seahawks-54-bobby-wagner-steel-blue-tea...
Nike Seahawks #54 Bobby Wagner Steel Blue Team Color Men's Stitched NFL Game Jersey.

Nike Seattle Seahawks #54 Bobby Wagner Steel Blue Team ...
www.ebayjerseysshop.net/Nike-Seattle-Seahawks--54-Bobby-Wagner-Steel...
Nike Seahawks #54 Bobby Wagner Steel Blue Team Color Men's Stitched NFL ... **Nike** Seattle **Seahawks #54 Bobby Wagner** Grey Alternate **NFL Game Jersey**

Darrelle Revis Grey Men's Stitched NFL Elite Drift Fashion ...
www.ist.cl/22-2642-lynd6ter0b.php
Jason Terry Revolution 30 White **Stitched** NBA **Jersey**, Fighting Irish #5 Everett ... Navy **Blue Team Color** With C Patch **Men's Stitched NFL Game Jersey** |**Nike** ...

At Least One of Those Sites Has Been Shut Down



www.nbajerseyscheap.cc/nike-seahawks-54-bobby-wagner-steel-blue-team-color-mens-stitched-nfl-game-jersey-p-90099.html
GREER BURNS & CRAIN
INTELLECTUAL PROPERTY LAW

WARNING: Website Shut Down!

The online store that formerly used this domain has been disabled, pursuant to a U.S. federal court order, for the sale of products bearing counterfeit trademarks.

For more information on where to purchase genuine Bulgari products

This domain was previously held for the sale of alleged counterfeit Bulgari products. Control of this domain has been transferred to Bulgari, S.p.A. ("Bulgari"), the rightful owner of the BVLGARI Trademarks, pursuant to a temporary court order. Bulgari took this action to protect the Bulgari brand and the consumer from unknowingly purchasing counterfeit products. The websites listed in the complaint are not affiliated with the genuine Bulgari brand. Bulgari and its counsel cannot provide any additional information regarding any orders placed with any of the websites.

Refund Information

We recommend that you contact your payment provider to obtain a refund.

Method of Payment:

Where We're Taken By Some Other Top Results

www.jerseysnflnba[dot]com → hosted on CloudFlare

www.mbprinting[dot]net → hosted on CloudFlare

wholesaleforjerseys[dot]com → 5.157.2.40 ("Reverse-Proxy310")

www.fancysoccerdeal[dot]eu → 23.245.199.139 (scalabledns.com)

www.energyfm964[dot]com → 31.222.204.83 (idear4business.net)

www.jerseyfactoryshop[dot]com → 63.141.229.104 (Zhou Pizhong, datashack.net)

www.officialjerseyssale[dot]com → 70.39.121.194 (Sharktech)

www.ebayjerseysshop[dot]net → 178.17.169.43 (Moldova)

www.wholesalejerseysfrees[dot]com → 179.43.152.77 (Private Layer)

www.buyjerseys[dot]ru → 195.154.47.62 (Iliad Entreprises, FR)

www.jerseysus.[dot]com → 198.2.211.210 ('China Outcom-urhosts.net')

www.cpjerseys[dot]com → 198.2.220.229 ('Wang Ye')

www.chinajerseyssupply[dot]com → 198.55.28.188 (Inter Net Bilgisayar)

www.wejerseys[dot]in → 198.204.244.72 (server2046, datashack.net)

www.wholesalejerseyssupply.us[dot]com → 199.180.116.70 (VolumeDrive)

Checking Passive DNS for Those IPs

```
$ dnsdb_query.py -i 5.157.2.40
hermsbags4u[dot]com. IN A 5.157.2.40
ctrwatchesoutlet[dot]com. IN A 5.157.2.40
wholesaleforjerseys[dot]com. IN A 5.157.2.40

$ dnsdb_query.py -i 23.245.199.139
www.dtjerseys[dot]eu. IN A 23.245.199.139
www.bruinsfanshop[dot]eu. IN A 23.245.199.139
www.fancysoccerdeal[dot]eu. IN A 23.245.199.139
www.fashionlinechina[dot]eu. IN A 23.245.199.139
www.baseballfansstore[dot]eu. IN A 23.245.199.139
www.bruinsfanshoponline[dot]eu. IN A 23.245.199.139
www.ceutomnikenfljerseys[dot]eu. IN A 23.245.199.139
www.blackhawksshopofficial[dot]eu. IN A 23.245.199.139
www.cheapjerseysoutletstore[dot]eu. IN A 23.245.199.139
click2.bbvini[dot]com. IN A 23.245.199.139
```

```
$ dnsdb_query.py -i 31.222.204.83
[selected output only]
cheapjerseyschina[dot]ru. IN A 31.222.204.83
nflsupply[dot]us. IN A 31.222.204.83
chinanikejerseys[dot]us. IN A 31.222.204.83
wholesalenikenfljerseys[dot]us. IN A 31.222.204.83
nfljerseyschina.us[dot]com. IN A 31.222.204.83
cheapjerseyschina.us[dot]com. IN A 31.222.204.83
wholesalecheapjerseysstore.us[dot]com. IN A 31.222.204.83
energyfm964[dot]com. IN A 31.222.204.83
luxury-cheap-watches[dot]com. IN A 31.222.204.83
```

```
$ dnsdb_query.py -i 63.141.229.104
[selected output only]
nfljerseyhome[dot]com. IN A 63.141.229.104
jerseyhomecheap[dot]com. IN A 63.141.229.104
jerseyfactoryshop[dot]com. IN A 63.141.229.104
nancystore[dot]org. IN A 63.141.229.104
hervelegerdressonsale[dot]org. IN A 63.141.229.104
```

```
$ dnsdb_query.py -i 70.39.121.194
[selected output only]
dns9.sh3lls[dot]net. IN A 70.39.121.194
ns3.rx365-ok[dot]ru. IN A 70.39.121.194
ns2.rxmartmega724[dot]ru. IN A 70.39.121.194
ns4.rxmeds-tips724[dot]ru. IN A 70.39.121.194
ns3.new-networkrx724[dot]ru. IN A 70.39.121.194
ns4.new-networkrx724[dot]ru. IN A 70.39.121.194
ns3.online-bestmed365[dot]ru. IN A 70.39.121.194
ns4.online-bestmed365[dot]ru. IN A 70.39.121.194
ns3.networkrx-simple365[dot]ru. IN A 70.39.121.194
ns4.networkrx-simple365[dot]ru. IN A 70.39.121.194
ns2.get-rx724[dot]com. IN A 70.39.121.194
ns3.vipsuperrx[dot]com. IN A 70.39.121.194
officialjerseyssale[dot]com. IN A 70.39.121.194
www.officialjerseyssale[dot]com. IN A 70.39.121.194
```

```
$ dnsdb_query.py -i 178.17.169.43
```

