FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

ISA - Síťové aplikace a správa sítí

Manuál k projektu Programování síťové služby Whois tazatel

2019 Juraj Holub (xholub40)

Obsah

1 Úvod

Doménové meno je jednoznačný identifikátor objektu (počítač, sieť a podobne) v Internete. Doménové meno môže poskytovať množstvo informácií o tomto objekte ako sú informácie o vlastníkovy, geografické informácie a podobne. Tieto informácie sa dajú získavať pomocou rôznych internetových protokolov. Tento manuál popisuje aplikáciu, ktorá získava takéto informácií pomocou internetových protokolov Domain Name System (DNS), Whois a taktiež pomocou geolokačnej databázy.

1.1 DNS protokol

Ako popisuje RFC 1034 [4], štruktúra unikátneho pomenovania domén na internete sa v pribehu času vyvýjala na základe rôznych požiadaviek. Meno hostiteľa (anglicky hostname) spravoval systém Network Information Center (NIC). Systém nedostačoval vzhľadom na rapidný nárast počtu uživateľov. Aplikácie na internete boli stále sofistikovanejšie a potrebovali obecnejší systém. Výsledokom bol vznik Domain Name System (DNS). DNS je hierarchický a decentrlizovaný systém, ktorý spája meno hostiteľa s rôznymi informáciami, pričom najpodstatnejšou informáciou je Internet Protocol adresa (IP). DNS server poskytuje databázu do ktorej sa dá dotazovať a server poskytuje odpovede. Komunikáciu s DNS serverom definuje DNS protokol.

1.2 Whois protokol

Pre viac podrobné informácie o doméne (detaily o vlastníkovy domény) existuje internetový protokol Whois [2]. Systém umožnuje podobný dotaz/odpoveď servis.

1.3 Geolokačné databázy

Ďalšou možnosťou získania ešte podrobnejších informácií spojených s geografickou polohou objektu reprezentovaného pod doménovým menom je možnosť využitia geolokačných databáz. Tieto databázy spravujú rôzne spoločnosti, ktoré vlastnia veľké množstvo geolokačných informácií. Spôsob ako datá získavajú nie je predmetom tejto práce.

2 Architektúra a implementácia aplikácie

Program je implementovaný v C++ a používa funkcionalitu štandardnej knihovny. Ďalej pre vytváranie TCP socketov používa knihovnu BSD sockets a pre komunikáciu s DNS serverom používa knihovnu `<resolv.h>`. Architektúra aplikácie je rozdelená na niekoľko samostatných celkov (tried), ktoré sú popísané v tejto kapitole.

2.1 Argument Parser

Spracováva argumenty s príkazovej riadky. Unifikuje vstupné doménové mená, IPv4 a IPv6 adresy na IPv4 adresy aby ostatné komponenty programu mohli pracovať s jednotnou reprezentáciou.

2.2 TCP socket

Umožnuje vytvárať TCP komunikáciu. TCP komunikáciu aplikácia využíva pri komunikácii s DNS serverom a taktiež pri komunikácii s geolokačnou databázou. Komponenta využíva pre TCP komunikáciu štandardné funkcie knihovny BSD sockets.

2.3 DNS query

Vytvára dotazy na DNS databázu. Pre vytváranie a prijímanie dotazov a odpovedí sa využíva funkcionalita z knihovny `resolv.h`. Aplikácia sa dotazuje na informácie, ktoré šadnardne obsahuje DNS protokol (A, AAAA, MX, CNAME, NS, SOA, TXT a PTR). Význam jednotlivých položiek v protokole je popísaný v RFC 1045 [5]. Komunikácia prebieha tak, že sa postupne aplikácia dotazuje na jednotlivé políčka a vyhodnocuje prijaté odpovede. Získané datá sa zobrazia uživateľovi.

2.4 Whois query

Vytvára dotazy na whois databázu a prijíma odpovede. Server na ktorý sú dotazy zasielané špecifikuje uživateľ. Dotaz zasiela ako TCP paket na server špecifikovaný uživateľom na port 43, na tomto porte beží služba hostiteľa Stanford Research Institute's Network Information Center (SRI NIC [3]). Whois server zašle odpoveď pomocou TCP komunikácie a táto komponenta ho zanalyzuje. Na rozdiel od DNS dotazovania, tu sa zašle jediný dotaz, ktorý obsahuje IP adresu analyzovanej domény a whois server zašle späť všetky jeho dostupné datá. Komponenda následne datá zanalyzuje, vyhodnotí a zobrazí ich uživateľovi.

