Vysoké učení technické v Brně
Fakulta informačních technologií

Dokumentace k projektu pro předmět ISA

ISA-TAZATEL
(WHOIS, DNS)

18. listopadu 2019

Autor: Daniel Štěpánek, xstepa61@stud.fit.vutbr.cz
VUT Brno, Fakulta informačních technologií

Obsah:

1 Základní informace o programu:

Program, který na vstupu specifikuje IP adresu (IPv4 i IPv6) či hostname. K danému vstupu pak vypíše všechny známé podrobnosti o vlastníkovi.

Parametry:

-q <IP| hostname>, povinný argument
-w <IP| hostname>, povinný argument
-d <IP> nepovinný argument, přičemž implicitně se používá DNS resolver v operačním systému

Ukázka spuštění: ./isa-tazatel -q www.fit.vutbr.cz -d dns.google.com -w whois.ripe.net

Omezení: Dotazování DNS serveru podle -d argumentu není implementováno. Vždy se dotazuje resolver v operačním systému.

Seznam souborů: isa-tazatel.cpp, Makefile, README, manual.pdf

2 Uvedení do problematiky:

Program řeší problematiku získávání informací o doménách a jejich vlastníkovi pomoci dotazování serveru DNS a serveru WHOIS.

Pro pochopení aplikace je nutné znát jisté pojmy, a alespoň základy programování síťových služeb.

WHOIS je označení databáze obsahující údaje o majitelích internetových domén a IP adres. Definován v RFC 3912. Pro komunikaci se servery se využívá protokol TCP na portu 43. Klient na server pošle požadavek, který je ukončen ASCII CR a poté ASCII LF znaky. Komunikace končí zprávou od serveru ihned poté, co odešle všechny informace dostupné k požadavku.

Ukázka komunikace (RFC 3912):

```
 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) ------------------------------>
```

DNS (Domain Name System) je systém doménových jmen, který využívá servery DNS a slouží jako databáze síťových informací. Definován v RFC1035. Pro komunikaci s DNS servery lze využít TCP i UDP protokoly. A využívají porty 53. DNS servery mají stromovou strukturu, kde kořenový uzel má hodnotu , . ‘(tečka).

3 Návrh aplikace:

Vzhledem k proměnnému počtu argumentů bylo vhodné využít funkci „getopt“. Následně získat z -q argumentu doménové jméno pro DNS dotaz a IP adresu pro WHOIS dotaz. Z dalších dvou argumentů -w a -d, pokud již nebyly zadané, IP adresy pro vytvoření socketů. Komunikace se servery WHOIS je nutné vytvořit TCP socket. Při dotazování DNS je využito knihovních funkcí „resolv.h“. Při implementaci jsem postupoval dle návodu na tomto odkazu [1] .

Při návrhu a implementaci nebylo využito objektového programování.

4 Popis implementace:

Program je implementován v jazyce C/C++. Aplikace je primárně vytvořena pro operační systémy GNU/ Linux, vyvíjena byla na Ubuntu 18.04.3. Testována na Ubuntu 18.04.3 a na serveru merlin.fit.vutbr.cz.

4.1 Převod mezi IP a doménovým jménem:

Jelikož je možné zadat vstup ve formě IPv4, IPv6 i doménové jméno, je nutné pro jednotlivé služby převést adresy na doménová jména a naopak.

Před voláním funkce obsluhující komunikaci s whois je třeba získat IP adresu z -q i -w parametrů. Tento proces provádí funkce „hostname_to_ip“. Pro podporu obou verzi IP protokolu jsem zvolil knihovní funkci „getaddrinfo“ Výsledek je převeden pomocí „inet_ntop“. Pokud nastane během převodu chyba, je program ukončen s chybovým kódem 20 a vypsáním chybové hlášky.

Naopak pro DNS server je nutné získat z q parametru doménové jméno, pokud je zadaná, je tento proces přeskočen. Pokud ne, tak program zavolá funkci „ip_to_hostname“. V první řadě je vytvořen socket typu sockaddr_in a následně zavolána knihovní funkce „getnameinfo“. Pokud nastane chyba, program skončí s chybovým kódem 20 a vypsáním chybové hlášky.

4.2 Implementace WHOIS:

Celá komunikace je implementována ve funkci „get_whois“. Po začátku vykonávání této funkce se vytvoří dotaz na server, který je typu char* a zakončen ASCII znaky CR a LF, jak je v definováno v RFC 3912. Jelikož může být adresa serveru typu IPv4 i IPv6, je tato skutečnost zohledněna při vytváření soketu.

Poté probíhá TCP komunikace, tedy napřed je navázáno spojení funkcí „connect“, následně zaslán dotaz a pokud vše proběhne v pořádku, tak je vypsána celá odpověď. Pokud nastane chyba, končí program s chybovým kódem -1. Funkce končí uzavřením spojení od klienta funkcí „close“.

