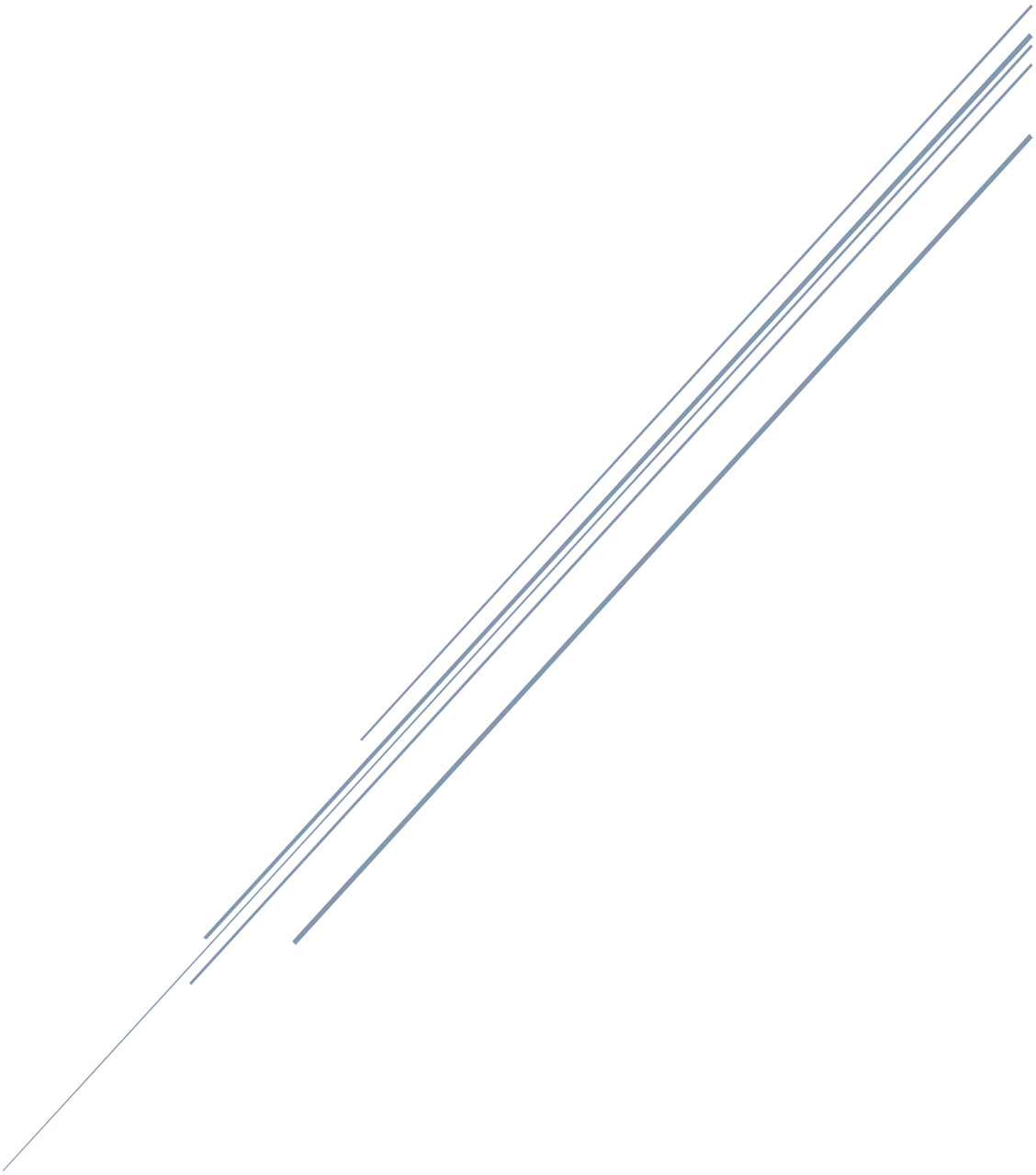
Analiza komunikacije između dva računala korištenjem Wireshark aplikacije