2.5 Geolocation database

Umožnuje získavanie informácií z geolokačnej databázy ip-api.com. Ide o voľne dostupnú, neplatenú geolokačnú databázu, ktorú je momžné voľne využívať pre nekomerčné účely (viac viď. podmienky používania [1]). Databáza je dostupná online a umožnuje komunikáciu pomocou HTTP protokolu. Trieda vytvorí TCP paket s HTTP hlavičkou, ktorej url obsahuje dotazovanú IP adresu vo formáte definovanom aplikačným rozhraním tejto databázy. V HTTP hlavičke sa defunuje taktiež formát v akom chceme prijať datá. Databáza následne zašle späť datá v požadovanom formáte (json, csv, xml). Trieda následne prijaté datá zanalyzuje a zobrazí uživateľovi.

3 Návod na použitie

Program je nativne vyvýjaný pre OS GNU/Linux (na Windows netestované). Preložiť program je možné priloženým `Makefile`. Program sa používa následovne: `isa-tazatel <arguments>`, pričom argumenty sú rozdelené na povinné a nepovinné.

Povinné argumenty:

- `-q <IP|hostname>` - IP adresa alebo názov hostiteľa, ktorý bude analyzovaný.
- `-w <IP|hostname>` - IP adresa alebo názov hostiteľa Whois serveru, na ktorý budú zasielané dotazy.

Nepovinné argumenty:

- `-d <IP>` IP adresa DNS serveru na ktorý budú zasielané dotazy. Ak nie je argument zadaný tak sa bude implicitne používať DNS resolver v operačnom systéme.
- `-h` - Zobrazí nápovedu na používanie programu.

4 Testovanie

Pre testovanie boli ako referenčný nástroj použité open source utility **nslookup** , **host**, **dig** a **whois**. Pre overenie správnosti zasielaných paketov sa využil analyzátor sieťových protokolov **wireshark** .

Pre získanie referenčných dát z DNS serveru pre testovanú doménu sa využil nástroj `dig`, pomocou ktorej sa postupne dotazovalo na A, AAAA, MX, CNAME, NS, SOA a PTR. Výsledky dotazov sú zprehľadnené v sekcii s prílohami zvlášť pre každú testovanú doménu vo forme prehľadovej tabuľky. Pre referenčné Whois datá sa použila utilita `whois` s atribútom IPv4 adresy analyzovanej domény. IP adresa bola získaná predchádzajúcim dotazom utilitou `dig`. Datá získané z referenčných nástrojov pre testované domény a datá získané aplikáciu `isa-tazatel` pre rovnaké domény sú priložené v prílohách. V rámci testovania sa experimentovalo s piatimi doménami. Testované domény a výsledky testov:

- **www.youtube.com**: Výsledok DNS dotazov sa zhodoval. Výsledky whois dotazov sa nezhodovali lebo doména je spravovaná whois serverom `whois.arin.net` a mi sme zasielali dotaz na server `whois.ripe.net`. Výstup experimentu je v prílohe A.1.
- **www.netflix.com** Výsledok experimentu je veľmi podobný predchádzajúcemu. Výstup je v prílohe A.2.
- **www.fit.vutbr.cz** Výsledok DNS aj Whois zhodný ale keďže aplikácia neodchytáva všetky whois datá tak boli niektoré informácie oproti referenčnému nástroju zahodené. Výsledky experimentu sú v prílohe A.3.

- **www.seznam.cz** Výsledok experimentu je veľmi podobný predchádzajúcemu. Výstup je v prílohe A.4
- **vutbr.cz** DNS server oproti predchádzajúcim experimentom poskytol viacej informácií ako len IP adresy. Inak je výsledok experimentu podobný predchádzajúcim. Výstup je v prílohe A.5

Datá získané touto aplikáciu sa zhodovali s datami získanými z referenčných nástrojov (okrem whois dotazov u ktorých referenčný nástroj využil iný whois server). Avšak referenčné nástroje dokázali získať niektoré datá navyše, ktoré táto aplikácia nezískala. Informácie získané geolokačným serverom som neporovnával voči žiadnemu referenčnéu nástroju avšak zbežný pohľad do výstupov (napr. geografická adresa poskytnutá whois a geolokačným serverom) ukazuje na to, že informácie poskytované geolokačným serverom by mohli byť dôveryhodné.

