Brno University of Technology
Faculty of Information Technology

ISA - Network Applications and Network Administration

Whois whisperer

November 18, 2019

Peter Havan (xhavan00)

Contents

1 DNS

The Domain Name System (DNS) provides replicated distributed secure hierarchical databases that store "resource records" (RRs) under domain names.[2] It is an important part of the web's infrastructure, serving as the Internet's phone book: every computer connected to the Internet is identified by IP address. However, humans are not good at remembering numbers. DNS bridges the gap between humans and computers by resolving (translating) hostnames into IP addresses. The client (e.g web broswer, this app.) performs a DNS query against DNS server. DNS resolver checks whether hostname is available in local cache and if not it contants other DNS servers.

1.1 DNS records

There are numerous DNS record types, this project focused on the most common ones:

- A Record - Address Mapping record - stores hostname and its corresponding IPv4 address
- AAAA Record - IP Version 6 Address record - stores hostname and its corresponding IPv6 address
- CNAME Record - Canonical Name record - alias of hostname
- MX Record - Mail exchanger record - specifies mail exchange server for domain name
- NS Record - Name Server record - specifies authoritative server/s for the zone
- PTR Record - Reverse-lookup Pointer record - contrast to A record, maps IP address hostname for reverse lookup
- SOA Record - Start of Authority - every zone has one SOA, specifies name of primary server and email address of administrator

2 WHOIS

WHOIS is a TCP-based transaction-oriented query/response protocol that is widely used to provide information services to Internet users. For historic reasons, WHOIS lacks many of the protocol design attributes, for example internationalisation and strong security. A WHOIS server listens on TCP port 43 for requests from WHOIS clients. The WHOIS client makes a text request to the WHOIS server, then the WHOIS server replies with text content. All requests are terminated with ASCII CR and then ASCII LF. [3] The fact that WHOIS respeonses are not stardardized makes creating parsers of them difficult. Despite the age of WHOIS protocol, there are only handful parsers out there. Some examples of whois servers:

- textttwhois.nic.cz
- textttwhois.ripe.net
- textttwhois.markmonitor.com

3 Implementation

3.1 DNS Query

After the app. parses through the arguments, there is an attempt to resolve IP address to hostname textttgetnameinfo() so that we can get maximum information from DNS. PTR record is still gathered. This behaviour might not be wanted though, as normally you'd only get PTR record. Running the program with option -o disables this "feature/mistake". Whether or not is option -o enabled, the next step is textttresolv.h fuction res_init() that initializes global struct variables, most importantly it reads textttresolv.conf and gets default domain name, name server addresses and search order. If option -d was given, the DNS address in texttt_res structure is manually overwritten. Next, we proceed with actual DNS querying: fuction textttresolveDns handles this. textttresolveDns fuction is called for each DNS record separately. The fuctions makes great use of textttresolv.h library which makes it possible to query DNS without raw sockets. The primary goal of textttresolveDns function is to parse the DNS answer and write output in readable format. Secondary goal is to fill texttta Records and textttaaaaRecords arrays with respective A and AAAA records, that are in the next step used for WHOIS protocol. Reverse lookup for IPv6 is not implemented.

3.2 WHOIS Query

The first thing that has to be done is to resolve -w argument if hostname was given for whois server. This is done with the help of textttgetaddrinfo, however in hindsight, our own textttresolveDns fuction could have been used and the resulting code would probably be simpler. Finally, the `myWhois` takes responsibility for querying whois server and parsing the answer. `myWhois` function is first called for argument of option -q and then for each A record and AAAA record, previously stored by `resolveDns`. The parsing is handled with the help of regular expressions and was made based on textttwhois.nic.cz, textttwhois.ripe.net and textttwhois.arin.net. Answer from the server is read line by line and compared with the regular expression and printed of it matches.