[selected output, trimmed to fit two columns]

```
nbajerseyscheap.com[dot]au.
nbajerseyswholesale.com[dot]au.
ebayjerseys[dot]cc.
www.jerseysonsale[dot]co.
www.jersey-kingdom[dot]co.
www.cheapclothesfactory[dot]co.
jerseycaptain[dot]eu.
www.ebayjerseys[dot]in.
goodnflshop[dot]in.
jersey-kingdom[dot]ru.
58jerseysfamily[dot]ru.
ebayjerseys[dot]biz.
nfljerseysshop[dot]biz.
cheapjerseyjds[dot]com.
18jerseysfamily[dot]com.
58jerseysfamily[dot]com.
cosyjerseystore[dot]com.
ebayjerseysshop[dot]com.
sewnjerseystore[dot]com.
cheapclothesfactory[dot]com.
goodnflshop[dot]net.
superbowlfans[dot]net.
nfljerseysshop[dot]net.
bestjerseyshome[dot]net.
ebayjerseysshop[dot]net.
goodnflshop[dot]org.
```

```
$ dnsdb_query.py -i 179.43.152.77
[discussed previously, above]

$ dnsdb_query.py -i 195.154.47.62
[selected output only]
atcheapjerseys[dot]cc. IN A 195.154.47.62
buyjerseys[dot]ru. IN A 195.154.47.62
atcheapjerseys[dot]com. IN A 195.154.47.62

$ dnsdb_query.py -i 198.2.211.210
[selected output only]
ukfootballshirtscheap[dot]co.uk. IN A 198.2.211.210
jerseysus[dot]com. IN A 198.2.211.210
cheapalljerseys[dot]org. IN A 198.2.211.210
2014worldcupjersey[dot]org. IN A 198.2.211.210
wholesalejerseyall[dot]org. IN A 198.2.211.210
```

```
$ dnsdb_query.py -i 198.2.220.229
cpjerseys[dot]com. IN A 198.2.220.229
www.cpjerseys[dot]com. IN A 198.2.220.229

$ dnsdb_query.py -i 198.55.28.188
[selected output only]
aaaqualityshoes[dot]com. IN A 198.55.28.188
lvdiscountestore[dot]com. IN A 198.55.28.188
chinajerseyssupply[dot]com. IN A 198.55.28.188
cheapcelebrityshoes[dot]com. IN A 198.55.28.188
louboutin-christian[dot]com. IN A 198.55.28.188
sergiorossiallshoes[dot]com. IN A 198.55.28.188
vipsunglassesmarket[dot]com. IN A 198.55.28.188
giuseppezanottigzall[dot]com. IN A 198.55.28.188
cheap-giuseppezanotti[dot]com. IN A 198.55.28.188
```

```
$ dnsdb_query.py -i 198.204.244.72
[selected output only]
wejerseys[dot]in. IN A 198.204.244.72
vjerseys[dot]com. IN A 198.204.244.72
1688jerseys[dot]com. IN A 198.204.244.72
wejerseysok[dot]com. IN A 198.204.244.72
wejerseyshop[dot]com. IN A 198.204.244.72
wejerseysshop[dot]com. IN A 198.204.244.72
cheapwejerseys[dot]com. IN A 198.204.244.72
wejerseystoday[dot]com. IN A 198.204.244.72
wholesalewejerseys[dot]com. IN A 198.204.244.72
wejersey[dot]net. IN A 198.204.244.72
www.wejerseys[dot]name. IN A 198.204.244.72
```

```
$ dnsdb_query.py -i 199.180.116.70
```

[selected output, sorted and trimmed to fit two columns]

```
www.2015discountsunglasses[dot]com.
www.arizonacardinals.us[dot]com.
www.basketpumahomme[dot]com.
www.bearsnflofficialprostore[dot]com.
www.big-discount-sunglasses[dot]com.
www.broncosshopnfl[dot]com.
www.casquetteunkut[dot]com.
www.chargersofficialauthentic[dot]com.
www.cheapjerseyfreeshipping.us[dot]com.
www.cheapjerseysace.us[dot]com.
www.cheapjerseysaol[dot]com.
www.cheapjerseysaol[dot]us.
www.cheapjerseysaols[dot]com.
www.cheapmacwholesales[dot]com.
www.cheapnfljerseyschina.us[dot]com.
www.cheapnfljerseysusaonline[dot]com.
www.chinacheapnfljerseys.us[dot]com.
www.chinanfljersey.us[dot]com.
www.colorfulcheapsunglasses[dot]com.
www.coltsnflprostore[dot]com.
www.coltsshop.us[dot]com.
www.denverbroncos.us[dot]com.
www.discount-outlets-shop[dot]com.
www.discount-sunglasses-shop[dot]com.
www.dolphinsshop.us[dot]com.
www.eaglesofficialonline[dot]com.
www.elitecheapjerseys[dot]us.
www.falconsofficialnfljerseys[dot]com.
www.fashionbag4u[dot]com.
www.footballbroncosproshop[dot]com.
www.footballseahawksprostore[dot]com.
www.giantsfootballprostore[dot]com.
www.handbagstoby2014[dot]com.
www.ibestreplicawatches[dot]net.
```

www.iofferreplica[dot]us.
www.jerseys-nfl[dot]org.
www.jerseyschinaonline.us[dot]com.
www.jerseyschinawholesale.us[dot]com.
www.jerseywholesalechina[dot]us.
www.jetsshop.us[dot]com.
www.kansascitychiefs.us[dot]com.
www.louisvuittonoutlet.us[dot]org.
www.maccosmetickitsale[dot]com.
www.macmakeupsites[dot]com.
www.mskeyoffer[dot]com.
www.nbajerseyscheap[dot]cc.
www.nflbengals.us[dot]com.
www.nflbills.us[dot]com.
www.nflbroncosofficialshops[dot]com.
www.nflbuccaneers.us[dot]com.
www.nflcheapjersey[dot]us.
www.nflchinajersey[dot]us.
www.nflcowboysofficialshops[dot]com.
www.nflgiantsofficialonlines[dot]com.
www.nfljerseys2015[dot]us.
www.nfljerseywholesale.us[dot]com.
www.nfljets.us[dot]com.
www.nflpackers.us[dot]com.
www.nflpackersofficial[dot]com.
www.nflpanthers.us[dot]com.
www.nflpatriots.us[dot]com.
www.nflravens.us[dot]com.
www.nflshoppa[dot]com.
www.nikedunk[dot]fr.
www.officialbullsauthentics[dot]com.
www.officialchargersnflshop[dot]com.
www.officialfalconsnflauthentic[dot]com.
www.officialfootballbills[dot]com.
www.officiallysnfljersey[dot]com.
www.officialnbaauthentic[dot]com.
www.officialnflshopco[dot]com.
www.officialpackersnflproshop[cot]com.

