CENTR vzw/asbl, Belliardstraat 20, 1040 Brussels, Belgium Tel +32 2 627 5550, Fax +32 2 627 5559
Tel +32 2 627 5550, Fax +32 2 627 5559, secretariat@centr.org http://www.centr.org

WHAT IS WHOIS?

SUMMARY
The WHOIS tool is an important query and response protocol within the DNS system. WHOIS allows a user to perform a search on a given domain (or IP address) and retrieve various information about its registration. This paper gives an introduction to WHOIS and discusses the main issues surrounding it today.

WHAT-IS-WHOIS.01

Facts and Background

The appropriately named WHOIS protocol is a query/response tool which allows a user to perform a query on a database and retrieve information on a domain name registration. Depending on the Top Level Domain (TLD) one is searching under, details such as the domain owner's name, address, email address and often much more information can be found. The extent to which data can be extracted from the database is dependent on the terms and conditions of the TLD registry, local laws and often bound by third parties such as ICANN (Internet Corporation for Assigned Names and Numbers).

The original specifications to the WHOIS protocol can be found in the RFC 954 which was created in 1985 (an update to RFC 812). The more recent RFC 3912 is now generally accepted as the standard to how the protocol works.[1]
Users of WHOIS access the tool in three different methods: command-line, web and automated client applications. Originally all clients used the text based command line (usually UNIX operating system) however currently the web based service is the most common.

Key Applications of WHOIS

- To determine availability of domain names or check registration status
- To locate and repair any system problems
- To aid in legal trademark infringements or combat misuses of the internet (eg. Fraud, spam etc)
- To increase accountability of domain name holders

Users of WHOIS[2]

- *Network Operators*: To identify appropriate contacts regarding network problems associated with the domain. In the traditional sense, this involves discussing technical DNS errors, routing, and other fundamental operations; or for more contemporary reasons such as identifying the source of spam and network attacks.
- *Registries and Registrars*: To determine the availability of a domain name, to identify the contacts linked to a domain name, or to check whether a domain name is available. It is worth noting, registries and registrars usually have more specialised protocols and procedures for these purposes, rather than using the anonymous WHOIS service.
- *Intellectual Property interests*: WHOIS can be used to quickly identify a domain name holder who may be infringing on intellectual property rights.
- Registrants: Registrant can use WHOIS to determine whether a Domain name is available or not.
- *Law enforcement personnel*: When a Web site is the instrument of criminal activity, law enforcement Agencies can use WHOIS database to potentially find more information on the fraudulent party.
- *Consumers*: Domain names are the first identifier of an e-commerce site. WHOIS data can potentially be used by consumers to make sure the company behind the site is legitimate.
- *Business users*: Domain names are valuable to many businesses and their marketing strategies.

Thin vs. Thick

There are two methods of storage within a WHOIS database; thin and thick. Thick is a WHOIS server that stores complete WHOIS information from all the registrars (so that one WHOIS server can respond with WHOIS information on all .org domains, for example). Thin refers to a WHOIS server that stores only the name of the WHOIS server of the registrar of a domain, which in turn has the full details on the data being looked up[3]. Different registries will have differing approaches to this however there has been some

1 RFC 3912 (with links to obsolete RFC 954 and 812): http://tools.ietf.org/html/rfc3912
2 CENTR WHOIS Paper with Article 29 comments 07/01/08 (members only)
3 http://en.wikipedia.org/wiki/Whois

debate and discussion on the differences stating that a thin WHOIS could increase the risk for a registrant should a registrar go out of business or fail on a technical level. Generally country code TLD's (ccTLDs) (eg. .be for Belgium, .uk for United Kingdom etc) adopt the thick approach, however this is not a standardised rule.

With the introduction of new generic TLDs[4] (gTLDs), the ICANN community is debating whether to enforce all gTLD Registries to implement a thick Registry – a Policy Development Process (PDP) was launched at ICANN43 in Costa Rica on the issues defined in the Final Issue Report on thick Whois.[5]

Example of WHOIS search and response

When a search is made on 'centr.org' into the PIR WHOIS tool (PIR is the registry for .org) WHOIS tool, the following screen is displayed (below). The areas in red show important data such as date of creation, the Registrant's name, address, phone and email. There is also different sections allowing for a separation of data details ie - technical contact, administrative contact. In this case, the details are the same.

