

Vysoké učení technické v Brně

Fakulta informačních technologií

ISA

Sít'ové aplikace a správa sítí

Programování sít'ové služby: Whois Tazatel

| | |
|--|-----------|
| Zadání | 2 |
| Problematika & Vysvětlení | 2 |
| 1. WHOIS | 2 |
| 2. DNS | 2 |
| Požadovaný výstup | 2 |
| 1. WHOIS | 2 |
| 2. DNS | 3 |
| Návod spuštění | 3 |
| Vysvětlivky | 3 |
| Implementace | 4 |
| 1. Parsování argumentů | 4 |
| 2. DNS | 5 |
| 3. WHOIS | 5 |
| Testování | 6 |
| Použité zdroje & Literatura | 13 |

Zadání

Úkolem je vytvořit program v programovacím jazyce C nebo C++, který má dvě části. První částí je implementace tzv WHOIS Lookup, který bude o uživatelem zvolené doménové adrese/IP adrese zjišťovat informace z uživatelem uvedeného WHOIS serveru. Druhou částí je implementace tzv. DNS Lookup, který o zadané adrese bude zjišťovat DNS záznamy jako A, AAA, CNAME pomocí výchozího DNS v operačním systému. Program má podporovat IPv6.

Problematika & Vysvětlení

1. WHOIS

Pojem WHOIS značí databázi, sloužící k evidenci informací o internetových doménách, IP adresách a jejich náležitých majitelích. Databáze domén na nejvyšším (národním) řádu, je strukturována hierarchicky, kde každý národní registrátor má svůj vlastní WHOIS server. Všechny komunikace pro takovéto WHOIS dotazy běží na portu 43.

Po důkladnějším nastudování informací o této databázi je ale zřejmé, že velkým nedostatkem, někdy i problémem, je, že WHOIS servery nedodržují žádné standardy které by mohly definovat nutnost unifikace formátu pro dotazy na takové servery. Tato služba je volně dostupná a existuje mnoho služeb/způsobu na získání WHOIS informací, ovšem většina je vytvořena v podobě webové aplikace.

2. DNS

Domain Name Servers. Systém doménových jmen s informacemi, na kterém serveru se domény nacházejí. Jedná se v podstatě o “překladač” doménových jmen na odpovídající IP adresy a obráceně (dotaz pro reverzní překlad IP adresy). Naštěstí narozdíl od WHOIS je formát informací u absolutní většiny doménových serverů standardizovaný.

Požadovaný výstup

1. WHOIS

Pro WHOIS Lookup jsou výstupem informace o zadané adrese, získané ze zadaného WHOIS serveru. Mezi údaje patří (tyto údaje mohou mít variabilní název, každý whois server má svůj

vlastní formát, tahle aplikace neslouží pro vytvoření standardizovaného formátu výstupu, nýbrž pro zjištění důležitých, zajímavých informací, níže uvedený formát je z whois.ripe.net) inetnum, netname, descr, country, address, phone (*). Nejedná se o všechny hledané údaje, ale jen o ty nejdůležitější. Pokud nějaká informace není nalezena, nebude vypsána.

2. DNS

U DNS Lookup části je očekávaný výstup list záznamů získaných z DNS o zadané domén. Patří mezi ně: A, AAA, MX, CNAME, NS, SOA a PTR. (*). Seznam nenalezených záznamů bude vypsán na konci DNS Lookup.

(*) vysvětlivky lze nalézt na internetu, např <https://ns1.com/resources/dns-records-explained>

Návod spuštění

Program je navržen jako aplikace primárně určena pro operační systém Linux. Výsledkem implementace je binární soubor isa-tazatel (pomocí příkazu make). Soubor isa-tazatel pro spuštění příkazem ./isa-tazatel přijímá tyto argumenty/přepínače (pořadí není důležité):

| | |
|------------------|-------------|
| -help | |
| -q <IP Hostname> | (povinné) |
| -w <IP Hostname> | (povinné) |
| -d <IP> | (nepovinné) |
| -f | (nepovinné) |
| -o | (nepovinné) |

Vysvětlivky

-help - nelze kombinovat s ostatními argumenty, vypisuje nápovědu k používání a spouštění