5 Záver

Tento manuál popisuje aplikáciu na získavanie informácií o vlastníkoch internetových domén. Aplikácie vznikla ako školský projekt. V rámci vývoja som využíval rôzne open source utility, ktoré už túto funkcionalitu poskytujú. Priestor pre ďalšie rozšírenia vidím v implementácii získavania ďalších whois informácií, ktoré táto aplikácia oproti referenčným nástrojom neposkytuje. Ďalším možným rozšírením je dynamická voľba whois serveru. Aktuálne získané informácie získané z whois komunikácie sú závislé na servery, ktorý špecifikuje uživateľ. V rámci aplikácie som si vyskúšal implementáciu dotazov na DNS a Whois servery. Ako bonusové rozšírenie som naimplementoval získavanie dát z online geolokačnej databázy pomocou HTTP komunikácie.

Reference

[1] IP-API Terms and Policies. [online], 2019 [vid. 2019-08-10].
URL https://ip-api.com/docs/legal

[2] Daigle, L. WHOIS Protocol Specification. RFC 3912, RFC Editor, September 2004.

[3] Harrenstien, K.; Stahl, M.; Feinler, E. NICNAME/WHOIS. RFC 954, RFC Editor, October 1985.

[4] Mockapetris, P. Domain names - concepts and facilities. STD 13, RFC Editor, November 1987, http://www.rfc-editor.org/rfc/rfc1034.txt.
URL http://www.rfc-editor.org/rfc/rfc1034.txt

[5] Mockapetris, P. Domain names - implementation and specification. STD 13, RFC Editor, November 1987, http://www.rfc-editor.org/rfc/rfc1035.txt.
URL http://www.rfc-editor.org/rfc/rfc1035.txt

A Výsledky experimentovania s aplikáciou.

A.1 Experiment 1

```
user@pc:~$ ./isa-tazatel -q www.youtube.com -w whois.ripe.net
================================--------DNS-------================================
AAAA:           2a00:1450:4014:801::200e
A:              172.217.23.238
A:              172.217.23.206
CNAME:          youtube-ui.l.google.com

================================--------WHOIS-------================================
inetnum:        172.103.96.0 - 172.240.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
country:        EU \# Country is really world wide
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
admin-c:        IANA1-RIPE

==============================-GEOLOCATION SERVER-==============================
continent       Europe
continentCode   EU
country         Czechia
countryCode     CZ
region          10
regionName      Hlavni mesto Praha
city            Prague
timezone        Europe/Prague
currency        CZK
isp             Google LLC
org             Google LLC
as              AS15169 Google LLC
asname          Google
reverse         prg03s06-in-f238.1e100.net
query           172.217.23.238
```

Listing 1: Výsledok dotazu nad doménov **www.youtube.com**.

Záznam	Výsledok dotazu
A	172.217.23.238 172.217.23.206
AAAA	2a00:1450:4014:80c::200e
CNAME	youtube-ui.l.google.com.
SOA	-
NS	-
PTR	-
MX	-

Tabulka 1: Referenčné DNS dotazy nad doménov **www.youtube.com**.

```
user@pc:~$ whois 172.217.23.238 #ip address from dig www.youtube.com A
...
NetRange:       172.217.0.0 - 172.217.255.255
CIDR:           172.217.0.0/16
NetName:        GOOGLE
NetHandle:      NET-172-217-0-0-1
```

```
Parent:          NET172 (NET-172-0-0-0-0)
NetType:         Direct Allocation
OriginAS:        AS15169
Organization:    Google LLC (GOGL)
RegDate:         2012-04-16
Updated:         2012-04-16
Ref:             https://rdap.arin.net/registry/ip/172.217.0.0
OrgName:         Google LLC
OrgId:           GOGL
Address:         1600 Amphitheatre Parkway
City:            Mountain View
StateProv:       CA
PostalCode:      94043
Country:         US
RegDate:         2000-03-30
Updated:         2019-10-31
Comment:         Please note that the recommended way to file abuse complaints are located in
Comment:
Comment:         To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:         For legal requests: http://support.google.com/legal
Comment:
Comment:         Regards,
Comment:         The Google Team
Ref:             https://rdap.arin.net/registry/entity/GOGL
OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN
OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
```

Listing 2: Referenčný Whois dotaz nad doménov **www.youtube.com**.