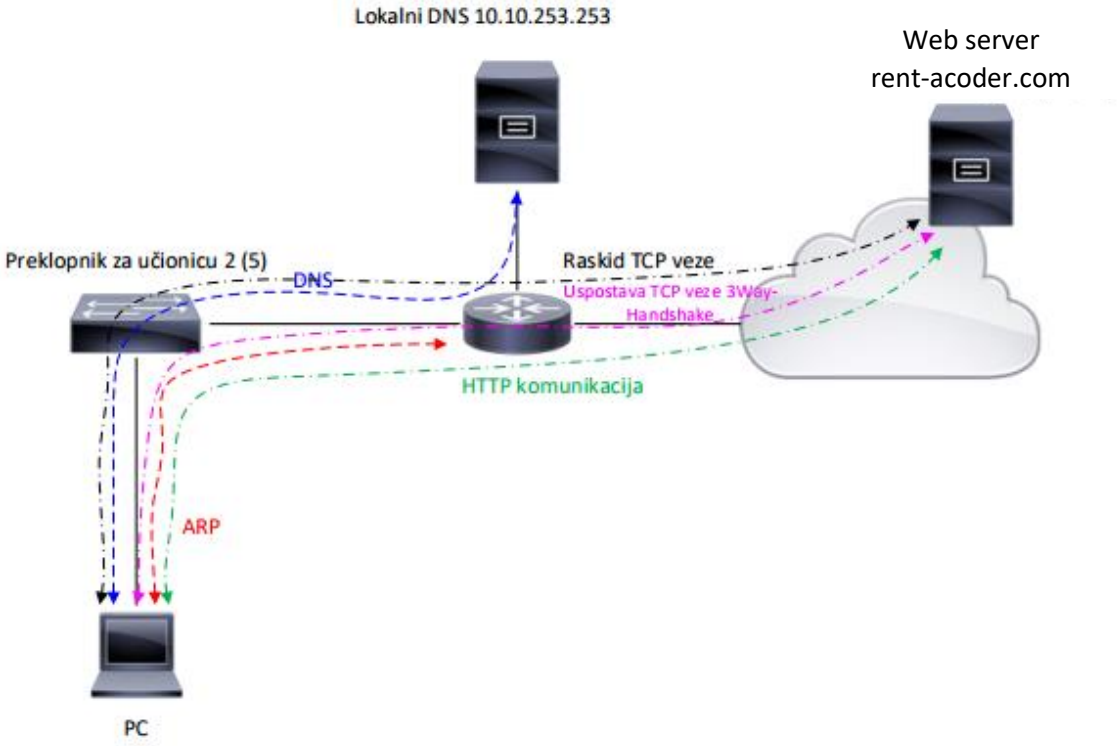
Tomislav Kućar

Sadržaj

Tablica slika:

Uvod

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

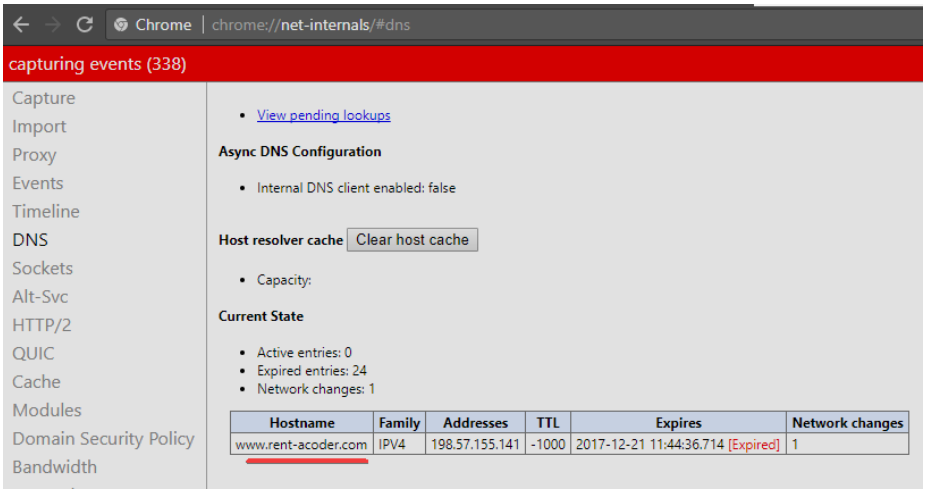


Slika 1: Komunikacija dva računala

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 nejgovom 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 slijedeceg koraka. U slučaju chroma cache praznimo pristiskom na „Clear host cache“.

Nakon provjere internog cachea browser poziva odgovarajuču 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.