4.3 Implementace DNS:

Popis funkce „get_dns“. Jako první je nutné upravit doménové jméno dotazu, neboť nemůže obsahovat předponu „www.“ To je realizováno standardními funkcemi z knihovny „string.h“.

Pro spojení s DNS servery je využito knihoven „resolv.h“ a “netdb.h”. Postup je inspirován návodem na tomto odkazu [1]. Pro každý údaj (A, AAAA, MX, …) musí být inicializovaná speciální knihovní struktura **res** pomocí „res_init“ a vytvořen specifický dotaz pomocí „res_mkquerry“. Zaslání požadavku a získání údajů zastává funkce „res_query“, která vrací též délku odpovědi. Všechny „res“ funkce při chybě vrací hodnotu -1, díky tomu lze zamezit běhové chybě v následujících krocích.

Každý údaj je získán ve specifické formě, a je nutné tedy zpracovat každý podle těchto specifik. Základ tvoří cyklus procházející všechny získané odpovědi k danému údaji, které jsou upraveny knihovními funkcemi z knihovny „string.h“ a poté vypsány bez redundantních dat.

4.4 Použité knihovny:

Výpis použitých knihoven využitých při implementaci.

```
#include<iostream>
#include<unistd.h>
#include<string>
#include<cstring>
#include<netdb.h>
#include<sys/types.h>
#include<sys/socket.h>
#include<netinet/in.h>
#include<arpa/inet.h>
#include<arpa/nameser.h>
#include<resolv.h>
#include<netdb.h>
#include<stdbool.h>
```

5 Reference:

[1] :
https://docstore.mik.ua/orelly/networking_2ndEd/dns/ch15_02.htm?fbclid=IwAR0rcGQ2T1muWvRsFFbPtfMzq4rmeW2efUGbJEMyXO1KkoMXgjoGT5JJSZY

6 Ukázky běhu programu:

Ukázka spuštění:

./isa-tazatel -q www.fit.vutbr.cz -w whois.ripe.net

Ukázky výstupů:

./isa-tazatel -q www.arin.net -w whois.arin.net

```
===DNS===
NS:
ns3.arin.net.
ns2.arin.net.
u.arin.net.
ns1.arin.net.
SOA:
ns1.arin.net.
MX:
smtp2.arin.net.
smtp3.arin.net.
smtp4.arin.net.
smtp1.arin.net.
A:
199.43.0.47
AAAA:
2001:500:4:201::47
=== WHOIS ===


NetRange:       199.43.0.0 - 199.43.0.255
CIDR:           199.43.0.0/24
NetName:        ARIN-ASH
NetHandle:      NET-199-43-0-0-1
Parent:         NET199 (NET-199-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS10745
Organization:   ARIN Operations (ARINOPS)
RegDate:        2005-11-09
Updated:        2015-07-15
Ref:            https://rdap.arin.net/registry/ip/199.43.0.0


OrgName:        ARIN Operations
OrgId:          ARINOPS
Address:        PO Box 232290
City:           Centreville
StateProv:      VA
PostalCode:     20120
Country:        US
RegDate:        2012-09-07
Updated:        2019-03-05
Ref:            https://rdap.arin.net/registry/entity/ARINOPS


OrgTechHandle: MJO282-ARIN
```

OrgTechName: O'Neill, Michael J
OrgTechPhone: +1-703-227-0660
OrgTechEmail: mjo@arin.net
OrgTechRef: https://rdap.arin.net/registry/entity/MJO282-ARIN

OrgAbuseHandle: AOA4-ARIN
OrgAbuseName: ARIN Operations Abuse
OrgAbusePhone: +1-703-227-0660
OrgAbuseEmail: abuse@arin.net
OrgAbuseRef: https://rdap.arin.net/registry/entity/AOA4-ARIN

OrgTechHandle: NEWTO24-ARIN
OrgTechName: Newton, Andy
OrgTechPhone: +1-703-227-0660
OrgTechEmail: andy@arin.net
OrgTechRef: https://rdap.arin.net/registry/entity/NEWTO24-ARIN

OrgTechHandle: ROWLE12-ARIN
OrgTechName: Rowley, Matt
OrgTechPhone: +1-703-227-0660
OrgTechEmail: matt@arin.net
OrgTechRef: https://rdap.arin.net/registry/entity/ROWLE12-ARIN

./isa-tazatel -q www.draw.io -w whois.nic.cz

===DNS===
NS:
	amy.ns.cloudflare.com.
	phil.ns.cloudflare.com.
SOA:
	amy.ns.cloudflare.com.
MX:
	 in1-smtp.messagingengine.com.
	 in2-smtp.messagingengine.com.
A:
	104.20.89.78
	104.20.88.78
AAAA:
	2606:4700:10::6814:584e
	2606:4700:10::6814:594e
=== WHOIS ===

./isa-tazatel -q www.facebook.com -w whois.arin.net

===DNS===
NS:
	b.ns.facebook.com.
	a.ns.facebook.com.
SOA:
	a.ns.facebook.com.

