ISA - Síťové aplikace a správa sítí
Whois tazatel

17. novembra 2019

Adrián Boros (xboros03)

Obsah

1 Úvod **2**

2 Dôležité pojmy **2**
2.1 DNS 2
2.2 WHOIS 3

3 Návrh a implementácia **3**
3.1 Spracovanie a kontrola argumentov 3
3.2 DNS 3
3.3 WHOIS 4
3.3.1 Získanie IP adresy WHOIS serveru 4
3.3.2 Tvorba WHOIS dotazu 4
3.3.3 WHOIS dotazovanie 4
3.3.4 Výpis získaných informácií 5
3.4 Rozšírenie 5

4 Spustenie programu **5**
4.1 Význam parametrov 5
4.2 Príklady spustenia 5

5 Testovanie **6**
5.1 Testovanie DNS časti 6
5.2 Testovanie WHOIS časti 8

6 Záver **10**

1 Úvod

Táto dokumentácia popisuje návrh a implementáciu projektu do predmetu *ISA–Sieťové aplikácie a správa sietí*. Úlohou bolo vytvoriť program (**Whois tazatel**) ktorý na vstupe špecifikuje IP adresu (IPv4 alebo IPv6) či hostname a k danému vstupu vypíše všetky známe podrobnosti o vlastníkovi.

Dokument je rozdelený na niekoľko logických celkov, od teoretickej časti popisujúcej princíp fungovania protokolu DNS (definoveného v RFC1035[1]) a WHOIS (definovaného v RFC3912[2]) až po samotnú implementáciu programu pracujúceho v súlade s protokolmi DNS a WHOIS.

Testovanie bolo vykonané na poskytnutom referenčnom virtuálnom stroji s operačným systémom Ubuntu 18.04 LTS, ktorý je vytvorený špeciálne pre sieťové predmety.

2 Dôležité pojmy

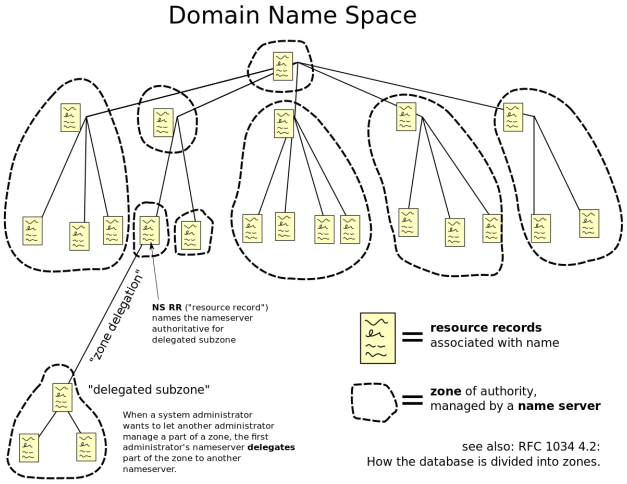
Pre návrh a implementáciu programu **isa-tazatel** je dôležité mať znalosti o tom, ako fungujú použité protokoly, t.j DNS a WHOIS. V tejto časti sa nachádzajú základné informácie o týchto protokoloch.

2.1 DNS

Podľa [3] je DNS (Domain Name System) hierarchický a decentralizovaný systém názvov pre počítače, služby alebo iné zdroje pripojené k internetu alebo súkromnej sieti. Prekladá názvy domén na adresy IP potrebné na lokalizáciu a identifikáciu počítačových služieb a zariadení. DNS deleguje zodpovednosť za prideľovanie doménových mien a mapovanie týchto názvov do internetových zdrojov určením autoritatívnych názvových serverov pre každú doménu.

Najbežnejšie typy záznamov uložených v databáze DNS sú pre začiatok autority (**SOA**), IP adresy (**A** a textbfAAAA), poštové výmenníky SMTP (**MX**), menové servery (**NS**), ukazovatele pre spätné vyhľadávanie DNS (**PTR**) a aliasy doménových mien (**CNAME**).

Domain name space pozostáva zo stromovej štruktúry údajov. Každý uzol alebo list v strome má štítok a nula alebo viac záznamov o prostriedku (**RR**), ktoré uchovávajú informácie spojené s názvom domény. Strom sa ďalej delí na zóny začínajúce v koreňovej zóne. Zóna DNS môže pozostávať iba z jednej domény alebo z mnohých domén a subdomén.