www.outlet-prada[dot]com.

www.outlet-toms[dot]org.

www.outletsralph-lauren[dot]org.

www.packlinemondiale[dot]com.

www.panthersauthenticofficial[dot]com.

www.panthersshop.us[dot]com.

www.patriotsnflofficialonline[dot]com.

www.patriotsnflofficialproshop[dot]com.

www.perfectkickz[dot]ru.

www.raybanon-line[dot]cc.

www.rb-bestseller[dot]com.

www.rb-discount-store[dot]com.

www.rogervivier-china[dot]com.

www.shopbrownsnfljerseys[dot]com.

www.sneakersbrand[dot]com.

www.sneakersseller[dot]com.

www.special-offer-sunglasses-shop[dot]com.

www.special-offer-sunglasses-store[dot]com.

www.special-offer-sunglasses[dot]com.

www.sportsoutletsonline[dot]com.

www.starstatusfashion[dot]com.

www.summer-sale-sunglasses-shop[dot]com.

www.superolexweb[dot]com.

www.supplynfljerseys.us[dot]com.

www.teamjerseybuy[dot]biz.

www.teamusahockeyjersey[dot]com.

www.texansnflofficialonline[dot]com.

www.texansonlineprostore[dot]com.

www.tissotmontre[dot]com.

www.topendnewatch[dot]com.

www.usa-outlets-store[dot]com.

www.warriorsofficialshop[dot]com.

www.wholesalejerseyschina[dot]cc.

[etc]

That's A LOT of Apparently-Related Domains

- Checking passive DNS (to see what other domains have been seen on the same IP) allows us to find other apparently-related domains.

- **Before action is taken against ANY domain, it should be visited and documented as actually offering problematic products.** (But recall my caution from earlier about potentially malicious domains, too!)

- **DO NOT just assume that a site with a domain name that *appears* to be infringing actually is – CONFIRM IT.**

- Some may not be what they seem; others may already be down. Many, however, may be exactly what you expect.

8. Following Name Servers in Passive DNS

A Different Approach to Finding Related Domains

What **name servers** are used by one of those domains?

```
$ dig +trace www.wholesalejerseyssupply.us.com
[snip]
wholesalejerseyssupply.us.com. 3600 IN      NS   nsdo.cloudang.com.
wholesalejerseyssupply.us.com. 3600 IN      NS   nsph.cloudang.com.
[snip]
```

What other domains ALSO use one of those name servers?

Using Passive DNS to Follow A Name Server

```
$ dnsdb_query.py -n nsdo.cloudang[dot]com > nsdo.cloudang.com.txt
$ wc -l  nsdo.cloudang.com.txt
   2286 nsdo.cloudang.com.txt
```

Note the -n instead of -i in the dnsdb_query.py statement

How many *unique* domains did we find?

```
$ awk '{print $1}' < nsdo.cloudang.com.txt | sort | uniq | wc -l
   1283       ← number of domains associated with nsdo.cloudang[dot]com ...
```

We're not going to show you all 1,283 of those, but just to show you SOME of those...

[...]

cheapjerseyfreeshipping.us[dot]com.

cheapjerseynfl[dot]us.

cheapjerseys.us[dot]com.

cheapjerseysace.us[dot]com.

cheapjerseysaol[dot]com.

cheapjerseysaol[dot]us.

cheapjerseysaols[dot]com.

cheapjerseyselite.us[dot]com.

cheapjerseysfromchina.us[dot]com.

cheapjerseysoccer.us[dot]com.

cheapjerseysofchina[dot]com.

cheapjerseysrl[dot]com.

cheapjerseyssc[dot]com.

cheapjerseyssoccer[dot]us.

cheapjerseysstitched[dot]us.

cheapjerseystn[dot]com.

cheapjerseysvs[dot]com.

cheapjerseyswholesale[dot]us.

cheapjerseyswholesale.us[dot]com.

cheapjerseyswholesalechina[dot]us.

cheapjerseysww[dot]com.

cheapjerseyusa[dot]us.

cheapjerseywholesale[dot]us.

cheapjerseywholesaleonline[dot]net.

cheapjimmychoo-sale[dot]com.

cheaplacostestore[dot]com.

cheaplululemoncanada[dot]com.

cheapmaccosmetickit[dot]com.

cheapmacwholesales[dot]com.

cheapmcmbagsprices[dot]com.

cheapmlbjerseys[dot]me.

cheapnfljersey.us[dot]com.

cheapnfljerseyforsale[dot]us.

cheapnfljerseyhouse[dot]com.

cheapnfljerseys[dot]me.

cheapnfljerseysatusa[dot]com.

[...]

Some of Those May Date To June 2010...

- We should probably focus on just "recent" stuff (last 30 days?)
- (At least some) Passive DNS solutions can "time fence" results

- $ dnsdb_query.py **--after=30d** *[etc]*

```
$ dnsdb_query.py --after=30d -n nsdo.cloudang.com > nsdo.cloudang.com.txt
$ wc -l nsdo.cloudang.com.txt
   511 nsdo.cloudang.com.txt
$ awk '{print $1}' < nsdo.cloudang.com.txt | sort | uniq > temp-cloudang.txt
$ wc -l temp-cloudang.txt
   314 temp-cloudang.txt
```

- Notice the reduced number of domains. This is GOOD (you won't waste time on old stuff that isn't currently being used). **A list of the domains from temp-cloudang.txt is on the following slides.**

