DNS SERVIS
II DEO

Predmet: Mrežni servisi

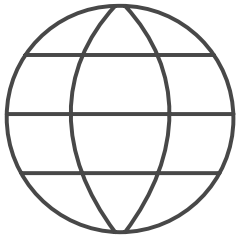
Predavač: dr Dušan Stefanović

DNS ZAPISI

DNS zapis (Resource Record) je osnovna jedinica podataka u DNS bazi.

Svaki zapis povezuje određeni domen sa nekim tipom informacije.

format DNS zapisa: <ime> <TTL> <klasa> <tip> <podatak>

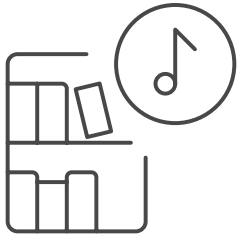


Ime domena

Definiše naziv domena

TTL

Vreme u sekundama koliko se čuva keširani podatak

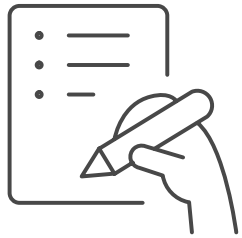


Klasa

DNS klasa zapisa (najčešće IN - Internet)

Tip

Tip DNS zapisa

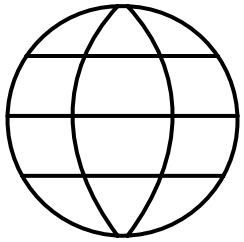


Vrednost

Sadrži vrednost zapisa

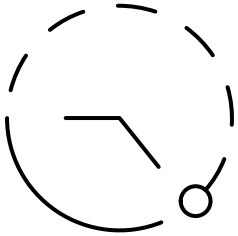
KOMPONENTE DNS ZAPISA
PRIMER

odseknis.akademijanis.edu.rs. 3600 IN A 160.99.37.100



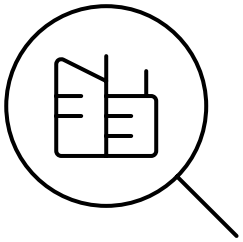
Ime hosta

ime hosta u DNS zapisu.



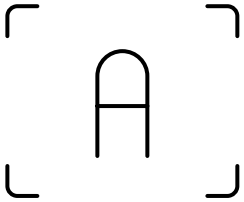
TTL

3600 sek. predstavlja vreme trajanja keširanog podatka.



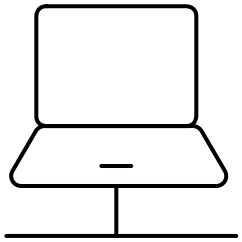
IN

IN (Internet) označava klasu zapisa.



Tip zapisa

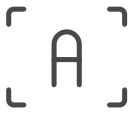
A označava tip DNS zapisa.



IP adresa

160.99.37.100 je adresa koja odgovara imenu hosta.

OSNOVNI DNS ZAPISI



A Record

Preslikava ime hosta u IPv4 adresu

AAAA Record

Preslikava ime hosta u IPv6 adresu

CNAME Record

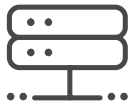
Alias jednog domena ka drugom

MX Record

Definiše mejl server za domen

SOA Record

Početni zapis DNS zone



NS Record

Označava autoritativne DNS servere

SRV Record

Locira specifične servise u domenu

TXT Record

Unosi proizvoljne tekstualne podatke

PTR Record

Omogućava obrnutu DNS rezoluciju

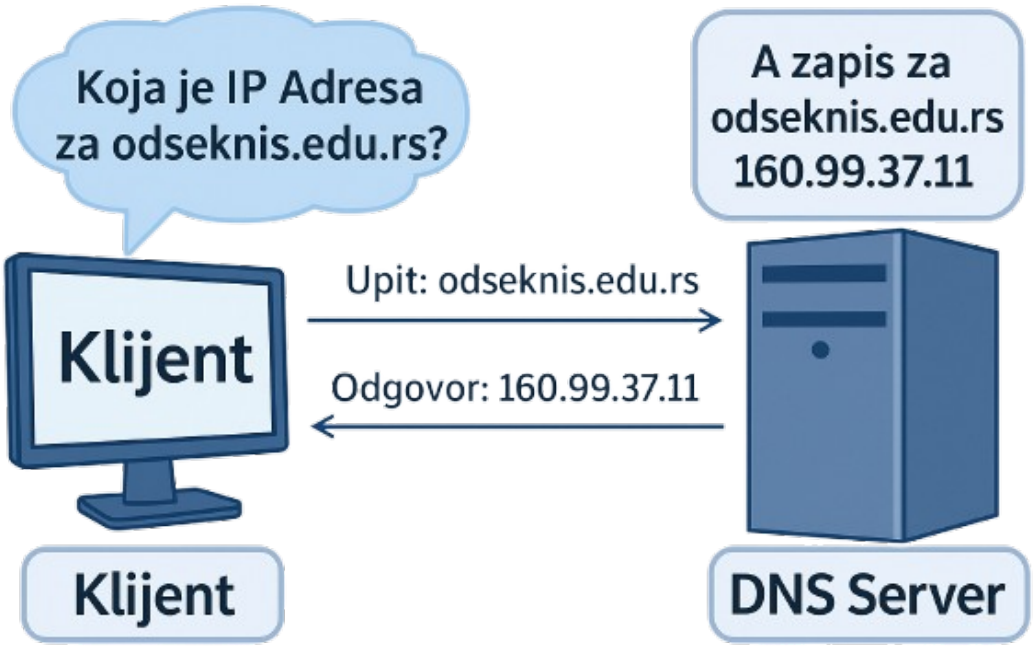
A I AAAA HOST ZAPIS

HOST zapis čuva IP adresu za dato DNS ime

Najčešći tip zapisa jer ime svakog uređaja se razrešava korišćenjem Host zapisa

A zapis se koristi za IPv4 adrese

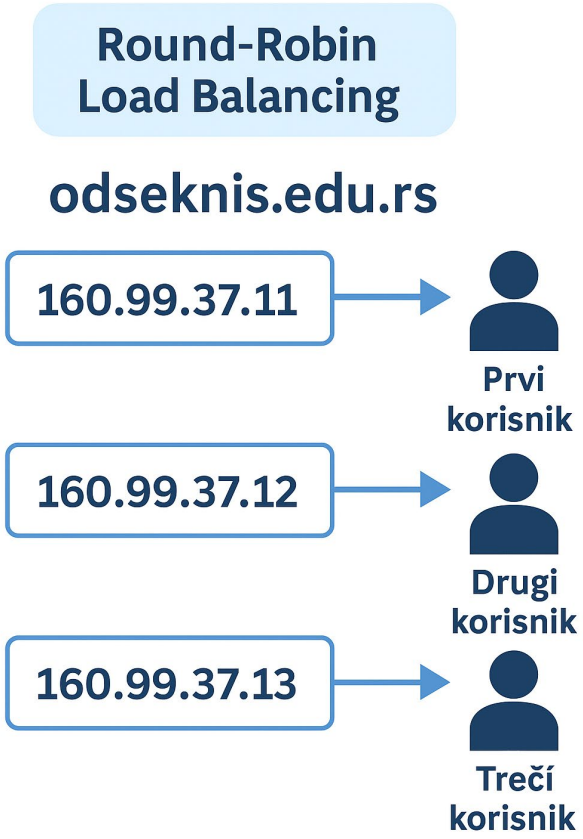
AAAA zapis se koristi za IPv6 adrese



<ime> <TTL> IN A <IPv4 adresa>

www.odseknis.edu.rs. 3600 IN A 192.0.2.1

LOAD BALANCING A ZAPIS



Round-Robin Load Balancing

odseknis.edu.rs. 3600 IN A 160.99.37.11
odseknis.edu.rs. 3600 IN A 160.99.37.12
odseknis.edu.rs. 3600 IN A 160.99.37.13

Geografski Load Balancing (GeoDNS)

odseknis.edu.rs. 3600 IN A 160.99.37.11 ; Evropa
odseknis.edu.rs. 3600 IN A 203.0.113.8 ; Azija
odseknis.edu.rs. 3600 IN A 192.0.2.5 ; SAD