-q <IP|Hostname>

- je IP adresa nebo doménové jméno, o kterém chce uživatel získat informace

-w <IP|Hostname>

- je IP adresa nebo doménové jméno WHOIS serveru, ze kterého chce získat informace o -q

-d <IP> (rozšíření)

- IP adresa DNS, pomocí kterého se bude provádět DNS lookup na adresu v -q

- Argument je nepovinný, jako výchozí DNS se vezme výchozí DNS z OS

-f (rozšíření)

- Pokud uživatel nechce, aby program jakkoliv modifikoval/upravoval formát přijatých informací, může si přepínačem -f nechat vypsát úplně celou odpověď, kde budou například i komentáře, přebytečné informace, duplicitní záznamy, atd.. Jedná se o vlastní rozšíření.

-o (rozšíření)

- Tento program ve WHOIS Lookup zjišťuje informace o všech nalezených IP adresách při zadání doménového jména do -q, tento přepínač bude limitovat program, aby zjistil informace pouze o první nalezené IP adrese. Jedná se o vlastní rozšíření

Přesné chování programu je popsáno v sekci Implementace níže

Implementace

Program je implementován pomocí jazyka C++. Volba jazyka nebyla složitá. Díky přítomnosti “datového typu” string a možnosti intuitivní práce s vektory odpadá spousta nepříjemností a zbytečné práce, které by implementaci samotného nápadu akorát zdržovali.

Mezi zajímavé části implementace patřilo tvoření vlastních struktur pro získání ip adres v přehledné formě, invertování a modifikace formátu IP adres a také parsování odpovědí u DNS dotazů.

1. Parsování argumentů

Program nejprve kontroluje argumenty od uživatele, přesněji počet těchto zadaných argumentů. 2 povinné argumenty s nutnou hodnotou značí, že minimální “počet argumentů” je 4(+1 cesta). Pokud je tohle pravidlo splněno, program využije funkci `getopt`, která parsování argumentů velice zjednoduší, protože umí zachytit potřebné hodnoty z jednotlivých argumentů. Pokud chybí povinný argument, či zachytí neznámý argument, program skončí s chybou a vypíše uživateli odpovídající chybovou hlášku.

Přepínače -o a -f v případě přítomnosti nastavují příslušné proměnné typu bool na pozdější fázi. Celé parsování argumentů je implementováno funkcí `parse_args`, která vrací string pole. Na pozici 0 je hodnota argumentu -q a na pozici 1 hodnota -w. Program zkontroluje, jestli náhodou IP hodnoty -q a -w jsou ve správném formátu, aby se například nestalo, že projde adresa 70.72.0.

2. DNS

Tato fáze programu vyhledá záznamy o adrese -q ve zvoleném DNS přes argument -d, pokud není přítomen, pracuje se s výchozím DNS operačního systému. Pokud je zadán argument -d neexistující adresa, či nemá správný formát, program taktéž bude pracovat s výchozí DNS operačního systému. Takového chování je dosaženo využitím funkce `res_init()`, a modifikací `_res.nsaddr_list[0].sin_addr` funkcí `inet_pton`.

Implementace je provedena funkcí `get_dns`. Tato funkce nejdříve pomocí funkce `getaddrinfo` zjistí, jestli doménová adresa je validní, pokud ano, provede kontrolu, jestli se jedná o IPv4 či IPv6 (funkce `inet_ntop` z knihovny `arpa/inet.h`), protože v případě, že je zadaná IP adresa, je nutné provést tzv “reverzní lookup”, při kterém se z DNS získá záznam PTR, s jehož pomocí můžeme následně získat zbytek záznamů. U tohoto způsobu je nutné otočit a modifikovat formát IP adresy do příslušného tvaru (IPv6 jinak než IPv4).

Při IPv4 se nejdříve z řetězce vytvoří vektor pomocí funkce `vectorize_string` s rozdělovacím znakem tečky, ve kterém se poté invertuje pořadí prvků a znovu se IP adresa poskládá zpět. Na závěr se přidá řetězec “in-addr.arpa”. U IPv6 je nutné nejdříve roztáhnout adresu na plnou délku, tahle část je zajištěna pomocí funkce `sprintf`, poté je potřeba tuto adresu invertovat a místo dvojtečky program přidá za každou číslici znak tečku.

