FIT.VUTBR.CZ

PROJEKT KURZU ISA 2019

WHOIS TAZATEL

AUTOR: LIBOR DVOŘÁČEK

XDVORA2T

ÚVOD

Zadáním bylo implementovat program, který bude k vloženému hostname/IP adrese zobrazovat maximum informací dostupných k danému záznamu z WHOIS a DNS.

DNS

V počátcích internetu bylo při přístupu k webové stránce nutno znat její IP adresu.K tomu nám dnes slouží DNS, které název hostitele na tyto adresy překládá. Záznamy pro překlad jsou uchovány na tzv. DNS serverech, které se nacházejí po celém světě.

DNS ZÁZNAMY

DNS servery ukládají do databáze tzv. Zdrojové záznamy (resource records)

Každý zdrojový záznam obsahuje čtveřici údajů. Jméno, hodnota, typ, TTL. Poslední zmiňovaný (TimeToLive) určuje životnost záznamu, ostatní informace jsou převedeny do tabulky níže.

Zdrojové záznamy

Typ	Hodnota
A	IPv4 adresa
AAAA	IPV6 adresa
MX	Kanonický název poštovního serveru
CNAME	Kanonický název hostitele
NS	Název hostitele autoritativního DNS serveru
SOA	Autoritativní info o DNS zóně
PTR	Ukazatel na kanonický název hostitele

WHOIS

Dotazování na WHOIS záznamy slouží k zjišťování údajů o konkrétních internetových doménách.

Typicky se WHOIS záznam skládá z informací jako je jméno a kontaktní údaje vlastníka domény a to samé pro organizaci, která doménu zaregistrovala. Dále pak obsahuje data registrace, DNS servery, poslední update a datum expirace.

SPUŠTĚNÍ PROGRAMU

Whois-tazatel očekáva na vstupu standardně dva povinné argumenty s parametrem:

-q <hledaný záznam ve tvaru IPv4/IPv6/hostname>

-w <dotazovaný whois server ve tvaru IPv4/IPv6/hostname>

Další nepovinný argument slouží pro bližší specifikaci dotazovaného DNS serveru

-d <IPv4 adresa dns serveru>

v případě absence se jako DNS server pro dotaz použije nastavení operačního systému.

Posledním argumentem **-h** je pak možno zobrazit k programu krátkou nápovědu.

Příklad spuštění potom může vypadat následovně:

./isa-tazatel -w whois.lacnic.bnet -q brazil.gov.br

IMPLEMENTACE

ARGUMENTY

Po spuštění programu nejdříve zpracuji argumenty přípazové řádky. Zjistím, zda byly zadány všechny povinné a určím o jaký typ (IPv4/IPv6/hostname) se jedná. Pokud je zadaný typ IPv4, nebo IPv6 adresa, převedu ji pomocí funkcí *inet_pton()* a *getnameinfo()* na hostname. Poté přistoupím k DNS dotazu.

DNS

Dotazování řeším s pomocí knihovny resolv.h. Na začátku volám funkci *res_init()*, která čte soubor /etc/resolv.conf a z něj získá adresy DNS serverů. Pokud byl program spuštěn s argumentem -d, přepíši strukturu *_res.nsaddr_list[0].sin_addr.s_addr* jeho parametrem. Následně se dotazuji pomocí funce *res_query()* na jednotlivé DNS záznamy. Pokud na některý záznam nedostanu korektní odpověd, nic na výstup nevypisuji a přejdu k dalšímu.

Jelikož některé whois servery neposkytují uspokojivé odpovědi při dotazování na IP adresu, ale vyžadují na vstupu hostname, vytvořil jsem v programu vector, do kterého ukládám

parametr argumentu -q a výsledky z PTR a A záznamů, abych měl co nejvíce možností pro samotné dotazování.

WHOIS

Při WHOIS dotazech se pak ptám nejdříve na IPv4 adresy z A záznamů. Až v případě neuspěchu se ptám na hostname případně na doménu z PTR záznamu. Toto pořadí jsem zvolil protože z mých testů vyplynula největší pravděpodobnost odpovědi právě na IP. Dotazování končí při prvním úspěšném vyhledání, nebo při posažení konce vyhledávacího "seznamu".

Jelikož se položky odpovědí mohou v některých případech lišit, bylo nutné zajistit konzistenci konečného výpisu uživateli. To jsem vyřešil vektorem stringů s klíčovými slovy, který porovnávám s odpovědí. V případě shody vypíši na obrazovku patřičně formátovaný string následující.

