WHOIS High-Level Technical Brief

Background

When the predecessor to the Internet (the ARPANet) was first being developed, it was quickly determined that there needed to be a contact list of the researchers who were connecting their mainframe computers and other devices to the network. This contact list included the name of the researcher, his or her telephone number, email address (if it existed, this was in the late 1960s after all), postal address, and other related information. In the event of network problems such as outages, misbehaving hardware or software, or other issues, researchers could look up their colleagues in this contact list and initiate a telephone/fax/email conversation to resolve the issue.

Initially, this contact list was on paper or in databases or spreadsheets on individual researcher's computers. This obviously led to challenges with the contact information going "stale", e.g., when researchers changed jobs, got new email addresses or other contact points, or when new institutions, networks, or devices were connected to the growing network. To deal with this data staleness problem, the ARPANet researchers created a centralized database of contact information and developed an extremely simple protocol to look up contacts within that database over the network. That protocol, which became known as "WHOIS", works as follows:

1. A connection to the centralized database is initiated.
2. Once the connection is established, the object, e.g., address, name, etc., for which contact information is desired is sent.
3. On the centralized database's side of the connection, the question is received.
4. The database is queried using the question sent by the client.
5. The result of the query is dumped back to the initiator of the connection.
6. The connection is closed.

This protocol, documented much after the fact in RFC 3912[1], says essentially nothing about what is in the contact information or how it should be displayed. It also assumes all the data are public and as such, no authorization is necessary to view the data. The client side of this very simple protocol was implemented on most, if not all, of the machines that were being connected to the network, allowing the increasing number of researchers to find their colleagues when there were questions about the devices on the Internet, and the centralization of the database made changes easy: the researchers simply needed to contact the centralized database administrator, known as the Network Information Center or NIC, and ask for their contact information to be updated.

As the Internet grew beyond a set of researchers who largely knew and trusted each other, the WHOIS "system" evolved. A downside of centralization is that it can be challenging to keep up

[1] https://tools.ietf.org/pdf/rfc3912.pdf

with growth: the number of updates can overwhelm the database administrator, the number of queries can overwhelm the routers or networks that connect the database to the Internet, and it can be unsustainably expensive to keep expanding the database administration staff or network to keep up with the growth. A solution to this problem is to decentralize the contact database and the route taken by the successors to the centralized NIC was to push administration of the contact information for the various objects that are used to identify resources on the Internet to the bodies responsible for allocating those resources. The result is today's distributed system of registration databases operated by domain registries and registrars and IP address registries.

The Registry System

Today, the WHOIS system exists as a set of independently operated distributed databases that are responsible for their portion of the Internet's identifiers, the responsible parties being known as Registries. There are two categories of distributed databases:

1. Domain names
2. Internet numbers

According to one industry expert, at the end of 2017 there were an estimated 332.4 million domain names across all 1,543 top-level domains[2]. These domain names are registered by organizations or natural persons for specific purposes such as providing services over the Internet, resale, brand protection, etc. Originally, domain names were free, with the registration service being provided at no charge to people registering the names (known now as registrants) by an organization under contract to the US Government. In 1993, the US National Science Foundation permitted the then contracted registration services provider, Network Solutions, Inc. acting as the InterNIC registration services provider (the successor to the original NIC operated by Stanford Research International), to charge a fee to end users for registration of domain names in .COM, .NET, and .ORG. Today, the vast majority of domain name registration services across nearly all top-level domains are provided for a fee and registrants enter into a contractual relationship with the registries or registrars for the service of domain name registration.

