VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta informačních technologií

Projekt ISA: Programování síťové služby

Whois tazatel

Jméno: Petr Marek

Login: xmarek69

Datum: 21.10. 2019

Obsah

WHOIS protokol

WHOIS je transakčně orientovaný protokol založený na TCP, který funguje na principu pokládání dotazu a následné získání odpovědi z WHOIS serveru. Jeho smyslem je poskytovat informace o vlastnících domén v (lidmi) čitelné podobě (například adresu, telefon, název organizace apod).

Protokol specifikuje, že WHOIS server naslouchá na TCP portu 43 na požadavky od klientů. Klienti posílají na server požadavky v textové podobě zakončené ASCII znaky CR a LF (posunutí kurzoru na začátek řádku a posun o řádek). Server odpovídá opět v textové podobě (jak již bylo naznačeno), konec odpovědi signalizuje ukončením TCP spojení (a nikoli znaky CR a LF, protože odpověď má zpravidla více řádků). [1]

DNS protokol

DNS je hierarchický, decentralizovaný systém jmen pro počítače a ostatní zdroje, připojené do sítě internet, nebo do privátních sítí. Spojuje informace s doménovými jmény a překládá doménová jména na IP adresy. Tím jsou je jednou ze základních funkcí internetu. [2]

Na DNS serveru může být s danou doménou spojeno několik typů údajů (typů záznamů):

A záznam – Přiřazení (nasměrování) domény/subdomény k IP adrese verze 4.

AAAA záznam – Přiřazení (nasměrování) domény/subdomény k IP adrese verze 6.

MX – Přiřazení (nasměrování) mail serveru, kam se má doručovat pošta pro danou doménu.

CNAME – Přiřazení (nasměrování) (sub)domény na libovolnou jinou (sub)doménu (tedy „alias“ pro danou (sub)doménu).

NS – Přiřazení jména autoritativního DNS serveru k dané doméně.

PTR – Přiřazení IP adresy k doméně (jedná se o reverzní překlad). [3]

Základní informace o programu

Program WHOIS tazatel slouží jako WHOIS klient, zasílající dotazy na WHOIS server. Přijaté odpovědi program zpracuje a zobrazí uživateli v přehledné tabulce (v konzoli). Mimo to také zasílá dotazy na DNS server a získanou odpověď rovněž zpracuje a zobrazí přehledně uživateli.

Program pro svou činnost vyžaduje 2 argumenty – doménu/IP adresu, na kterou se WHOIS a DNS serverů ptáme a dále WHOIS server, kterého se program má zeptat. Dále je zde možné specifikovat několik dalších argumentů, viz Návod k použití.

Návrh aplikace a implementace

Aplikaci jsem se rozhodl implementovat v jazyku C. Celý program jsem rozdělil do dvou souborů – *whois.c* (obsahující implementaci) a *whois.h* (hlavičkový soubor pro zahrnutí ostatních knihoven do projektu a k definici konstant, struktur a prototypů funkcí).

Program nejprve ve funkci *check_args()* zkontroluje, zda byli programu při spuštění předány správné argumenty a uloží předané argumenty do struktury Argument. Dále pokud je předán argument -d (explicitní DNS server), a pokud se jedná o IPv4 adresu, tak se nastaví adresa DNS serveru pro knihovnu resolv.h (jinak se použije výchozí DNS server, nastavený v resolv.config). Dále funkcemi get_DNS_entries() a print_DNS_entries() získáme a vytiskneme DNS záznamy pro adresu, na kterou se uživatel ptá (a kterou specifikuje povinným argumentem -q). Dále pokud si uživatel přeje rozšířenou funkci programu (argumentem -e), tak program získá a vytiskne i záznamy pro upravenou adresu (po přidání/odebrání „www.“), případně pokud uživatel zadal IP adresu jako požadavek na který se ptá WHOIS serveru (argument -q), tak program získá a vytiskne ještě DNS záznamy pro hostname s a bez „www.“. Následně ve funkci get_whois() posíláme požadavek na WHOIS server, a zároveň v této funkci voláme funkci parse_WHOIS_response(), která tiskne získanou odpověď. Ve funkci get_whois() je jedna taková zvláštnost a sice ta, že pokud server vrátí odpověď „Your connection limit exceeded“, program se pokusí opakovaně posílat na WHOIS server požadavky, dokud neobdrží validní odpověď, nebo nedosáhne počtu limitu připojení (nastaveného na 20). Důvodem pro tuto implementaci je chování WHOIS serveru whois.nic.cz, který občas vrací tuto odpověď (i přesto, že se jedná třeba i o první připojení na server). Dále se funkce get_whois() volá, pokud si uživatel přál rozšířené funkce programu (argumentem -e). V tomto případě se funkce volá pro všechny IP adresy získané z DNS serveru a taky pro hostname s „www.“ i bez něj.