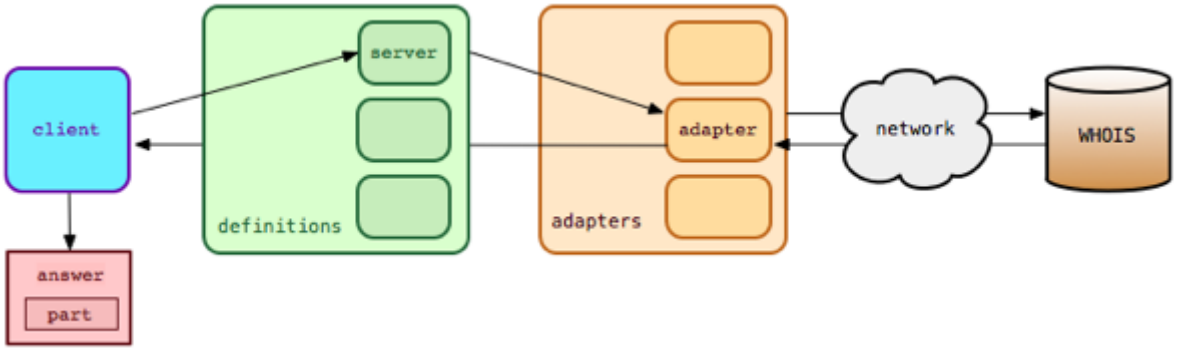


Obr. 1: Hierarchický systém názvov domén pre internet, usporiadaný do zón

2.2 WHOIS

WHOIS[4] je protokol dotaz / odpoveď, ktorý sa používa na prehľadávanie databáz, ktoré uchovávajú informácie o internetových zdrojoch, ako sú názvy domén. WHOIS bola vytvorená v 80. rokoch 20. storočia ako služba, ktorú používajú internetoví operátori na identifikáciu jednotlivcov alebo subjektov zodpovedných za prevádzku sieťového zdroja na internete. V súčasnosti protokol WHOIS používajú predovšetkým užívatelia aby získali informácie o názvoch domén a skontrolovali dostupnosť týchto domén.

RFC 3912[2] obsahuje podstatu špecifikácie protokolu WHOIS. Server WHOIS počúva na porte TCP 43 žiadosti klientov WHOIS. Klient pošle textovú požiadavku na server, potom server odpovie textovým obsahom. Všetky požiadavky sú ukončen0 `ASCII CR` a potom `ASCII LF`. Odpoveď môže obsahovať viac ako jeden riadok textu, takže prítomnosť `ASCII CR` alebo `ASCII LF` znakov neznamená koniec odpovede. Server ukončí svoje pripojenie ihneď po dokončení výstupu. Uzavreté pripojenie TCP je pre klienta znamením, že odpoveď bola prijatá.



Obr. 2: Štandardný pracovný postup pre dotaz WHOIS.

3 Návrh a implementácia

3.1 Spracovanie a kontrola argumentov

Prvým krokom po spustení programu je kontrola argumentov a ich následné zapísanie do globálnej štruktúry `Arguments`, ktorá nesie všetky potrebné informácie získané z povinných parametrov ako hostname a WHOIS server. Je možné zadať aj tretí, nepovinný argument, a tým je DNS server, ale iba vo forme IPv4 adresy. Kontrolu a zápis parametrov zabezpečuje funkcia `args_proc`. Kedže poradie argumentov môžu byť rôzne, na ich spracovanie bola použitá odporúčaná funkcia `getopt`.

3.2 DNS

Po získaní všetkých potrebných informácií nasleduje získanie DNS záznamov volaním funkcie `DNS_query`. Prvým krokom v tejto funkcii je nastavenie príslušného DNS serveru, a to buď na IP adresu ktorú zadal užívateľ, alebo na IP adresu resolvera získaného z operačného systému. Nasleduje nastavenie zdrojovej IP adresy a portu (53), časového intervalu opakovaného prenosu a počtu opakovania prenosu. Následne volaním `res_mkquery` sa vytvorí dotaz ktorý sa pomocom `res_send` pošle. Následne sa pomocou funkcie `ns_msg_count` získa počet odpovedí z `Answer Section` a `Name Server Section`. Takto získané odpovede sa rozparsujú podľa požadovaných typov a

následne sú vypísané na štandardný výstup. Ak sa nezískali žiadne údaje, vypisuje sa varovanie že informácie daného typu neboli nájdené.