With the increasing importance of the security extension DNSSEC, there is also a field displayed whether or not the domain has had DNSSEC signed to it. Please see the CENTR Issue Paper on DNSSEC for more information.

Domain ID:D2063208-LROR
Domain Name:CENTR.ORG
Created On:29-Sep-1998 04:00:00 UTC
Last Updated On:12-Jul-2010 13:27:37 UTC
Expiration Date:28-Sep-2015 04:00:00 UTC
Sponsoring Registrar:Network Solutions LLC (R63-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:20486664-NSI
Registrant Name:Council of European Nat'l TLD Registries
Registrant Organization:Council of European Nat'l TLD Registries
Registrant Street1:Belliardstraat 20
Registrant Street2:6th floor
Registrant Street3:
Registrant City:Brussels
Registrant State/Province:
Registrant Postal Code:1040
Registrant Country:BE
Registrant Phone:+32.26275550
Registrant Phone Ext.:
Registrant FAX:+32.26275550
Registrant FAX Ext.:
Registrant Email:secretariat@centr.org
Admin ID:20486662-NSI
Admin Name:CENTR Secretariat
Admin Organization:CENTR
Admin Street1:Belliardstraat 20
Admin Street2:6th floor
Admin Street3:
Admin City:Brussels
Admin State/Province:
Admin Postal Code:1040
Admin Country:BE
Admin Phone:+32.26275550
Admin Phone Ext.:
Admin FAX:+32.26275559
Admin FAX Ext.:
Admin Email:secretariat@centr.org
Tech ID:20486664-NSI
Tech Name:Council of European Nat'l TLD Registrie
Tech Organization:Council of European Nat'l TLD Registries
Tech Street1:Belliardstraat 20
Tech Street2:6th floor
Tech Street3:
Tech City:Brussels
Tech State/Province:
Tech Postal Code:1040
Tech Country:BE
Tech Phone:+32.26275550
Tech Phone Ext.:
Tech FAX:+32.26275550
Tech FAX Ext.:
Tech Email:secretariat@centr.org
Name Server:NS1.OPENMINDS.BE
Name Server:NS2.OPENMINDS.BE
Name Server:NS3.OM-POWERED.NET
DNSSEC:Unsigned

PRIVACY- (PROTECTION-OF-DATA).02

At the beginning of November 2010, the European Commission set out a strategy to 'strengthen EU data protection rules'[6] The intention is to (with the use of public consultation) revise the EU's 1995 Directive on Data Protection. See a Press Release from the European Commission here made on 25 January 2012.

The Concerns and discussions

While there is no express mention to the WHOIS protocol within the Data Protection Directive, 'personal data' is covered and protected by the 1995 Directive and therefore encompasses WHOIS.

Much of the concerns and dialogue on data protection and WHOIS have focused around the protection of private individual data (as opposed to commercial or legal persons). Discussions have also moved around the topic of freedom of speech and basic human rights to which are under threat when personal data is available publicly.

One recurring concern is that when a private person registers a domain, sometimes the only contact address they can give is their home address. This is said to be a potential risk in promoting criminal activity such as stalking or harassment if the address is made public. Even in cases of commercial registration of domain names, the simple fact of having an email address in a public WHOIS could allow vulnerability to spammers, phishers and/or hackers.

To address the key concerns and provide advice to the European Commission on data protection issues, Article 29 of the Directive expressly set up the Article 29 Data Protection Working Party. The group is formed by member state representatives who bring expert opinion from their respective member states to promote uniform principles.

A document produced in 2003 by the Article 29 Working Group made specific mention to the WHOIS protocol calling for a better definition of the purpose/s of WHOIS. It noted that, the original (technical) purpose of the WHOIS must not be expanded upon unnecessarily and must not compromise data privacy. The document also highlighted the distinction between data provided by private individuals and that of business or legal persons. It was mentioned that (in reference to private individuals); "...while it is clear that the identity and contact information should be known to his/her service provider, there is no legal ground justifying the mandatory publication of personal data referring to this person.. "[7]

The theme was again raised at the Internet Governance Forum (IGF) in Greece in 2006 where it was mentioned by the Non-Commercial Users Constituency (NCUC) that (with reference to the Data Protection Directive 1995); "Allowing access to personal contact information by people not substantively involved in resolution of technical problems with Internet domains violates these provisions..."[8] (the provisions being those found in the 1995 Directive).