Návod k použití

Program se spouští v konzoli. Nejprve je potřeba jej pomocí přiloženého souboru Makefile zkompilovat tímto příkazem „make“:

Později se program spustí následujícím způsobem:

./isa-tazatel -q <IP | hostname> -w <IP|hostname> [-d <IP> -e -f]

Povinné argumenty:

-q = IP / hostname na který se ptáme

-w = IP / hostname tázaného WHOIS serveru

Nepovinné argumenty (v hranatých závorkách):

-d = IP / hostname tázaného DNS serveru – v případě že jej nespecifikujeme argumentem, tak se použije výchozí DNS server (daný resolverem v OS)

-f = Program vyfiltruje WHOIS odpověď a vypíše uživateli pouze jisté, předem dané položky (např. Adresu, telefonní číslo, přiřazený rozsah IP adres apod)

-e = Bezhodnotový argument, který rozšíří funkce programu. Například se WHOIS serveru nezeptá jen na adresu specifikovanou v argumentu -q, ale i na IP adresy získané z DNS serveru, příslušící k adrese v argumentu -q. Tento argument aktivuje všechna rozšíření popsaná v bonusové části zadání.

-s = Bezhodnotový argument, který aktivuje vypsání hlášek o všech pokusech o WHOIS dotazy, tedy i neúspěch v případě, že WHOIS server nemá pro danou adresu žádný záznam

Testování

V rámci testování jsem otestoval online WHOIS klienta https://www.nic.cz/whois/ . Ten vyhledává pouze pro WHOIS server nic.cz, nejedná se tedy o nějakého obecného klienta. V čem klient trochu zaostává je, že není sám schopný rozpoznat, zda hledaná adresa obsahuje počáteční „www.“ nebo ne. A rovněž program nevyhledává v IP adresách.

Dále jsem vyzkoušel online klienta https://www.iana.org/whois . Ten již zobrazoval informace z různých WHOIS serverů, ale nezobrazoval mnoho informací. Vesměs jen odkaz, který WHOIS server drží informace o dané adrese a některé dodatečné informace (ale záleží adresa od adresy).

Poslední program, který jsem testoval je program whois, který jsem nainstaloval na můj PC (s OS Ubuntu). Program poskytoval dost relevantních informací.