CNAME ZAPIS

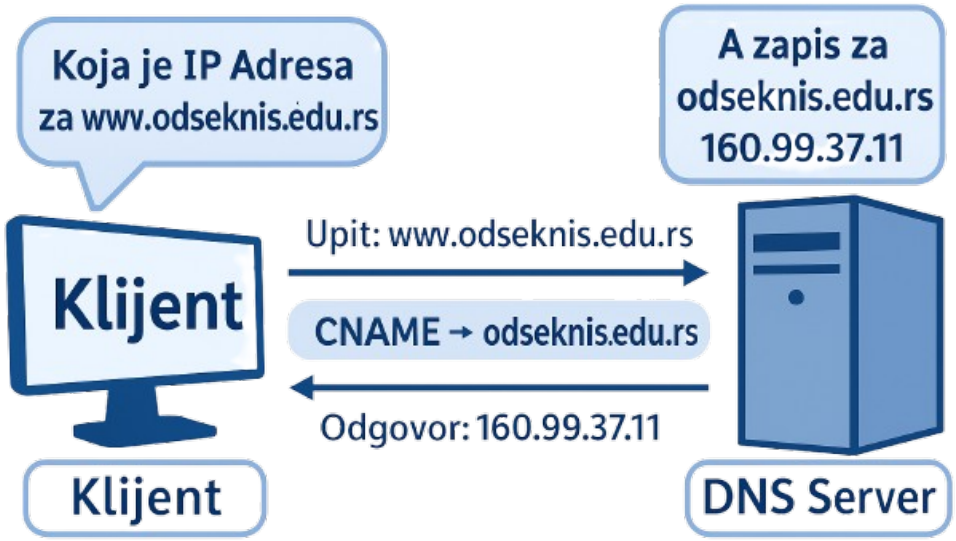
Alternativno ime ili alias

Upotrebom alijasa možemo promeniti naziv računara koji obezbeđuje neki Internet servis(Web,Ftp,..) a da mu ne menjamo adresni (A) zapis.

Omogućava **više imena za isti server**

Klijent će najpre tražiti CNAME zapis, a zatim dobiti odgovarajući **A zapis** za kanoničko ime.

www.odseknis.edu.rs. IN CNAME odseknis.edu.rs.
odseknis.edu.rs. IN A 160.99.37.11



NAME SERVER (NS) ZAPIS

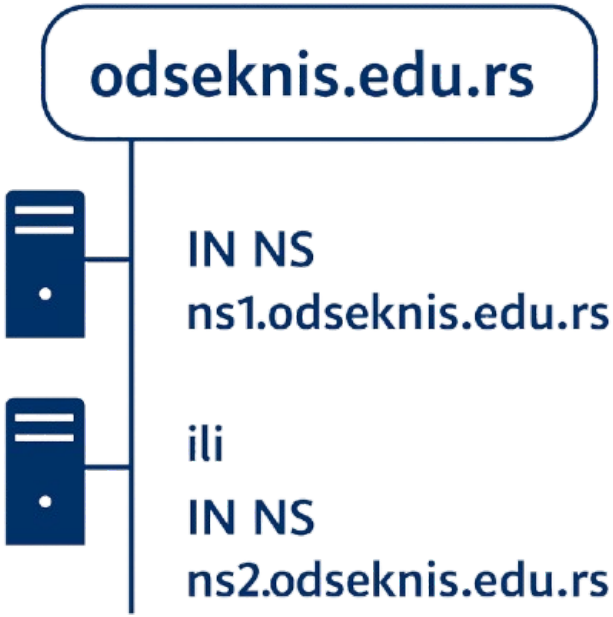
NS zapisi ukazuju na DNS servere koji su autorativni za taj domen

NS zapis se navodi za primarni i sve sekundarne NS servere

<ime domena> IN NS <ime servera>

<ime domena> je naziv domena za koji naznačeni server poseduje zonsku konfiguraciju

<ime servera> je naziv hosta koji je autorativan za taj domen



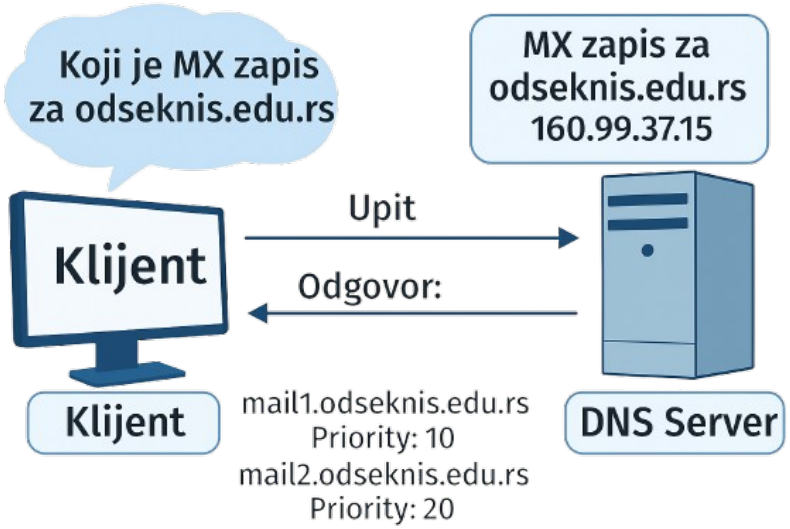
odseknis.edu.rs. IN NS ns1.odseknis.edu.rs.
IN NS ns2.odseknis.edu.rs.

MX (MAIL EXCHANGE) ZAPIS

Identifikuje mail server za dato DNS ime

MX zapis sadrži i priority vrednost koja se koristi ukoliko isti domen opslužuju više mail servera

Manja priority vrednost se prvo uzima, ukoliko su priority vrednosti iste, izbor je slučajan



mail1	A	160.99.37.15
mail2	A	160.99.37.16
odseknis.edu.rs.	MX	10 mail1
odseknis.edu.rs.	MX	20 mail2

SOA (START OF AUTHORITY) ZAPIS

SOA (Start of Authority) zapis je ključni DNS zapis koji definiše osnovne informacije o DNS zoni, kao što su autoritet, vremenski intervali za keširanje i sinhronizaciju među serverima.

SOA zapis je obavezan u svakoj DNS zoni.

Mora biti prvi zapis u datoteci zone.

Koristi se i za sinhronizaciju između primarnog i sekundarnih DNS servera

```
odseknis.edu.rs.  IN  SOA  ns1.odseknis.edu.rs.
admin.odseknis.edu.rs. (
        2025050301 ; Serial
        3600       ; Refresh (1h)
        600        ; Retry   (10min)
        1209600    ; Expire  (14d)
        86400 )    ; Minimum TTL (1d)
```

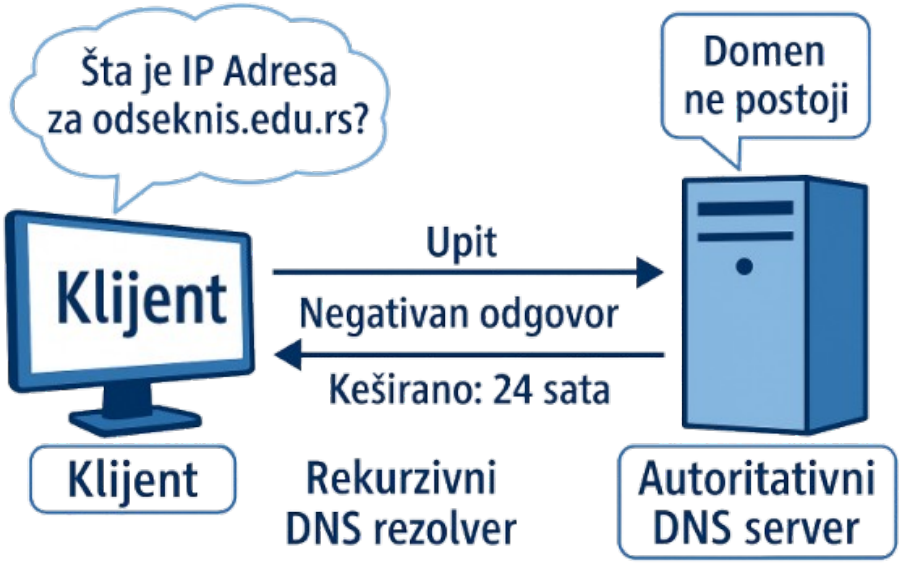
Polje	Opis
Primary NS	ns1.odseknis.edu.rs. – primarni DNS server za zonu
Email admina	admin.odseknis.edu.rs. – kontakt osoba za zonu (zameni @ sa .)
Serial	2025050301 – broj verzije zone (godina+mesec+dan+revizija)
Refresh	3600 – na svakih 1h sekundarni proverava da li ima novih podataka
Retry	600 – ako refresh ne uspe, ponavlja pokušaj za 10 minuta
Expire	1209600 – posle 14 dana sekundarni smatra zonu nevažećom
Minimum TTL	86400 – koliko dugo rekurzivni resolveri keširaju negativne odgovore (npr. NXDOMAIN)

NEGATIVNI ODGOVORI

Rekurzivni DNS resolveri keširaju negativne odgovore (npr. da neki domen ne postoji) u polju Minimum TTL (poznato i kao Negative TTL)

U ovom primeru:86400 sekundi = 24 sata

To znači da, ako DNS server sazna da neki zapis ne postoji (npr. xyz.odseknis.edu.rs), on će zapamtiti (keširati) tu informaciju kao negativan odgovor 24 sata.




```
odseknis.edu.rs.  IN  SOA  ns1.odseknis.edu.rs.
admin.odseknis.edu.rs. (
                2025050301 ; Serial
                3600       ; Refresh (1h)
                600        ; Retry   (10min)
                1209600    ; Expire  (14d)
                86400 )    ; Minimum TTL (1d)
```

SRV (SERVICE) ZAPIS

SRV (Service) zapis je DNS zapis koji omogućava lociranje specifičnih servisa unutar domena, kao što su VoIP, LDAP, SIP i drugi.

