Project documentation
ISA 2019/2020
Whois tazatel

18.11.2019

Author : Samuel Stuchlý
Login : xstuch06

Obsah

Description of the task

Task was to study the whois protocol and DNS and use that information in project implementation. Goal of the project was to implement a C/C++ program that will take some IP address or hostname, then IP address or hostname of whois server and displays information about given IP address or hostname.
Program would take 3 arguments :

- -q <IP|hostname>, compulsory argument
- -w <IP|hostname of WHOIS server>, which will be queried, compulsory argument
- -d <IP>, DNS server which will be queried, optional argument, implicitely DNS resolver in OS will be used

Output of the program was supposed to be information obtained through whois displayed in easily readable form(to a human).

Solution of the task

Argument parsing

First part of the project implementation is argument parsing. In assignment notes, it is mentioned to use function getopt() for parsing arguments. Implementation of this function was inspired from linux man pages http://man7.org/linux/man-pages/man3/getopt.3.html. (No code was directly copied, only used as example to base my implementation on, therefore term 'inspired' is used within this documentation.) Arguments are setup as described above in the 'Decription of task' section. Argument 'd' accepts only IP address in either IPv4 or IPv6 format. Does not accept hostname. However there is no functionality behind argument 'd'. The DNS part of the project is not implemented due to bonus nature of the feature and lack of time. Upon entering an incorrect argument value or argument option, program displays and an error message plus a help message with correct argument format. Program exits with EXIT_FAILURE.

Hostname to IP

Second part of the argument parsing is converting hostname to ip. In arguments 'q' and 'w' program recieves either IP addresse or hostname for each argument. To check if these arguemnts are valid program uses getaddrinfo() function, which takes hostname or ip and return list of addrinfo structures. Usage of gettaddrinfo() was inspired from https://gist.github.com/jirihnidek/bf7a2363e480491da72301b228b35d5d and linux man pages http://man7.org/linux/man-pages/man3/getaddrinfo.3.html. Program takes first returned addrinfo structure and stores it in structure variable passed in as parameter, so it can keep data after is_hostname_or_IP() is done. This function returns boolean value. Next step is to check if whois server hostname is a valid whois server. Program only accepts as whois hostname hostnames that pass getaddrino() and their hostname contains either of prefixes 'whois.', 'www.whois.'.

Whois query

Second part of the project implementation is query to whois server. To make the query program allocates a socket by using socket() function, which returns a socket file descriptor *sfd.* Socket is specified to be TCP connection based on 'RFC 3912: WHOIS protocol Specification'. Then using *sfd, sockaddr_in or sockaddr_in6 which is* filled with info from previously stored addrinfo structure for whois server, and port is set to 43, based on 'RFC 3912: WHOIS protocol Specification', it tries to

connect to the whois server. Once it connects, it sends a query to the whois server by function send().In case'q' argument is hostname(not IP address), program tries to query with ip address first and if whois server fails to find record, then program tries query with hostname as is in 'q' argument. The Query format is hostname or ip in text followed by <CR><LF> characters. This is specified in 'RFC 3912: WHOIS protocol Specification' in section 3 Protocol Example :

```
client                          server at whois.nic.mil

   open TCP    ---- (SYN) ------------------------------>
               <---- (SYN+ACK) -------------------------
   send query  ---- "Smith<CR><LF>" --------------------->
   get answer  <---- "Info about Smith<CR><LF>" ---------
               <---- "More info about Smith<CR><LF>" ----
   close       <---- (FIN) ------------------------------
               -----  (FIN) ------------------------------>
```

Whois Answer

Last part of project implementation is receiving and parsing the answer from whois server. As seen in protocol example above, whois server can send answer in multiple responses, therfore while loop is used on function recv(), to get all of the whois answer.This answer is stored in char * answer. Output of program is specified in asignment to contain at least (inetnum, netname, descr, country, address, phone, admin-c) information, but others can be displayed as well. Therefore for parsing answer , progrem uses array of keywords :

```
std::string keywords [25] = {"inetnum:", "netname:", "descr:", "country:",
"address:", "phone:", "admin-:", "org:", "domain:", "remarks:", "refer:",
"name:", "NetRange:", "Organization:", "Address:", "Country:", "Ref:",
"Domain:", "Name:", "Contact:", "Phone:", "Email:", "Street:", "City:",
"Code:"};
```

These are keywords specified in assignement plus couple interesting ones, plus due to nature of my parsing it was needed to put some options with capital letters as well to get data from whois servers that format their answers differently. To parse the answer program uses strtok() function in combiantion with std::string.find(). There are limitations to displaying the whois answer. These are specified in README file.