Detailní vysvětlení uvedeno zde:

<https://www.ripe.net/manage-ips-and-asns/db/support/configuring-reverse-dns>

Záznamy o adrese z DNS program získává použitím `query_info_dns` funkce, která při každém úspěšně získaném záznamu přidá důležité informace do vektoru řetězců (C++ string). V této funkci také dochází k samotnému dotazu na DNS pomocí funkce `res_query` z knihovny `resolv.h`, kde se specifikuje konkrétní záznam (A, AAA, NS..).

U každého záznamu zanalyzuje odpověď, následně nahradí tabulátory mezerama, vymaže přebytečné mezery a rozdělovacím znakem mezery rozseká odpověď pomocí funkce `vectorize_string` na prvky vektoru, a podle typu záznamu sestaví konečný výstup a ponechá si pouze informace, které potřebuje.

Po dotázání na všechny záznamy pomocí práce s vektory zjistí, které záznamy chybí, a vrátí je hlavní funkci, která je následně vypíše.

3. WHOIS

Po dokončení DNS dotazování program přejde do funkce `get_whois`, která musí vyhledat informace o zvolené adrese na zvoleném WHOIS serveru. Tahle funkce začíná samozřejmě, jako všechny funkce, deklarací potřebných struktur a proměnných pro správný chod programu, poté

se pomocí `inet_pton` zkontroluje, jestli hodnota v `-q` není IP adresa, pokud není, tak si program zapamatuje, že má posílat dotaz i na konkrétní doménové jméno, a ne jen na nalezené IP adresy.

Po kontrole IP si vytvoří pomocí funkce `get_ip_structs` vlastní struktury, ve kterých jsou uvedeny všechny nalezené IP adresy, s přidanou bool vlastností, determinující verzi IP adresy (4/6). Funkce `get_ip_structs` funguje na základě funkce `getaddrinfo` a `for` cyklu, ve kterém pomocí `ai_next` uvnitř získané struktury funkcí `getaddrinfo`.

Jakmile program získá všechny potřebné IP adresy a struktury, vejde do dlouhého cyklu `for`, ve kterém pro každou nalezenou adresu pro `-q` provede následující:

- 1) Zkontroluje, jestli se jedná o IPv6, následně vytvoří příslušný socket, naplní posílaný paket
- 2) Nastaví timeout 4 vteřin pro následující `connect` funkci
- 3) Využije funkci `connect` na základě verze IP
- 4) Pošle zprávu a zachytí odpovídající paket skrz funkci `send_and_collect`.
 - V této funkci se také zjišťuje bool hodnota, kterou program nastavoval dříve.
 - Vyplní se zde zpráva, ve které je adresa, o které chceme zjišťovat informace.
 - Zprávu program pošle funkcí `send` a pomocí cyklu `while` a funkce `recv` vytáhne informace z odpovědi od serveru.
 - Tyto informace vrací nadřazené funkci.
- 5) Informace z předešlé funkce se nyní analyzují, a:
 - Vymažou se řádky, které nejsou potřebné (komentáře, prázdné řádky..).
 - Program vytvoří dlouhý seznam záznamů, které má ignorovat (např. `OrgAbuse`, `Parent`, `RAbuseName`..), a aplikuje tento “filtr”.
- 6) Finální informace se vrací hlavní funkci a jsou poté vypsány uživateli ve vhodné podobě

Uživatel může ovlivnit do určité úrovně výstup programu, díky přepínačům `-o` a `-f`, které jsou uvedené a vysvětlené v předešlých kapitolách.

Tento program nijak nemodifikuje zadané adresy, například neodmazává, či nepřidává automaticky ‘`www`’ v doménovém názvu, nýbrž spoléhá na znalosti uživatele o whois serverech, na které se dotazuje.

Testování

Testoval jsem převážně na online dostupných zdrojích & Web WHOIS & DNS Lookup aplikacích

Níže uvádím několik testovacích subjektů a jejich výsledky, pod nimi/vedle nich je vložen vždy výstup z existujícího online testovacího zdroje (např `ripe.net` a `nic.cz`).