_ldap._tcp.odseknis.edu.rs. 3600 IN SRV 10 0 389 ldap1.odseknis.edu.rs.

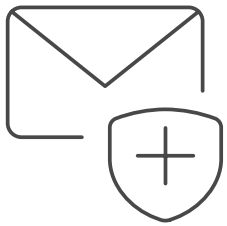
Polje	Vrednost	Objašnjenje
Servis	_ldap	Traži se LDAP servis
Protokol	_tcp	LDAP koristi TCP protokol
Domen	odseknis.edu.rs	Za koji domen se traži LDAP servis
TTL	3600	Vreme keširanja (1 sat)
Priority	10	Niža vrednost = veći prioritet
Weight	0	Nema balansiranja jer postoji samo jedan server
Port	389	Standardni port za LDAP
Target	ldap1.odseknis.edu.rs.	DNS ime servera koji nudi LDAP uslugu

TXT (TEXT) ZAPIS

TXT (Text) zapis u DNS-u služi za **unošenje proizvoljnog teksta** vezanog za neki domen.

U praksi, koristi se za brojne **sigurnosne i verifikacione svrhe**

odseknis.edu.rs. IN TXT "v=spf1 ip4:160.99.37.0/24 -all"

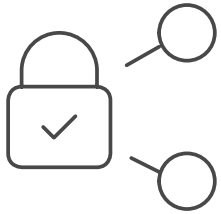


SPF

Verifikacija okvira politike pošiljaoca.

DKIM

Protokol bezbednosti identifikovanih domena.

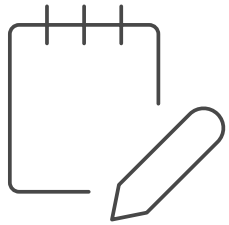


DMARC

Verifikacija poruka, izveštavanje i usklađenost.

Verifikacija domena

Verifikacija domena za usluge.



Napomene

Skladištenje napomena i informacija o vlasništvu.

PRIMERI PRAKTIČNE UPOTREBE TXT ZAPISA

SPF (Sender Policy Framework) je DNS mehanizam za zaštitu od lažiranja pošiljalaca e-pošte (spoofing).

On definiše koje IP adrese imaju dozvolu da šalju mejlove u ime određenog domena.

odseknis.edu.rs. IN TXT "v=spf1 ip4:160.99.37.0/24 -all"

Deo	Značenje
v=spf1	Verzija SPF protokola (uvek počinje ovako)
ip4:160.99.37.0/24	Dozvoljeno slanje mejlova sa bilo koje IP adrese iz ovog opsega
-all	Sve ostale IP adrese su **izričito zabranjene** (hard fail)

"v=spf1 ip4:160.99.37.10 ip4:160.99.37.11 include:_spf.google.com -all"

Dozvoljene IP:160.99.37.10 i 160.99.37.11

Takođe svi koji su u SPF zapisu za google.com (npr. ako se koristi Gmail za slanje)

PRIMERI PRAKTIČNE UPOTREBE TXT ZAPISA

DKIM (DomainKeys Identified Mail) je mehanizam za autentifikaciju e-pošte koji omogućava digitalno potpisivanje poruka tako da primalac može da proveri:

1. da poruka nije izmenjena u transport
2. da je zaista poslata sa servera ovlašćenog za domen

Pošiljalac (mail server) generiše digitalni potpis iz sadržaja poruke + zaglavlja.

Potpis se dodaje u zaglavlje mejla kao DKIM-Signature:

Primalac vidi DKIM-Signature zaglavlje. Primalac pronalazui javni ključ u DNS zapisu pomoću koga proverava da li se potpis poklapa sa sadržajem poruke

default._domainkey.odseknis.edu.rs. IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GC...QAB"

Element	Opis
v=DKIM1	Verzija DKIM
k=rsa	Algoritam za enkripciju
p=...	Javni RSA ključ koji koristi primalac za verifikaciju potpisa

PRIMERI PRAKTIČNE UPOTREBE TXT ZAPISA

DMARC (Domain-based Message Authentication, Reporting and Conformance) je mehanizam za autentifikaciju e-pošte koji se nadovezuje na SPF i DKIM i omogućava domenu da:

1. Sopšti serverima šta da urade ako SPF i/ili DKIM provera ne uspe (npr. da odbace mejl).
2. Prati i prijavljuje pokušaje zloupotrebe domena za slanje lažnih mejlova (phishing).
3. Štiti brend i korisnike od prevara u e-pošti.

DMARC politika u TXT zapisu za domen odseknis.edu.rs

_dmarc.odseknis.edu.rs. IN TXT
"v=DMARC1; p=reject; rua=mailto:dmarc@odseknis.edu.rs; ruf=mailto:forenzika@odseknis.edu.rs; fo=1"

Element	Značenje
v=DMARC1	Verzija protokola
p=reject	Odbaci mejlove koji ne prođu SPF/DKIM
rua=	Adresa za agregatne izveštaje (ko šalje, koliko, rezultati)
ruf=	Adresa za forenzičke (detaljne) izveštaje
fo=1	Pošalji forenzički izveštaj za bilo koji neuspeh

FORMAT DNS PORUKE

DNS poruke:

Upiti (*query)* i *odgovori (reply)* imaju isti format poruke

Zaglavlje DNS poruke

identification: 16 bit broj za identifikaciju upita, odgovor sadrži istu vrednost

flags:

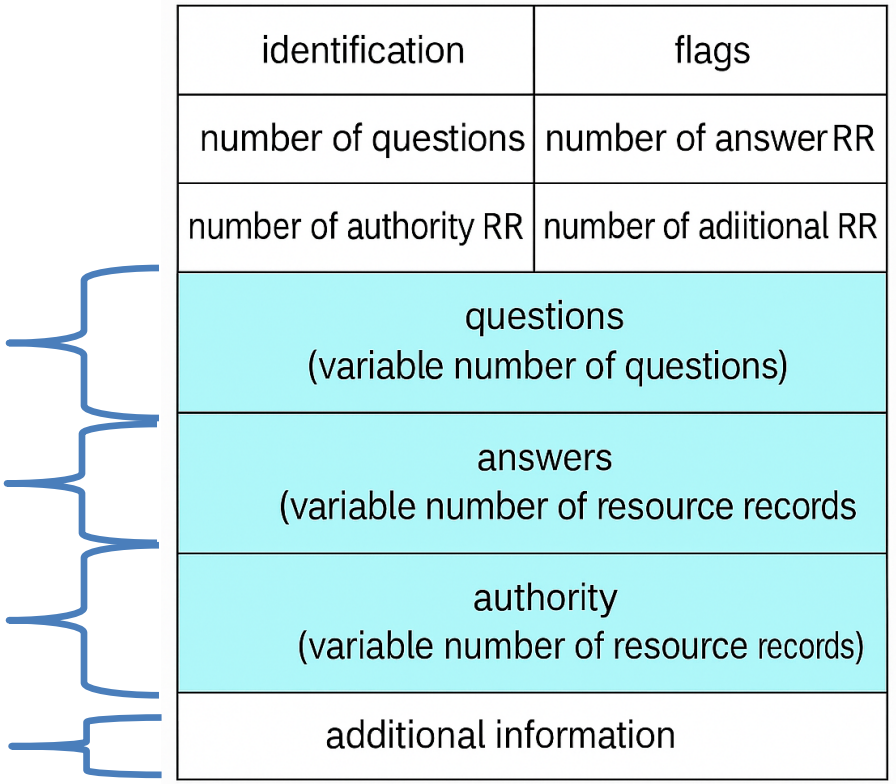
- 1bit: upit (0) ili odgovor (1)
- 1bit: rekurzivni upit se traži (1) ili ne (0)
- 1bit: rekurzija podržana (1) ili ne (0)
- 1 bit: odgovor je od autorizovanog n.s.(1)

Sadrži informacioje o upitu koji se traži: ime, tip zapisa za upit (npr. tip A-ime hosta)

