Guide to Reporting Domain Name Abuse

A resource for law enforcement professionals and others impacted by Internet abuse.

Rightside™

Introduction

This document is a resource for law enforcement, government agencies, copyright/trademark holders, or anyone researching a complaint about a domain name or names. The Internet is a vast and complex landscape and often not the complaining party's area of expertise. The differences between a domain name and the content of a website can be unclear. Navigating the nuances can be tricky.

The purpose of this document is to provide clarification regarding the key terms and issues regarding domain names, as well as to help direct inquiries and complaints to the appropriate parties; hopefully, saving time and resources for everyone involved. This document also provides guidance on submitting effective subpoenas and court orders.

Glossary

TLD	*Top-Level Domain* The name following the "dot" such as com, net, info, ninja, news
Registry	An organization which maintains a database containing the information regarding a particular TLD name registered
Registrar	An organization that has an account with a Registry and provides the ability to buy and manage domain names

Reseller	Someone who has an agreement with a registrar to use their back end technology to resell domains to their own customers
ICANN	*Internet Corporation for Assigned Names and Numbers*
WHOIS	a TCP-based protocol used for querying a database in order to determine the holder of a domain name
Registrant Contact	A WHOIS contact field and the domain holder
Administrative Contact	A WHOIS contact field, able to approve transfers
gTLD	*Generic Top-Level Domain* e.g. .com, .net, .info, .ninja, .news, etc.
ccTLD	*Country Code Top-Level Domain* e.g. China = .cn
SLD	*Second-Level Domain* The word, number, or letters before the "dot" such as Google, Microsoft, Rightside, etc.
Sub-Domain	Sometimes called *Third-Level Domain* e.g. "maps" in maps.google.com

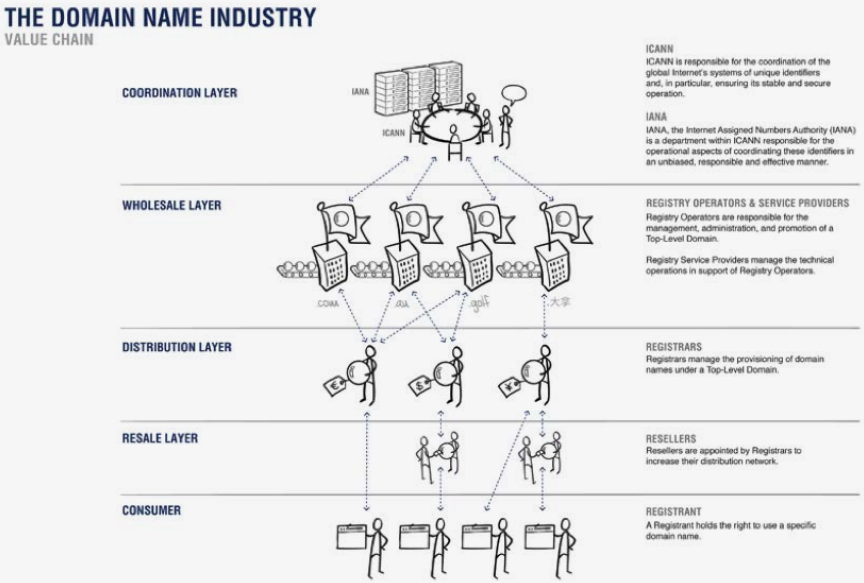

FIGURE 1: The different layers of the domain industry

The Four "Rs" of Domains

To understand domain name registration, you must know the difference between the four "Rs"—**registries, registrars, resellers, and registrants**.

Registries are the database managers of a specific top level domain name, or "TLD." For example, the registry for .COM and .NET is VeriSign, a company based in Reston, Virginia. Registrars sell domain names to end users. They are permitted to do so under contracts they sign with the registry. Consumers can also buy domain names from domain name "resellers" which are third parties that contract with registrars to use their registrar registration platform to sell domain names to their customers. If you suspect a domain name is registered with a reseller you can use the reseller lookup tool located here.

Finally, there is the registrant, or end user of a domain name. **FIGURE 1** (above) is visual rendering of the different layers of the domain industry published by the Internet Corporation of Assigned Names and Numbers (ICANN).

The Difference Between a Domain Name and a Website

A common misconception is that a domain name and website are the same thing. They are not and the difference is important. The domain name is a string of letters that represents a web address, and that address makes it easier to find the content and information the user is looking for on the Internet. It's like a phone number.