Test 1

./isa-tazatel -q 147.229.9.23 -w whois.ripe.net

```
===== DNS =====
PTR:          www.fit.vutbr.cz.
A:            147.229.9.23
AAAA:         2001:67c:1220:809::93e5:917
MX:           0 - tereza.fit.vutbr.cz.
Missing records:
CNAME  NS   SOA

===== WHOIS =====

Querying for:
147.229.9.23
-----
inetnum:       147.229.0.0 - 147.229.254.255
netname:       VUTBRNET
descr:         Brno University of Technology
country:       CZ
admin-c:       CA6319-RIPE
address:       Brno University of Technology
address:       Antoninska 1
address:       601 90 Brno
address:       The Czech Republic
phone:         +420 541145453
phone:         +420 723047787
descr:         VUTBR-NET1
```

<https://apps.db.ripe.net/db-web-ui/#/query?searchtext=147.229.9.23>

Responsible organisation: [Brno University of Technology](#)
Abuse contact info: abuse@vutbr.cz

| | | | |
|----------------|---|-----------------|----------|
| inetnum: | 147.229.0.0 - 147.229.254.255 | Login to update | RIPEstat |
| 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 | | |

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

Test 2

`./isa-tazatel -q google.cz -w whois.nic.cz`

<https://nic.cz/whois/domain/google.cz>

Whois.nic.cz je patří mezi servery, které odpovídají jen na zprávu s doménovým jménem uvnitř.

```
===== DNS =====
A:                216.58.201.67
AAAA:             2a00:1450:4014:800::2003
MX:               40 - alt3.aspmx.l.google.com.
MX:               10 - aspmx.l.google.com.
MX:               30 - alt2.aspmx.l.google.com.
MX:               20 - alt1.aspmx.l.google.com.
MX:               50 - alt4.aspmx.l.google.com.
NS:               ns2.google.com.
NS:               ns3.google.com.
NS:               ns4.google.com.
NS:               ns1.google.com.
SOA:              ns1.google.com.
Admin-email:      dns-admin@google.com.
Missing records:
CNAME PTR

===== WHOIS =====

Querying for:
google.cz

-----
domain:           google.cz
registrant:       MM1171195
admin-c:          MM1171195
registered:       21.07.2000 15:21:00
expire:           22.07.2020
contact:          MM1171195
org:              Google LLC
name:             Domain Administrator
address:          1600 Amphitheatre Parkway
address:          Mountain View
address:          94043
address:          CA
address:          US
contact:          MM193020
org:              MarkMonitor Inc.
name:             Domain Provisioning
address:          3540 East Longwing Lane
address:          Suite 300
address:          Meridian
address:          83646
address:          ID
address:          US

Querying for:
2a00:1450:4014:800::2003
-----
No information was received from given whois server.

Querying for:
216.58.201.67
-----
No information was received from given whois server.
```

cz.nic | SPRÁVCE
DOMÉNY CZ


DOMÉNY

O DOMÉNÁCH A DNS | REGISTRACE | PRAVIDLA A POSTUPY | HLEDAT V R

VYHLEDÁVÁNÍ V REGISTRU (WHOIS)

Výsledek vyhledávání google.cz:

PROHLÍZENÍ DOMÉNOVÉHO JMÉNA

| | |
|---------------------------|---|
| Doménové jméno | google.cz |
| Registrace od | 21.07.2000 |
| Poslední aktualizace | 23.04.2018 |
| Datum expirace | 22.07.2020 |
| Držitel | MM1171195 Google LLC |
| Administrativní kontakt | MM1171195 Google LLC |
| Určený registrátor | REG-MARKMONITOR MarkMonitor Inc. od 7. února 2011 18:40 |
| Zabezpečeno pomocí DNSSEC |  |
| Stav | |

| | |
|-----------------------|---|
| Sada jmenných serverů | MM1543911 |
| Jmenný server | ns1.google.com |
| Jmenný server | ns2.google.com |
| Jmenný server | ns3.google.com |
| Jmenný server | ns4.google.com |
| Technický kontakt | MM193020 MarkMonitor Inc. |
| Určený registrátor | REG-MARKMONITOR MarkMonitor Inc. od 18. května 2011 23:27 |
| Stav | Je navázán na další záznam v registru |

 Ověřený výpis z registru

[Nové vyhledávání v registru.](#)

© 2019 CZ.NIC, z. s. p. o.