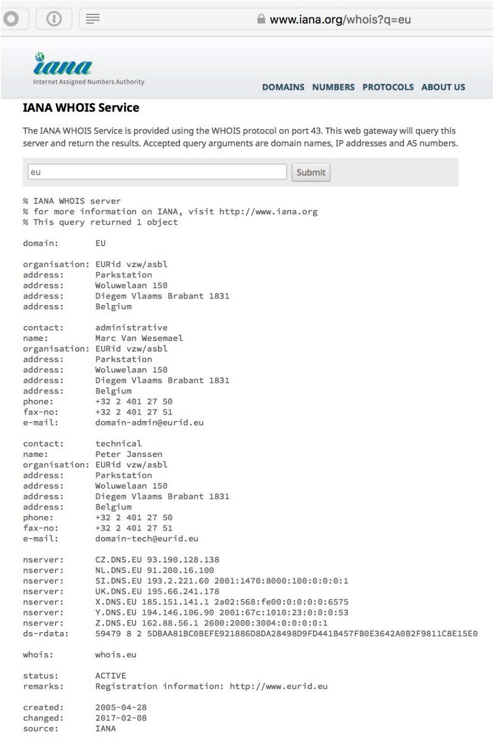
The databases in which the registration information is stored are distributed according to the hierarchical DNS namespace. That is, there is a database for the root zone, a set of databases that correspond to each of the top-level domains, and (in some rare cases), a set of databases that correspond to second-level domains. The data made available in WHOIS generally includes two parts: technical information and contact information. The technical information includes such data as name server names and their IP addresses, information used for securing the domain name using DNSSEC, date of creation, modification, and expiry of the domain name, and the registrar that was used to obtain the domain name from the registry. The contact information generally includes ways in which the administrative, technical, or other roles can be contacted.

[2] https://www.verisign.com/en_US/domain-names/dnib/index.xhtml

The other category of distributed databases, those associated with Internet Numbers (IPv4 and IPv6 addresses and autonomous system numbers), won't be addressed here other than to say that they are independently operated and unassociated with the domain name databases.

Root Zone WHOIS

In the root zone's WHOIS database, which is operated by ICANN as part of the IANA functions, there is contact information, also known as registration data, for each of the top-level domain names. An example of the output of the WHOIS database for a top-level domain is shown in Figure 1.



IANA WHOIS Service