Ak sa dotazuje na typ záznamu **A** alebo **PTR**, tak okrem výpisu informácií sa získané údaje ukladajú do globálnej štruktúry `IP_addresses` ktorá obsahuje IP adresy potrebné pre ďalšie dotazovanie, a to buď DNS alebo WHOIS serveru. Ak sa jedná o reverzný DNS lookup (záznam typu **PTR**), použije sa uložená IP adresa(záznam typu **A** alebo **AAAA**) ktorá sa zmodifikuje aby dotaz mal požadovaný tvar, t.j IP adresa sa reverzne a na koniec sa pripojí špeciálna doména `in-addr.arpa` v prípade IPv4 a `ip6.arpa` v prípade IPv6. V prípade IPv6 sa ešte pred otočením adresa expandne z komprimovanej formy a rozšíri sa na plnú 128-bitovú notáciu. Po získaní reverznej IPv6 adresy sa zavolá funkcia `modify_IPv6_rev_DNS` ktorá najprv vymaže dvojbodky medzi oktetmi a následne za každú číslovku umiestni bodku. Na účely získania DNS záznamov boli použité funkcie z knižnice `resolv.h`.

3.3 WHOIS

3.3.1 Získanie IP adresy WHOIS serveru

Ak bol zadaný hostname WHOIS serveru, zavolá sa funkcia `hostname_to_IP` ktorá z daného hostname-u získa IP adresu pomocou metódy `getaddrinfo`. Prvá nájdená IP adresa sa zapíše do premennej `whois_server` v štruktúre `Addresses`. V prípade že je zadaná IP adresa, táto metóda skontroluje správnosť formátu tejto adresy.

3.3.2 Tvorba WHOIS dotazu

V prvom kroku sa vo funkcii `whois_query` vytvoria štruktúry `sockaddr_in` a `sockaddr_in6` pre IPv4 resp. IPv6. Tieto štruktúry obsahujú cieľový port, IP adresu a IP protokol. Následne sa podľa typu IP adresy WHOIS serveru naplní príslušná štruktúra, t.j nastaví sa rodina adries uvedená v poli `sin_family`, nastaví sa IP adresa a port (43) WHOIS serveru a vytvorí sa socket pomocou metódy `socket` ktorá vracia deskriptor súboru ktorý sa môže použiť v neskorších volaniach funkcií pracujúcich so socketmi.

Následne volaním metódy `fcntl` s parametrom **F_GETFL** sa získajú status flagy pre vytvorený socket. Nastavením premennej **tv_sec** v štruktúre `timeval` na hodnotu 5 sa zaručí, že ak sa nepodarí pripojiť na daný WHOIS server do piatich sekúnd, tak sa vypíše chybové hlásenie a program končí.

Po nastavení všetkých potrebných údajov sa pomocou metódy `connect` pripojuje na WHOIS server. Ak sa pripojenie nepodarí, končí sa chybovým hlásením. Naopak, ak sa podarí pripojiť tak je vytvorený paket poslaný pomocou `send` s príslušným dotazom v tvare `query\r\n`.

Získanie odpovede prebieha pomocou `recv` v cykle, pretože odpoveď od WHOIS serveru sa zvyčajne nachádza vo viacerých packetoch. V jednej iterácii sa prijme maximálne 1024 bitov.

3.3.3 WHOIS dotazovanie

Celé dotazovanie prebieha niekoľkokrát z dôvodu, že niektoré WHOIS servery prijímajú query vo forme IP adresy a iné vo forme hostname-u a to buď s `www.` alebo bez. Najprv sa dotazuje pomocou IP adresy získanej z DNS záznamu typu **A**. Ak je dotaz neúspšný, dotazuje sa pomocou hostname-u ktorý zadal užívateľ buď ako parameter `-q` alebo sa tento hostname získal z DNS záznamu typu **PTR**. Ak je aj tento dotaz neúspešný, hostname sa upraví pomocou funkcie `whois_query_edit` ktorá pred hostname pridá `www.` alebo ho odstráni. V prípade neúspechu všetkých dotazov sa vypíše informácie že údaje o danom vstupe neboli nájdené.