[...]
1to1replica[dot]com
2014winteroutlet[dot]com
2015discountsunglasses[dot]com
27dress[dot]com
88-percent-off[dot]com
a123ev[dot]com
adornfaceart[dot]com
amaxeshop[dot]com
arizonacardinals[dot]us[dot]com
asicstrainers[dot]me[dot]uk
basketpumahomme[dot]com
bcombag[dot]com
bearsnflofficialprostore[dot]com
bengalsnflprostore[dot]com
big-discount-sunglasses[dot]com
brand-sunglasses-outlets[dot]com
brand-sunglasses-sale[dot]com
brandnamebagdiscount[dot]it
broncosauthenticofficialstore[dot]com
broncosnflofficialonline[dot]com
broncosnflofficialproshop[dot]com
broncosofficialnflonline[dot]com
broncosshopnfl[dot]com
cappelliobey[dot]com
casquettenewera2014[dot]com
casquetteunkut[dot]com
chargersofficialauthentic[dot]com
cheapjerseyfreeshipping[dot]us[dot]com
cheapjerseysace[dot]us[dot]com
cheapjerseysaol[dot]com
cheapjerseysaol[dot]us
cheapjerseysaols[dot]com
cheapjerseysfromchina[dot]us[dot]com
cheapjerseyssoccer[dot]us
cheapjerseysvs[dot]com
cheapjerseyswholesale[dot]us
[continued]

cheapjimmychoo-sale[dot]com
cheapmaccosmetickit[dot]com
cheapmcmbagsprices[dot]com
cheapnfljersey[dot]us[dot]com
cheapnfljerseysatusa[dot]com
cheapnfljerseyschina[dot]cc
cheapnfljerseyschina[dot]us[dot]com
cheapnfljerseyschinazz[dot]com
cheapnfljerseystn[dot]com
cheapnfljerseysusa[dot]us[dot]com
cheapnfljerseysusaonline[dot]com
cheapnfljerseyswr[dot]com
cheapnfljerseyszz[dot]com
cheapnikenfljerseysonline[dot]com
cheapoakleyhut2015[dot]com
chiefsauthenticofficialshop[dot]com
chiefsnflofficialauthentics[dot]com
chinacheapnfljerseys[dot]us[dot]com
chinanfljersey[dot]us[dot]com

christianlouboutinstore[dot]cc
colorfulcheapsunglasses[dot]com
coltsnflprostore[dot]com
coltsonlineofficialstore[dot]com
coltsonlineprostore[dot]com
coltsshop[dot]us[dot]com
cowboysnflofficialshop[dot]com
ctcefour[dot]com
denverbroncos[dot]us[dot]com
dinofree[dot]com
discount-outlets-shop[dot]com
discount-outlets-store[dot]com
discount-sunglasses-shop[dot]com
dobussiness[dot]com
dolphinsshop[dot]us[dot]com
e6case[dot]com
eaglesnflofficialauthentic[dot]com
eaglesofficialonline[dot]com
[continued]

eb-prada[dot]com
elitecheapjerseys[dot]us
eraybanxx[dot]com
falconsofficialnfljerseys[dot]com
focaltopend[dot]com
footballbroncosproshop[dot]com
footballjaguarsstore[dot]com
footballseahawksproshop[dot]com
footballseahawksprostore[dot]com
g-star-outlet[dot]net
gcombag[dot]com
giantsfootballprostore[dot]com
glasinbuy[dot]com
glasses-tops[dot]com
glassesonline[dot]cc
glassessup[dot]com
great-discount-sunglasses[dot]com
gstarrawuk[dot]com
guccishoprakuten[dot]com

handbagstoby2014[dot]com
high-quality-sunglasses-shop[dot]com
high-quality-sunglasses-store[dot]com
high-quality-sunglasses[dot]com
hogan-good[dot]com
hogan-its[dot]com
hogancoupons[dot]com
ibestreplicawatches[dot]com
ibestreplicawatches[dot]net
iphone-cases-4[dot]com
jersales[dot]com
jerseys-nfl[dot]org
jerseysauthentic[dot]us
jerseyscheap[dot]cc
jerseyschinaonline[dot]us[dot]com
jerseyschinawholesale[dot]us[dot]com
jerseyselite[dot]us
jerseywholesalechina[dot]us

[continued]

jerseywholesaleprostore[dot]com
jetsshop[dot]us[dot]com
kansascitychiefs[dot]us[dot]com
lionsofficialauthentic[dot]com
louisvuitton-online-outlets[dot]com
louisvuittonoutlet[dot]us[dot]org
louisvuittonstyle[dot]com
lv-online-outlets[dot]com
lzzstock[dot]com
maccosmetickitsale[dot]com
macmakeup-kit[dot]com
macmakeupsites[dot]com
michaelkorsoutlet[dot]ca
mk-online-outlet[dot]com
mk-online-outlets[dot]com
mk-outlet-shop[dot]com
mk-shop-online[dot]com
mk-store-online[dot]com
moncler-online-outlets[dot]com

moncler-outlets-online[dot]com
mskeyoffer[dot]com
nbacheapjerseys[dot]com
nbacheapjerseys[dot]us
nbajerseyscheap[dot]cc
nflbears[dot]us[dot]com
nflbearsofficial[dot]com
nflbengals[dot]us[dot]com
nflbills[dot]us[dot]com
nflbroncosofficialonlines[dot]com
nflbroncosofficialshops[dot]com
nflbuccaneers[dot]us[dot]com
nflchargersofficial[dot]com
nflcheapjersey[dot]us
nflchinajersey[dot]us
nflcowboys[dot]us[dot]com
nflcowboysofficialshops[dot]com
nfleagles[dot]us[dot]com

[continued]

nflfalcons[dot]us[dot]com
nflgiants[dot]us[dot]com
nflgiantsofficialonlines[dot]com
nfljerseychina[dot]us[dot]com
nfljerseys2015[dot]us
nfljerseys2016[dot]com
nfljerseyschina[dot]cc
nfljerseyschinaokc[dot]com
nfljerseysforsale[dot]us[dot]com
nfljerseysnikecheap[dot]com
nfljerseywholesale[dot]us[dot]com
nfljets[dot]us[dot]com
nfllionsofficial[dot]com
nflpackers[dot]us[dot]com
nflpackersofficial[dot]com
nflpanthers[dot]us[dot]com
nflpatriots[dot]us[dot]com
nflpatriotsofficial[dot]com
nflravens[dot]us[dot]com