Test 3

./isa-tazatel -q 2a04:4e42:400::323 -w whois.lacnic.net -f

<http://lacnic.net/cgi-bin/lacnic/whois?lg=EN>

```
===== DNS =====  
Missing records:  
A AAAA MX CNAME NS SOA PTR
```

```
===== WHOIS =====
```

```
Querying for:  
2a04:4e42:400::323  
-----
```

```
% Joint Whois - whois.lacnic.net  
% This server accepts single ASN, IPv4 or IPv6 queries  
  
% RIPENCC resource: whois.ripe.net  
  
% This is the RIPE Database query service.  
% The objects are in RPSL format.  
%  
% The RIPE Database is subject to Terms and Conditions.  
% See http://www.ripe.net/db/support/db-terms-conditions.pdf  
% Note: this output has been filtered.  
% To receive output for a database update, use the "-B" flag.  
% Information related to '2a04:4e40::/29'  
% Abuse contact for '2a04:4e40::/29' is 'abuse@fastly.com'  
inet6num: 2a04:4e40::/29  
netname: US-FASTLY-20130718  
country: EU  
org: ORG-FI26-RIPE  
admin-c: FRA59-RIPE  
tech-c: FRA59-RIPE  
status: ALLOCATED-BY-RIR  
mnt-by: RIPE-NCC-HM-MNT  
mnt-lower: FASTLY  
mnt-routes: FASTLY  
created: 2013-07-18T14:46:58Z  
last-modified: 2016-04-14T08:24:37Z  
source: RIPE # Filtered  
organisation: ORG-FI26-RIPE  
org-name: Fastly, Inc.  
org-type: LIR  
address: PO Box 78266  
address: 94107  
address: San Francisco, CA  
address: UNITED STATES  
phone: +14157580146  
mnt-ref: FASTLY  
mnt-ref: RIPE-NCC-HM-MNT  
mnt-by: RIPE-NCC-HM-MNT  
abuse-c: FAT25-RIPE  
tech-c: FRA59-RIPE  
created: 2013-07-08T09:37:51Z  
last-modified: 2016-04-08T02:44:51Z  
source: RIPE # Filtered  
admin-c: FRA59-RIPE  
role: Fastly RIR Administrator  
org: ORG-FI26-RIPE  
address: PO Box 78266  
address: San Francisco CA 94107  
phone: +1 (415) 404-9374  
nic-hdl: FRA59-RIPE  
mnt-by: FASTLY  
created: 2014-09-24T14:49:45Z  
last-modified: 2014-09-25T15:10:14Z  
source: RIPE # Filtered
```

```
% Joint Whois - whois.lacnic.net  
% This server accepts single ASN, IPv4 or IPv6 queries  
  
% RIPENCC resource: whois.ripe.net  
  
% This is the RIPE Database query service.  
% The objects are in RPSL format.  
%  
% The RIPE Database is subject to Terms and Conditions.  
% See http://www.ripe.net/db/support/db-terms-conditions.pdf  
  
% Note: this output has been filtered.  
% To receive output for a database update, use the "-B" flag.
```

```
% Information related to '2a04:4e40::/29'
```

```
% Abuse contact for '2a04:4e40::/29' is 'abuse@fastly.com'
```

```
inet6num: 2a04:4e40::/29  
netname: US-FASTLY-20130718  
country: EU  
org: ORG-FI26-RIPE  
admin-c: FRA59-RIPE  
tech-c: FRA59-RIPE  
status: ALLOCATED-BY-RIR  
mnt-by: RIPE-NCC-HM-MNT  
mnt-lower: FASTLY  
mnt-routes: FASTLY  
created: 2013-07-18T14:46:58Z  
last-modified: 2016-04-14T08:24:37Z  
source: RIPE # Filtered
```

```
organisation: ORG-FI26-RIPE  
org-name: Fastly, Inc.  
org-type: LIR  
address: PO Box 78266  
address: 94107  
address: San Francisco, CA  
address: UNITED STATES  
phone: +14157580146  
mnt-ref: FASTLY  
mnt-ref: RIPE-NCC-HM-MNT  
mnt-by: RIPE-NCC-HM-MNT  
abuse-c: FAT25-RIPE  
tech-c: FRA59-RIPE  
created: 2013-07-08T09:37:51Z  
last-modified: 2016-04-08T02:44:51Z  
source: RIPE # Filtered  
admin-c: FRA59-RIPE
```

```
role: Fastly RIR Administrator  
org: ORG-FI26-RIPE  
address: PO Box 78266  
address: San Francisco CA 94107  
phone: +1 (415) 404-9374  
nic-hdl: FRA59-RIPE  
mnt-by: FASTLY  
created: 2014-09-24T14:49:45Z  
last-modified: 2014-09-25T15:10:14Z  
source: RIPE # Filtered
```