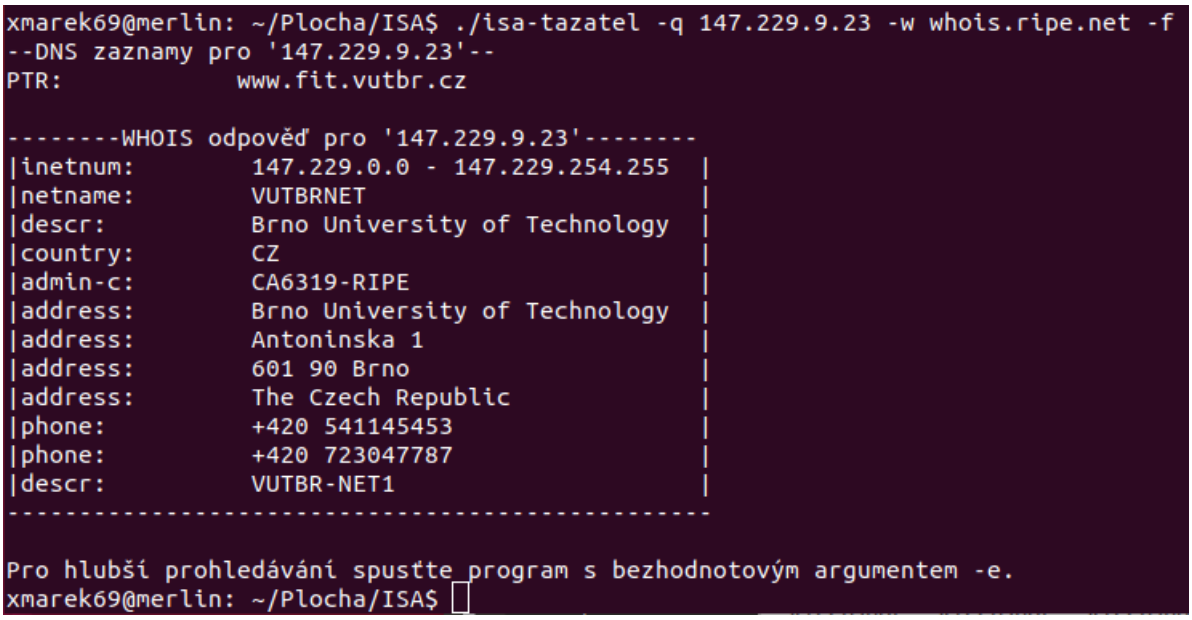
Při testování mého programu jsem vyzkoušel různé WHOIS servery a rovněž různé domény které jsem těmto serverům posílal jako požadavky, viz následující obrázky:

```
xmarek69@merlin: ~/Plocha/ISA$ ./isa-tazatel -q seznam.cz -w whois.nic.cz -f
--DNS zaznamy pro 'seznam.cz'--
A:              77.75.75.172
A:              77.75.75.176
AAAA:           2a02:598:4444:1::2
AAAA:           2a02:598:4444:1::1
MX:             mx2.seznam.cz
MX:             mx1.seznam.cz
SOA:            ans.seznam.cz
admin email:    hostmaster.seznam.cz
NS:             ams.seznam.cz
NS:             ans.seznam.cz

----WHOIS odpověď pro 'seznam.cz'----
|admin-c:       SEZNAM-CZ-AS-TECH    |
|name:          Seznam.cz, a.s.      |
|address:       Radlická 3294/10    |
|address:       Praha 5              |
|address:       15000                |
|address:       CZ                   |
|name:          Vlastimil Pečínka  |
|address:       Radlická 3294/10    |
|address:       Praha 5              |
|address:       150 00               |
|address:       CZ                   |
-------------------------------------

Pro hlubší prohledávání spustte program s bezhodnotovým argumentem -e.
xmarek69@merlin: ~/Plocha/ISA$
```

```
xmarek69@merlin: ~/Plocha/ISA$ ./isa-tazatel -q 199.43.0.43 -w whois.arin.net -f
--DNS zaznamy pro '199.43.0.43'--
Nenalezeny žádné DNS záznamy

-------WHOIS odpověď pro '199.43.0.43'-------
|NetRange:        199.43.0.0 - 199.43.0.255  |
|NetName:         ARIN-ASH                   |
|OrgName:         ARIN Operations            |
|Address:         PO Box 232290              |
|City:            Centreville                |
|StateProv:       VA                         |
|PostalCode:      20120                      |
|Country:         US                         |
|OrgTechName:    Rowley, Matt                |
|OrgAbuseName:    ARIN Operations Abuse      |
|OrgTechName:    Newton, Andy                |
|OrgTechName:    O'Neill, Michael J          |
-----------------------------------------

Pro hlubší prohledávání spustte program s bezhodnotovým argumentem -e.
xmarek69@merlin: ~/Plocha/ISA$
```

```
xmarek69@merlin: ~/Plocha/ISA$ ./isa-tazatel -q domain.com -w whois.domain.com -f
--DNS zaznamy pro 'domain.com'--
A:              18.221.195.49
MX:             mx.domain.com
SOA:            n
admin email:    2022.awsdn
NS:             20.com
NS:             60.co.uk
NS:             28.org
NS:             21.net

-------------------WHOIS odpověď pro 'domain.com'-------------------
|Domain Name: DOMAIN.COM                                            |
|Reseller: Domain Name Holding Company, Inc                         |
|Registrant Name: Domain Administrator                              |
|Registrant City: Burlington                                        |
|Registrant Country: US                                             |
|Admin Name: REDACTED FOR PRIVACY                                   |
|Admin City: REDACTED FOR PRIVACY                                   |
|Admin Country: REDACTED FOR PRIVACY                                |
|Tech Name: REDACTED FOR PRIVACY                                    |
|Tech City: REDACTED FOR PRIVACY                                    |
|Tech Country: REDACTED FOR PRIVACY                                 |
|Name Server: ns-166.awsdns-20.com                                  |
|Name Server: ns-683.awsdns-21.net                                  |
|Name Server: ns-1250.awsdns-28.org                                 |
|Name Server: ns-2022.awsdns-60.co.uk                               |
|    Domain Name Holding Company, Inc, corpdomains@endurance.com    |
|    DNS/Nameserver changes, and general domain support questions.  |
---------------------------------------------------------------------

Pro hlubší prohledávání spustte program s bezhodnotovým argumentem -e.
xmarek69@merlin: ~/Plocha/ISA$
```

```
xmarek69@merlin: ~/Plocha/ISA$ ./isa-tazatel -q microsoft.com -w whois.markmonitor.com
f
--DNS zaznamy pro 'microsoft.com'--
A:              40.76.4.15
A:              13.77.161.179
A:              40.113.200.201
A:              40.112.72.205
A:              104.215.148.63
MX:             com.mail.protection.outlook.com
SOA:            ns1.msft.net
admin email:    msnhst.microsoft.com
NS:             ns1.msft.net
NS:             ns3.msft.net
NS:             ns2.msft.net
NS:             ns4.msft.net

------------------------WHOIS odpověď pro 'microsoft.com'------------------------
|Domain Name: microsoft.com                                                     |
|Registrant Name: Domain Administrator                                          |
|Registrant City: Redmond                                                       |
|Registrant Country: US                                                         |
|Admin Name: Domain Administrator                                               |
|Admin City: Redmond                                                            |
|Admin Country: US                                                              |
|Tech Name: MSN Hostmaster                                                      |
|Tech City: Redmond                                                             |
|Tech Country: US                                                               |
|Name Server: ns4.msft.net                                                      |
|Name Server: ns3.msft.net                                                      |
|Name Server: ns1.msft.net                                                      |
|Name Server: ns2.msft.net                                                      |
|and specify the domain name in the subject line. We will review that request and   |
|name's registration record. While MarkMonitor believes the data to be accurate,  |
|data, or email to MarkMonitor (or its systems) or the domain name contacts (or     |
--------------------------------------------------------------------------------

Pro hlubší prohledávání spustte program s bezhodnotovým argumentem -e.
xmarek69@merlin: ~/Plocha/ISA$
```