nflredskinsofficial[dot]com
nflsaints[dot]us[dot]com
nflseahawksofficial[dot]com
nflshopauthenticonline[dot]com
nflshopny[dot]com
nflshoppa[dot]com
nfltexans[dot]us[dot]com
nflvikings[dot]us[dot]com
nike-in[dot]com
nikeair[dot]fr
nikedunk[dot]fr
nikefreegousa[dot]com
nikeicool[dot]com
nikeiok[dot]com
nikenflcheapjerseys[dot]us
nikeoks[dot]com
nikeplace[dot]com
nikesneaker[dot]com
[continued]

nikesneakerbox[dot]com

oakleystore[dot]cc

official49ersnflproshop[dot]com

officialauthenticdolphins[dot]com

officialbaseballcardinals[dot]com

officialbaseballrangers[dot]com

officialbullsauthentic[dot]com

officialbullsauthentics[dot]com

officialchargersnflshop[dot]com

officialfalconsnflauthentic[dot]com

officialfootballbills[dot]com

officialfootballravensstore[dot]com

officiallysnfljersey[dot]com

officialmoncler[dot]us[dot]com

officialnbaauthentic[dot]com

officialnflshopco[dot]com

officialnflvikingsprostore[dot]com

officialnikeshoes[dot]com

officialpackersnflproshop[dot]com

officialpatriotsonlineprostore[dot]com

officialravensnflauthentic[dot]com

officialsanfranciscogiantsshop[dot]com

officialtitansnflauthentics[dot]com

officialusahockeystore[dot]com

okbagsjp[dot]com

omyglasses[dot]com

outlet-nike[dot]org

outlet-prada[dot]com

outlet-toms[dot]org

outletjuicy-couture[dot]org

outlettoms[dot]org

packersshop[dot]us[dot]com

packlinemondiale[dot]com

panthersauthenticofficial[dot]com

panthersnflofficialprostore[dot]com

panthersofficialproshop[dot]com

panthersshop[dot]us[dot]com

[continued]

patriotsnflofficialonline[dot]com
patriotsnflofficialproshop[dot]com
perfectcopymall[dot]com
perfectkickz[dot]ru
philalvin[dot]com
r4-ds-r4i[dot]com
ravensnflofficialproshop[dot]com
rayban-globals[dot]com
rayban-me[dot]com
rayban-sports[dot]com
rayban-website[dot]com
raybanhutofficial[dot]org
raybanon-line[dot]cc
raybanshop4us[dot]com
raybansport[dot]com
raybanssaleofficials[dot]org
rb-bestseller[dot]com
rb-discount-store[dot]com
redskinsonlineprostore[dot]com

rogervivier-china[dot]com
saclvdesigner[dot]fr
saclvnice[dot]com
salebrandsunglass[dot]com
sandiegochargers[dot]us[dot]com
sassorentacar[dot]com
seahawksfootballprostore[dot]com
seahawksofficialprostore[dot]com
seattleseahawks[dot]us[dot]com
serabatt-rb[dot]com
serabatte-rb[dot]com
shoesinstore[dot]org
shopbrownsnfljerseys[dot]com
shopeaglesnfljerseys[dot]com
sneakerhead[dot]fr
sneakersbrand[dot]com
sneakersseller[dot]com
special-offer-sunglasses-shop[dot]com
[continued]

special-offer-sunglasses-store[dot]com
special-offer-sunglasses[dot]com
sportsoutletsonline[dot]com
ssyfw[dot]com
starstatusfashion[dot]com
steelersonline[dot]us[dot]com
stylomontblancbille[dot]com
stylomontblancvend[dot]com
summer-rayban[dot]com
summer-sale-sunglasses-shop[dot]com
summer-sale-sunglasses-store[dot]com
sunglass-coupons[dot]com
sunglasses-omg[dot]com
sunglassesdiscount2015[dot]com
sunglasseshop[dot]eu
sunglassetopsale[dot]com
sunglasshut[dot]cc
sunglasshut[dot]us[dot]com
super-eshops[dot]com
superolexweb[dot]com
tdmexico[dot]com
teamjerseybuy[dot]biz
teamsjerseysbuy[dot]com
teamusahockeyjersey[dot]com
texansnflofficialonline[dot]com
texansonlineprostore[dot]com
thebestsunglasses2015[dot]com
thingroom[dot]org
timberlandtimes[dot]com
tissotmontre[dot]com
tods-china[dot]com
tomsoutletlocations[dot]com
topendmall[dot]com
topendnewatch[dot]com
topshowtime[dot]com
uggaustralia-outlets[dot]com
ugguggs[dot]fr

[continued]

umeb[dot]net

usa-brand-sunglasses-shop[dot]com

usa-brand-sunglasses[dot]com

usa-outlets-store[dot]com

usa-sunglasses-shop[dot]com

vikingsonlineofficialstore[dot]com

warriorsofficialshop[dot]com

watchesforbuck[dot]com

wazlam[dot]com

wholesalefactory88[dot]com

wholesalejerseysagent[dot]us[dot]com

wholesalejerseysaz[dot]com

wholesalejerseyschina[dot]cc

wholesalejerseysonline[dot]cc

wholesalejerseyssupply[dot]us[dot]com

wholesalejerseysusonline[dot]us

wholesalenfljerseys[dot]us[dot]com

wildcarewv[dot]org

Finding Other Potentially Problematic Nameservers

- We've just found **a single name server** that has had over 300 potentially-problematic domains used in the last 30 days (as always, explicitly review and confirm ACTUAL problematic domain usage prior to any action)
- An easy way to find more name servers of potential interest is to do an rdata query on a domain known to be of interest:

  ```
  $ dnsdb_query.py -r elitejerseyscheapnfl[dot]com/ns
  ```

  This query looks for **other** name server records that have historically been seen used by that domain name. Condensing the output from that query, it appears that the subject domain has used name servers from the set: dns.bizcn.com, dns.cnmsn.net, f1g1ns[12].dnspod.net, and ns[5678].cnmsn.net
- Each of those could then be investigated further, etc.

9. (Potentially) Tricky Bits

Bits That Require A Little Finesse

- Most uses for passive DNS are pretty straight forward, but there are some situations that require a little more *savoir faire*.

