WHOIS Primer

This is a very introductory reference to WHOIS, geared towards establishing a baseline for people who are curious about it or for those who don't even know it exists. I have been researching WHOIS and WHOIS policy for decades and **wrote a book about the subject in 2015**.

What is WHOIS?

The simplest explanation is that WHOIS is the *record system* for the public Internet. Every point on the Internet has a record somewhere and the records are supposed to be available on demand. The record set includes Domains (website roots), Internet Protocol numbers (machine addresses), Name Servers (machines that tie domains and IP numbers together) and all of the Service Providers as well as all of the managing entities for the Internet. The reason for this record set is fairly straightforward. As a public resource that literarily links every person and organization connected through it, it is critical that engaging parties be identifiable to each other. Whether it is in accepting communication or conducting business it simply makes sense to know with whom the transaction is occurring. The recordset does not apply to smartphones, individual computers or user accounts within organizations and internal networks.

The term WHOIS is a bit arcane and would be better thought of as “who owns” or “who controls” some resource. The term WHOIS is also somewhat ambiguous since it is applied generally to the entire structure. This includes *programs* that access WHOIS, the *databases* that store WHOIS records and the *record data* itself. As a system it is not truly a unified system. There is no single WHOIS, rather a series of thousands of databases with different rules and structures. WHOIS programs *query* databases that store specific records depending on the type of record sought. There are other Internet records that can be accessed that are technically outside of WHOIS but help to form the greater body of information and may be referenced in our discussions.

How Can WHOIS be accessed?

The two main ways to retrieve WHOIS records are through 1) a command-line utility and 2) a webpage that performs the command-line query for you. Pretty much every Unix-based system (and this includes many MacOS systems) comes with WHOIS (Command+Spacebar, then search for "Terminal"). If your Linux distribution does not have WHOIS installed it can be easily added usually with “yum install whois” on the command line. Windows devices typically do not have WHOIS preinstalled but it is possible to install such a program. In future articles I will go into detail on how to do this or use other applications for searches.

For many who are not technically minded or not comfortable using a command there are a number of websites that will produce the same results. This is important because everyone should be able to access WHOIS and understand why it is necessary. One useful site for WHOIS lookups is **Domain Tools** (**https://whois.domaintools.com**). This service will provide additional information about the record along with statistics.

What does WHOIS tell me?

Starting with a simple example, we can perform a WHOIS look up from the command line for the professional social-media site, LinkedIn:

```
whois linkedin.com
```

Will return in part:

```
Domain Name: LINKEDIN.COM
Registry Domain ID: 91818680_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-09-01T17:16:55Z
Creation Date: 2002-11-02T15:38:11Z
Registry Expiry Date: 2022-11-02T15:38:11Z
Registrar: MarkMonitor Inc. Registrar
IANA ID: 292
Registrar Abuse Contact Email:
abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
```

The full record may be much longer but this is the part that is immediately meaningful. The top section or *Registrar block* tells us who the *registrar* is, not the owner, that is an important distinction. Registrars are authorized companies that place *domains* on the Internet which makes them available as websites. The Registrar in this case is a company called MarkMonitor that specializes in serving corporate brand customers, LinkedIn being one. The Registrar's main function is as a gateway to creating and maintaining Internet domain websites. An important part of this function is collecting and holding WHOIS records. When a domain is purchased or *registered*, the owner or *registrant* supplies relevant information.

The role of the registrar here is not only to provide a functional service in sponsoring a domain in the Internet, but most importantly to clarify who this domain *belongs to* in order to resolve disputes or handle problems. What if I inappropriately claimed to be the owner of “linkedin.com"? This is easily resolved by reviewing the records. What if the website is unreachable or has some other major technical failure? Well, there is a way to alert responsible parties in the record. Note there is an email and phone number specifically for abuse issues. Registrars may also provide a number of other technical and business services to website operators including content hosting and online stores. Domain websites simply do not exist without Registrar sponsorship.

What’s going on in the background?

WHOIS is essentially a remote database query. whois is the program and the domain name (or other object) is the *parameter* being passed to it. If your WHOIS program and the responding databases are configured properly, the query will be referred until the correct database is found and the correct record returned. As stated, WHOIS records are not stored in a single place. In the example above note the field Registrar WHOIS Server with the address "whois.markmonitor.com". This is where the record is retrieved from. It is important to note that this server run by MarkMonitor will only have records for domains held by MarkMonitor.

When I run the bare WHOIS query *whois linkedin.com* my query starts at the “top” of the Internet by first asking who controls the “.com” portion of the Internet. .COM is operated by a company called Verisign, and the Verisign WHOIS database responds by telling my query that MarkMonitor holds the WHOIS record for the domain and then tries to retrieve the record from there. Now that I know this, in the future I can go directly to MarkMonitor for the record. How? By pointing my WHOIS query at their server:

```
whois -h whois.markmonitor.com linkedin.com
```

The “-h” tells my WHOIS query to only look at whois.markmonitor.com for the record of linkedin.com and bypasses any other WHOIS service. The returned record might contain less lines and be formatted differently but should contain all the same core information.

In the opening of this document I stated that every point on the Internet has a record, now let’s test that. Working off the information in our example record, let’s say we needed to find out more information about the Registrar MarkMonitor. This query will return specific information:

```
whois -i "registrar MarkMonitor Inc."
```

The “-i” switch tells my WHOIS query to search for very specific information, particularly a record for MarkMonitor as a registrar. This gets tricky because you need to have the exact spelling of the company’s name to return the correct record. The returned record should have the business contact information for the registrar. While the domain record we reviewed came from MarkMonitor, the record for MarkMonitor came from that other organization Verisign. Verisign is also a kind of Registrar but a special type called a *registry* that manages the entire .COM space. You can perform a look up on the ownership of .COM itself:

```
whois .com
```

The returned record will indicate VeriSign Global Registry Services is responsible for that segment of the Internet.

Why should WHOIS be important to everyone?

As you read or talk about WHOIS you may hear that it is a *technical* or *investigative* tool. This is absolutely true. There are many tasks that cannot be performed without understanding WHOIS. Network administrators, security professionals, attorneys and investigators all use WHOIS on a regular basis. But *why* do they use it? The Internet is a critical and ubiquitous resource but it is also a terrifying place because trust has been absolutely shattered by malicious actors.

All communication and business is ultimately based on trust. This trust only comes with identification. How do you know the website you are about to buy something from, give personal information to or accept an email from is trusted? You have every reason not to trust anything you see on the Internet.

In our above example MarkMonitor has been trusted with protecting and presenting brands. Verisign has been trusted with managing the framework of the .COM space. This is a trust chain that only goes so far. In order to find out if the organization behind a web domain can be trusted, you need the details.

Buying a pair of shoes online? Is it worth five or ten minutes of your time to see if your product will actually arrive? To determine if you could return the item? If it is in fact the licensed brand advertised? Who exactly are you giving your credit card to? Most definitely the website will *tell* you they are trustworthy - but see for yourself to save trouble in the future.

Start using WHOIS and put it in your personal tool belt.