Kromě těchto testů je rovněž v Makefile připravena řada testů, které se spouštějí tímto způsobem: make test[číslo]

Tedy např:
make test3

Popis jednotlivých testů:
test1 = Příklad použití domény, na kterou se tážeme WHOIS serveru

test2 = Příklad použití IPv4 adresy, na kterou se tážeme WHOIS serveru

test3 = Příklad použití IPv6 adresy, na kterou se tážeme WHOIS serveru

test4 = Příklad specifikování IPv4 adresy DNS serveru

test5 = Příklad použití IPv6 adresy DNS serveru

test6 = Příklad použití IPv4 adresy WHOIS serveru

test7 = Příklad použití IPv6 adresy WHOIS serveru

test8 = Příklad použití argumentu -e (rozšířené funkčnosti programu)

test9 = Příklad použití argumentu -s (výpis oznámeni o chybách)

Omezení

Projekt využívá knihovny resolv.c, která neumí pracovat s IPv6 adresami. Z toho důvodu program nefunguje pro IPv6 adresu, zadanou jako hodnotu argumentu programu -d.

Ostatní funkce programu by měli být plně funkční

Bonusová část zadání

V rámci projektu jsem se rozhodl implementovat některé nepovinné části zadání. Všechny zde zmíněná rozšíření se aktivují pouze v případě použití argumentu -e při spouštění programu. Bez tohoto argumentu funguje program velice jednoduše – pouze se DNS serveru dotáže na adresu, která byla specifikovaná argumentem -q a vypíše získané záznamy a

podobně se zeptá na tuto adresu WHOIS serveru (specifikovaného argumentem -w) a vypíše odpověď (ořezanou pouze o prázdné řádky a komentáře).

Prvním (a nejjednodušším) rozšířením (v případě použití argumentu -e) je dotazování se WHOIS serveru na doménu s odstraněním/přidáním řetězce "www." k požadavku v případě, že WHOIS server nenalezl žádný záznam a zároveň byla jako požadavek zadána doména. Podobně je i DNS server dotazován i na doménu s odstraněním/přidáním řetězce "www." v případě, že byla jako požadavek (-q) zadána doména.

Dalším rozšířením je dotazování se WHOIS serveru na všechny IP adresy (verze 4 i 6) příslušící k doméně, o které hledáme informace (specifikované v argumentu -q).

Dále jsem implementoval dotaz i na doménu (získanou z DNS) v případě, že jako požadavek na WHOIS server (argument -q) byla uživatelem zadána IP adresa.

V případě zadání IP adresy jako požadavku se rovněž nejprve DNS serveru zeptáme na PTR záznam pro získání domény a později se jej znovu dotazujeme na získanou doménu (pro získání ostatních DNS záznamů). Využívám zde tedy jisté rekurzivní dotazování.

Zdroje

[1] RFC 3912 (https://tools.ietf.org/html/rfc3912)

[2] https://www.extrahop.com/resources/protocols/dns/

[3] https://www.lukas-vlcek.cz/nezarazene/typy-dns-zaznamu/