3.3.4 Výpis získaných informácií

V prípade že sa získali informácii k zadanému vstupu, tak sa zavolá funkcia `print_whois_data` ktorá najprv danú odpoveď rozdelí po riadkoch a skontroluje prvý znak v riadku. Ak daný znak nie je **%, #,** **r** alebo **medzera** tak sa daný riadok skopíruje do poľa `dest`. Je to preto, aby sa dalo zistiť či sa získali nejaké vhodné informácie a nie informácie o tom že sa nič nenašlo a aj kvôli tomu aby sa odstránili zbytočné riadky z výpisu. Daná funkcia je vracia typ **bool**. Ak funkcia vracia **false**, tak sa vie že sa musí dotazovať na upravený hostname alebo na IP adresu pretože sa nenašli hľadané informácie. V opačnom prípade sa získané informácie vypíšu. Rozhodol som sa nefiltrovať získanú odpoveď, iba som výpis rozdelil do blokov (po každom desiatom riadku sa pridá prázdny riadok) pre lepšiu prehľadnosť.

3.4 Rozšírenie

Súčasťou projektu je aj rozšírenie a to v podobe že užívateľ má možnosť definovať špecifický DNS server ktorý sa má dotazovať. Tento DNS server má možnosť zadať len vo forme IPv4 adresy, nakoľko použitá knižnica `resolv.h` nepodporuje IPv6.

4 Spustenie programu

Pre vytvorenie spustiteľnej aplikácie je nutné projekt preložiť pomocou príkazu `make`. Použitím príkazu `make clean` sa naopak spustiteľný súbor zmaže.

Program sa spúšťa s dvomi povinnými a jedným nepovinným parametrom za ktorými musí nasledovať hodnota, inak bude program ukončený a na `stderr` sa vypíše chybové hlásenie.

Formát spustenia programu je nasledovný:

```
$./isa-tazatel -q <IP|host> -w <IP|host WHOIS serveru> [-d <IP>]
```

Argumenty umiestnené v zložených zátvorkach značia povinné argumenty a argument v hranatej zátvorke značí povinný argument. Zvislá čiara medzi argumentmi značí že je možné vybrať jeden z povolených argumentov. IP adresa môže byť zadaná ako IPv4 alebo IPv6, ale IP adresa DNS serveru môže byť zadaná iba vo forme IPv4. Program je možné spustiť aj s prepínačom `-h`, kedy program vypíše nápovedu a končí.

4.1 Význam parametrov

- `-q <IP|hostname>` : povinný argument ktorý udáva IP adresu alebo hostname domény, ktorého informácie sa majú získať
- `-w <IP|hostname WHOIS serveru>` : povinný argument udávajúci IP adresu alebo hostname WHOIS serveru ktorý sa má dotazovať
- `-d <IP>` : nepovinný argument značiaci IPv4 adresu DNS serveru ktorý sa má dotazovať

4.2 Príklady spustenia

```
$ ./isa-tazatel -w whois.ripe.net -q aktuality.sk
$ ./isa-tazatel -w 217.31.205.42 -q 77.75.75.176
$ ./isa-tazatel -w whois.ripe.net -q 2a00:1450:4014:801::200e
$ ./isa-tazatel -w 2001:67c:2e8:22::c100:687 -q 2a00:1450:4014:801::200e
```

5 Testovanie

Program bol testovaný priebežne počas celého vývoja projektu. Testovanie prebehlo na poskytnutom referenčnom virtuálnom stroji pre sieťové predmety. Na kontrolu odosielania požiadavkov či už na DNS server alebo na WHOIS server bol použitý program `Wireshark`. Na kontrolu vrátených údajov z DNS serveru som použil command line nástroje ako `nslookup` alebo `dig`. Na kontrolu údajov z WHOIS serveru bol použitý príkaz `whois` s príslušným doménovým menom, alebo online whois vyhľadávače ako `www.nic.cz/whois/` alebo `apps.db.ripe.net/db-web-ui/#/query`.