Test 4

./isa-tazatel -q 2a02:598:3333:1::1 -w whois.ripe.net

<https://apps.db.ripe.net/db-web-ui/#/query?searchtext=2a02:598:3333:1::1>

```
===== DNS =====
Missing records:
A AAAA MX CNAME NS SOA PTR
===== WHOIS =====

Querying for:
2a02:598:3333:1::1
-----
inet6num:      2a02:598:3333::/48
netname:       DC-Kokura-DNS
country:       CZ
admin-c:       SZN5-RIPE
address:       Radlicka 3294/10 150 00 Prague 5 Czech Republic
phone:         +420 602 126 570
admin-c:       PZ172-RIPE
person:        Tomas Paczek
address:       Radlicka 3294/10 150 00 Prague 5 Czech Republic
phone:         +420 234 694 111
descr:         SEZNAM - II
xmacha73@merlin: ~/ISA$
```

Responsible organisation: [Seznam.cz, a.s.](#)
Abuse contact info: abuse@seznam.cz

```
inet6num:      2a02:598:3333::/48
netname:       DC-Kokura-DNS
country:       CZ
admin-c:       SZN5-RIPE
tech-c:        SZN11-RIPE
status:        ASSIGNED
mnt-by:        SEZNAM-MNT
created:       2016-08-17T12:00:37Z
last-modified: 2016-08-17T12:00:37Z
source:        RIPE
```

```
route6:        2a02:598:3333::/48
descr:         SEZNAM - II
origin:        AS43037
mnt-by:        SEZNAM-MNT
created:       2014-04-29T13:56:34Z
last-modified: 2014-04-29T13:56:34Z
source:        RIPE
```

RIPE Database Software Version 1.95.1

Test 5

<http://lacnic.net/cgi-bin/lacnic/whois?lg=EN>

./isa-tazatel -w whois.lacnic.net -q 2606:4700:10::6814:155

Naprosto stejných výsledků lze dosáhnout použitím -f přepínače

```
% Joint whois - whois.lacnic.net
% This server accepts single ASN, IPv4 or IPv6 queries

% ARIN resource: whois.arin.net

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.
#

NetRange: 2606:4700:: - 2606:4700:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
CIDR: 2606:4700::/32
NetName: CLOUDFLARENET
NetHandle: NET6-2606-4700-1
Parent: NET6-2600 (NET6-2600-1)
NetType: Direct Allocation
OriginAS: AS13335
Organization: Cloudflare, Inc. (CLOUD14)
RegDate: 2011-11-01
Updated: 2017-02-17
Comment: All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref: https://rdap.arin.net/registry/ip/2606:4700::

OrgName: Cloudflare, Inc.
OrgId: CLOUD14
Address: 101 Townsend Street
City: San Francisco
StateProv: CA
PostalCode: 94107
Country: US
RegDate: 2010-07-09
Updated: 2019-09-25
Ref: https://rdap.arin.net/registry/entity/CLOUD14

OrgTechHandle: ADMIN2521-ARIN
OrgTechName: Admin
OrgTechPhone: +1-650-319-8930
OrgTechEmail: rir@cloudflare.com
OrgTechRef: https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

OrgNOCHandle: NOC11962-ARIN
OrgNOCName: NOC
OrgNOCPhone: +1-650-319-8930
OrgNOCEmail: noc@cloudflare.com
OrgNOCRef: https://rdap.arin.net/registry/entity/NOC11962-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-650-319-8930
OrgAbuseEmail: abuse@cloudflare.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName: NOC
RNOCPhone: +1-650-319-8930
RNOCEmail: noc@cloudflare.com
RNOCRef: https://rdap.arin.net/registry/entity/NOC11962-ARIN

RABuseHandle: ABUSE2916-ARIN
RABuseName: Abuse
RABusePhone: +1-650-319-8930
RABuseEmail: abuse@cloudflare.com
RABuseRef: https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName: Admin
RTechPhone: +1-650-319-8930
RTechEmail: rir@cloudflare.com
RTechRef: https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.
#
```

```
===== DNS =====
Missing records:
A AAAA MX CNAME NS SOA PTR

===== WHOIS =====

Querying for:
2606:4700:10::6814:155
-----

NetRange: 2606:4700:: - 2606:4700:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
CIDR: 2606:4700::/32
NetName: CLOUDFLARENET
NetHandle: NET6-2606-4700-1
NetType: Direct Allocation
Organization: Cloudflare, Inc. (CLOUD14)
OrgName: Cloudflare, Inc.
OrgId: CLOUD14
Address: 101 Townsend Street
City: San Francisco
StateProv: CA
PostalCode: 94107
Country: US
xmacha73@merlin: ~/ISA$
```