4 ICANNs new gTLD program: http://newgtlds.icann.org/en/

5 http://gnso.icann.org/issues/whois/final-report-thick-whois-02feb12-en.pdf

6 http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_en.pdf

8 Contribution Memorandum: Privacy Implications of WHOIS Database Policy (Non-Commercial Users Constituency (NCUC)

The above concerns on data privacy for individuals are also aggravated by fundamental differences between ICANN policy and other local laws (eg. EU law). Within the ICANN Affirmation of Commitments, it states (in reference to the WHOIS data); "... existing policy requires that ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information."
Within Europe, ccTLD Registries are not bound by ICANN policy as they have developed their own policy tailored to their country or region – usually a 'best fit' model created in co-operation with local community and government.
European Registrars and gTLDs based in Europe are often however in potential conflict with ICANN policy under their ICANN agreements. Whereas ICANN policy requires disclosure of complete registrant data, the European Directive on Data Protection essentially goes the other way by allowing a registrant the choice of disclosure.

Addressing the gTLD Conflicts

ICANN produced in December 2006 a 'Procedure for Handling WHOIS Conflicts with Privacy Law'[9] with effective date in January 2008. The document spelled out a 6-step procedure to be followed in cases of conflicts between local privacy law and ICANN policy : notification, consultation, analysis and recommendation, resolution, public notice and ongoing review.
The Article 29 Working Group responded to the report referring again to the Data Protection Directive and once again emphasising the importance of distinction between legal and natural persons. The Working group suggested introducing a distinction between publicly accessible and publicly inaccessible data to combat the problems of potential conflict.

Privacy and WHOIS

Many of the European ccTLD registries employ a method whereby registrants are able to hide certain elements of data provided upon registration of a domain (24 out of the 45 ccTLDs survey by CENTR in 2010 have this feature[10]). In the case of Nominet (the registry for .uk) for example, they call it an 'Opt out' feature. In this case, a non-trading registrant has the choice of anonymity without having to rely on proxy registration.
Whois is an important tool used by law enforcement authorities around the world and during the ICANN meeting in Seoul 2009 a list of recommendations supported by various international law enforcement bodies was provided. Within the Law Enforcement (LE) recommendations, it was stated in reference to WHOIS;
"Although LE does not support the use of proxy/privacy registrations, the LE agencies urge ICANN to exercise the following on proxy/privacy registrations:
a. The proxy/privacy registrant is a private individual using the domain name for non-commercial purposes only, and;
b. The proxy/privacy registration service has been accredited by ICANN using the same due diligence process as a Registrar/Registry, and;
c. Information from the WHOIS database can be provided to law enforcement authorities when the information will assist in the prevention, detection, investigation prosecution or punishment of criminal offences or breaches of laws imposing penalties, or when authorised or required by law."[11]

Although the above recommendations were made with gTLDs in mind (particularly in reference to the Registrar Accreditation Agreement), ccTLDs are often in context in this discussion. For example, during a Government Advisory Committee (GAC) session at the ICANN Meeting in Singapore in June 2011, ccTLDs were referred to several times as a source of providing 'best practices' in terms of their tailored WHOIS policies.

ACCURACY-AND-VERIFICATION-OF-DATA. 03

Accuracy in the WHOIS is of high importance both in the ccTLD and the gTLD spaces.
ICANN accredited Registrars and gTLDs are bound by the ICANN policy which is uniform and has specific provisions for the attainment of accurate data in the WHOIS. In cases where inaccuracy is found, they have obligations requiring them to investigate.
ccTLDs often have similar standards on accuracy however as they are not bound by ICANN policy they develop their own policies (eg. requirements on Registrars for accurate data) often with consultation with recognised National departments/organisations, the broader community and knowledge sharing organisations such as CENTR.
Any TLD has a vested interest in ensuring accuracy of data due to the adverse outcomes inaccurate data could have. For example, if a registrant's contact details are missing or false when a phishing attack or site hijack has been detected, the registry may encounter problems when 'taking down' the site and potentially run into legal claims.
Several surveys and studies have been carried out on WHOIS accuracy and discussions are regularly held between ccTLD registries to share experiences, concerns and methods of combating potential issues. Generally the feeling is that there are indeed problems of data accuracy and that they have a social responsibility to address them.
In a CENTR survey conducted between April and May 2010 it was noted that several European ccTLDs perform verification checks. Registries that do not run a verification process often have a process in place in place to deal with claims of false domain holder contact