Testing

This program was tested on reference machine provided with assignement. We managed to get some private information, for example in medipharm-sluzby.sk we found out name of the owner and address of his company.

Here are 5 of program outputs compared to the 5 different online tools outputs :

```
./isa-tazatel -q www.fit.vutbr.cz -w
whois.ripe.net
=== WHOIS ===
inetnum:        147.229.0.0 -
147.229.254.255
netname:        VUTBRNET
netname:        VUTBRNET
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




==========================================
www.fit.butbr.cz on website
https://www.whois.com/whois/

%  (c) 2006-2019 CZ.NIC, z.s.p.o.
%
% Intended use of supplied data and
information
%
% Data contained in the domain name
register, as well as information
% supplied through public information
services of CZ.NIC association,
% are appointed only for purposes connected
with Internet network
% administration and operation, or for the
purpose of legal or other
% similar proceedings, in process as
regards a matter connected
% particularly with holding and using a
concrete domain name.
%
% Full text available at:
% http://www.nic.cz/page/306/intended-use-
of-supplied-data-and-information/
%
% See also a search service at
http://www.nic.cz/whois/
%
%
% Whoisd Server Version: 3.12.0
% Timestamp: Sat Nov 16 21:31:51 2019

domain:       vutbr.cz
registrant:   SB:VUTBR-CZ
admin-c:      VUTBR-TPODER
admin-c:      CID:IHAZMUK
nsset:        NSS:VUTBR:1
keyset:       KEYSET-VUTBR.CZ:1
registrar:    REG-INTERNET-CZ
registered:   19.05.1994 02:00:00
changed:      05.02.2019 10:36:30
expire:       12.10.2023

contact:      SB:VUTBR-CZ
org:          Vysoke uceni technicke v Brne
name:         Vysoke uceni technicke v Brne
address:      Antoninska 548/1
address:      Brno
address:      601 90
address:      CZ
registrar:    REG-INTERNET-CZ
created:      10.08.2001 22:13:00
changed:      15.05.2018 21:32:00

contact:      VUTBR-TPODER
org:          Vysoké učení technické v Brně
name:         Tomáš Podermański
address:      Antonínská 548/1
address:      Brno
address:      601 90
address:      Jihomoravský kraj
address:      CZ
registrar:    REG-INTERNET-CZ
created:      05.02.2019 10:32:19

contact:      CID:IHAZMUK
org:          Vysoké učení technické v Brně
name:         Ivo Ažmuk
address:      Antonínská 548/1
address:      Brno
address:      601 90
address:      Jihomoravský kraj
address:      CZ
registrar:    REG-INTERNET-CZ
created:      06.10.2008 17:30:01
changed:      05.08.2019 11:24:03

nsset:        NSS:VUTBR:1
nserver:      rhino.cis.vutbr.cz
(147.229.3.10,
2001:67c:1220:e000::93e5:30a)
nserver:      pipit.cis.vutbr.cz
(77.93.219.110, 2a01:430:120::4d5d:db6e)
tech-c:       CID:IHAZMUK
tech-c:       VUTBR-TPODER
registrar:    REG-INTERNET-CZ
created:      14.10.2008 11:03:11
changed:      05.02.2019 10:45:05

keyset:       KEYSET-VUTBR.CZ:1
dnskey:       257 3 5
AwEAAfhR+s/4SLZZNA+kD2u1UgYBUu+X3Avi60QCaE1
o2STterM405s8mWMWJOlZGtjjIky3TEMxQ0+ZtMbEeJ
u2wNDLdV/XglX+pJAjyy728WJH4u2/gJR8ZWsEIc0Jw
b4FjwmBiF2Koz0SGVvrzEZ9T1H7dHq2X6f8KzYBotJy
rAIWr9tZi/9tHrngZJ5wXELmMPWCfEFapdQMoKWoNvz
rMYFli17RMz7gJzCmNxMRV8/WkjsNPgYsTKpsAT8qEs
XiTN9987AIKPHvc5j+/njq+fTXdOqGVpIgSiso+qJMd
dEMBcu/MBBYVFOwRQe1ez2tMwIX7y5mwDvK0wsmyRvH
ugfFuxSnfiJvQr05kSnj0wxD9s9LNhrF4PocrcYqnBN
/lBx9D6633jJ3zT3T5Foe/Vj9A/X7F2oN6FOkdwO+YS
EUot980pJQut6DR22UP4bLakyDMiTdOQ31c/dRIoTsc
cxw+838pXFyEPgiqOHRSeN/w9km6BIDcl+32Xq97kXS
MQH6AxOUsx9/Mxdj7ISwbS4utaAWoP460+TMcnfJfWf
BNEWhuFvnfB9l63ZjZToB2PUVhrTxRwKUlfMLegSJKo
Zfiae82kK1pN4xFYyquKSykm/oXsM2w4OQvpqGcTwAX
zZ5s95J45f7PsCap0bscGKumxsHcDswWpUz/UVosIrr
tech-c:       CID:IHAZMUK
tech-c:       VUTBR-TPODER
registrar:    REG-INTERNET-CZ
created:      13.10.2008 10:27:37
changed:      14.02.2019 13:36:06
```

```
./isa-tazatel -q seznam.cz -w whois.nic.cz
=== WHOIS ===
domain:       seznam.cz
admin-c:      SEZNAM-CZ-AS-TECH
org:          Seznam.cz, a.s.
name:         Seznam.cz, a.s.
address:      Radlická 3294/10
address:      Praha 5
address:      15000
address:      CZ
org:          Seznam.cz, a.s.
name:         Vlastimil Pečínka
address:      Radlická 3294/10
address:      Praha 5
address:      150 00
address:      CZ
```