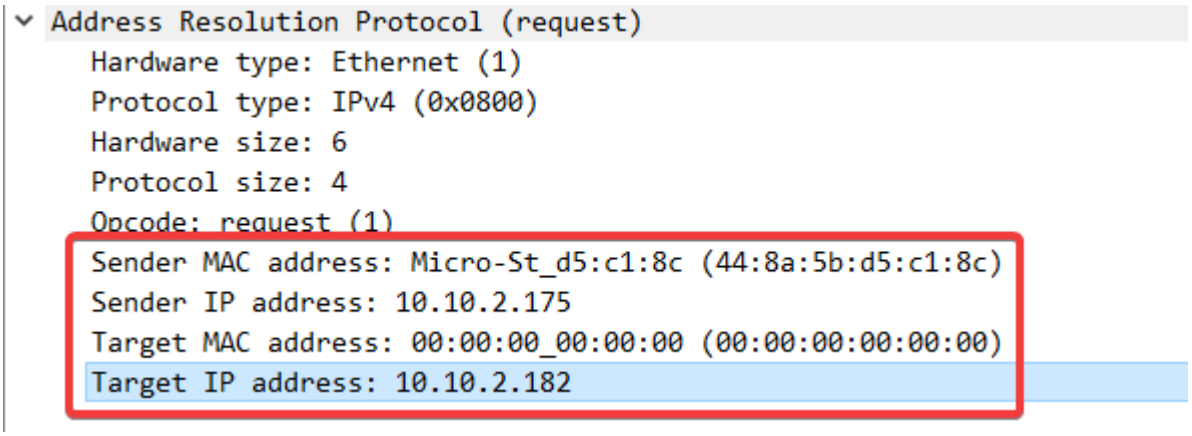
ARP proces

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 ce znati koji MAC koristiti. ARP cache listamo komandom arp –a, a brisemo apr –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.

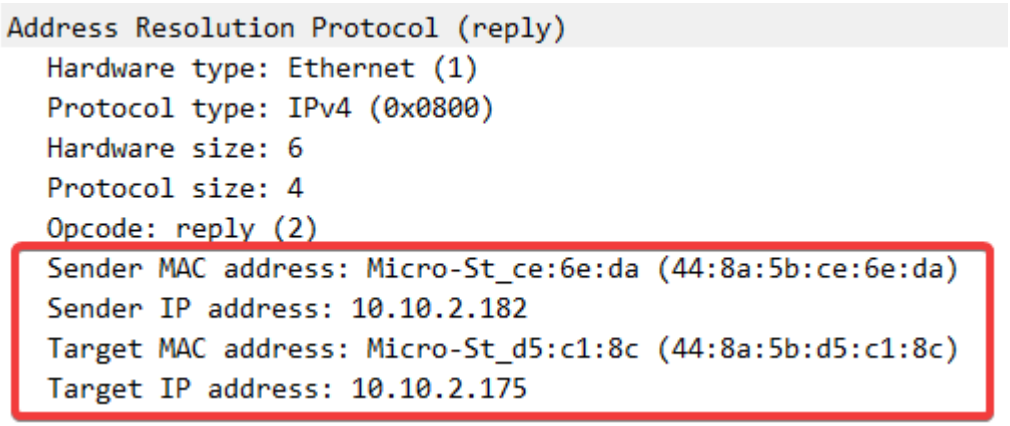


Slika 4: ARP request za rent-acoder.com

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 ce 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 ce biti poslan na taj port, ako je router tu odgovotiti će sa ARP reply.