- We'll just quickly consider four such scenarios:

  (i) Busy name servers
  (ii) Already-mitigated domains
  (iii) Parked domains
  (iv) Wildcarded domains

(i) Busy Name Servers

- Another Google result for our original jersey query was www.johnstonbaughs[dot]com

- www.johnstonbaughs[dot]com ➔ wholesaleforjerseys[dot]com

- $ **dig +trace wholesaleforjerseys[dot]com**

```
wholesaleforjerseys[dot]com. 172800    IN   NS  f1g1ns1.dnspod.net.
wholesaleforjerseys[dot]com. 172800    IN   NS  f1g1ns2.dnspod.net.
[snip]
wholesaleforjerseys[dot]com. 600   IN   A    5.157.2.40
wholesaleforjerseys[dot]com. 600   IN   NS  f1g1ns2.dnspod.net.
wholesaleforjerseys[dot]com. 600   IN   NS  f1g1ns1.dnspod.net.
[snip]
```

What Do We See If We Check f1g1ns2.dnspod.net?

-
  ```
  $ dnsdb_query.py --after 30d -l 1000000 -n f1g1ns2.dnspod.net > f1g1ns2.dnspod.net.txt
  ```

-
  ```
  $ wc -l f1g1ns2.dnspod.net.txt
   1000000 f1g1ns2.dnspod.net.txt
  ```
  [note: a max of 1,000,000 results may be returned from DNSDB]

-
  ```
  $ grep jersey f1g1ns2.dnspod.net.txt
  ajerseys[dot]biz. IN NS f1g1ns2.dnspod.net.
  luckyjerseys[dot]biz. IN NS f1g1ns2.dnspod.net.
  cheapnfl-jerseys[dot]biz. IN NS f1g1ns2.dnspod.net.
  ```
  [that's not much]
- If you visit https://www.dnspod.cn/ in Chrome (for automatic site translation from Chinese into English), you'll see that this is a **major** Chinese outsourced DNS provider servicing 3.42 million websites, and accessed 31.1 billion times/day.

Time Fencing More Aggressively

- We found more than a million results with a 30 day window
- What do we see for a 7 day window? Still a million+
- Two day window? Still a million+
- How about a 36 hour window? Still a million +
- How about a 30 hour window? Still a million +
- 29 hour window? Still a million+
- 28 hour window? Still a million+
- How about a 27 hour window? Finally, **"just"** 553,876 hits

- Now when we search those results for "jersey" we find 662 hits, many of which appear to be worth investigating further.

- By constraining our search, we found more relevant results.

(ii) Already-Mitigated Domains

- In other cases, some domains may (still) resolve, but they may nonetheless be already mitigated. You don't want to waste your time on domains that have already been mitigated.

- As an example, assume you saw nearly 400 suspicious domain names on 74.81.170.110. For example, one domain that resolves to 74.81.170.110 is:

  ```
  $ dig www.nhlnfljersey[dot]com +short
  74.81.170.110
  ```

- You might (wrongly) think, "Ahah! 74.81.170.110 must be some sort of hotbed of infringement! Let me focus on that IP and the domains associated with it..."

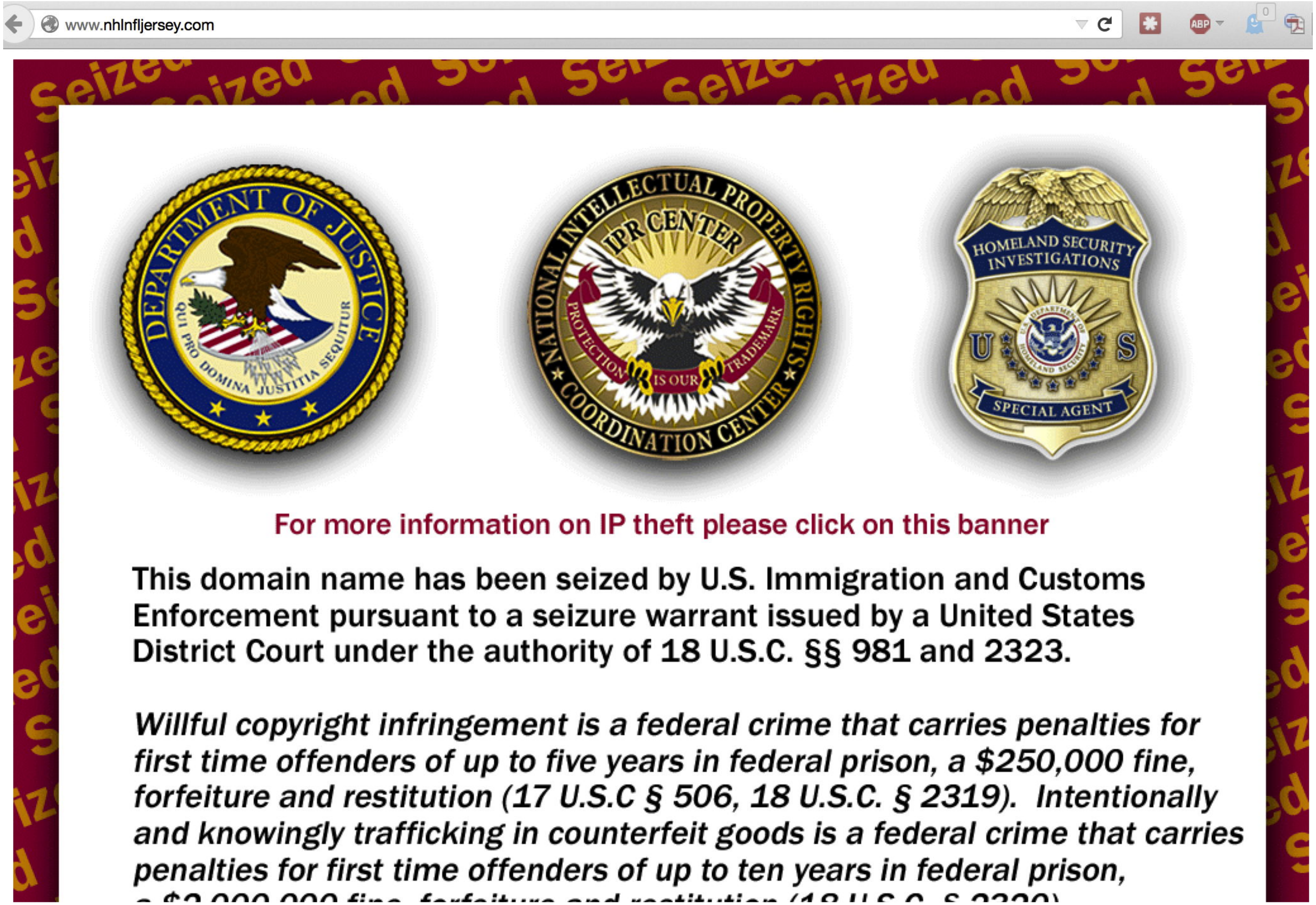
So Who Has 74.81.170.110? Let's Check whois

-
  ```
  $ whois 74.81.170.110
  [snip]
  CaroNet Managed Hosting, Inc. CI-74-81-170-0-23 (NET-74-81-170-0-1)
  74.81.170.0 - 74.81.171.255
  Carolina Internet, Ltd. CARO-NET-ARIN-4 (NET-74-81-160-0-1) 74.81.160.0 -
  74.81.191.255
  ```

-
  ```
  $ whois -h whois.arin.net NET-74-81-170-0-1
  NetRange:       74.81.170.0 - 74.81.171.255
  [snip]
  ReferralServer:  rwhois://rwhois.carohosting.com:43
  ```

-
  ```
  $ telnet rwhois.carohosting.com 43
  74.81.170.110
  [snip]
  OrgName: immixGroup
  OrgID: immixgroup
  NetRange: 74.81.170.107 - 76.76.23.162
  ```
- Googling for immixGroup yields clue #1
- Actually looking at any of the domains hosted on that IP provides clue #2 ☺