---

seznam.cz on website https://www.whois.net/

```
% (c) 2006-2019 CZ.NIC, z.s.p.o.
%
% Intended use of supplied data and
information
%
% Data contained in the domain name
register, as well as information
% supplied through public information
services of CZ.NIC association,
% are appointed only for purposes connected
with Internet network
% administration and operation, or for the
purpose of legal or other
% similar proceedings, in process as
regards a matter connected
% particularly with holding and using a
concrete domain name.
%
% Full text available at:
% http://www.nic.cz/page/306/intended-use-
of-supplied-data-and-information/
%
% See also a search service at
http://www.nic.cz/whois/
%
%
% Whoisd Server Version: 3.12.0
% Timestamp: Mon Nov 18 22:09:12 2019

domain: seznam.cz
registrant: SB:SEZNAM-CZ-AS
admin-c: SEZNAM-CZ-AS-TECH
nsset: SEZNAM-NAMESERVERS
keyset: SEZNAM-CZ-AS-ECDSA
registrar: REG-IGNUM
status: Sponsoring registrar change
forbidden
registered: 07.10.1996 02:00:00
changed: 29.05.2019 14:05:04
expire: 29.10.2020

contact: SB:SEZNAM-CZ-AS
org: Seznam.cz, a.s.
name: Seznam.cz, a.s.
address: Radlick?? 3294/10
address: Praha 5
address: 15000
address: CZ
registrar: REG-IGNUM
created: 10.08.2001 22:13:00
changed: 27.11.2018 10:30:01

contact: SEZNAM-CZ-AS-TECH
org: Seznam.cz, a.s.
name: Vlastimil Pe????nka
address: Radlick?? 3294/10
address: Praha 5
address: 150 00
address: CZ
registrar: REG-MOJEID
created: 27.02.2017 13:51:01
changed: 04.12.2018 15:48:58

nsset: SEZNAM-NAMESERVERS
nserver: ans.seznam.cz (77.75.74.80,
2a02:598:3333::3)
nserver: ams.seznam.cz (77.75.75.230,
2a02:598:4444::4)
tech-c: SB:SEZNAM-CZ-AS
registrar: REG-IGNUM
created: 18.10.2007 18:01:01
changed: 11.12.2014 11:08:04

keyset: SEZNAM-CZ-AS-ECDSA
dnskey: 257 3 13
+qiXHs6rSZgd2hCEut/9gKAbGHgNKE686hhiP6wUZqy
XJKsV5Sm4mqXoM5zwxBdPl7Qi4cpKEj5pQdN1KwoAlg
==
tech-c: SB:SEZNAM-CZ-AS
registrar: REG-IGNUM
created: 27.03.2018 17:36:55
```

```
./isa-tazatel -q medipharm-sluzby.sk -w
whois.sk-nic.sk
=== WHOIS ===
Domain:                         medipharm-
sluzby.sk
Admin Contact:                  ASYS-0003
Tech Contact:                   ASYS-0003
Name:                           Atlantis
Systems, s.r.o.
Organization:                   Atlantis
Systems, s.r.o.
Phone:
+421.220633999
Email:
registry@atlantis.sk
Street:                         Gorkého 6
City:                           Bratislava
Postal Code:                    81101
Country Code:                   SK
Contact:                        ATL-10015
Name:                           Ing. Jiri
Stuchly
Organization:                   MEDIPHARM-
SLUZBYs.r.o.
Email:
registry@atlantis.sk
Street:                         Podnikateľská
5
City:                           Košice
Postal Code:                    04017
Country Code:                   SK
```

```
==========================================
medipharm-sluzby.sk on website
http://whois.domaintools.com/

Domain:                         medipharm-
sluzby.sk
Registrant:                     ATL-10015
Admin Contact:                  ASYS-0003