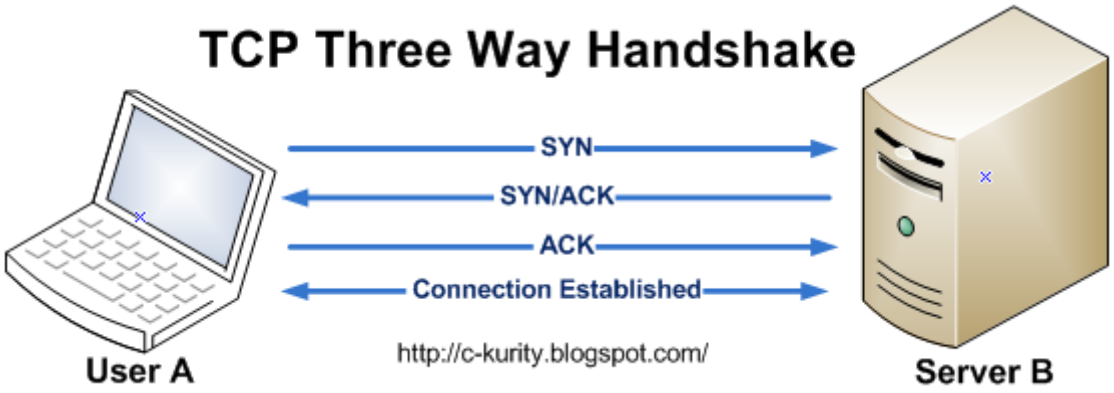


Slika 5: ARP reply za rent-acode.com

Sada kad računalo ima IP aresu 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 rekorzivno traženje koje se kreće kroz listu DNS serevra dok se ne pronađe traženi odgovor.

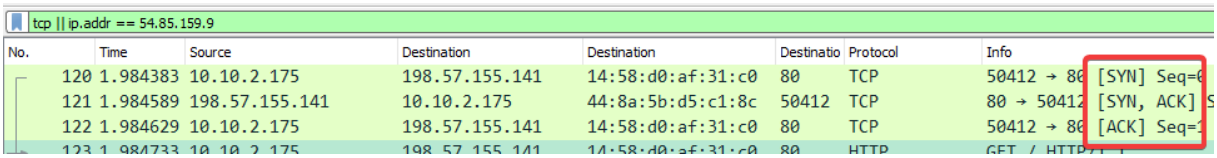
THREE WAY HANDSHAKE

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.



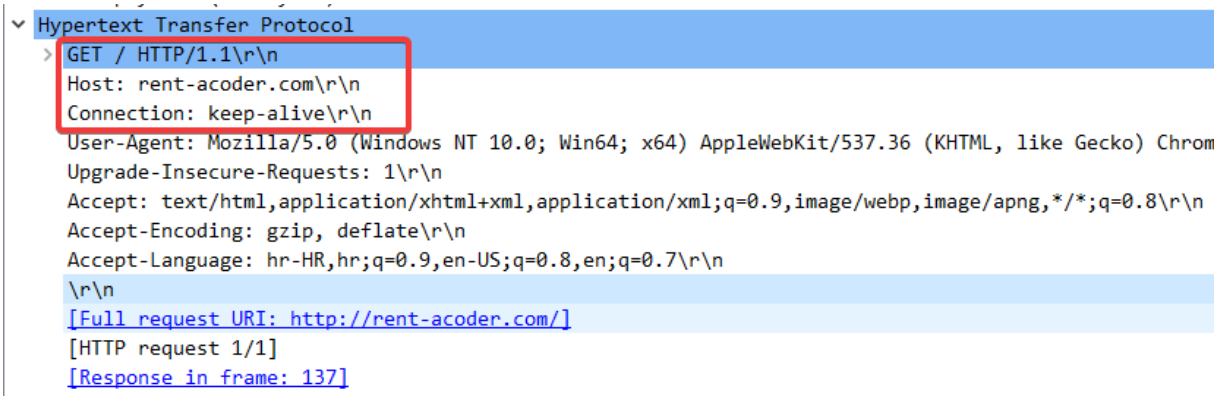
Slika 6: Three Way Handshake

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.



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

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



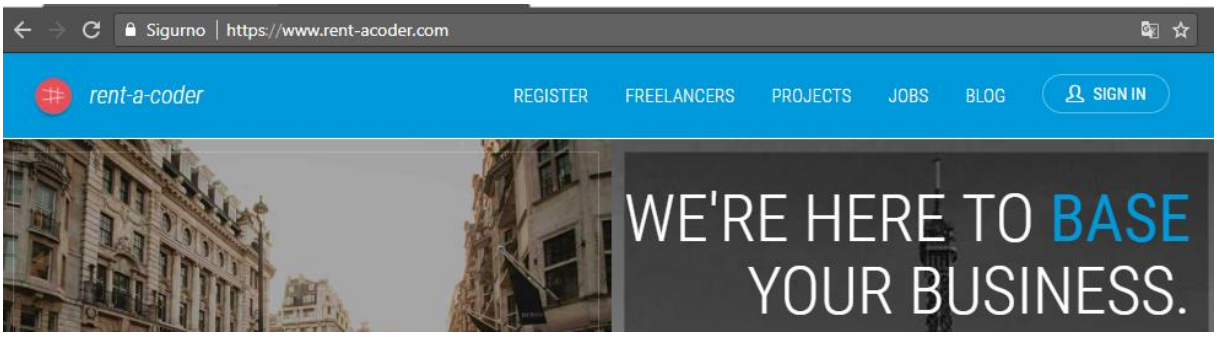
Slika 8: wireshark HTTP request

\n označuje newline čime browser obzanjuje kraj sadržaja requesta. Obično će server odgovoriti sa 200 i serveritai stranicu no u ovom slucaju 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