What Visitors See If/When A Domain Gets Seized


www.nhlnfljersey.com
Seized
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER
IPR CENTER
PROTECTION IS OUR TRADEMARK
HOMELAND SECURITY INVESTIGATIONS
U S
SPECIAL AGENT

For more information on IP theft please click on this banner

This domain name has been seized by U.S. Immigration and Customs Enforcement pursuant to a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. §§ 981 and 2323.

Willful copyright infringement is a federal crime that carries penalties for first time offenders of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C § 506, 18 U.S.C. § 2319). Intentionally and knowingly trafficking in counterfeit goods is a federal crime that carries penalties for first time offenders of up to ten years in federal prison, a $2,000,000 fine, forfeiture and restitution (18 U.S.C. § 2320).

(iii) Parked Domains

- Some domain names that may "superficially" appear to potentially be of interest may actually resolve to IP addresses that have a "gazillion" domains on them.
- For example, consider the IP address 141.8.225.80:

```
$ dnsdb_query.py --after 30d -l 1000000 -i 141.8.225.80 >
    141.8.225.80.txt
$ wc -l 141.8.225.80.txt
  150393 141.8.225.80.txt                    ← a lot of results found
```

- When we check whois, however, we see that that IP address is associated with Rook Media. Rook Media is known to be a Swiss domain monetization service (e.g., a company that sells ads on parked domain names)

(iv) Wildcarded Domains

- Other times you may run into IP addresses that have a large number of unique fully qualified domain names (FQDNs), but only a handful of unique base domains.

- This is often symptomatic of wildcarded domain names.

- Wildcarded domain names may be used for a variety of purposes, including:

  -- Attempting to keep any individual FQDN from looking too 'hot' to traffic analysts

  -- Tracking individuals on a per-person basis (e.g., in an attempt to identify message "opens"/potential customer interest, or in an attempt to "out" data sources submitting data for "list washing" purposes)

Stripping Wildcards

- When you encounter wildcarded domains, you will likely want to strip the wildcarded chunk from the left hand side of those domains, and keep the base domain.
- This can be done with a series of regex expressions in the vi editor, e.g., you might copy and paste a series of expressions such as the following, one per top level domain:

  ```
  :1,$s/\(^.*\.\)\(.*\)\(\.com\.$\)/\2\3/
  :1,$s/\(^.*\.\)\(.*\)\(\.ru\.$\)/\2\3/
  :1,$s/\(^.*\.\)\(.*\)\(\.xyz\.$\)/\2\3/
  :1,$s/\(^.*\.\)\(.*\)\(\.science\.$\)/\2\3/
  :1,$s/\(^.*\.\)\(.*\)\(\.co\.uk\.$\)/\2\3/
  [etc]
  ```
- Note that this is less than ideal since there will be some *effective* TLD domains that might exist *above* the real TLDs (see https://wiki.mozilla.org/Public_Suffix_List)

A Cleaner Approach: public_suffix script

```
#!/usr/bin/perl
use strict;
use warnings;
use IO::Socket::SSL::PublicSuffix;

my $pslfile = 'fullpathhere/effective_tld_names.dat';
my $ps = IO::Socket::SSL::PublicSuffix->from_file($pslfile);
my $line;

foreach $line (<>) {
        chomp($line);
        my $second_lvl_domain = $ps->public_suffix($line,1);
        printf( "%s\n", $second_lvl_domain );
}
```

10. Watching Passive DNS Data in Real Time

The REALLY Impressive Bit: Real Time DNS Data

- Cool as it is to work with **historical** passive DNS data, it's even *cooler* to work with **real time** passive DNS data. If you participate at the FSI Security Information Exchange, you can watch real time pDNS data, as it's received at SIE and gets added to DNSDB.

  For example, we can set up an encrypted channel to monitor raw passive DNS traffic on Channel 202 at the SIE:

  ```
  $ sratunnel -s 'ssh username@host' -c 202 -w ch=202 \
  -o nmsg:udp:127.0.0.1,8000 &
  ```

  We can then monitor that local data stream for rrnames='jersey'

  ```
  $ nmsgtool -l 127.0.0.1/8000 | grep rrname | grep jersey
  ```