4 Test runs and examples

```
$ ./isa-tazatel -q www.fit.vutbr.cz -w whois.ripe.net
================DNS================
A:       147.229.9.23
AAAA:    2001:67c:1220:809::93e5:917
MX:      tereza.fit.vutbr.cz
===============WHOIS===============
for:     www.fit.vutbr.cz
-----------------------------------

for record A:    147.229.9.23

inetnum:         147.229.0.0 - 147.229.254.255
descr:           Brno University of Technology
country:         CZ
admin-c:         CA6319-RIPE
address:         Brno University of Technology
address:         Antoninska 1
address:         601 90 Brno
address:         The Czech Republic
```

```
phone:          +420 541145453
phone:          +420 723047787
descr:          VUTBR-NET1
-----------------------------------
for record AAAA:        2001:67c:1220:809::93e5:917

country:        CZ
admin-c:        MS6207-RIPE
address:        Antoninska 548/1
address:        60190
address:        Brno
address:        CZECH REPUBLIC
phone:          +420541145453
address:        Brno University of Technology
address:        Antoninska 1
address:        Brno
address:        601 90
address:        The Czech Republic
phone:          +420 541 145 441
address:        Brno University of Technology
address:        Center of Computing and Information Services
address:        Antoninska 1
address:        Brno
address:        601 90
address:        The Czech Republic
phone:          +420 541145630
descr:          VUTBR6-NET
```

```
$ ./isa-tazatel -q google.com -w whois.ripe.net
```

```
================DNS================
A:      172.217.23.238
AAAA:   2a00:1450:4014:80d::200e
MX:     aspmx.l.google.com
MX:     alt3.aspmx.l.google.com
MX:     alt1.aspmx.l.google.com
MX:     alt2.aspmx.l.google.com
MX:     alt4.aspmx.l.google.com
NS:     ns4.google.com
NS:     ns2.google.com
NS:     ns1.google.com
NS:     ns3.google.com
SOA:    ns1.google.com
===============WHOIS===============
for:    google.com
-----------------------------------

for record A:   172.217.23.238

inetnum:        172.103.96.0 - 172.240.255.255
descr:          IPv4 address block not managed by the RIPE NCC
```

```
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
----------------------------------
for record AAAA:        2a00:1450:4014:80d::200e

descr:          EU metro frontend
country:        ie
admin-c:        GOOG1-RIPE
address:        Google Ireland Limited
admin-c:        GOOG-RIPE
admin-c:        JWS7-RIPE
```

```
$ ./isa-tazatel -q 172.217.23.238 -w whois.ripe.net

================DNS===============
A:      172.217.23.238
PTR:    prg03s06-in-f14.1e100.net
PTR:    prg03s06-in-f238.1e100.net
===============WHOIS==============
for:    172.217.23.238
inetnum:        172.103.96.0 - 172.240.255.255
descr:          IPv4 address block not managed by the RIPE NCC
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
----------------------------------

for record A:   172.217.23.238

inetnum:        172.103.96.0 - 172.240.255.255
descr:          IPv4 address block not managed by the RIPE NCC
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
```

```
$ ./isa-tazatel -q 172.217.23.238 -w whois.ripe.net -o
================DNS===============
PTR:    prg03s06-in-f14.1e100.net
PTR:    prg03s06-in-f238.1e100.net
===============WHOIS==============
for:    172.217.23.238
inetnum:        172.103.96.0 - 172.240.255.255
descr:          IPv4 address block not managed by the RIPE NCC
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
```

```
$ ./isa-tazatel -q vutbr.cz -w whois.nic.cz

================DNS================
A:      147.229.2.90
MX:     mx.vutbr.cz
NS:     rhino.cis.vutbr.cz
NS:     pipit.cis.vutbr.cz
SOA:    rhino.cis.vutbr.cz
===============WHOIS===============
for:    vutbr.cz
admin-c:        VUTBR-TPODER
admin-c:        CID:IHAZMUK
address:        Antoninska 548/1
address:        Brno
address:        601 90
address:        CZ
address:        Antoninska 548/1
address:        Brno
address:        601 90
address:        Jihomoravsky kraj
address:        CZ
address:        Antoninska 548/1
address:        Brno
address:        601 90
address:        Jihomoravsky kraj
address:        CZ
-----------------------------------

for record A:   147.229.2.90
```

```
$ ./isa-tazatel -q 2a00:1450:4014:80d::200e -w whois.ripe.net -d 8.8.8.8

================DNS================
AAAA:   2a00:1450:4014:80d::200e
===============WHOIS===============
for:    2a00:1450:4014:80d::200e
descr:          EU metro frontend
country:        ie
admin-c:        GOOG1-RIPE
address:        Google Ireland Limited
admin-c:        GOOG-RIPE
admin-c:        JWS7-RIPE
-----------------------------------
for record AAAA:        2a00:1450:4014:80d::200e

descr:          EU metro frontend
country:        ie
admin-c:        GOOG1-RIPE
address:        Google Ireland Limited
admin-c:        GOOG-RIPE
```

```
admin-c:        JWS7-RIPE
```

```
  $ ./isa-tazatel -q 2a00:1450:4014:80d::200e -w whois.ripe.net -d 8.8.8.8 -o
```

```
================DNS================
================WHOIS================
for:    2a00:1450:4014:80d::200e
descr:          EU metro frontend
country:        ie
admin-c:        GOOG1-RIPE
address:        Google Ireland Limited
admin-c:        GOOG-RIPE
admin-c:        JWS7-RIPE
```

References

[1] Dns: Types of dns records, dns servers and dns query types. `https://ns1.com/resources/dns-types-records-servers-and-queries`. Accessed: 2019-11-18.

[2] D. Eastlake 3rd. Domain Name System (DNS) IANA Considerations. RFC 6895, RFC Editor, April 2013.

[3] L. Daigle. WHOIS Protocol Specification. RFC 3912, RFC Editor, September 2004.

[4] J. Gargano and K. Weiss. WHOIS Protocol Specification. RFC 1834, RFC Editor, August 1995.

[5] C. Hendrick. Routing Information Protocol. RFC 1058, RFC Editor, November 1998.

[6] G. Malkin. RIP Version 2. RFC 2453, RFC Editor, Jún 1988.

[7] G. Malkin and R. Minnear. RIPng for IPv6. RFC 2080, RFC Editor, Január 1997.

[8] EARN Staff. Guide to Network Resource Tools. RFC 1580, RFC Editor, March 1994.