A website, however, is the content users see when they use a domain to navigate the Internet. The person who registers a domain name is quite often the same person who provides the content on a website, but he or she may also be different.

When a domain name is registered with a registrar, it is up to the registrant to determine who will "host" the content they wish to appear at that web address. Hosting is a separate service for which registrants must pay an additional fee. While registrars may offer web hosting services there are many instances where the registrar and web host are not the same entity. In some cases the registrant may simply be redirecting the domain name to another existing website.

Registrars direct newly registered domain names to a "parking page" until the registrant specifies the content it wishes to be displayed or "resolve" on that website. A parking page is simply a placeholder page usually containing advertisements returned by a third party advertising provider like Google or Yahoo!.

The distinction between a domain name and a website is critical because a registrar that is NOT the host for the website will be unable to remove any content associated with a website. Conversely, a web host may be able to remove specific content, but would not have the ability to take down or delete a domain name.

Finding the Registrant Contact

Contacting the domain registrant is the appropriate first step to addressing an issue of abuse concerning the use of a domain name or the content of a website. "WHOIS" is a database that contains the registrant information for every domain name registered. There are many WHOIS lookup services out there, such as www.who.is (see **FIGURE 2**, below). If a domain registrant contact information is found to be invalid, evidence of such can be sent directly to the registrar of the domain name or to ICANN. Registrants are obligated under the terms of their service agreement to maintain accurate and complete registrant contact information. WHOIS information can also be searched at certain registries such as Neustar and Public Interest Registry. These registries maintain their own database of WHOIS information. There can be issues with synchronizing information between registry and registrar, and in those cases the registrar has the most updated information.

Privacy and Proxy Services

Privacy and proxy services provide privacy protection to registrants of domain names by masking their contact information that is shown in the WHOIS record. There are many reasons why a registrant may seek a privacy service including wanting to reduce unsolicited emails, personal or professional security concerns, or for companies preparing to launch new projects and don't want

Raw Registrar Data

```
Registrant Contact Information:
    Name: DNS Manager
    Organization: Rightside Group, Ltd.
    Address 1: 5808 Lake Washington Blvd. NE
    Address 2: Suite 300
    City: Kirkland
    State: WA
    Zip: 98033
    Country: US
    Phone: +1.4259744689
    Fax: +1.4259744791
    Email: domains@rightside.co

Administrative Contact Information:
    Name: DNS Manager
    Organization: Rightside Group, Ltd.
    Address 1: 5808 Lake Washington Blvd. NE
    Address 2: Suite 300
    City: Kirkland
    State: WA
    Zip: 98033
    Country: US
    Phone: +1.4259744689
    Fax: +1.4259744791
    Email: domains@rightside.co

Technical Contact Information:
    Name: DNS Manager
    Organization: Rightside Group, Ltd.
    Address 1: 5808 Lake Washington Blvd. NE
    Address 2: Suite 300
    City: Kirkland
    State: WA
    Zip: 98033
    Country: US
    Phone: +1.4259744689
    Fax: +1.4259744791
    Email: domains@rightside.co

Billing Contact Information:
    Name: DNS Manager
    Organization: Rightside Group, Ltd.
    Address 1: 5808 Lake Washington Blvd. NE
    City: Kirkland
    State: WA
    Zip: 98033
    Country: US
    Phone: +1.4259744689
    Fax: +1.4259744791
    Email: domains@whoisprivacyprotect.net


Information Updated: Wed, 19 Aug 2015 01:06:23 UTC
```

FIGURE 2: Sample Whois Output from www.who.is

a new domain name associated with their company name. Some of these services are provided by registrars, such as Whois Privacy Protection Service (provided by Name.com & eNom) or Domains By Proxy (provided by GoDaddy). Other services are offered by third parties like WhoisGuard. If the privacy service is not provided by the registrar, the registrar will not have access to the underlying registrant contact information.

Finding the Web Host and/or the Email Provider

If someone has a complaint regarding content on a website and the registrant can't be contacted (either because he is not responsive to inquiries or has purchased a privacy or proxy service), the next contact should be the web host. There are several ways to locate a web host. The easiest method is to use a lookup service, such as www.whoishostingthis.com. Another method is by "pinging" the domain name to find the IP address responding for that website. One resource for performing a ping can be found at www.network-tools.com (see **FIGURE 3**, below). This tool can also be used to view MX (mail) records for a domain name.