  When done, we'll kill that tunnel:

  ```
  $ kill %sratunnel
  ```

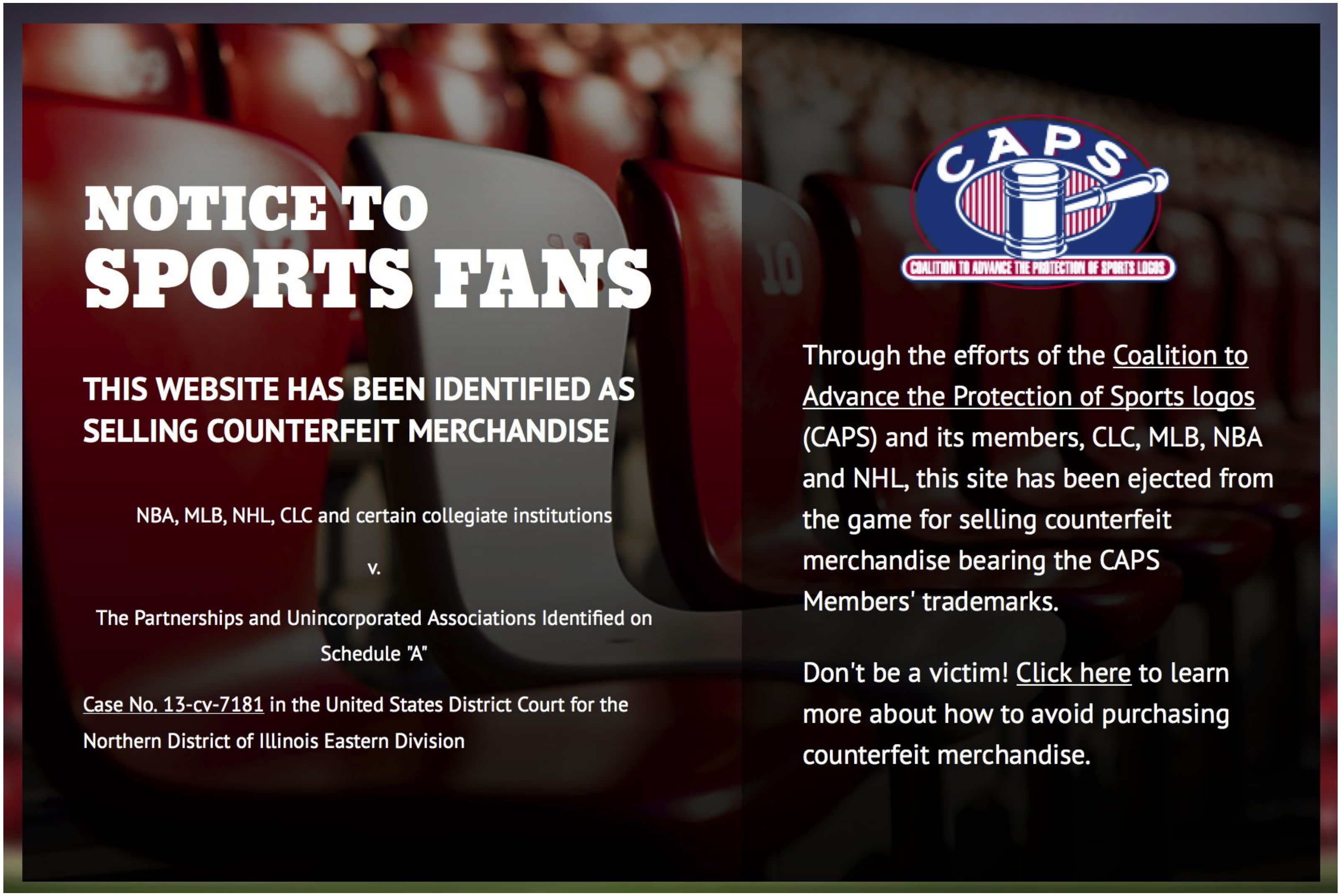
Selected Output (Dropping NJ Stuff, Dupes, Etc.)

```
rrname: www.repnfljerseys[dot]ru.
rrname: discountnfljerseysshop[dot]com.
rrname: www.cheapauthentic-jerseys[dot]com.
rrname: ww2.cheapjerseysdirect[dot]com.
rrname: authenticraidersjerseyshop[dot]com.
rrname: customnfljerseys[dot]com.
rrname: blog.authenticraidersjerseyshop[dot]com.
rrname: www.nbajerseys[dot]org.
rrname: www.jerseygoodstore[dot]ru.
rrname: wholesalenfljersey[dot]biz.
rrname: footballjerseyscheap[dot]ru.
rrname: nbajerseyssale.weebly[dot]com.
rrname: nikenfljerseyscool[dot]us.
[etc]
```

An Example From That List...

```
$ whois nikenfljerseyscool.us
Domain Name:                              NIKENFLJERSEYSCOOL.US
[snip]
Registrar URL (registration services):    whois.markmonitor.com
[snip]
Registrant Name:                          National Football League
Registrant Organization:                  NFL
Registrant Address1:                      345 Park Ave.
Registrant City:                          New York
Registrant State/Province:                ny
[snip]
Registrant Email:                         dns_admin@nfl.com
[snip]
```

If We Visit That "Unusually Named" Site, We See...



NOTICE TO
SPORTS FANS

THIS WEBSITE HAS BEEN IDENTIFIED AS SELLING COUNTERFEIT MERCHANDISE

NBA, MLB, NHL, CLC and certain collegiate institutions

v.

The Partnerships and Unincorporated Associations Identified on Schedule "A"

Case No. 13-cv-7181 in the United States District Court for the Northern District of Illinois Eastern Division

Through the efforts of the Coalition to Advance the Protection of Sports logos (CAPS) and its members, CLC, MLB, NBA and NHL, this site has been ejected from the game for selling counterfeit merchandise bearing the CAPS Members' trademarks.

Don't be a victim! Click here to learn more about how to avoid purchasing counterfeit merchandise.

List of 893 seized domains can be found at:
http://gbcinternetenforcement.net/files/caseNo-13-cv-7181/SCHEDULEA.PDF

11. Summary/Conclusion

We've Covered A LOT Of Ground Today, Including...

- Talking about why cyber crime is so attractive to the bad guys
- Why it's so hard for the good guys to investigate and prosecute
- Finding and expanding initial leads using common search engines
- Domain whois (including whois data accuracy considerations)
- Mapping domains → IP addresses with dig
- Hosting (regular & so-called "bulletproof" hosting) & takedowns
- The importance of finding ALL related domains when it comes to avoiding incomplete/ineffective takedowns
- DNS as a indirect/proxy measure for virtually everything that happens on the Internet
- How passive DNS works and the sort of questions it can answer
- A brand protection example, starting by querying pDNS by IP
- The importance of validating bad content on any identified sites

We've Covered A LOT Of Ground Today (cont.)

- Another approach, following name servers instead of IP addrs
- Doing a third type of passive DNS query (rdata queries) to find additional potential name servers we might check
- Dealing with some potentially tricky bits:
  - Particularly busy name servers
  - Recognizing already-mitigated allegedly-infringing domains
  - Identifying parked domains
  - Simplifying wildcarded domains
- We also watched passive DNS in real time for keywords
- **Whew!** I know that's been a LOT of material to absorb, but the good news is that this is just meant to be an intro/overview – we can't make you an expert on all these topics with just one quick session today. We do hope, however, that this session showed the power of this approach, and maybe piqued your interest.

THANK YOU!

- Are there any questions?