The IANA WHOIS Service is provided using the WHOIS protocol on port 43. This web gateway will query this server and return the results. Accepted query arguments are domain names, IP addresses and AS numbers.

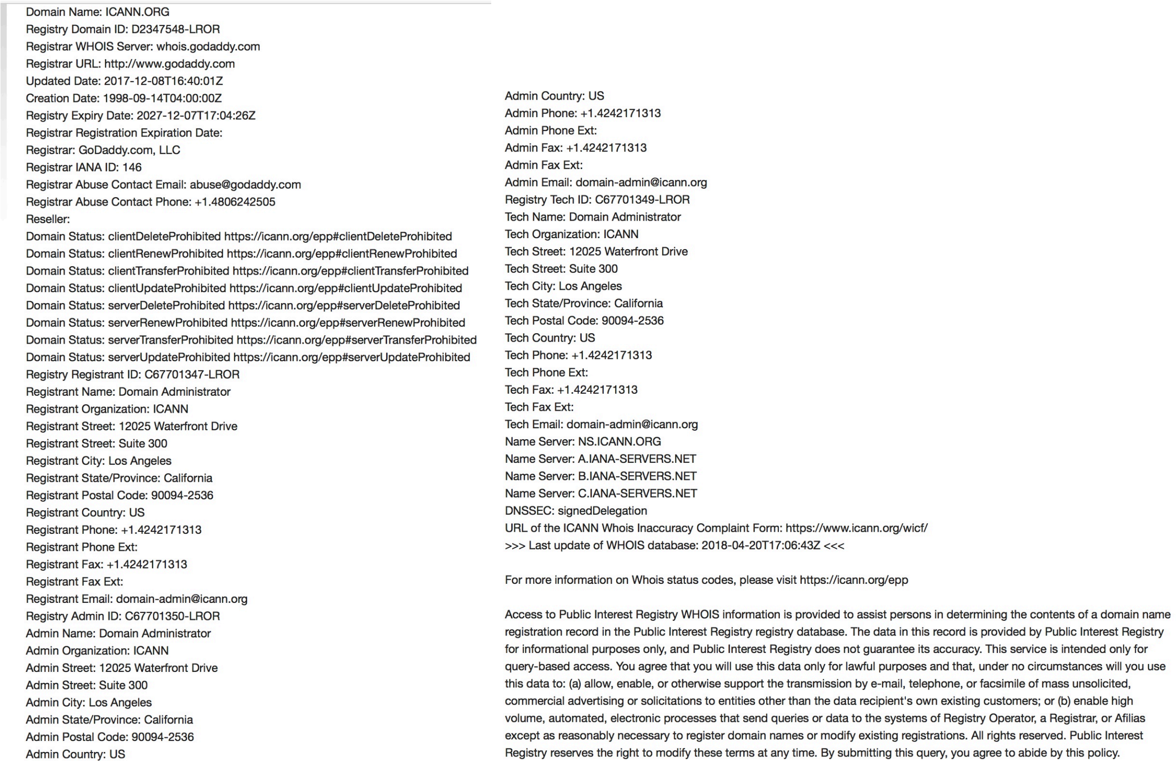
```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       EU

organisation: EURid vzw/asbl
address:      Parkstation
address:      Woluwelaan 150
address:      Diegem Vlaams Brabant 1831
address:      Belgium

contact:      administrative
name:         Marc Van Wesemael
organisation: EURid vzw/asbl
address:      Parkstation
address:      Woluwelaan 150
address:      Diegem Vlaams Brabant 1831
address:      Belgium
phone:        +32 2 401 27 50
fax-no:       +32 2 401 27 51
e-mail:       domain-admin@eurid.eu

contact:      technical
name:         Peter Janssen
organisation: EURid vzw/asbl
address:      Parkstation
address:      Woluwelaan 150
address:      Diegem Vlaams Brabant 1831
address:      Belgium
phone:        +32 2 401 27 50
fax-no:       +32 2 401 27 51
e-mail:       domain-tech@eurid.eu

nserver:      CZ.DNS.EU 93.190.128.138
nserver:      NL.DNS.EU 91.200.16.100
nserver:      SI.DNS.EU 193.2.221.60 2001:1470:8000:100:0:0:0:1
nserver:      UK.DNS.EU 195.66.241.178
nserver:      X.DNS.EU 185.151.141.1 2a02:568:fe00:0:0:0:0:6575
nserver:      Y.DNS.EU 194.146.106.90 2001:67c:1010:23:0:0:0:53
nserver:      Z.DNS.EU 162.88.56.1 2600:2000:3004:0:0:0:0:1
ds-rdata:     59479 8 2 5DBAA81BC0BEFE921886D8DA28498D9FD441B457FB0E3642A0B2F9811C8E15E0

whois:        whois.eu

status:       ACTIVE
remarks:      Registration information: http://www.eurid.eu

created:      2005-04-28
changed:      2017-02-08
source:       IANA
```