9 http://www.icann.org/en/processes/icann-procedure-17jan08.htm
10 Source: CENTR 2010 A-Level Survey (members only)
11 Law Enforcement due Diligence Recommendations for ICANN – Seoul :
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Ws%202/LEA_ICANN_Recom_oct2009.pdf

data. In cases where false data is found, often the contact point for the domain will receive notification and a time frame to rectify the data before potential suspension of the domain.
On the side of gTLDs, a 2009 WHOIS accuracy study from NORC (National Opinion Resource Centre) and commissioned by ICANN showed that only 23% of the records in the sample were fully accurate (using a strict interpretation of criteria/definition of accuracy)[12] however twice that number met a more relaxed version of accuracy. Overall around 70% of the sample had some form of contact. Similar outcomes have been found on ccTLD surveys which suggests verification of data is not being achieved as well as it could be.

The WHOIS Review Team

In accordance with principles set out in the ICANN Affirmation of Commitments (2009), a WHOIS Review Team began work recently on assessing WHOIS policy and its effectiveness. As part of this review, the team in June 2011 solicited input from the community based on several specific questions. Among other things, the team called for input from the ccTLD community on questions of privacy and accuracy in the WHOIS. Verification checks of data close to the point of registration was of particular note in responses from ccTLDs. For example, in the case of .fr it was noted that cross checks are made on companies and legal organisations against public databases to ensure registrant accuracy in the WHOIS database in France. For private registrants verification checks are also made with the help of the Registrars. In the response from .uk it was noted that accuracy of 'opted-out' (see above) domains was on average higher (92% had a traceable postal address[13]). One impressive figure came from the Chinese (.cn) response stating their end of 2010 accuracy to be 97% attributed the success to verification of registrant information. They also stated that collaboration with Registrars is critical in improving accuracy.

At the ICANN32 meeting in Costa Rica, the Review Team presented the findings of their work as well as 20 recommendations to improve the WHOIS. Some of the findings were listed as follows;

- No clear policy, ICANN should create a single policy on WHOIS.
- Outreach should be expanded on whois policy issues : cross community/consumer awareness
- Data accuracy (including contractibility) needs to be improved (see also NORC study on whois). ICANN should produce ongoing reports on data accuracy in whois.
- Privacy and proxy services need to be clarified given difficulties for investigations particularly with LE agencies. The team recommends clear requirements for all privacy services consistent with national laws.
- Data is difficult to find (consumer trust) so ICANN should set up dedicated interface to provide thick whois data.

A draft report from the Whois Review Team was published in December 2011 and public comments open till late March 2012. The final report and recommendations will be published by 30th April 2012.

FURTHER-READING.04

Data Privacy links from the EU

- **1995 Data Protection Directive:**

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- **2002 E-Privacy Directive:**

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

- **Proposal Document for review of 1995 Data Protection Directive (95/46/EC):**

A comprehensive approach on personal data protection in the European Union

- **Article 29 Working Party:**

http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm
Opinion 2/2003 on the application of the data protection principles to the Whois directories

ICANN

- **ICANN Procedure For Handling WHOIS Conflicts with Privacy Law:**

http://www.icann.org/en/processes/icann-procedure-17jan08.htm

- **Inventory of WHOIS Service Requirements – Final Report**

http://gnso.icann.org/issues/whois/whois-service-requirements-final-report-29jul10-en.pdf

- **WHOIS Policy Review Team – Discussion Paper**

http://www.icann.org/en/reviews/affirmation/whois-rt-draft-final-report-05dec11-en.pdf

12 Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information – pg 14 (http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf)Full accuracy criteria: deliverable address, name linked to address, and registrant confirmed ownership and correctness of all details during interview
13 Nominet response to WHOIS review team call for public comment: http://forum.icann.org/lists/whoisrt-discussion-paper/pdfkqoIQZXzHJ.pdf