TESTY

Ověření funkčnosti jsem prováděl průběžně a to ručním dotazováním na whois služby jednotlivých regionálních internetových registrátorů. V rámci porovnání výstupů jsem vyzkoušel příkazy nslookup a whois v kombinaci s webovými službami regionálních internetových registrátorů. Příklady následují.

```
student@student-vm:/mnt/hgfs/isa$ ./isa-tazatel -q 38.107.241.66 -w whois.arin.net
===DNS===
A:      38.107.241.66
MX:     lavabit.com.
PTR:    lavabit.com
SOA:    ns1.lavabit.com.
SOA:    support.lavabit.com.
NS:     ns3.lavabit.com.
NS:     ns1.lavabit.com.
NS:     ns4.lavabit.com.
NS:     ns2.lavabit.com.
=== WHOIS === 38.107.241.66
Address:        2450 N Street NW
City:           Washington
Country:        US
PostalCode:     20037
StateProv:      DC
```

```
student@student-vm:/mnt/hgfs/isa$ ./isa-tazatel -q bike-forum.cz -w whois.nic.cz
===DNS===
A:      185.175.84.197
MX:     mx0.fortion.net.
MX:     mx1.fortion.net.
MX:     mx2.fortion.net.
PTR:    ip-84-197.r1.fortion.net
NS:     ns.fortion.cz.
NS:     ns.fortion.net.
=== WHOIS === 185.175.84.197
=== WHOIS === bike-forum.cz
address:        11000
address:        32600
address:        Božkovská 9
address:        CZ
address:        Plzeň
address:        Praha 1
address:        U Půjčovny 952/2
admin-c:        SUB-681788
contact:        FORTION-VM
contact:        SUB-681788
org:            Fortion Networks, s.r.o.
org:            Netflock, s.r.o.
```