Tech Contact:                   ASYS-0003
Registrar:                      ASYS-0003
Created:                        2005-08-06
Updated:                        2019-07-24
Valid Until:                    2020-08-06
Nameserver:
ns0.atlantis.sk
Nameserver:
ns1.atlantis.sk
EPP Status:
clientTransferProhibited

Registrar:                      ASYS-0003
Name:                           Atlantis
Systems, s.r.o.
Organization:                   Atlantis
Systems, s.r.o.
Organization ID:                35844230
Phone:
+421.220633999
Email:
Street:                         Gorkého 6
City:                           Bratislava
Postal Code:                    81101
Country Code:                   SK
Created:                        2017-09-01
Updated:                        2019-11-15

Contact:                        ATL-10015
Name:                           Ing. Jiri
Stuchly
Organization:                   MEDIPHARM-
SLUZBYs.r.o.
Organization ID:                36572900
Email:
Street:                         Podnikateľská
5
City:                           Košice
Postal Code:                    04017
Country Code:                   SK
Registrar:                      ASYS-0003
Created:                        2018-08-13
Updated:                        2018-08-13
```

```
./isa-tazatel -q twitter.com -w
whois.arin.net
=== WHOIS ===
NetRange:       104.244.40.0 -
104.244.47.255
NetName:        TWITTER-NETWORK
Organization:   Twitter Inc. (TWITT)
Ref:
https://rdap.arin.net/registry/ip/104.244.4
0.0
OrgName:        Twitter Inc.
Address:        1355 Market Street
Address:        Suite 900
City:           San Francisco
PostalCode:     94103
Country:        US
Ref:
https://rdap.arin.net/registry/entity/TWITT
OrgAbuseName:   Twitter Network Abuse
OrgAbusePhone:  +1-415-222-9670
OrgAbuseEmail:  net-abuse@twitter.com
OrgAbuseRef:
https://rdap.arin.net/registry/entity/TNA33
-ARIN
OrgTechName:   Southern, Timothy
OrgTechPhone:  +1-415-222-9670
OrgTechEmail:  tsouthern@twitter.com
OrgTechRef:
https://rdap.arin.net/registry/entity/SOUTH
69-ARIN
OrgTechName:   Network Operations
OrgTechPhone:  +1-415-222-9670
OrgTechEmail:  noc@twitter.com
OrgTechRef:
https://rdap.arin.net/registry/entity/NETWO
3685-ARIN
OrgNOCName:   Network Operations
OrgNOCPhone:  +1-415-222-9670
OrgNOCEmail:  noc@twitter.com
OrgNOCRef:
https://rdap.arin.net/registry/entity/NETWO
3685-ARIN

==========================================
twitter.com on website
https://webwhois.verisign.com/webwhois-
ui/index.jsp?language=#

Domain Name: TWITTER.COM
Registry Domain ID: 18195971_DOMAIN_COM-
VRSN
Registrar WHOIS Server:
whois.corporatedomains.com
Registrar URL:
http://www.cscglobal.com/global/web/csc/dig
ital-brand-services.html
Updated Date: 2018-12-07T19:32:35Z
Creation Date: 2000-01-21T16:28:17Z
Registry Expiry Date: 2020-01-21T16:28:17Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email:
domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibi
ted
Domain Status: serverDeleteProhibited
https://icann.org/epp#serverDeleteProhibite
d
Domain Status: serverTransferProhibited