Test 6

(linux): dig skype.com any

./isa-tazatel -q skype.com -w whois.iana.org -o -d 8.8.8.8

Slouží pro ověření DNS výsledků, lze i zadávat argument -d (bonus)

```
===== DNS =====
Using DNS: 127.0.0.53

A:          23.102.255.237
A:          40.121.80.200
A:          40.115.34.155
A:          104.40.50.126
MX:         10 - skype-com.mail.protection.outlook.com.
NS:         ns2.msft.net.
NS:         ns1.msft.net.
NS:         ns4.msft.net.
NS:         ns3.msft.net.
SOA:        ns1.msft.net.
Admin-email: msnhst@microsoft.com.
Missing records:
AAAA CNAME PTR

===== WHOIS =====

Querying for:
skype.com
-----
refer:      whois.verisign-grs.com
domain:     COM
organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States
contact:    administrative
name:       Registry Customer Service
organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States
phone:      +1 703 925-6999
fax-no:     +1 703 948 3978
e-mail:     info@verisign-grs.com
contact:    technical
name:       Registry Customer Service
organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States
phone:      +1 703 925-6999
fax-no:     +1 703 948 3978
e-mail:     info@verisign-grs.com
whois:      whois.verisign-grs.com

; <<>> DiG 9.11.3-Ubuntu1.9-Ubuntu <<>> skype.com any
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35134
; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;skype.com.                IN      ANY

;; ANSWER SECTION:
skype.com.                5       IN      SOA      ns1.msft.net. msnhst.micr
osoft.com. 2019111803 7200 900 2419200 3600
skype.com.                5       IN      MX       10 skype-com.mail.protect
ion.outlook.com.
skype.com.                5       IN      A        40.115.34.155
skype.com.                5       IN      A        23.102.255.237
skype.com.                5       IN      A        40.121.80.200
skype.com.                5       IN      A        104.40.50.126
skype.com.                5       IN      NS       ns1.msft.net.
skype.com.                5       IN      NS       ns3.msft.net.
skype.com.                5       IN      NS       ns2.msft.net.
skype.com.                5       IN      NS       ns4.msft.net.

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 18 23:01:43 CET 2019
;; MSG SIZE rcvd: 285
```

Použité zdroje & Literatura

- [1] RFC 954: NICNAME/WHOIS
<https://tools.ietf.org/html/rfc954>
- [2] DNS Explained
https://cs.wikipedia.org/wiki/Domain_Name_System
- [3] RFC 1834: Whois and Network Information Lookup Service, Whois++
<https://tools.ietf.org/html/rfc1834>
- [4] Resolv.h Linux manual page
<http://man7.org/linux/man-pages/man3/resolver.3.html>
- [5] DNS Lookup - MxToolBox
<https://mxtoolbox.com/DNSLookup.aspx>
- [6] Whois - Wikipedie
<https://cs.wikipedia.org/wiki/Whois>
- [7] Stackoverflow (v případě zaseknutí nad problémem)
<https://stackoverflow.com/>