A.2 Experiment 2

Listing 3: Výsledok dotazu nad doménov **www.netflix.com**.

```
user@pc:~$ ./isa-tazatel -q www.netflix.com -w whois.ripe.net
=================================-------DNS-----------------------------------
AAAA:            2a01:578:3::341e:6717
AAAA:            2a01:578:3::22fc:b3a2
AAAA:            2a01:578:3::3411:db4d
AAAA:            2a01:578:3::364d:8fc4
AAAA:            2a01:578:3::3411:e3ae
AAAA:            2a01:578:3::3412:f09
AAAA:            2a01:578:3::36ab:bb3c
AAAA:            2a01:578:3::34d1:4fba
A:               52.210.7.69
A:               52.31.145.183
A:               54.171.116.69
A:               52.209.235.141
A:               52.30.45.198
A:               54.72.216.241
A:               54.77.108.2
```

```
A:              52.31.182.100
CNAME:          www.geo.netflix.com
TXT:            "v=spf1 -all"

==================================-------WHOIS-------=====================================
inetnum:        52.144.96.0 - 52.255.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
country:        EU # Country is really world wide
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
admin-c:        IANA1-RIPE

==============================-GEOLOCATION SERVER-==============================
continent       Europe
continentCode   EU
country         Ireland
countryCode     IE
region          L
regionName      Leinster
city            Dublin
zip             D02
timezone        Europe/Dublin
currency        EUR
isp             Amazon Technologies Inc.
org             AWS EC2 (eu-west-1)
as              AS16509 Amazon.com, Inc.
asname          Amazon
reverse         ec2-52-210-7-69.eu-west-1.compute.amazonaws.com
query           52.210.7.69
```

Záznam	Výsledok dotazu
A	2a01:578:3::341e:6717 2a01:578:3::22fc:b3a2 2a01:578:3::3411:db4d 2a01:578:3::364d:8fc4 2a01:578:3::3411:e3ae 2a01:578:3::3412:f09 2a01:578:3::36ab:bb3c 2a01:578:3::34d1:4fba
AAAA	52.210.7.69 52.31.145.183 54.171.116.69 52.209.235.141 52.30.45.198 54.72.216.241 54.77.108.2 52.31.182.100
CNAME	www.geo.netflix.com.
SOA	-
NS	-
PTR	-
MX	-

Tabulka 2: Referenčné DNS dotazy nad doménov **www.netflix.com**.

```
user@pc:~$ whois 52.210.7.69 #ip address from dig www.netflix.com A
...
NetRange:       52.208.0.0 - 52.215.255.255
CIDR:           52.208.0.0/13
NetName:        AMAZON-DUB
NetHandle:      NET-52-208-0-0-1
Parent:         AT-88-Z (NET-52-192-0-0-1)
NetType:        Reallocated
OriginAS:       AS16509
Organization:   Amazon Data Services Ireland Limited (ADSIL-1)
RegDate:        2015-12-14
Updated:        2015-12-14
Ref:            https://rdap.arin.net/registry/ip/52.208.0.0


OrgName:        Amazon Data Services Ireland Limited
OrgId:          ADSIL-1
Address:        Unit 4033, Citywest Avenue Citywest Business Park
City:           Dublin
StateProv:      D24
PostalCode:
Country:        IE
RegDate:        2014-07-18
Updated:        2014-07-18
Ref:            https://rdap.arin.net/registry/entity/ADSIL-1


OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-266-4064
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-266-4064
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-266-4064
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEA8-ARIN
```

Listing 4: Referenčný Whois dotaz nad doménov **www.netflix.com**.