Figure 1. Root Zone WHOIS Data

Top-Level Domain WHOIS

In the case of top-level domains, the situation is much more complicated. For the purposes of this discussion, there are two categories of top-level domains, those that are under contract with ICANN and those that aren't. These two categories are generally described as "generic top-level domains" and "country-code top-level domains". In the case of generic top-level domains or gTLDs, ICANN imposes a set of contractual obligations that require the parties that have entered into contracts with ICANN, namely the DNS registries and registrars, to make a specified set of registration data available via WHOIS with a specific format. An example of the gTLD WHOIS output (split into two columns due to length) is shown in Figure 2[3].

[3] Within the gTLDs, there is a further distinction that is currently made, between "thin" WHOIS registries which only show technical information and a pointer to the registrar which maintains the contact information, and



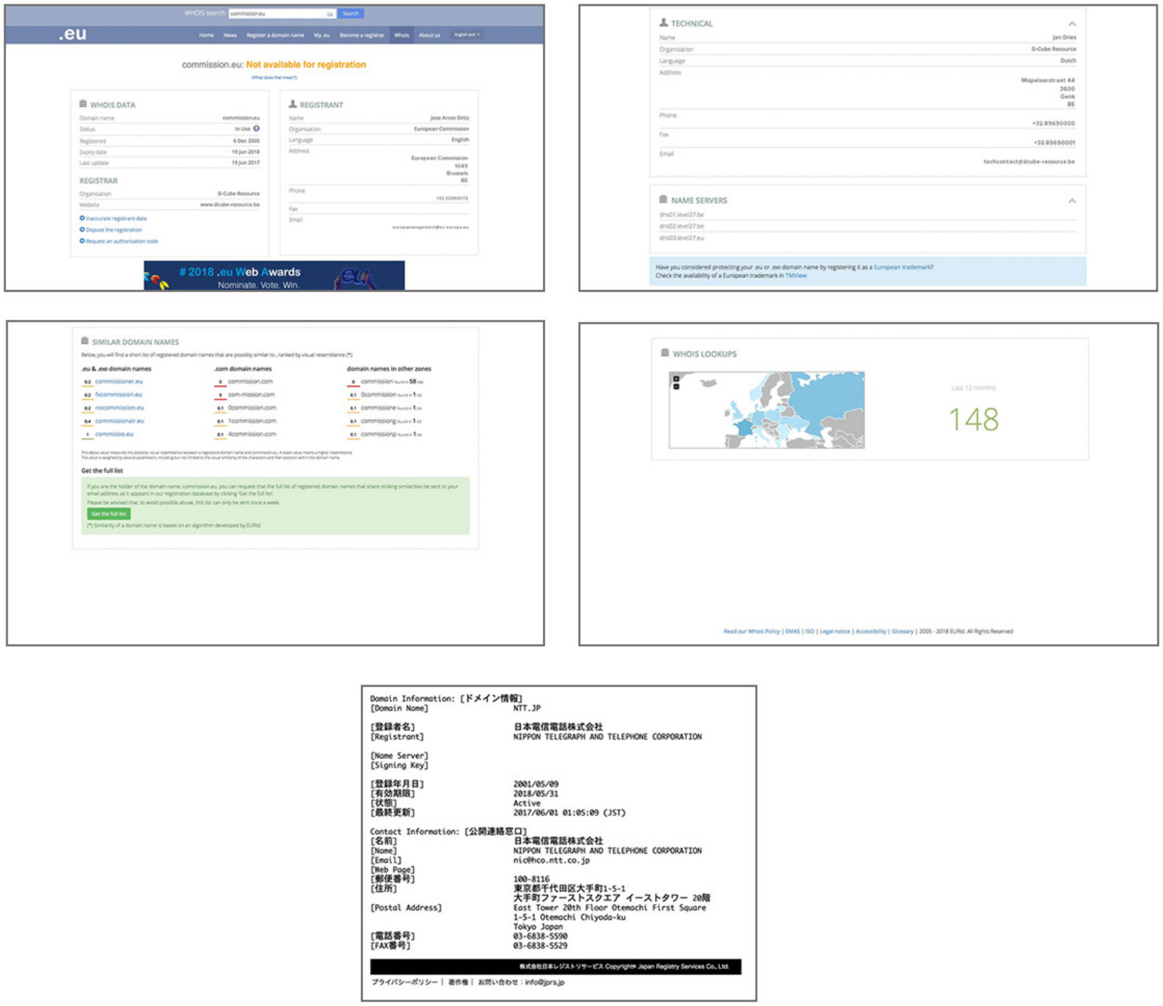
```
Domain Name: ICANN.ORG
Registry Domain ID: D2347548-LROR
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2017-12-08T16:40:01Z
Creation Date: 1998-09-14T04:00:00Z
Registry Expiry Date: 2027-12-07T17:04:26Z
Registrar Registration Expiration Date:
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverRenewProhibited https://icann.org/epp#serverRenewProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Registry Registrant ID: C67701347-LROR
Registrant Name: Domain Administrator
Registrant Organization: ICANN
Registrant Street: 12025 Waterfront Drive
Registrant Street: Suite 300
Registrant City: Los Angeles
Registrant State/Province: California
Registrant Postal Code: 90094-2536
Registrant Country: US
Registrant Phone: +1.4242171313
Registrant Phone Ext:
Registrant Fax: +1.4242171313
Registrant Fax Ext:
Registrant Email: domain-admin@icann.org
Registry Admin ID: C67701350-LROR
Admin Name: Domain Administrator
Admin Organization: ICANN
Admin Street: 12025 Waterfront Drive
Admin Street: Suite 300
Admin City: Los Angeles
Admin State/Province: California
Admin Postal Code: 90094-2536
Admin Country: US
```

```
Admin Country: US
Admin Phone: +1.4242171313
Admin Phone Ext:
Admin Fax: +1.4242171313
Admin Fax Ext:
Admin Email: domain-admin@icann.org
Registry Tech ID: C67701349-LROR
Tech Name: Domain Administrator
Tech Organization: ICANN
Tech Street: 12025 Waterfront Drive
Tech Street: Suite 300
Tech City: Los Angeles
Tech State/Province: California
Tech Postal Code: 90094-2536
Tech Country: US
Tech Phone: +1.4242171313
Tech Phone Ext:
Tech Fax: +1.4242171313
Tech Fax Ext:
Tech Email: domain-admin@icann.org
Name Server: NS.ICANN.ORG
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
Name Server: C.IANA-SERVERS.NET
DNSSEC: signedDelegation
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2018-04-20T17:06:43Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to Public Interest Registry WHOIS information is provided to assist persons in determining the contents of a domain name
registration record in the Public Interest Registry registry database. The data in this record is provided by Public Interest Registry
for informational purposes only, and Public Interest Registry does not guarantee its accuracy. This service is intended only for
query-based access. You agree that you will use this data only for lawful purposes and that, under no circumstances will you use
this data to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited,
commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high
volume, automated, electronic processes that send queries or data to the systems of Registry Operator, a Registrar, or Afilias
except as reasonably necessary to register domain names or modify existing registrations. All rights reserved. Public Interest
Registry reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.
```