5.1 Testovanie DNS časti

```
student@student:~/Documents/ISA$ nslookup -type=any www.seznam.cz
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.seznam.cz   rdata_46 = AAAA 13 3 300 20191124173111 20191110160111 36313 seznam.cz. EZCvk29L3ZOHgohBOOh6xGWhGasja587cP0085BUtzNRaa207hWvPzsV aSe5IdC0ULWtxDaRtgBoXCVOdECPbA==
Name:   www.seznam.cz
Address: 2a02:598:4444:1::2
Name:   www.seznam.cz
Address: 2a02:598:3333:1::2
Name:   www.seznam.cz
Address: 2a02:598:3333:1::1
Name:   www.seznam.cz
Address: 2a02:598:4444:1::1
www.seznam.cz   rdata_46 = A 13 3 300 20191124173111 20191110160111 36313 seznam.cz. +6EKJFf2oMQMFAnkANhpOVsS1WuxIQyjaa/VSLXDweM/5oDaHstg/A0i gj9cykGFEgQ7uBQxvswg8Kjoq114kg==
Name:   www.seznam.cz
Address: 77.75.75.176
Name:   www.seznam.cz
Address: 77.75.74.176
Name:   www.seznam.cz
Address: 77.75.75.172
Name:   www.seznam.cz
Address: 77.75.74.172

Authoritative answers can be found from:
```

Obr. 3: Výsledok prevedenia príkazu `nslookup -type=any www.seznam.cz`

```
student@student:~/Documents/ISA$ ./isa-tazatel -w 2001:67c:2e8:22::c100:687 -q www.seznam.cz
=== DNS ===
A:              77.75.74.172
A:              77.75.74.176
A:              77.75.75.176
A:              77.75.75.172
AAAA:           2a02:598:4444:1::1
AAAA:           2a02:598:3333:1::1
AAAA:           2a02:598:4444:1::2
AAAA:           2a02:598:3333:1::2
MX:             No data found
CNAME:          No data found
NS:             No data found
SOA:            No data found
PTR:            www.seznam.cz.
```

Obr. 4: Výsledok časti DNS získaný programom **isa-tazatel**

```
student@student:~/Documents/ISA$ dig -x 147.229.2.90

; <<>> DiG 9.11.3-1ubuntu1.10-Ubuntu <<>> -x 147.229.2.90
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2484
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;90.2.229.147.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
90.2.229.147.in-addr.arpa. 3584 IN      PTR     piranha.ro.vutbr.cz.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Nov 10 18:38:17 CET 2019
;; MSG SIZE  rcvd: 87
```

Obr. 5: Príklad reverzného dotazu pomocou nástroja `dig`

```
student@student:~/Documents/ISA$ ./isa-tazatel -w whois.ripe.net -q 147.229.2.90
=== DNS ===
PTR:            piranha.ro.vutbr.cz.
A:              147.229.2.90
AAAA:           No data found
MX:             No data found
CNAME:          No data found
NS:             No data found
SOA:            No data found
```