A.3 Experiment 3

```
user@pc:~$ ./isa-tazatel -q www.fit.vutbr.cz -w whois.ripe.net
================================------DNS-------================================
AAAA:           2001:67c:1220:809::93e5:917
A:              147.229.9.23
MX:             0 tereza.fit.vutbr.cz

==============================-------WHOIS------==============================
inetnum:        147.229.0.0 - 147.229.254.255
netname:        VUTBRNET
```

```
descr:          Brno University of Technology
descr:          VUTBR-NET1
country:        CZ
address:        Brno University of Technology
address:        Antoninska 1
address:        601 90 Brno
address:        The Czech Republic
phone:          +420 541145453
phone:          +420 723047787
admin-c:        CA6319-RIPE

==============================-GEOLOCATION SERVER-==============================
continent       Europe
continentCode   EU
country         Czechia
countryCode     CZ
region          64
regionName      South Moravian
city            Brno
zip             614 00
timezone        Europe/Prague
currency        CZK
isp             VUTBR
org             Brno University of Technology
as              AS197451 Brno University of Technology
asname          VUTBR-AS
reverse         www.fit.vutbr.cz
query           147.229.9.23
```

Listing 5: Výsledok dotazu nad doménov **www.fit.vutbr.cz**.

Záznam	Výsledok dotazu
A	147.229.9.23
AAAA	2001:67c:1220:809::93e5:917
CNAME	-
SOA	-
NS	-
PTR	-
MX	tereza.fit.vutbr.cz

Tabulka 3: Referenčné DNS dotazy nad doménov **www.fit.vutbr.cz**.

```
user@pc:~$ whois 147.229.9.23 #ip address from dig www.fit.vutbr.cz A
...
NetRange:       147.228.0.0 - 147.237.255.255
CIDR:           147.236.0.0/15, 147.232.0.0/14, 147.228.0.0/14
NetName:        RIPE-ERX-147-228-0-0
NetHandle:      NET-147-228-0-0-1
Parent:         NET147 (NET-147-0-0-0-0)
NetType:        Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2003-10-08
Updated:        2003-10-08
Comment:        These addresses have been further assigned to users in
Comment:        the RIPE NCC region.  Contact information can be found in
Comment:        the RIPE database at http://www.ripe.net/whois
Ref:            https://rdap.arin.net/registry/ip/147.228.0.0
```

```
ResourceLink:  https://apps.db.ripe.net/search/query.html
ResourceLink:  whois.ripe.net
OrgName:        RIPE Network Coordination Centre
OrgId:          RIPE
Address:        P.O. Box 10096
City:           Amsterdam
StateProv:
PostalCode:     1001EB
Country:        NL
RegDate:
Updated:        2013-07-29
Ref:            https://rdap.arin.net/registry/entity/RIPE
ReferralServer:  whois://whois.ripe.net
ResourceLink:  https://apps.db.ripe.net/search/query.html
OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName:   Abuse Contact
OrgAbusePhone:  +31205354444
OrgAbuseEmail:  abuse@ripe.net
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE3850-ARIN
OrgTechHandle: RNO29-ARIN
OrgTechName:   RIPE NCC Operations
OrgTechPhone:  +31 20 535 4444
OrgTechEmail:  hostmaster@ripe.net
OrgTechRef:    https://rdap.arin.net/registry/entity/RNO29-ARIN
```

Listing 6: Referenčný Whois dotaz nad doménov **www.fit.vutbr.cz**.

A.4 Experiment 4

```
user@pc:~$ ./isa-tazatel -q www.seznam.cz -w whois.ripe.net
================================--------DNS-------================================
AAAA:           2a02:598:4444:1::1
AAAA:           2a02:598:3333:1::1
AAAA:           2a02:598:4444:1::2
AAAA:           2a02:598:3333:1::2
A:              77.75.75.172
A:              77.75.74.172
A:              77.75.75.176
A:              77.75.74.176

==============================--------WHOIS-------==============================
inetnum:        77.75.74.0 - 77.75.74.255
netname:        SEZNAM-CZ
descr:          Seznam.cz
descr:          SEZNAM - II
country:        CZ
address:        Radlicka 3294/10 150 00 Prague 5 Czech Republic
phone:          +420 602 126 570
admin-c:        SZN5-RIPE
admin-c:        PZ172-RIPE

============================-GEOLOCATION SERVER-============================
continent       Europe
continentCode   EU
country         Czechia
countryCode     CZ
region          10
regionName      Hlavni mesto Praha
```

```
city            Prague
zip             150 00
timezone        Europe/Prague
currency        CZK
isp             Seznam - II
as              AS43037 Seznam.cz, a.s.
asname          SEZNAM-CZ
reverse         www.seznam.cz
query           77.75.74.176
```

Listing 7: Výsledok dotazu nad doménov **www.seznam.cz**.