Figure 2. gTLD Zone (.ORG) WHOIS output

In the case of country-code top-level domains or ccTLDs, which with very few exceptions are **not** under contract with ICANN, the provision of the WHOIS protocol, what parts of the registration database are made public, the format of the registration data, etc., are entirely at the discretion of the ccTLD administrator. Examples of the different forms of output for ccTLDs (in this case, .EU for the European Union, split due to length, followed by .JP for Japan) is shown in Figure 3.

"thick" registries which contain both technical and contact information. Discussion of this distinction is outside of the scope of this document.



commission.eu: Not available for registration

(What does that mean?)

WHOIS DATA

Domain name	commission.eu
Status	In Use
Registered	6 Dec 2005
Expiry date	19 Jun 2018
Last update	19 Jun 2017

REGISTRAR

Organisation	D-Cube Resource
Website	www.dcube-resource.be

Inaccurate registrant data

Dispute the registration

Request an authorisation code

REGISTRANT

Name	Jose Arcos Ortiz
Organisation	European Commission
Language	English
Address	European Commission 1049 Brussels BE
Phone	+32 22956072
Fax	
Email	europamanagement@ec.europa.eu

TECHNICAL

Name	Jan Dries
Organisation	D-Cube Resource
Language	Dutch
Address	Mispelaarstraat 44 3600 Genk BE
Phone	+32.89690000
Fax	+32.89690001
Email	techcontact@dcube-resource.be

NAME SERVERS

dns01.level27.be

dns02.level27.be

dns03.level27.eu

Have you considered protecting your .eu or .ею domain name by registering it as a European trademark?
Check the availability of a European trademark in TMView

SIMILAR DOMAIN NAMES

Below, you will find a short list of registered domain names that are possibly similar to , ranked by visual resemblance (*)

.eu & .ею domain names	.com domain names	domain names in other zones
0.2 commissioner.eu	0 commission.com	0 commission found in 58 tlds
0.2 fxcommission.eu	0 com-mission.com	0.1 0commission found in 1 tld
0.2 nocommission.eu	0.1 0commission.com	0.1 commissione found in 1 tld
0.4 commissionair.eu	0.1 1commission.com	0.1 commissiong found in 1 tld
1 commissio.eu	0.1 4commission.com	0.1 commissionp found in 1 tld

The above value measures the possible, visual resemblance between a registered domain name and commission.eu. A lower value means a higher resemblance.
The value is weighted by several parameters, including but not limited to the visual similarity of the characters and their position within the domain name.

Get the full list

If you are the holder of the domain name, commission.eu, you can request that the full list of registered domain names that share striking similarities be sent to your email address as it appears in our registration database by clicking 'Get the full list'.

Please be advised that, to avoid possible abuse, this list can only be sent once a week.

(*) Similarity of a domain name is based on an algorithm developed by EURid.