Obr. 6: Reverzný dotaz pomocou **isa-tazatel**

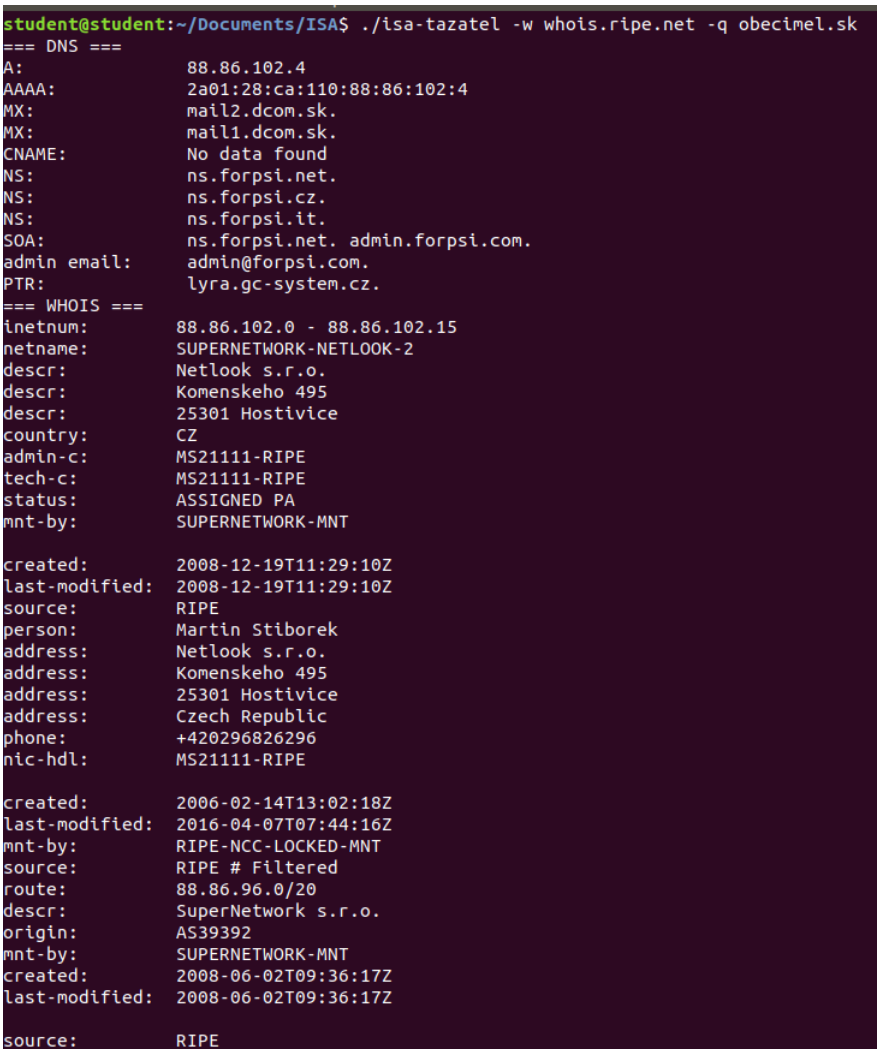
```
student@student:~/Documents/ISA$ ./isa-tazatel -w whois.nic.cz -q lidovky.cz -d 8.8.4.4
=== DNS ===
A:              185.17.117.33
AAAA:           No data found
MX:             smtp1.mafra.cz.
MX:             smtp2.mafra.cz.
MX:             smtp3.mafra.cz.
MX:             smtp4.mafra.cz.
CNAME:          No data found
NS:             ns.mafra.cz.
NS:             ns2.mafra.cz.
NS:             ns.mafracz.net.
SOA:            ns.mafra.cz. hostmaster.mafra.cz.
admin email:    hostmaster@mafra.cz.
PTR:            No data found
=== WHOIS ===
```