Záznam	Výsledok dotazu
A	2a02:598:4444:1::1 2a02:598:3333:1::1 2a02:598:4444:1::2 2a02:598:3333:1::2
AAAA	77.75.75.172 77.75.74.172 77.75.75.176 77.75.74.176
CNAME	-
SOA	-
NS	-
PTR	-
MX	-

Tabulka 4: Referenčné DNS dotazy nad doménov **www.seznam.cz**.

```
user@pc:~$ whois 147.229.9.23 #ip address from dig www.seznam.cz A
...
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 # Filtered
```

Listing 8: Referenčný Whois dotaz nad doménov **www.seznam.cz**.

A.5 Experiment 5

```
user@pc:~$ ./isa-tazatel -q vutbr.cz -w whois.ripe.net
================================--------DNS-----------------------------------
SOA:            origin rhino.cis.vutbr.cz
SOA:                    email hostmaster.vutbr.cz
SOA:                    serial 2019110200
SOA:                    refresh 28800
SOA:                    retry 7200
SOA:                    expire 1814400
SOA:                    minimum 1814400
A:              147.229.2.90
NS:             rhino.cis.vutbr.cz
NS:             pipit.cis.vutbr.cz
MX:             5 mx.vutbr.cz
TXT:            "v=spf1 ip4:147.229.0.0/16 ip6:2001:67c:1220::/48 include:spf.protection.outl
TXT:            "google-site-verification=kSdrjCE0ee5GKpv_Xtr-18k9Pm1OzRIVXrkm9kIwEAk"
TXT:            "MS=ms21627876"

================================--------WHOIS-----------------------------------
inetnum:        147.229.0.0 - 147.229.254.255
netname:        VUTBRNET
descr:          Brno University of Technology
descr:          VUTBR-NET1
country:        CZ
address:        Brno University of Technology
address:        Antoninska 1
address:        601 90 Brno
address:        The Czech Republic
phone:          +420 541145453
phone:          +420 723047787
admin-c:        CA6319-RIPE

==============================-GEOLOCATION SERVER-==============================
continent       Europe
continentCode   EU
country         Czechia
countryCode     CZ
region          64
regionName      South Moravian
city            Brno
zip             614 00
timezone        Europe/Prague
currency        CZK
isp             VUTBR
org             Brno University of Technology
as              AS197451 Brno University of Technology
asname          VUTBR-AS
reverse         piranha.ro.vutbr.cz
query           147.229.2.90
```

Listing 9: Výsledok dotazu nad doménov **vutbr.cz**.

```
user@pc:~$ whois 147.229.2.90 #ip address from dig vutbr.cz A
...
inetnum:        147.229.0.0 - 147.229.254.255
netname:        VUTBRNET
descr:          Brno University of Technology
country:        CZ
admin-c:        CA6319-RIPE
```

Záznam	Výsledok dotazu
A	147.229.2.90
AAAA	-
CNAME	-
SOA	rhino.cis.vutbr.cz. hostmaster.vutbr.cz. 2019110200 ; serial 28800 ; refresh (8 hours) 7200 ; retry (2 hours) 1814400 ; expire (3 weeks) 300 ; minimum (5 minutes)
NS	pipit.cis.vutbr.cz. rhino.cis.vutbr.cz.
PTR	-
MX	5 mx.vutbr.cz.

Tabulka 5: Referenčné DNS dotazy nad doménov **vutbr.cz**.

```
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 # Filtered
abuse-mailbox:   abuse@vutbr.cz

% Information related to '147.229.0.0/17AS197451'

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
```

Listing 10: Referenčný Whois dotaz nad doménov **vutbr.cz**.