MX:
smtpin.vvv.facebook.com.
A:
157.240.30.35
AAAA:
2a03:2880:f13d:83:face:b00c:0:25de
=== WHOIS ===

NetRange: 157.240.0.0 - 157.240.255.255
CIDR: 157.240.0.0/16
NetName: THEFA-3
NetHandle: NET-157-240-0-0-1
Parent: NET157 (NET-157-0-0-0-0)
NetType: Direct Assignment
OriginAS:
Organization: Facebook, Inc. (THEFA-3)
RegDate: 2015-05-14
Updated: 2015-05-14
Ref: https://rdap.arin.net/registry/ip/157.240.0.0

OrgName: Facebook, Inc.
OrgId: THEFA-3
Address: 1601 Willow Rd.
City: Menlo Park
StateProv: CA
PostalCode: 94025
Country: US
RegDate: 2004-08-11
Updated: 2012-04-17
Ref: https://rdap.arin.net/registry/entity/THEFA-3

OrgAbuseHandle: OPERA82-ARIN
OrgAbuseName: Operations
OrgAbusePhone: +1-650-543-4800
OrgAbuseEmail: domain@facebook.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/OPERA82-ARIN

OrgTechHandle: OPERA82-ARIN
OrgTechName: Operations
OrgTechPhone: +1-650-543-4800
OrgTechEmail: domain@facebook.com
OrgTechRef: https://rdap.arin.net/registry/entity/OPERA82-ARIN

./isa-tazatel -q www.fit.vutbr.cz -w whois.ripe.net

===DNS===
NS:
gate.feec.vutbr.cz.
kazi.fit.vutbr.cz.
rhino.cis.vutbr.cz.
guta.fit.vutbr.cz.

SOA:
guta.fit.vutbr.cz.
MX:
eva.fit.vutbr.cz.
kazi.fit.vutbr.cz.
=== WHOIS ===

inetnum: 147.229.0.0 - 147.229.254.255
netname: VUTBRNET
descr: Brno University of Technology
country: CZ
admin-c: CA6319-RIPE
tech-c: CA6319-RIPE
status: ASSIGNED PA
mnt-by: VUTBR-MNT
created: 2014-11-19T08:23:45Z
last-modified: 2015-01-30T08:37:07Z
source: RIPE

role: Brno University of Technology - Backbone Admins
address: Brno University of Technology
address: Antoninska 1
address: 601 90 Brno
address: The Czech Republic
phone: +420 541145453
phone: +420 723047787
nic-hdl: CA6319-RIPE
mnt-by: VUT-BATCH-MNT
mnt-by: VUTBR-MNT
created: 2015-01-30T08:31:35Z
last-modified: 2016-11-04T14:01:52Z
source: RIPE abuse-mailbox: abuse@vutbr.cz

route: 147.229.0.0/17
descr: VUTBR-NET1
origin: AS197451
mnt-by: VUTBR-MNT
created: 2014-12-04T19:07:00Z
last-modified: 2014-12-04T19:07:00Z
source: RIPE

./isa-tazatel -q www.seznam.cz -w whois.ripe.net

===DNS===
NS:
ans.seznam.cz.
ams.seznam.cz.
SOA:
ans.seznam.cz.
MX:
mx2.seznam.cz.
mx1.seznam.cz.
A:

77.75.75.172
77.75.75.176
AAAA:
2a02:598:4444:1::1
2a02:598:4444:1::2
=== WHOIS ===

inetnum: 77.75.75.0 - 77.75.75.255
netname: SEZNAM-CZ
descr: Seznam.cz
country: CZ
admin-c: SZN5-RIPE
tech-c: SZN5-RIPE
status: ASSIGNED PA
mnt-by: SEZNAM-MNT
created: 2007-06-20T11:44:33Z
last-modified: 2007-06-20T11:44:33Z
source: RIPE

role: Seznam.cz IT department
address: Radlicka 3294/10 150 00 Prague 5 Czech Republic
phone: +420 602 126 570
abuse-mailbox: abuse@seznam.cz
admin-c: PZ172-RIPE
tech-c: SZN11-RIPE
tech-c: SZN10-RIPE
nic-hdl: SZN5-RIPE
mnt-by: SEZNAM-MNT
created: 2007-05-06T15:50:27Z
last-modified: 2015-07-03T13:19:00Z
source: RIPE

route: 77.75.75.0/24
descr: SEZNAM - II
origin: AS43037
mnt-by: SEZNAM-MNT
created: 2014-04-29T13:54:56Z
last-modified: 2014-04-29T13:54:56Z
source: RIPE