Once the IP address is acquired it can be entered into a WHOIS lookup service, such as www.who.is or www.arin.net to find the contact information for the Administrator of the IP Address. This IP Administrator may actually be the web host or have more information regarding the host of the content.

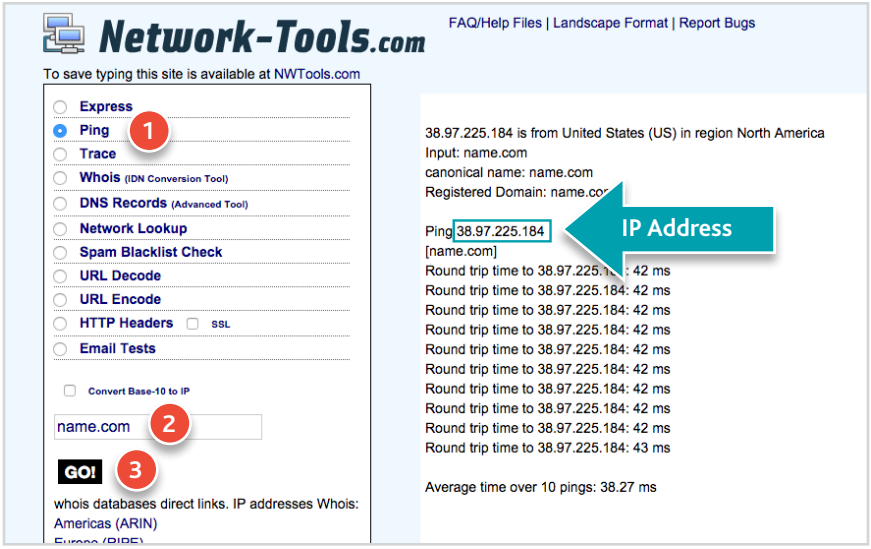

FIGURE 3: Example Ping—www.network-tools.com

DMCA

In most cases, the registrar is NOT the web host for a domain name and is technically incapable of removing specific items of objectionable content. However, if the registrar is also acting as the web host it is appropriate to report copyright issues to the registrar. The Digital Millennium Copyright Act or DMCA, is designed to protect both copyright holders and web hosts. The process involves the copyright holder or authorized representative submitting the complete details of the infringement under penalty of perjury. The web host will remove the content and the customer has the opportunity to submit a counter notification to have the content reinstated if no lawsuit is filed by the complainant in the time period allowed by the DMCA.

Trademark

In the case where the domain name itself is alleged to infringe a trademark, ICANN has created a process for resolving such disputes called the Uniform Dispute Resolution Proceedings (UDRP). This process was created so that ICANN, registries, and registrars do not have to act as intermediaries between two adverse parties. Registries and registrars, in particular, are not in a position to adequately investigate or make a determination in a trademark dispute. In every UDRP case, the final decision of the administrative hearing dictates what happens to the domain name. Registries and registrars must "lock" the domain name during UDRP proceedings and agree to transfer the domain if so instructed by the UDRP panel.

Subpoenas

Most registries and registrars generally require a properly issued subpoena before they can take release information related to a domain name or registrant. When issuing a subpoena to a registrar or registry, always identify the specific domains that are covered by the subpoena as this will help registrars locate data and information related to the domain name and the registrant. One common error for registrar subpoenas is requesting information relating to a specific IP address at a specific time. In most cases this information is regarding who accessed a website at a specific date and time. Sometimes when the investigating party searches the IP address the domain name owned by the IP administrator is registered with eNom. If the registrar is not the administrator of an IP address they will not be able to provide the information sought. The registrar will only have information regarding who registered the domain name unless they are also acting as the web host or email provider.

The specific time period for a request should be included if known. Domain names can change hands over time and narrowing down a request can result in less confusing data being returned to the requestor. If the registrant should not be notified of the subpoena request, a confidentiality request should be included in the subpoena.

Court Orders

Court orders should never include the name of a registrar or registry as a party to the litigation but should be as clear as possible with respect to what action the registrar or registry needs to take with respect to a particular domain.

Below are some terms that are helpful when crafting an order for a registrar to take action on a domain:

Hold/Suspend	Stop a domain name from resolving to its content
Transfer	Take a domain name away from the current registrant and place it into another's possession
Redirect	Change the destination to which a domain resolves
Lock	Prevent a domain from being transferred to another registrar

Bankruptcy

Typically, a registry or registrar will not be able to assist with bankruptcy proceedings but will comply with any order issued by a bankruptcy court. If assets including domain names are part of such proceedings, the complainant will need to retrieve access from the current registrant of the domain name. The registry or registrar cannot make any determination as to who the rightful registrant of the domain name should be. If the registrant is not compliant and the complainant requires the transfer of domains or account access, a court order of appropriate jurisdiction instructing the registry or registrar to take specific action will be required.