WHOIS LOOKUPS

Read our Whois Policy | EMAS | ISO | Legal notice | Accessibility | Glossary | 2005 - 2018 EURid. All Rights Reserved

```
Domain Information: [ドメイン情報]
[Domain Name]                   NTT.JP

[登録者名]                      日本電信電話株式会社
[Registrant]                    NIPPON TELEGRAPH AND TELEPHONE CORPORATION

[Name Server]
[Signing Key]

[登録年月日]                    2001/05/09
[有効期限]                      2018/05/31
[状態]                          Active
[最終更新]                      2017/06/01 01:05:09 (JST)

Contact Information: [公開連絡窓口]
[名前]                          日本電信電話株式会社
[Name]                          NIPPON TELEGRAPH AND TELEPHONE CORPORATION
[Email]                         nic@hco.ntt.co.jp
[Web Page]
[郵便番号]                      100-8116
[住所]                          東京都千代田区大手町1-5-1
                                大手町ファーストスクエア イーストタワー 20階
[Postal Address]                East Tower 20th Floor Otemachi First Square
                                1-5-1 Otemachi Chiyoda-ku
                                Tokyo Japan
[電話番号]                      03-6838-5590
[FAX番号]                       03-6838-5529
```

株式会社日本レジストリサービス Copyright© Japan Registry Services Co., Ltd.

プライバシーポリシー | 著作権 | お問い合わせ：info@jprs.jp

Figure 3. .EU and .JP WHOIS Data

The rules and policies for registering domain names in ccTLDs vary significantly. Since ccTLDs are treated by ICANN as national sovereign resources, it is important to note that there is no mechanism by which ICANN or any other body other than those within the country responsible for the ccTLD can mandate the ccTLD WHOIS be made available, what data are provided, or the format of those data.

Gaining Access to WHOIS Data

Services available over the Internet are provided by machines establishing a connection to another machine on a "well known port". Ports, which are an example of "protocol parameters" maintained by the IANA Functions operated by ICANN, are a number between 0 and 65,535 and well known ports have an associated name. The WHOIS protocol was defined to use port 43 with the unsurprising name of "whois" and historically, WHOIS client software would establish a connection to a WHOIS server by connecting to the IP address of the server and sending data to port 43. Much more recently, WHOIS service has been provided via the World Wide Web (port 80 for "http" and port 443 for "https"). However, at least conceptually, these two access methods are querying the exact same underlying database holding registration data. ICANN requires gTLD registries to provide WHOIS service on both port 43 as well as via the Web, however the data presented in response to the queries must be the same, regardless of access method.

“Bulk” WHOIS Data Access

As mentioned, ICANN requires that there be two ways in which registration data about gTLDs can be obtained over the Internet, namely via port 43 or via the Web (port 80 or 443). Regardless of the port by which the gTLD’s registration information database is accessed, the following are currently true:

1. A single query can be issued, resulting in a single response. This is a function of the specification of the underlying WHOIS protocol;
2. There is no way to use wildcards, e.g., a query for “*.COM” in order to get back all 2nd level domains in .COM is not possible. This inability is not a requirement of the protocol or ICANN, and in fact historically, some WHOIS servers did allow for wildcard queries, however over time, commercial and technical interests have reduced the availability of wildcard query functionality to the point that it is generally unavailable today;
3. The registration data, i.e., fields in the registration record, that are presented in response to WHOIS queries are explicitly specified by ICANN policy; and
4. There are limitations on how many queries are allowed per given time period. These limitations were not specified by protocol or ICANN policy, rather they evolved in response to network abuse (e.g., denial of service attacks against WHOIS servers) or commercial interests (e.g., exhaustive queries for all domain names within the database to build customer lists for spam or other purposes).

As a result, the WHOIS service as is defined by ICANN policy and/or the WHOIS protocol does not have a concept of “bulk” access to data. There are third parties that have obtained copies of WHOIS data and make more general query interfaces to those data that do support wildcards and thus bulk access[4], however those organizations/services are outside the constructs/control of ICANN.

ICANN WHOIS Service

ICANN operates a WHOIS server at WHOIS.ICANN.ORG. This server gives end users the ability to do registration data lookup for any gTLD, providing the convenience of a simple and consistent interface at a single location instead of requiring the end users to find the WHOIS server that will provide the information for the domain name they are interested in. While giving the impression of a centralized database, it is not. This WHOIS service actually works by maintaining a list of the WHOIS servers operated by the gTLD registries, all of which are contractually obligated to respond to WHOIS queries, and forwarding queries to those servers. When the gTLD registry’s WHOIS server responds back to ICANN’s WHOIS server, that response is

[4] For a few examples of these services (without endorsement), see http://domaintools.com, https://whoisdatabasedownload.com, https://www.whoxy.com, etc.

returned to the end user. Since ICANN cannot require ccTLDs to provide WHOIS service, the ICANN WHOIS server only provides gTLD-related registration information.