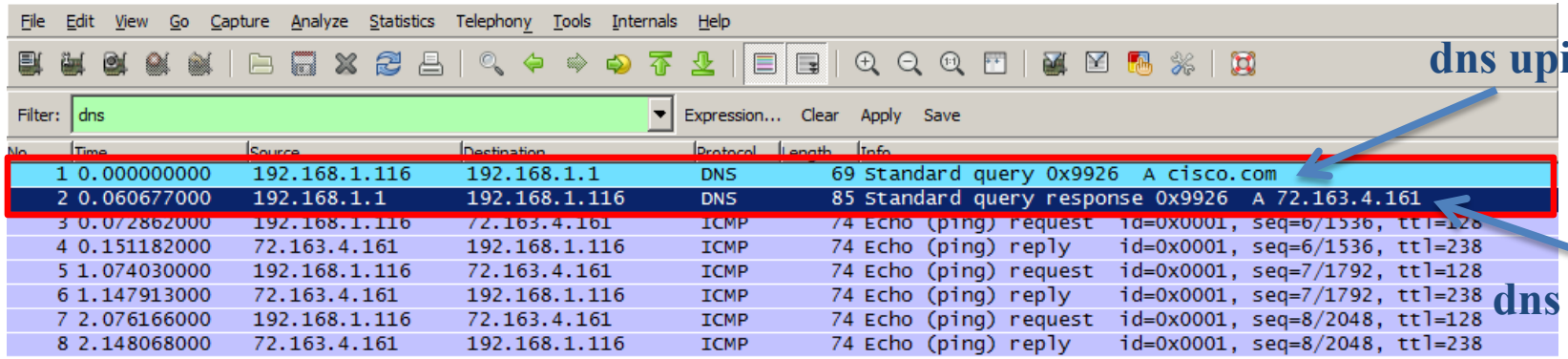
RR zapisi kao odgovor na pitanje

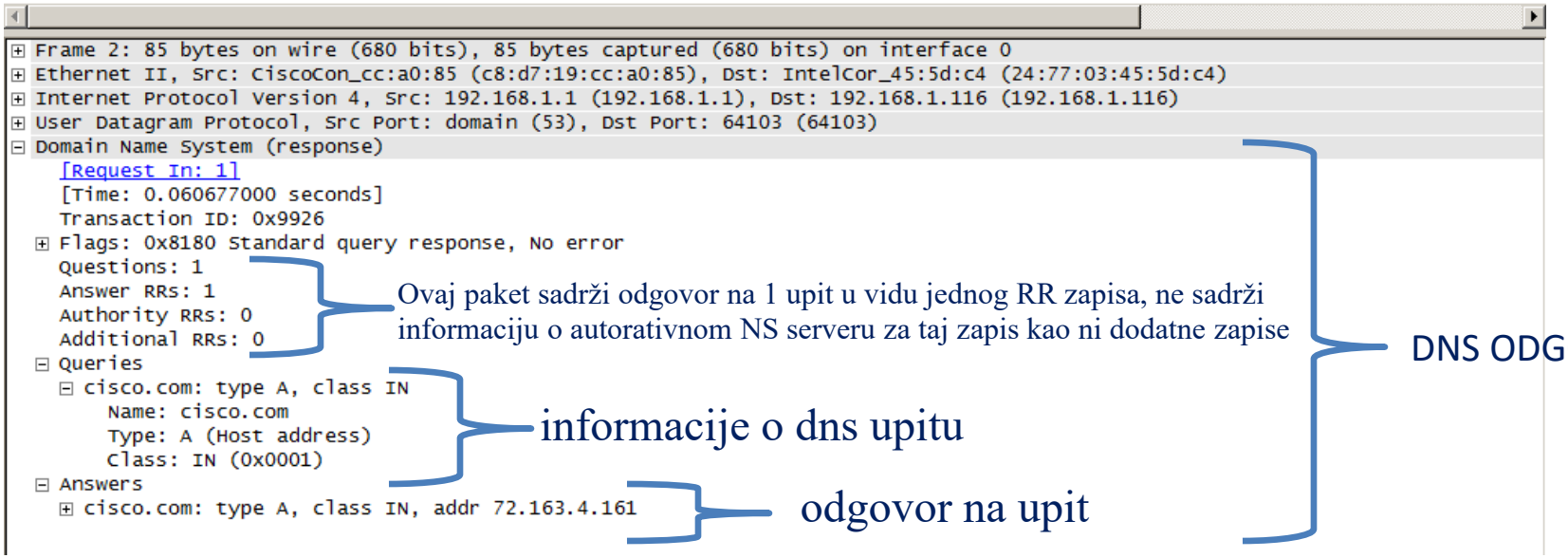
Zapisi o autorizovanim serverima

Dodatne "korisne" informacije (npr. ako je u polju "answers" bio MX zapis: ime mail servera, tada u ovom polju može biti njegova IP adresa)



PRIMER DNS UPITA I ODGOVORA





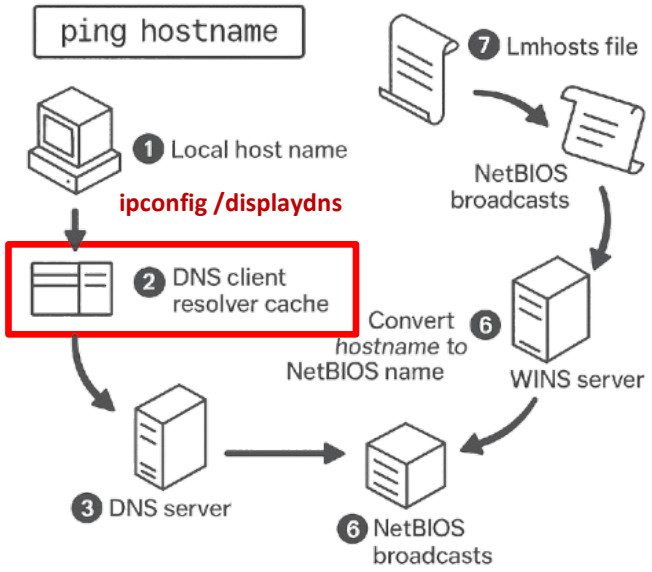
INFORMACIJE O LOKALNOM DNS SERVERU

ipconfig /all

google dns server
IP: 8.8.8.8

```
C:\Users\Korisnik>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Korisnik-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 38-59-F9-17-23-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Dell Wireless 1702 802.11b/g/n
   Physical Address. . . . . . . . . : 38-59-F9-17-23-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::51a8:395a:a2d4:58db%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 24. avgust 2014 18:58:18
   Lease Expires . . . . . . . . . . : 25. avgust 2014 19:52:50
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 322460153
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-16-30-01-FD-18-03-73-5E-ED-53

   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

LOKALNI DNS KEŠ




```
C:\Users\Korisnik>ipconfig /displaydns

Record Name . . . . . : 1.0.0.127.in-addr.arpa.
Record Type . . . . . : 12
Time To Live  . . . . : 86400
Data Length . . . . . : 8
PTR Record  . . . . . : localhost

www.youtube.com
----------------------------------------
Record Name . . . . . : www.youtube.com
Record Type . . . . . : 5
Time To Live  . . . . : 294
Data Length . . . . . : 8
CNAME Record  . . . . : youtube-ui.l.google.com

dijasporanis.com
----------------------------------------
Record Name . . . . . : dijasporanis.com
Record Type . . . . . : 1
Time To Live  . . . . : 294
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 194.9.95.45

www.google-analytics.com
----------------------------------------
Record Name . . . . . : www.google-analytics.com
Record Type . . . . . : 5
Time To Live  . . . . : 68
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : www-google-analytics.l.google.com

103.110.101.79.in-addr.arpa
----------------------------------------
Record Name . . . . . : 103.110.101.79.in-addr.arpa.
Record Type . . . . . : 12
Time To Live  . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record  . . . . . : pretrazivac

vtsnis.edu.rs
----------------------------------------
Record Name . . . . . : vtsnis.edu.rs
Record Type . . . . . : 1
Time To Live  . . . . : 294
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 194.9.94.7
```

ipconfig /displaydns

Prikaz lokalnog DNS keša na hostu, nakon isteka TTL vrednosti, DNS zapis se briše iz keša.

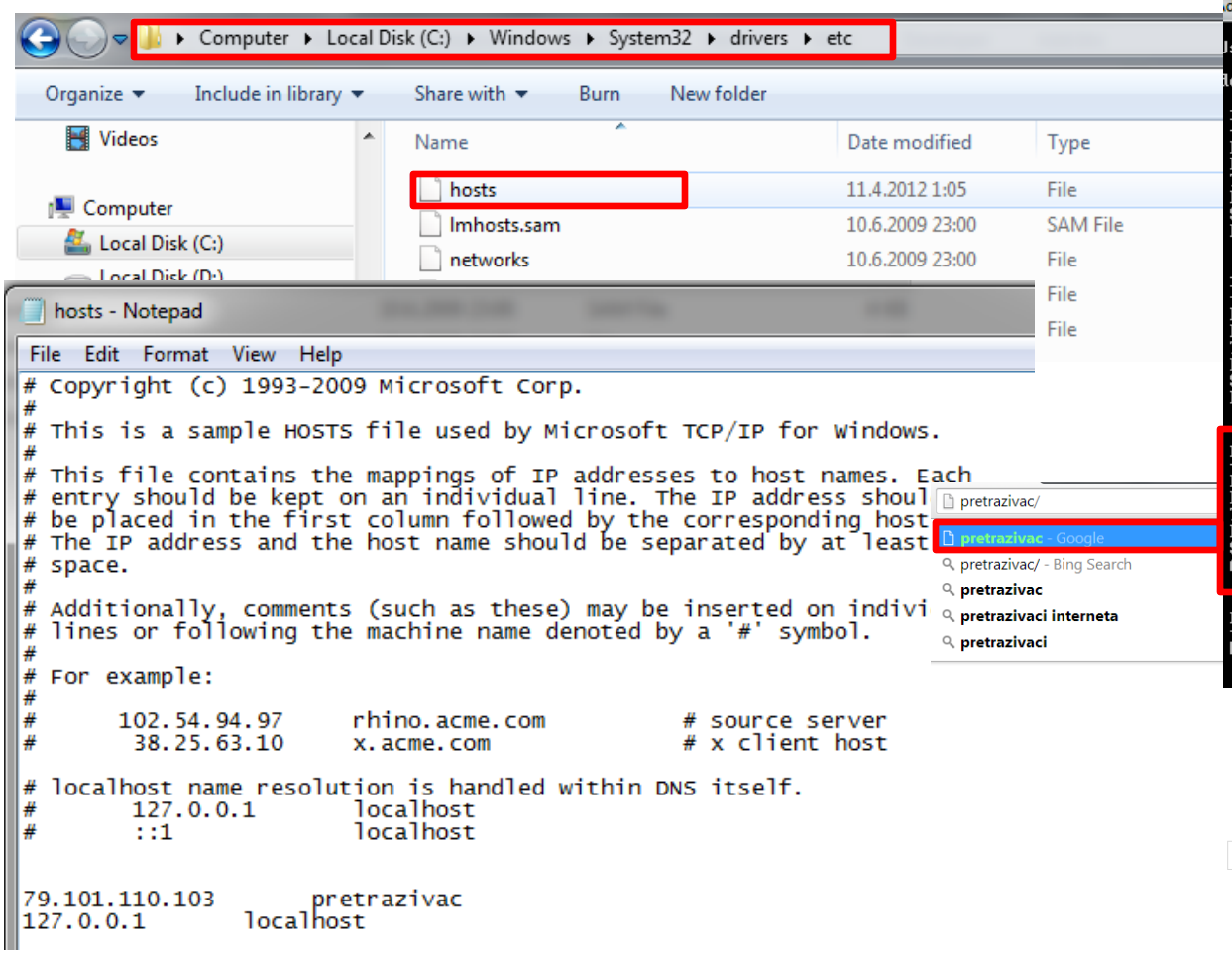
ipconfig /flushdns

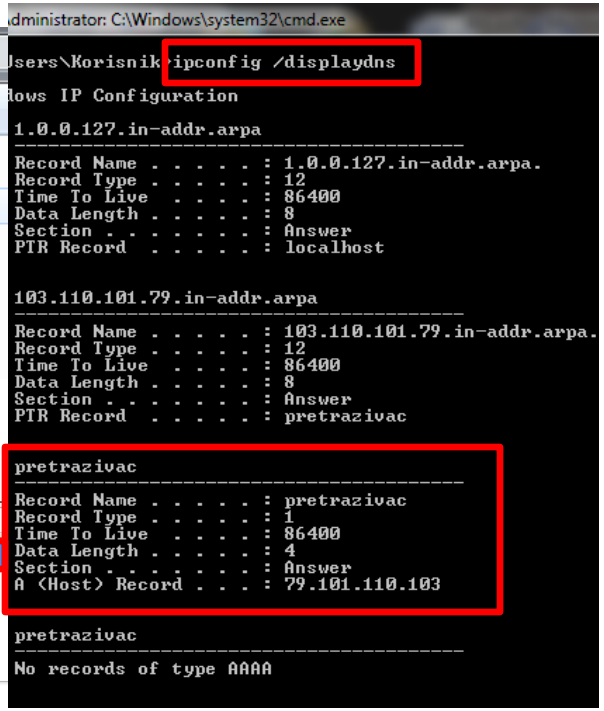
Ručno brisanje svih zapisa iz lokalnog DNS keša hosta

Podrazumevana TTL vrednost za pozitivne odgovore je 86,400 sekunde (1 dan).

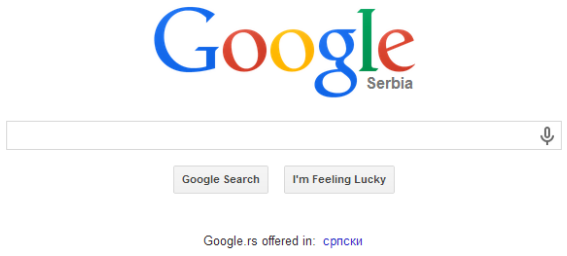
Podrazumevana TTL vrednost za negativne odgovore je 300 sekunde.

HOSTS FAJL

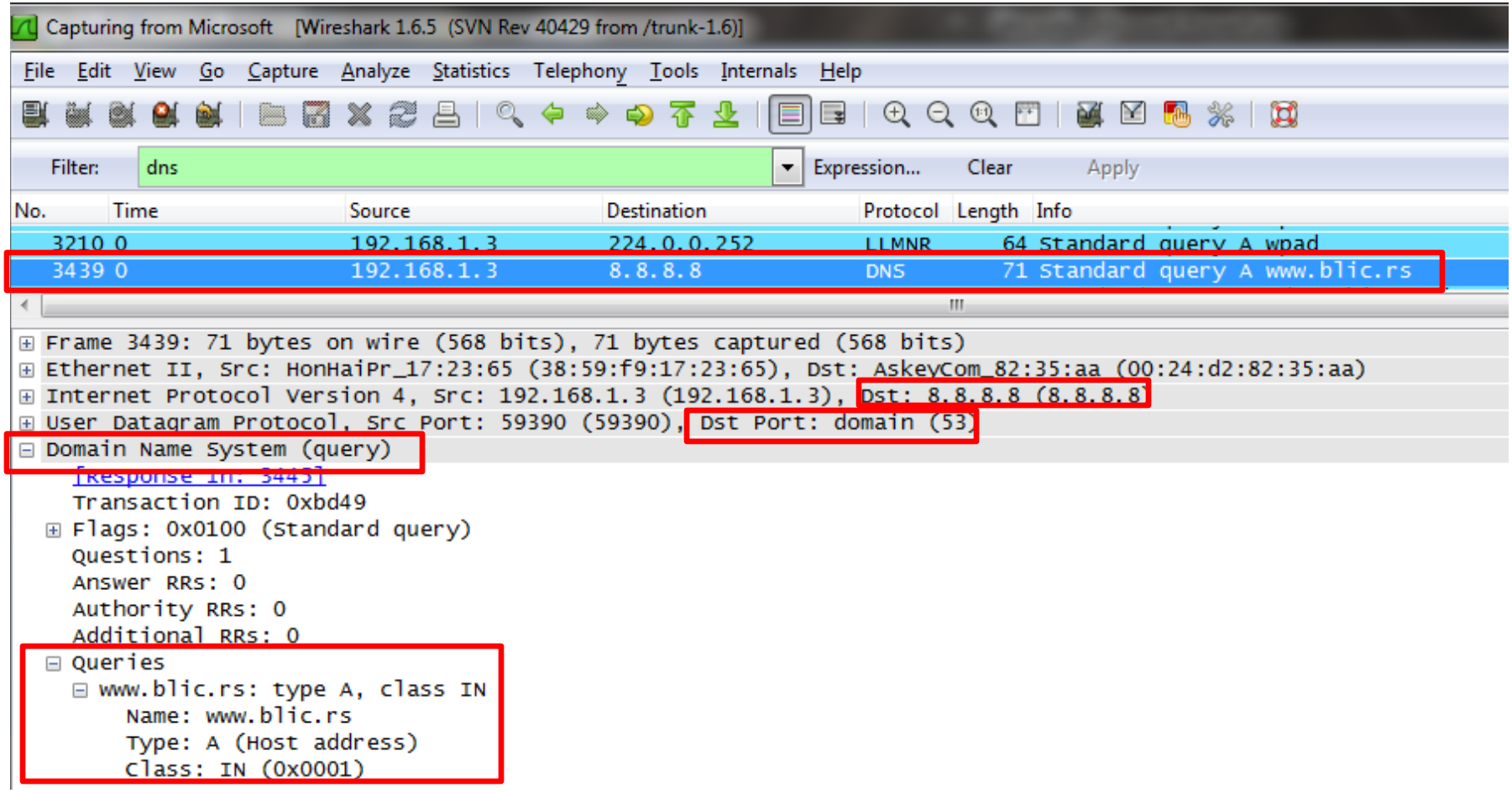

Computer ▸ Local Disk (C:) ▸ Windows ▸ System32 ▸ drivers ▸ etc
Organize
Include in library
Share with
Burn
New folder
Videos
Computer
Local Disk (C:)
Name
Date modified
Type
hosts
11.4.2012 1:05
File
lmhosts.sam
10.6.2009 23:00
SAM File
networks
10.6.2009 23:00
File
hosts - Notepad
File Edit Format View Help
Copyright (c) 1993-2009 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address shoul
be placed in the first column followed by the corresponding host
The IP address and the host name should be separated by at least
space.
#
Additionally, comments (such as these) may be inserted on indivi
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97   rhino.acme.com   # source server
38.25.63.10   x.acme.com   # x client host
localhost name resolution is handled within DNS itself.
127.0.0.1   localhost
::1   localhost
79.101.110.103   pretrazivac
127.0.0.1   localhost


dministrator: C:\Windows\system32\cmd.exe
Users\Korisnik>ipconfig /displaydns
dows IP Configuration
1.0.0.127.in-addr.arpa
Record Name . . . . . : 1.0.0.127.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : localhost
103.110.101.79.in-addr.arpa
Record Name . . . . . : 103.110.101.79.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : pretrazivac
pretrazivac
Record Name . . . . . : pretrazivac
Record Type . . . . . : 1
Time To Live . . . . . : 86400
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 79.101.110.103
pretrazivac
No records of type AAAA

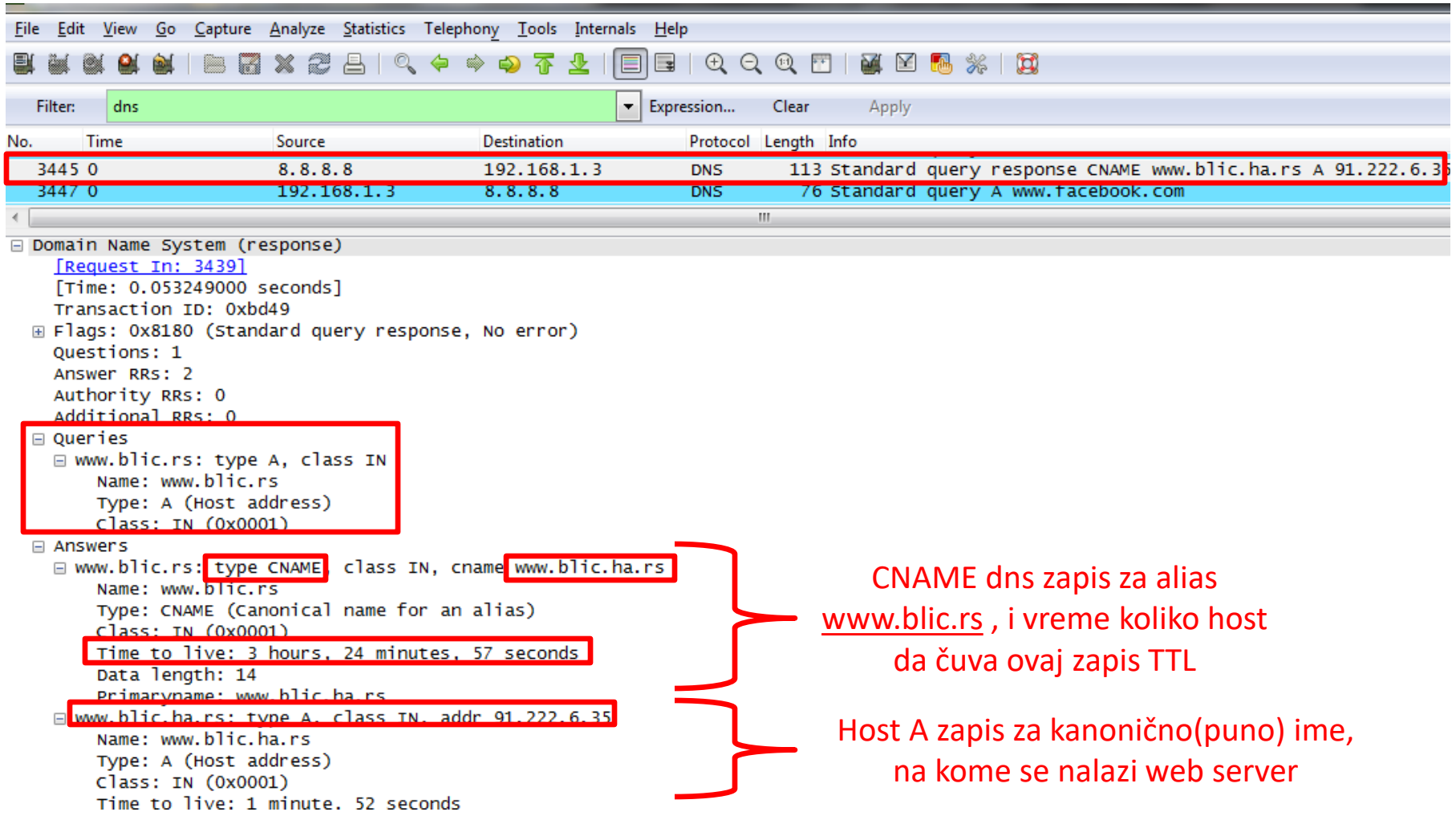
pretrazivac/
pretrazivac - Google
pretrazivac/ - Bing Search
pretrazivac
pretrazivaci interneta
pretrazivaci


Google
Serbia
Google Search
I'm Feeling Lucky
Google.rs offered in: српски

PRIMER DNS UPITA ZA WWW.BLIC.RS



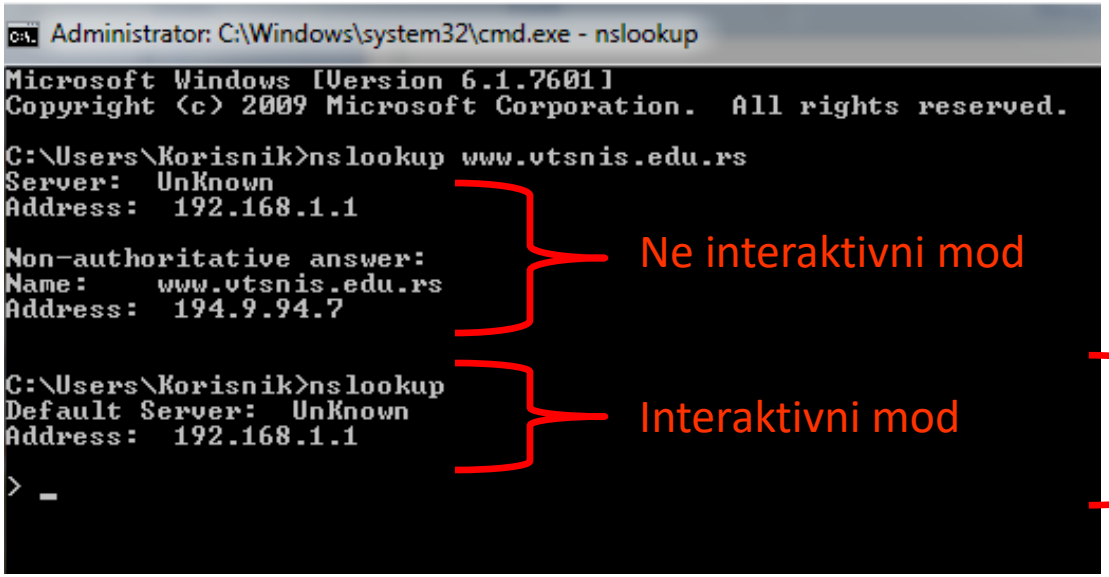
PRIMER DNS ODGOVORA ZA WWW.BLIC.RS UPIT



CNAME dns zapis za alias www.blic.rs , i vreme koliko host da čuva ovaj zapis TTL

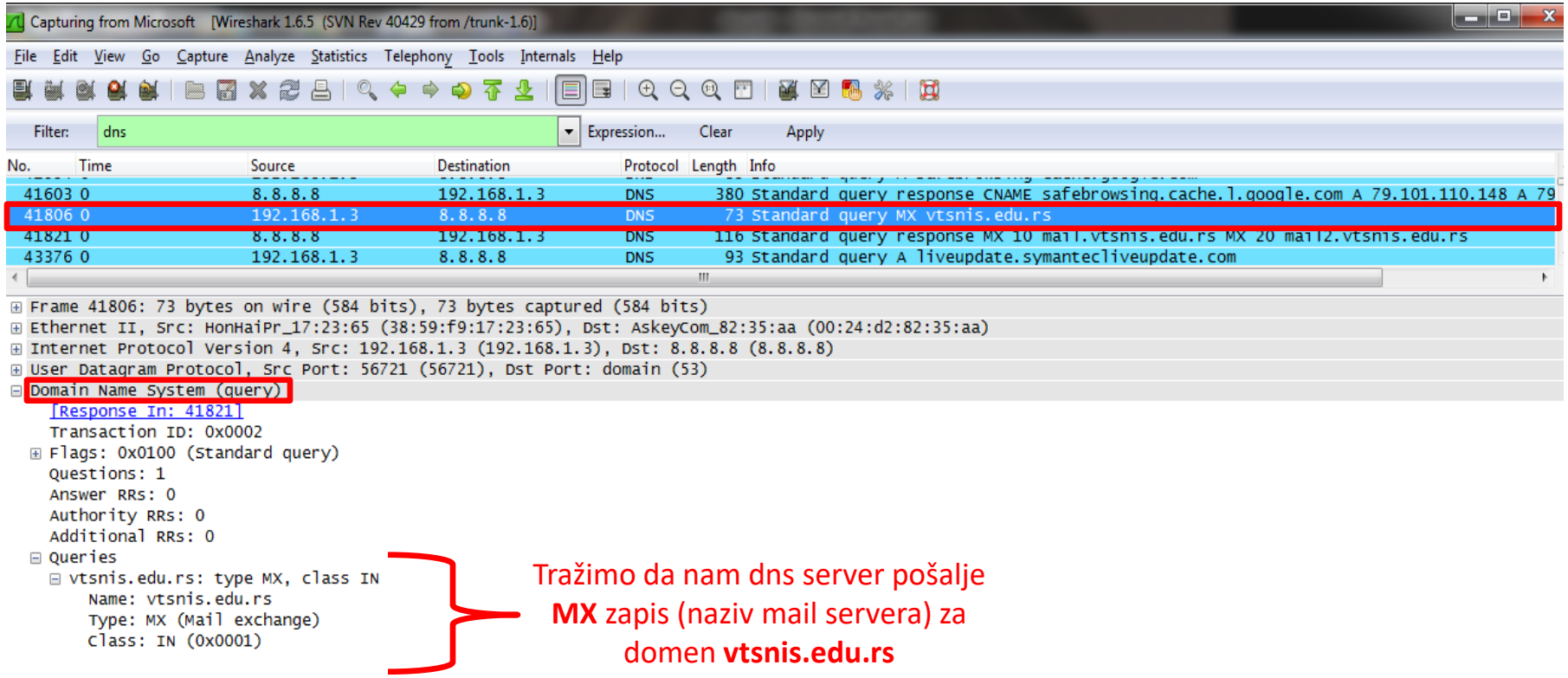
Host A zapis za kanonično(puno) ime, na kome se nalazi web server

DETALJNIJA PRETRAGA DNS ZAPISA
NSLOOKUP ALAT



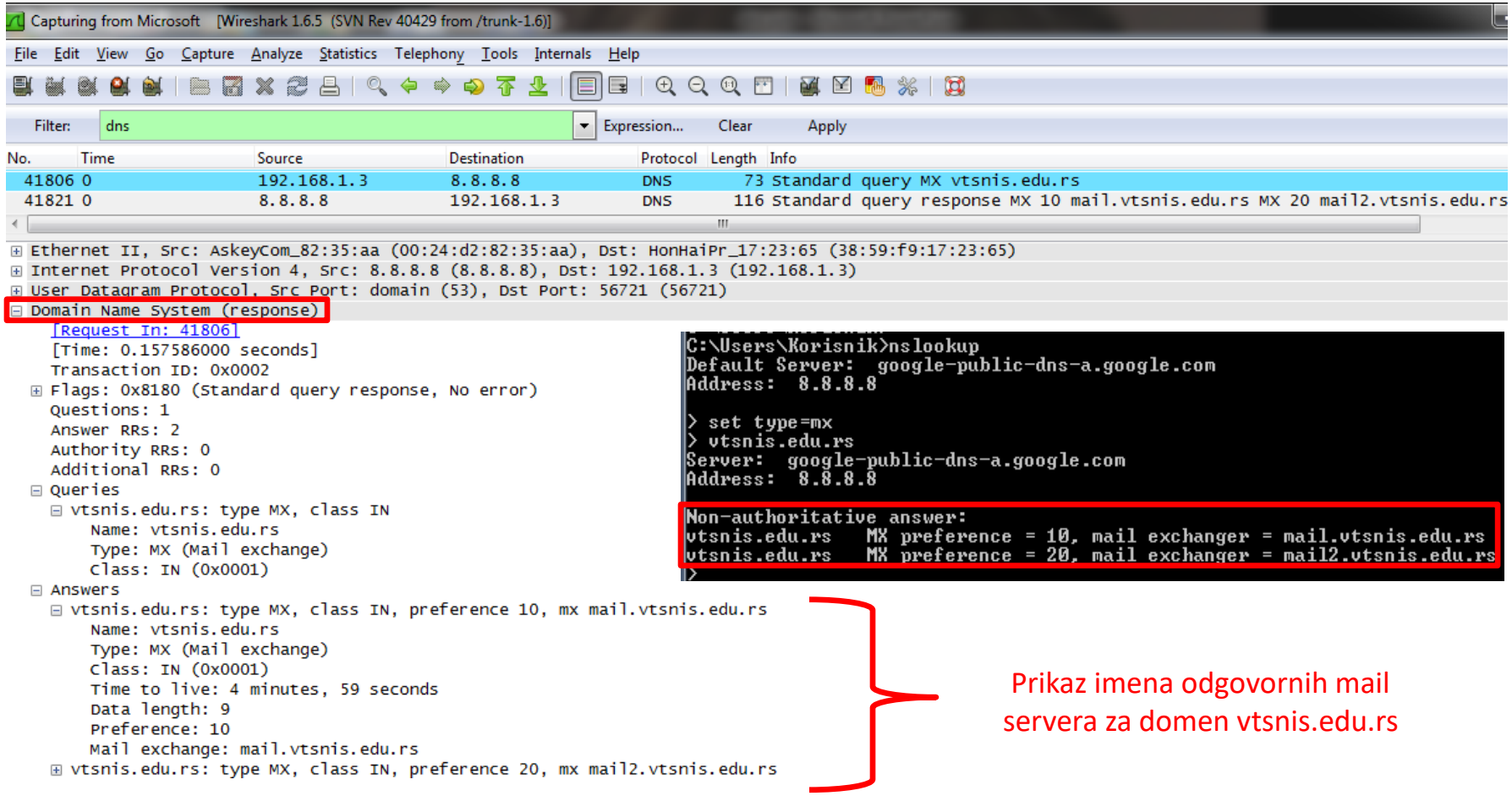
Obezbeđuje nam više mogućnosti u ispitivanju DNS servera

PRIMER MX DNS UPITA ZA VTSNIS.EDU.RS DOMEN



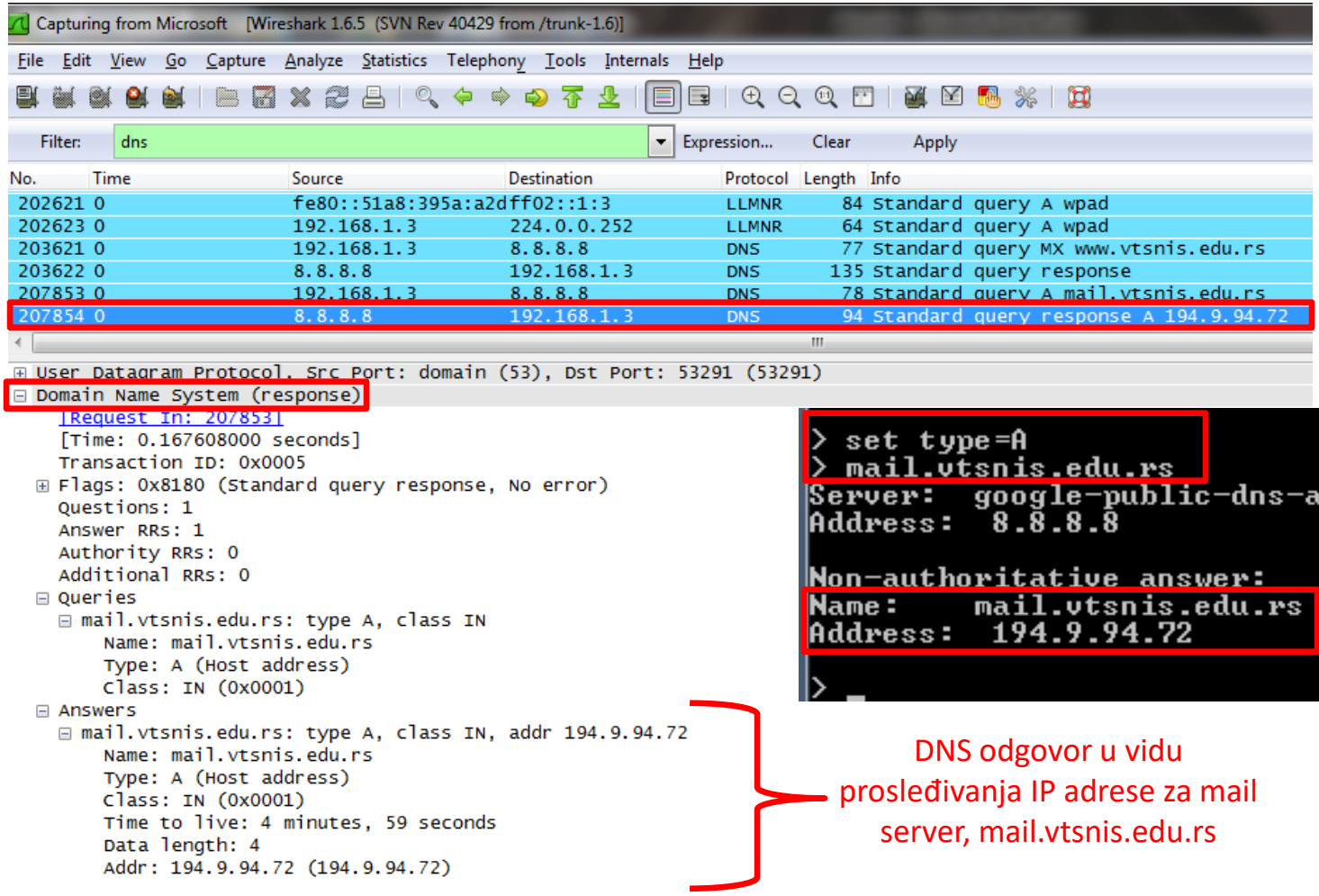
Tražimo da nam dns server pošalje **MX** zapis (naziv mail servera) za domen **vtsnis.edu.rs**

PRIMER MX DNS ODGOVORA ZA VTSNIS.EDU.RS DOMEN



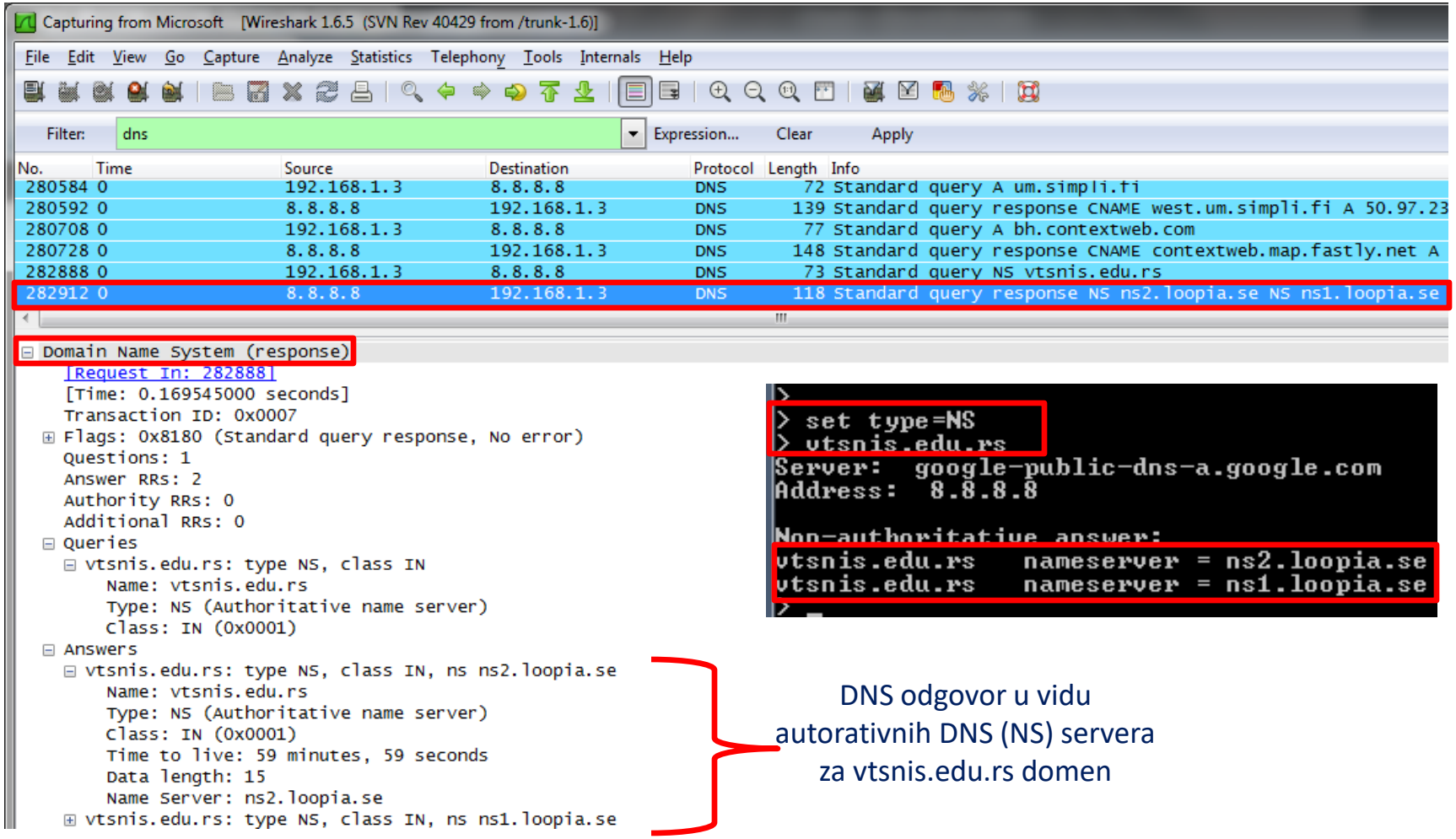
Prikaz imena odgovornih mail servera za domen vtsnis.edu.rs

PRIMER HOST DNS ODGOVORA ZA VTSNIS.EDU.RS



DNS odgovor u vidu prosleđivanja IP adrese za mail server, mail.vtsnis.edu.rs

PRIMER NS DNS ODGOVORA ZA VTSNIS.EDU.RS DOMEN



DNS odgovor u vidu autorativnih DNS (NS) servera za vtsnis.edu.rs domen

NSLOOKUP KOMANDE