Obr. 7: Ukážka výpisu DNS informácií so špecifikovaním DNS serveru

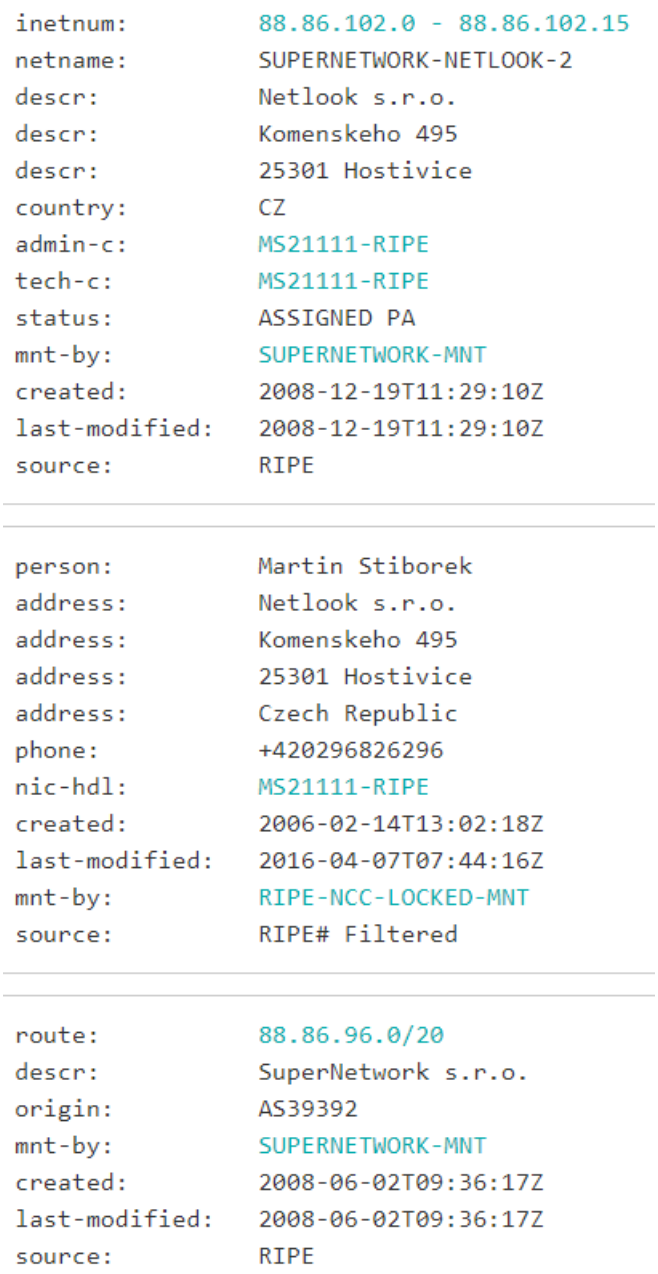
5.2 Testovanie WHOIS časti

```
inetnum:        88.86.102.0 - 88.86.102.15
netname:        SUPERNETWORK-NETLOOK-2
descr:          Netlook s.r.o.
descr:          Komenskeho 495
descr:          25301 Hostivice
country:        CZ
admin-c:        MS21111-RIPE
tech-c:         MS21111-RIPE
status:         ASSIGNED PA
mnt-by:         SUPERNETWORK-MNT
created:        2008-12-19T11:29:10Z
last-modified:  2008-12-19T11:29:10Z
source:         RIPE

person:         Martin Stiborek
address:        Netlook s.r.o.
address:        Komenskeho 495
address:        25301 Hostivice
address:        Czech Republic
phone:          +420296826296
nic-hdl:        MS21111-RIPE
created:        2006-02-14T13:02:18Z
last-modified:  2016-04-07T07:44:16Z
mnt-by:         RIPE-NCC-LOCKED-MNT
source:         RIPE # Filtered

% Information related to '88.86.96.0/20AS39392'

route:          88.86.96.0/20
descr:          SuperNetwork s.r.o.
origin:         AS39392
mnt-by:         SUPERNETWORK-MNT
created:        2008-06-02T09:36:17Z
last-modified:  2008-06-02T09:36:17Z
source:         RIPE
```

Obr. 8: Výsledok príkazu `whois 88.86.102.4`



Obr. 9: Výsledok získaný pomocou **isa-tazatel** po prevedení príkazu `$ ./isa-tazatel -w whois.ripe.net -q obecimel.sk`. Vidíme aj úplný výpis získaných údajov spolu s DNS časťou.



Obr. 10: Výsledok získaný príkazom `88.86.102.4` z online whois vyhľadávača `apps.db.ripe.net/db-web-ui/#/query`

6 Záver

Cieľom projektu bolo vytvorenie programu na komunikáciu a získavanie údajov z DNS a WHOIS serverov podľa RFC 1035[1] a RFC 3912[2]. Program využíva sockety na komunikáciu z WHOIS serverom.

V tejto dokumentácii boli opísané základy fungovania protokolov DNS a WHOIS a takisto aj praktická časť popisujúca riešenie projektu spolu s výsledným testovaním a implementovaným rozšírením.

Literatúra

[1] P. Mockapetris. *Domain names - implementation and specification*. 1987, [Online].
URL https://tools.ietf.org/rfc/rfc1035.txt

[2] L. Daigle. *WHOIS Protocol Specification*. 2004, [Online].
URL https://tools.ietf.org/html/rfc3912

[3] Wikipedia. *Domain Name System*. 2019, [Online].
URL https://en.wikipedia.org/wiki/Domain_Name_System

[4] Simone Carletti. *Understanding the WHOIS protocol*. 2012, [Online].
URL https://simonecarletti.com/blog/2012/03/whois-protocol/