Examples of the use of WHOIS data

At a high level, the use of the WHOIS system has remained the same since its creation, namely it is a way for users of the network to be able to identify the “owner” of resources that are attached to the network in order to contact those individuals to address problems or issues associated with the connection of the resources to the network. However, the user population and the resource owners have evolved drastically as the Internet has grown from a small research network to an increasingly critical component of everyday life. Some of the users of WHOIS data include:

1. **Victim notification:** When a web site is compromised, or a previously legitimate mail server begins emitting spam, WHOIS provides investigators and law enforcement officers with information to quickly contact the victim and assist in redress. IP address and domain name WHOIS are also used to notify organizations whose systems have been infected by viruses, especially ones that are infected, compromised and subsequently enrolled in “botnets” that are used for various nefarious purposes.
2. **Attribution of criminal acts to a perpetrator:** Many WHOIS data are critical information in online crime investigation. For instance, information found in the WHOIS can be used as search terms into other databases, e.g., name server IP addresses in the DNS, email address databases maintained by anti-spam organizations, etc., which can assist law enforcement in obtaining a larger picture of the perpetrators activities. This aids law enforcement in both identifying the criminals as well as learning the scope of their activities.
3. **Identifying misuses of intellectual property:** The ability to identify the holder of a domain name that is infringing on a trademarked term is another use of the WHOIS system today. In some cases, trademarked domain names are registered in order to facilitate “phishing”, or the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. In other cases, use of a trademark in a domain is more benign, people either unknowingly or inappropriately registering a trademark that can cause confusion. In either case, being able to obtain the contact information associated with these domain names allows the intellectual property owners to engage with the people who have registered the domain name in order to address the infringement.
4. **Name Availability Service:** WHOIS is sometimes used to announce the availability for sale of the name in the response to the WHOIS query. In these cases, the contact information is used to advertise the email address or telephone number of the registrar that can be contacted if someone wants to purchase the domain name.

These examples are non-exhaustive of the use of WHOIS data, however they should provide an idea of the varied uses to which the WHOIS system is now subject.

WHOIS in the Context of Security and Stability

Article 1, section 1.1(a) specifies that ICANN’s mission is:

> *“[…] to ensure the stable and secure operation of the Internet's unique identifier systems […]”.*

Within ICANN’s limited technical remit, this mission is tightly constrained. As one of ICANN’s primary roles is to be responsible for the administration of the topmost levels of the Internet’s identifiers, facilitating the ability to identify the holders of those identifiers is a core function of ICANN. The WHOIS system has evolved to provide mechanisms that allow Internet users to make contact with the end points of Internet communication, namely domain names and Internet addresses. In cases of attack or abuse that threaten the stable and secure operation of the Internet, the functionality provided by WHOIS becomes critical. In particular, given the global and decentralized nature of the Internet and the ability of abusers to attack at any time, timely availability of contact information is often the first step to mitigate the attacks. Similarly, without contact information, determining whether a website or email address accurately reflects the assumed real-life counterpart of the domain name or IP address becomes significantly harder.

Summary

The WHOIS system as it is used today is the result of the evolution of the network from a small set of researchers who largely knew each other to the Internet of today. WHOIS is a decentralized database that provides anyone, from law enforcement to anti-abuse volunteers to intellectual property interests to end users, with the ability to obtain contact information of individuals who have registered Internet resources such as domain names and IP addresses. The ability to obtain this information is critical to helping to track down abuse of those resources such as via phishing, spam, or fraud through misrepresentation of trademarks as well as information purposes such as announcing the availability of domain names.

ICANN’s mission to ensure the security and stability of the operation of the Internet’s system of unique identifiers has led to the obligations associated with providing WHOIS that are imposed on the parties with which ICANN has contracts. While the WHOIS system, like any human system is imperfect, the service it provides is deemed essential by many within the community, particularly those involved in combatting fraud and abuse.