A Note About gTLDs, nTLDs and ccTLDs

Generic TLDs are subject to ICANN policies and are generic terms like .com, .net, .biz, .info. There are also new generic TLDs (nTLDs) approved by ICANN such as .ninja, .attorney, and many others providing Registrants with the the ability to customize the domain to their specific interest or business application. ICANN has created a faster dispute resolution process for nTLDs called the Uniform Rapid Suspension or URS.

Country code TLDs are two characters long and generally reserved for a specific country such as .us, .de, and .cn. The registries managing the ccTLDs each have their own rules and procedures for their specific domains including their own processes for domain disputes. For example, .ca domains have their own dispute resolution process called the CDRP. Registrants of ccTLDs may also have a relationship directly with the registry and may still be able to make changes and or transfer domains even if the name has been locked at the registrar level. In those cases, complainants should seek enforcement at the registry level.

Legitscript and Rogue Pharmacies

Rightside has actively combated illegal online pharmacies through a multi-faceted approach and extensive collaboration with Internet leaders and law enforcement officials.

- Rightside's registrar eNom is a founding member of the Center for Safe Internet Pharmacies (CSIP), whose mission is to promote safe online pharmacies, and has an active member representative on the board of CSIP.

- Working diligently and pro-actively with LegitScript, the leading source of Internet pharmacy verification, Rightside identifies customers violating our terms of service by operating illegal online pharmacies and takes them offline. As a result of this partnership, we have developed an aggressive policy that has led to an exemplary process and success rate in combating rogue Internet pharmacies.

- Thousands of illegal online pharmacies have been shut down by Rightside registrars over the past few years.

- An independent study conducted by academic researchers concluded that our relationship with LegitScript has had the noticeable effect of removing a high percentage of these rogue pharmacy domain names from eNom's systems and the Internet.

Spam, Phishing, and Malware

Rightside's registrars have a zero tolerance policy for spam and a public track record of responsively and responsibly taking action when we discover spam or security issues with systems registered or hosted with our registrars.

- Working closely with many Internet security organizations, we share information critical to combating spam and malware across the Internet. Collaborating with companies like Spamhaus, HostExploit®, Arbor®, NetCraft®, Google® and many others, we actively strive to make the Internet a safer environment for consumers.

- We monitor the use of our system and services to ensure they are not used for the purpose of sending out unsolicited email. And we have taken measures to prevent the abuse of our registration engine, web hosting, and DNS services at a transaction point of origin by doing our part to eliminate spam.

- Rightside works with HostExploit® to establish accurate and reliable measurements of spam and malware activities on our systems and our efforts have resulted in our systems being relatively free of harmful spam and malware, as reported by HostExploit.

- Rightside's registrars investigate and take appropriate action with every spam or security report that we receive.

Contact Us

Rightside welcomes law enforcement, law firms and other parties to reach out to it with questions related to domain issues on its platform. We are happy to help point your investigation in the right direction if we are not the correct party to assist you. This document was created as part of our ongoing commitment to advancing the domain industry. Please feel free to reach out using one of the email addresses below:

abuse@name.com
legal@enom.com
registryabuse@rightside.co

About Rightside

Rightside™

Rightside® inspires and delivers new possibilities for consumers and businesses to define and present themselves online. The company, with its affiliates, is a leading provider of domain name services, offering one of the industry's most comprehensive platforms for the discovery, registration, usage, and monetization of domain names. In addition to being a new gTLD registry operator, Rightside is home to some of the most admired brands in the industry, including eNom and Name.com. Headquartered in Kirkland, WA, Rightside has offices in North America, Europe, and Australia. For more information please visit www.rightside.co.

Helpful Links

SUBPOENA POLICIES

http://www.enom.com/terms/subpoena_civil.asp
http://www.enom.com/terms/subpoena_criminal.asp
https://www.name.com/policies/name-civil
https://www.name.com/policies/name-federal

COPYRIGHT/TRADEMARK POLICIES

https://www.name.com/policies/policypage
http://www.enom.com/terms/copyright-policy.aspx

ABUSE REPORTING AND POLICIES

http://www.enom.com/help/AbusePolicy.aspx
https://www.name.com/abuse

Rightside™