https://icann.org/epp#serverTransferProhibi
ted
Domain Status: serverUpdateProhibited
https://icann.org/epp#serverUpdateProhibite
d
Name Server: A.R06.TWTRDNS.NET
Name Server: B.R06.TWTRDNS.NET
Name Server: C.R06.TWTRDNS.NET
Name Server: D.R06.TWTRDNS.NET
Name Server: D01-01.NS.TWTRDNS.NET
Name Server: D01-02.NS.TWTRDNS.NET
Name Server: NS3.P34.DYNECT.NET
Name Server: NS4.P34.DYNECT.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint
Form: https://www.icann.org/wicf/


>>> Last update of whois database: 2019-11-
18T21:05:38Z <<<
```

```
./isa-tazatel -q hokej.sk -w whois.ripe.net
=== WHOIS ===
inetnum:        92.240.252.0 -
92.240.252.255
netname:        SK-LSC-WEBGLOBE
netname:        SK-LSC-WEBGLOBE
descr:          WEBGLOBE, s.r.o.
descr:          Stara Prievozska 2
descr:          821 09, Bratislava,
Slovakia
country:        SK
admin-c:        LSCH1-RIPE
address:        LightStorm Communications
s.r.o.
address:        Parickova 18
address:        Bratislava
address:        821 07
address:        Slovak Republic
phone:          +421 2 32 400 000
admin-c:        TM782-RIPE
descr:          LightStorm Communications
s.r.o.
```

```
=====================================
hokej.sk on website https://who.is/whois/

Domain:                         hokej.sk
Registrant:                     FUNM-0003
Admin Contact:                  FUNM-0003
Tech Contact:                   FUNM-0003
Registrar:                      ARDE-0001
Created:                        2003-03-03
Updated:                        2019-03-14
Valid Until:                    2020-03-21
Nameserver:
ns.funradio.sk
Nameserver:                     ns.datcon.sk
EPP Status:                     ok

Registrar:                      ARDE-0001
Name:                           Sepia
Systems, s.r.o.
Organization:                   Sepia
Systems, s.r.o.
Organization ID:                36409448
Phone:
+421.903436336
Email:
Street:
Vysokoškolákov 41
City:                           Žilina
Postal Code:                    01008
Country Code:                   SK
Created:                        2017-09-01
Updated:                        2019-10-08

Contact:                        FUNM-0003
Name:                           FUN MEDIA
GROUP
Organization:                   FUN MEDIA
GROUP
Organization ID:                44845995
Phone:
+421.903436336
Email:
Street:                         Leškova 5
City:                           Bratislava
Postal Code:                    81104
Country Code:                   SK
Registrar:                      ARDE-0001
Created:                        2017-09-01
Updated:                        2017-09-01

Information Updated: 2019-11-18 21:06:52
```

Bibliography

(No code was directly copied, only used as example to base my implementation on, therefore term 'inspired' is used within this documentation.)

- RFC 1834: Whois and Network Information Lookup Service, Whois++
- RFC 3912: WHOIS protocol Specification
- Documentaion on https://www.ripe.net/manage-ips-and-asns/db/support/querying-the-ripe-database
- whois servery whois.ripe.net, whois.nic.cz