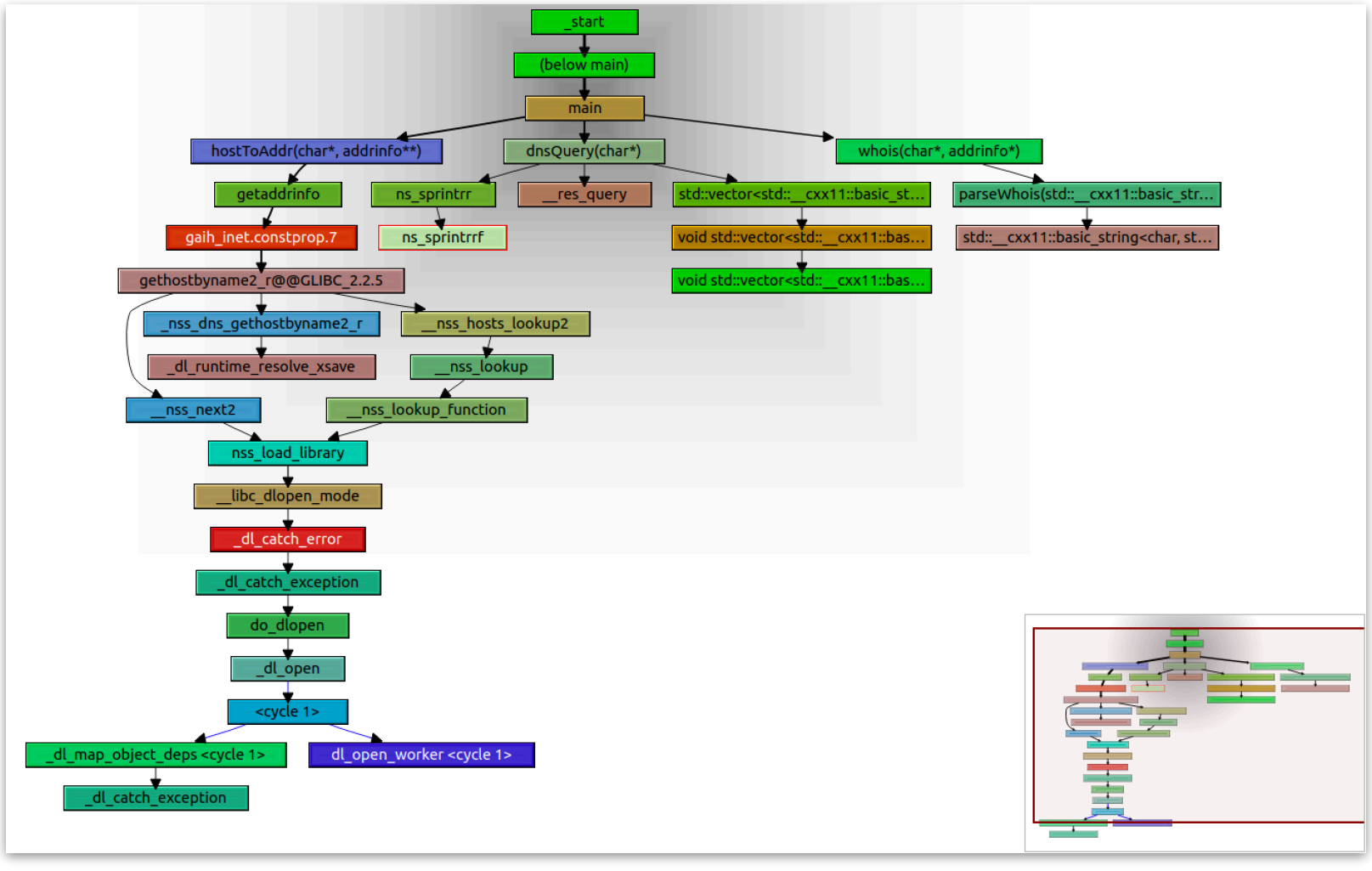
```
student@student-vm:/mnt/hgfs/isa$ ./isa-tazatel -q wired.com -w whois.arin.net
===DNS===
A:      151.101.130.194
A:      151.101.66.194
A:      151.101.2.194
A:      151.101.194.194
MX:     mx1.condenast.iphmx.com.
MX:     mx2.condenast.iphmx.com.
NS:     ns-1162.awsdns-17.org.
NS:     ns-1973.awsdns-54.co.uk.
NS:     ns-528.awsdns-02.net.
NS:     ns-276.awsdns-34.com.
=== WHOIS === 151.101.130.194
Address:        PO Box 78266
City:           San Francisco
Country:        US
NetName:        SKYCA-3
NetRange:       151.101.0.0 - 151.101.255.255
Organization:   Fastly (SKYCA-3)
PostalCode:     94107
StateProv:      CA
```

```
student@student-vm:/mnt/hgfs/isa$ ./isa-tazatel -w whois.lacnic.net -q brazil.gov.br
===DNS===
A:      170.246.255.25
NS:     alpha2.planalto.gov.br.
NS:     alpha.planalto.gov.br.
=== WHOIS === 170.246.255.25
inetnum:     170.246.252.0/22
aut-num:     AS266031
abuse-c:     MAR79
owner:       PRESID◆NCIA DA REP◆BLICA
responsible: Secretaria de Administra◆◆o
```

```
student@student-vm:/mnt/hgfs/isa$ ./isa-tazatel -q www.fit.vutbr.cz -w whois.ripe.net -d 8.8.8.8
===DNS===
A:     147.229.9.23
AAAA:  2001:67c:1220:809::93e5:917
MX:    tereza.fit.vutbr.cz.
PTR:   www.fit.vutbr.cz
SOA:   guta.fit.vutbr.cz.
SOA:   michal.fit.vutbr.cz.
NS:    gate.feec.vutbr.cz.
NS:    guta.fit.vutbr.cz.
NS:    kazi.fit.vutbr.cz.
NS:    rhino.cis.vutbr.cz.
=== WHOIS === 147.229.9.23
address:        601 90 Brno
address:        Antoninska 1
address:        Brno University of Technology
address:        The Czech Republic
admin-c:        CA6319-RIPE
country:        CZ
descr:          Brno University of Technology
descr:          VUTBR-NET1
inetnum:        147.229.0.0 - 147.229.254.255
netname:        VUTBRNET
phone:          +420 541145453
phone:          +420 723047787
```

PROFILING

Dále jsem v rámci testování aplikace vyzkoušel práci s některými profilery jako gprof, gpertools a callgrind. Grafický výstup posledního jmenovaného představující graf volaní procedur je znázorněn následujícím obrázkem. Výsledky pak ukazují, že program sice pracuje správně, ovšem na optimalizaci by se dalo ještě zapracovat.



LITERATURA

man whois
RFC 954: NICNAME/WHOIS
RFC 1580: Guide to Network Resource Tools
RFC 1834: Whois and Network Information Lookup Service, Whois++
RFC 3912: WHOIS protocol Specification
http://valgrind.org/docs/manual/cl-manual.html
https://www.thegeekstuff.com/2012/08/gprof-tutorial/
https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable