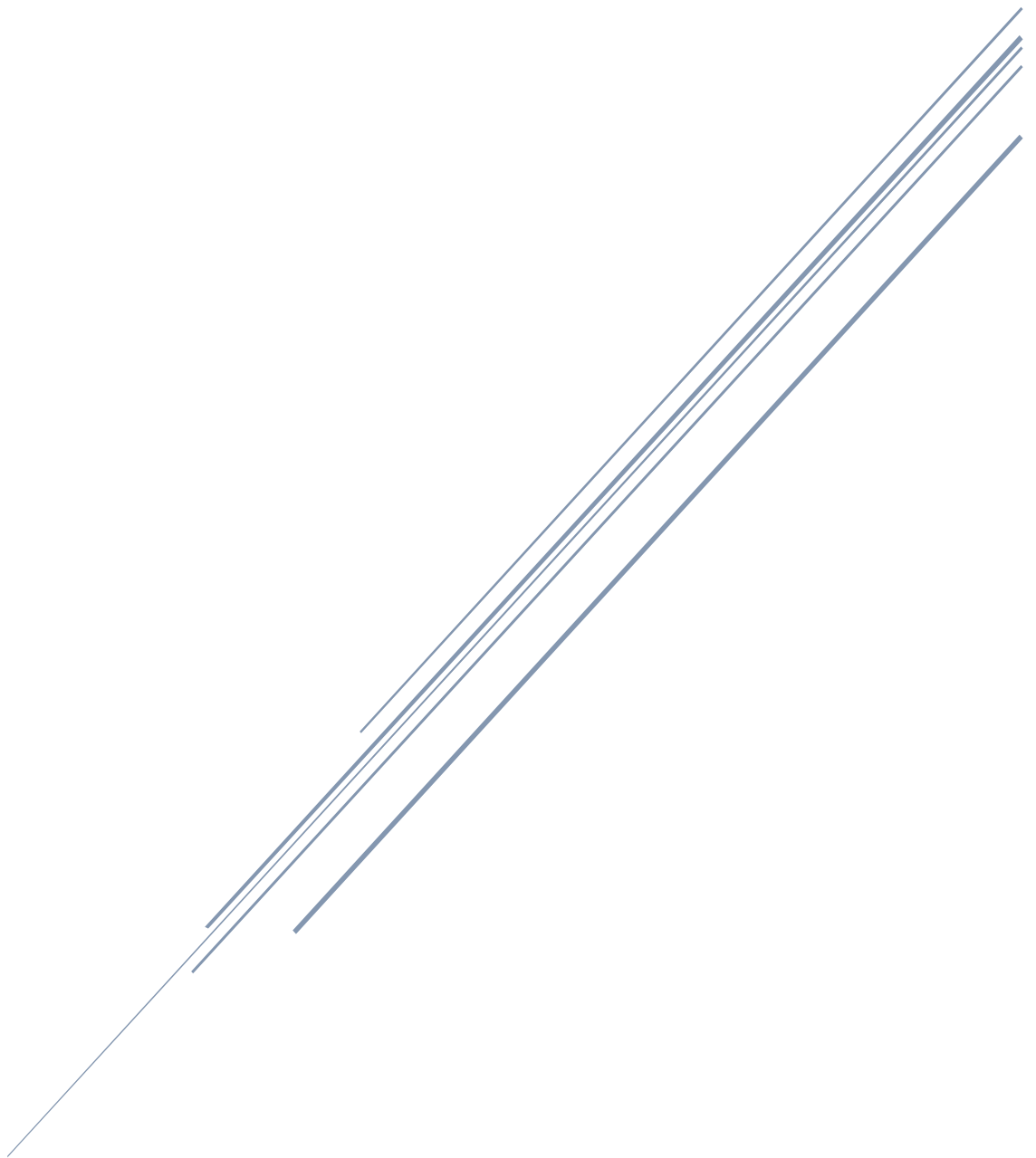


Analiza komunikacije između dva računala korištenjem Wireshark aplikacije



Sadržaj

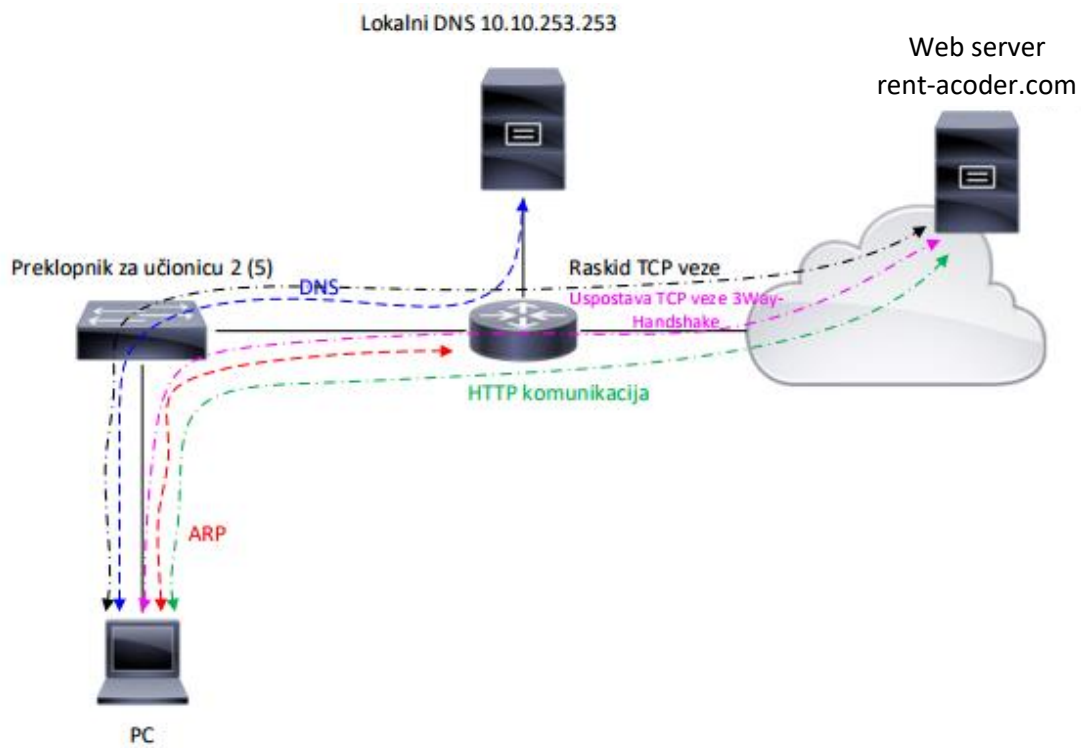
Uvod	2
DNS	3
ARP proces.....	3
THREE WAY HANDSHAKE	5
RASKID TCP-a	7
Appendix A: wireshark	8
Appendix B: provjere.....	9

Tablica slika:

Slika 1: Komunikacija dva računala	2
Slika 2: rent-acode.com u Chrome dns cache-u	3
Slika 3: ARP cache.....	3
Slika 4: ARP request za rent-acoder.com	4
Slika 5: ARP reply za rent-acode.com	4
Slika 6: Three Way Handshake	5
Slika 7: wireshark 3way handshake za rent-acode.com.....	5
Slika 8: wireshark HTTP request	5
Slika 9: wireshark praćenje streama.....	6
Slika 10: web stranica rent-acoder.com	6
Slika 11: zatvaranje tcp konekcije	7
Slika 12: Wireshark; raskid TCP-a	7

Uvod

Za primjer u analizi ću koristiti adresu <https://www.rent-acoder.com/>

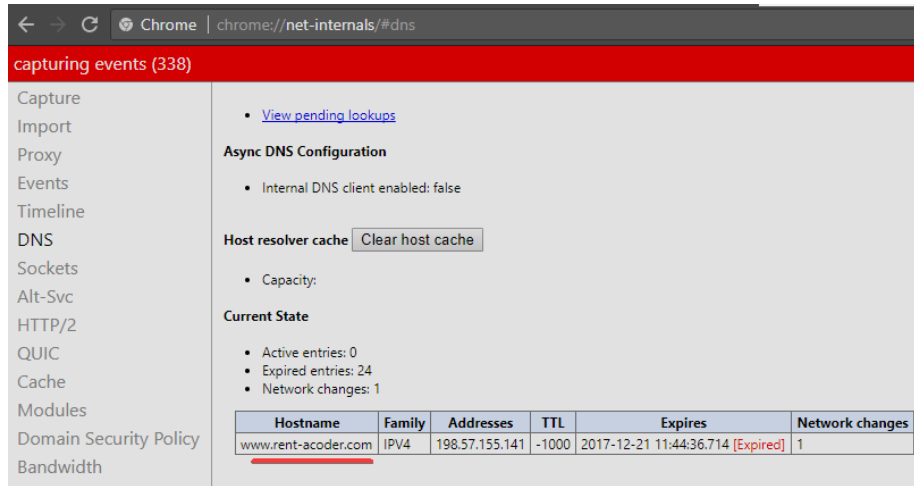


Slika 1: Komunikacija dva računala

Slika 1 je grafički prikaz komunikacije između dva računala koju ću analizirati u ovom dokumentu.

DNS

U trenutku stiskanja entera nakon upisane adrese stranice browser provjerava postoji li domena u njegovom cache-u. U slučaju Google Chroma cache možemo vidjeti na adresi `chrome://net-internals/#dns`



Slika 2: `rent-acode.com` u Chrome dns cache-u

Kako bi mogao napraviti što detaljniju analizu brisati ću cacheve prije svakog slijedećeg koraka. U slučaju chroma cache praznimo pristiskom na „Clear host cache“.

Nakon provjere internog cachea browser poziva odgovarajuću funkciju operativnog sistema (`gethostbyname`) kako bi provjerio postoji li adresa u hosts datoteci, ukoliko ona ne postoji zahtjev se šalje dalje na DNS server određen u postavkama računala i mreže.

Ako se DNS nalazi na istom subnetu `gethostbyname` prati dalje ARP proces do dns servera. Ako je DNS na drukčijem subnetu `gethostbyname` prati ARP proces do gateway-a.

ARP proces

Kako bi poslalo ARP broadcast naše računalo mora znati destinacijski IP te MAC adresu interface-a pomoću kojeg će poslati sam broadcast. Prvi korak je provjera ARP cachea te ako postoji zapis za traženi IP računalo će znati koji MAC koristiti. ARP cache listamo komandom `arp -a`, a brisemo `arp -d`.

```
C:\windows\system32>arp -a

Interface: 10.10.2.175 --- 0x7
 Internet Address      Physical Address      Type
 10.10.2.254           14-58-d0-af-31-c0    dynamic
 224.0.0.22            01-00-5e-00-00-16    static
 239.255.255.250      01-00-5e-7f-ff-fa    static

C:\windows\system32>arp -d

C:\windows\system32>
```

Slika 3: ARP cache

Ukoliko tražena stavka nije u ARP tablici odašilje se **ARP request** što možemo vidjeti u wiresharku. Korištenje wiresharka je opisano na kraju dokumenta.

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Micro-St_d5:c1:8c (44:8a:5b:d5:c1:8c)
  Sender IP address: 10.10.2.175
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.10.2.182
```

Slika 4: ARP request za rent-acoder.com

Ako je računalo spojeno direktno na ruter on odgovara sa **ARP reply**.

Ako je računalo spojeno na HUB on će broadcastati ARP na sve ostale portove. Ako je router na jednom od njih odgovoriti će sa ARP reply.

Ako smo spojeni na switch on će provjeriti svoju lokalnu CAM/MAC tablicu kako bi provjerio koji port ima traženi MAC, ukoliko ga nema proslijediti će ARP request na sve ostale portove. Ako postoji navod u tablici ARP request će biti poslan na taj port, ako je router tu odgovotiti će sa ARP reply.

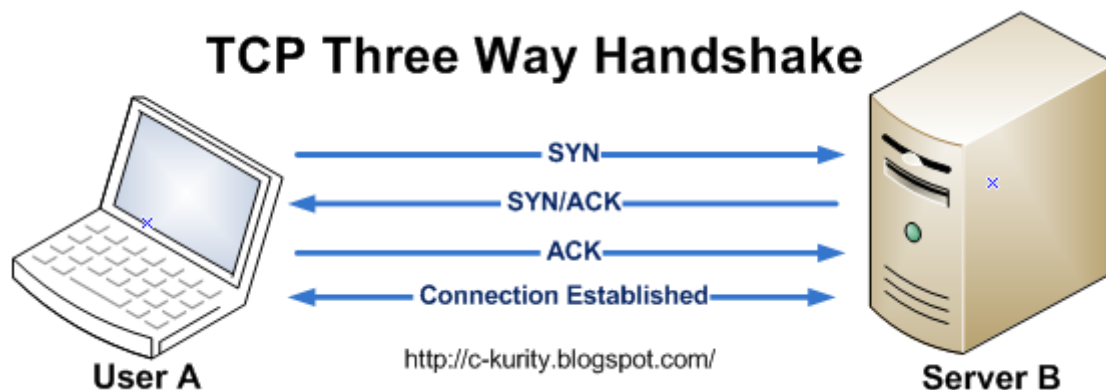
```
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Micro-St_ce:6e:da (44:8a:5b:ce:6e:da)
  Sender IP address: 10.10.2.182
  Target MAC address: Micro-St_d5:c1:8c (44:8a:5b:d5:c1:8c)
  Target IP address: 10.10.2.175
```

Slika 5: ARP reply za rent-acode.com

Sada kad računalo ima IP adresu našeg DNS servera ili default gateway-a može nastaviti DNS proces: otvara se port 53 kako bi se poslao UDP request DNS serveru, ukoliko lokalni/ISP-ov DNS nema odgovor započinje rekurzivno traženje koje se kreće kroz listu DNS servera dok se ne pronađe traženi odgovor.

THREE WAY HANDSHAKE

Nakon što je browser dobio IP adresu destinacijskog servera šalje zahtjev operativnom sistemu sa tim IPem i odgovarajućim portom (80 za http, 443 za https) kako bi se otvorio TCP socket stream.



Slika 6: Three Way Handshake

Klijent šalje SYN serveru na što mu server odgovara sa SYN i ACK paketom kojim potvrđuje primitak klijentovog SYN-a. Klijent potvrđuje serverov SYN svojim ACK-om. To možemo vidjeti u wiresharku primjenom tcp filtera.

The image shows a Wireshark packet capture for the IP address 54.85.159.9. The table below summarizes the captured packets:

No.	Time	Source	Destination	Destination	Destination	Protocol	Info
120	1.984383	10.10.2.175	198.57.155.141	14:58:d0:af:31:c0	80	TCP	50412 → 80 [SYN] Seq=6
121	1.984589	198.57.155.141	10.10.2.175	44:8a:5b:d5:c1:8c	50412	TCP	80 → 50412 [SYN, ACK] S
122	1.984629	10.10.2.175	198.57.155.141	14:58:d0:af:31:c0	80	TCP	50412 → 80 [ACK] Seq=1
123	1.984733	10.10.2.175	198.57.155.141	14:58:d0:af:31:c0	80	HTTP	GET / HTTP/1.1

Slika 7: wireshark 3way handshake za rent-acoder.com

Nakon uspostave komunikacije klijent šalje serveru HTTP request što također možemo jasno vidjeti:

```
▼ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
  Host: rent-acoder.com\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
  Upgrade-Insecure-Requests: 1\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: hr-HR,hr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Full request URI: http://rent-acoder.com/]
  [HTTP request 1/1]
  [Response in frame: 137]
```

Slika 8: wireshark HTTP request

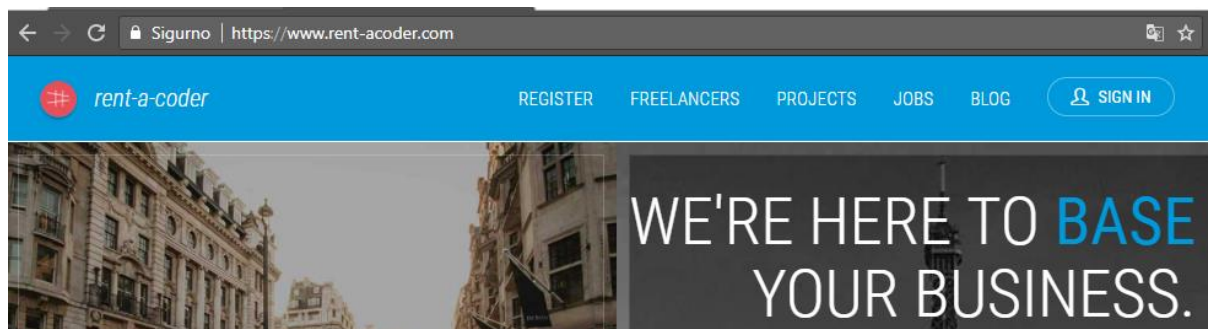
\n označuje newline čime browser obznanjuje kraj sadržaja requesta. Obično će server odgovoriti sa 200 i serveritai stranicu no u ovom slučaju odgovara kodom 302 što je redirect. Detalje možemo vidjeti prateći stream.

```
HTTP/1.1 302 Found
Date: Thu, 21 Dec 2017 11:08:27 GMT
Server: Apache
Location: https://rent-acoder.com/
Cache-Control: max-age=0
Expires: Thu, 21 Dec 2017 11:08:27 GMT
Content-Length: 208
Keep-Alive: timeout=2, max=102
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://rent-acoder.com/">here</a>.</p>
</body></html>
```

Slika 9: wireshark praćenje streama

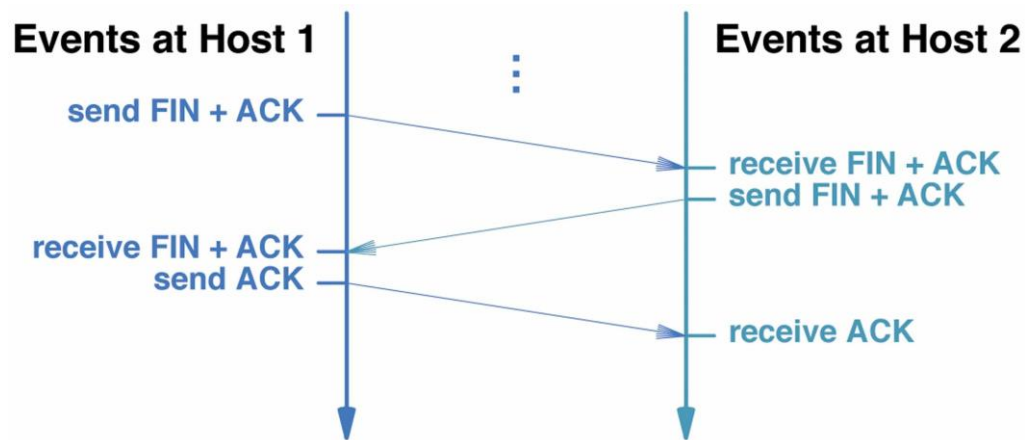
I napokon unutar browsera vidimo traženu stranicu.



Slika 10: web stranica rent-acoder.com

RASKID TCP-a

Nakon zatvaranje stranice u browseru moramo zatvoriti i tcp stream.



Slika 11: zatvaranje tcp konekcije

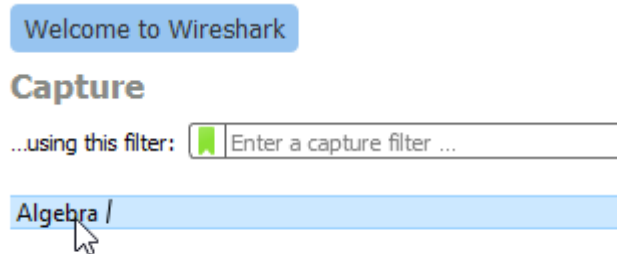
Kako bi se zatvorila konekcija browser šalje zahtjev FIN/ACK, server vraća FIN i potvrđuje primitak klijentovog fina svojim ACKom, klijent potvrđuje serverov FIN još jednim ACK-om i konekcija je zatvorena.

402	4.327296	10.10.2.175	198.57.155.141	14:58:d0:af:31:c0	80	TCP	50412 → 80	[ACK] Seq=42
1150	5.592085	10.10.2.175	198.57.155.141	14:58:d0:af:31:c0	80	TCP	50412 → 80	[FIN, ACK] Seq=
1152	5.592395	198.57.155.141	10.10.2.175	44:8a:5b:d5:c1:8c	50412	TCP	80 → 50412	[ACK] Seq=58

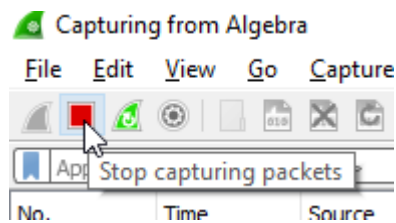
Slika 12: Wireshark; raskid TCP-a

Appendix A: wireshark

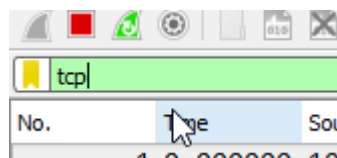
Wireshark je aplikacija za analizu prometa po mrežnoj kartici. Kako bi osigurali ispravan rad najbolje ju je pokrenuti kao administrator. Snimanje prometa započinjemo dvoklikom na zeljenu mrežnu karticu



Za zaustavljanje snimanja koristimo crveni kvadratić



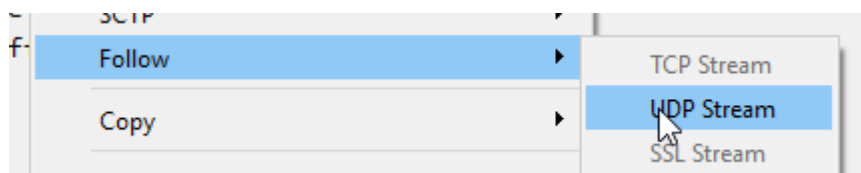
Kako bi se lakše orijentirali u hrpi dobivenih podataka mozemo koristiti filtre upisivanjem u traku



Ili klikanjem na kartice:

No.	Time	Source	Destination	Destination	Protocol	Info
1	0.000000	10...	ff:ff:ff:ff:ff:ff		NBNS	Name query NB TEST-ILI
			33:33:00:00:00:fb		MDNS	Standard query 0x0000

Nadalje mozemo pratiti kretanje određenog streama tako da desnim klikom odaberemo stavku -> follow -> [udp/tcp] stream



Appendix B: provjere

Svoju ip adresu mozemo dobiti komandom ipconfig iz CMD-a.

```
C:\Users\Cisco>ipconfig

Windows IP Configuration

Ethernet adapter Algebra:

    Connection-specific DNS Suffix  . : ucione.local
    Link-local IPv6 Address . . . . . : fe80::4d3:8165:241a:281e%7
    IPv4 Address. . . . . : 10.10.2.175
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.2.254
```

Komandom nslookup mozemo provjeriti na kojim IP adresama se nalazi server domene.

```
C:\Users\Cisco>nslookup rent-acoder.com
Server: ili-nastava-01.ucione.local
Address: 10.10.253.253

Non-authoritative answer:
Name:   rent-acoder.com
Address: 198.57.155.141
```

Komandom ping mozemo provjeriti dali je server online:

```
C:\Users\Cisco>ping 198.57.155.141

Pinging 198.57.155.141 with 32 bytes of data:
Reply from 198.57.155.141: bytes=32 time=182ms TTL=33
Reply from 198.57.155.141: bytes=32 time=182ms TTL=33
```

Komandom netstat mozemo vidjeti trenutno aktivne konekcije:

```
C:\Users\Cisco>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    10.10.2.175:49673       db5sch101101145:https  ESTABLISHED
TCP    10.10.2.175:49679       db5sch101101618:https  ESTABLISHED
TCP    10.10.2.175:49691       40.113.87.220:https    CLOSE_WAIT
TCP    10.10.2.175:49692       40.113.87.220:https    CLOSE_WAIT
TCP    10.10.2.175:50569       2.17.7.72:http         TIME_WAIT
TCP    10.10.2.175:50570       52.109.88.39:https     ESTABLISHED
```