```
C:\Users\Korisnik>nslookup www.vtsnis.edu.rs
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.vtsnis.edu.rs
Address:  194.9.94.7
```

DNS server kome je prosleđen upit nije autorativan za zonu vtsnis.edu.rs

```
C:\Users\Korisnik>nslookup www.vtsnis.edu.rs ns1.loopia.se
Server:  ns1.loopia.se
Address:  93.188.0.20

Name:    www.vtsnis.edu.rs
Address:  194.9.94.7


C:\Users\Korisnik>_
```

DNS server (ns1.loopia.se) kome je prosleđen upit je autorativan za zonu vtsnis.edu.rs

```
C:\Users\Korisnik>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> server ns1.loopia.se
Default Server:  ns1.loopia.se
Address:  93.188.0.20

>
```

Konekcija na DNS server sa nazivom ns1.loopia.se

PRIKAZ SVIH DNS ZAPISA ZA DOMEN VTSNIS.EDU.RS

```
>
> set type=any
> vtsnis.edu.rs
Server:  ns1.loopia.se
Address:  93.188.0.20

vtsnis.edu.rs   nameserver = ns1.loopia.se
vtsnis.edu.rs
        primary name server = ns1.loopia.se
        responsible mail addr = registry.loopia.se
        serial  = 1408579200
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
vtsnis.edu.rs   nameserver = ns2.loopia.se
vtsnis.edu.rs   internet address = 194.9.94.7
vtsnis.edu.rs   MX preference = 20, mail exchanger = mail2.vtsnis.edu.rs
vtsnis.edu.rs   MX preference = 10, mail exchanger = mail.vtsnis.edu.rs
ns1.loopia.se   internet address = 93.188.0.20
mail.vtsnis.edu.rs      internet address = 194.9.94.72
ns2.loopia.se   internet address = 93.188.0.21
mail2.vtsnis.edu.rs     internet address = 194.9.94.3
```