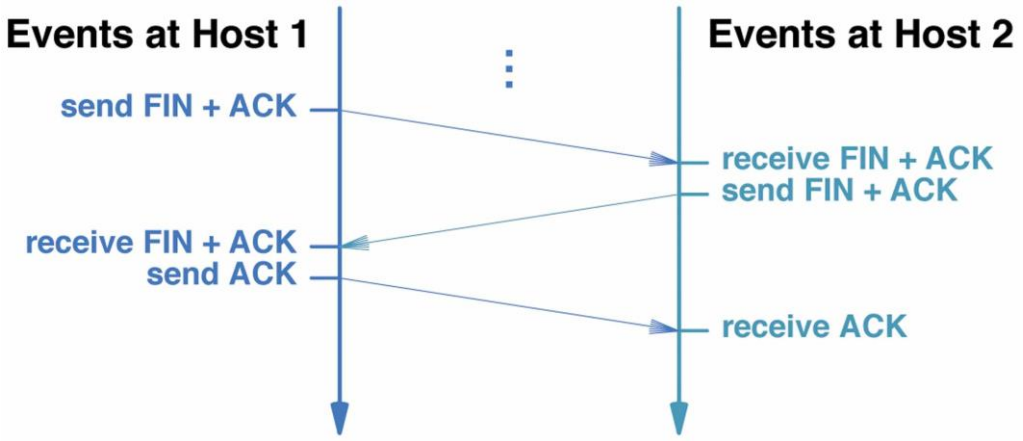
I napokon unutar browsera vidimo traženu stranicu.



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

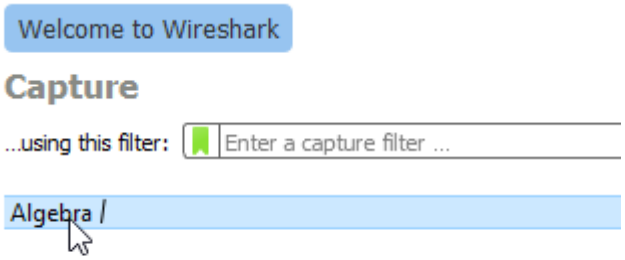
Kako bi se zatvorila konekcija browser šalje zahtjev FIN/ACK, server vraća FIN i potvrđuje primitak klijentovog fina svojim ACKom, klijent potvrđuje serverov FIN još jednim ACK-om i konekcija je zatvorena.

```
  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] S
 1152 5.592395 198.57.155.141 10.10.2.175      44:8a:5b:d5:c1:8c  50412  TCP    80 → 50412 [ACK] Seq=52
```

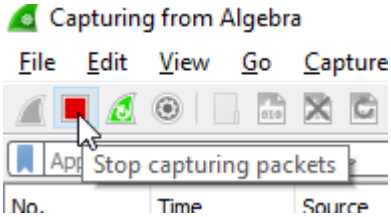
Slika 12: Wireshark; raskid TCP-a

Appendix A: wireshark

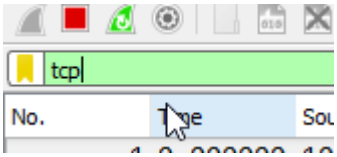
Wireshark je aplikacija za analizu prometa po mrežnoj kartici. Kako bi osigurali ispravan rad najbolje ju je pokrenuti kao administrator. Snimanje prometa započinjemo dvoklikom na zeljenu mreznu karticu



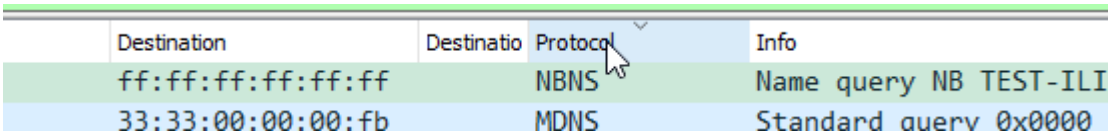
Za zaustavljanje snimanja koristimo crveni kvadratić



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



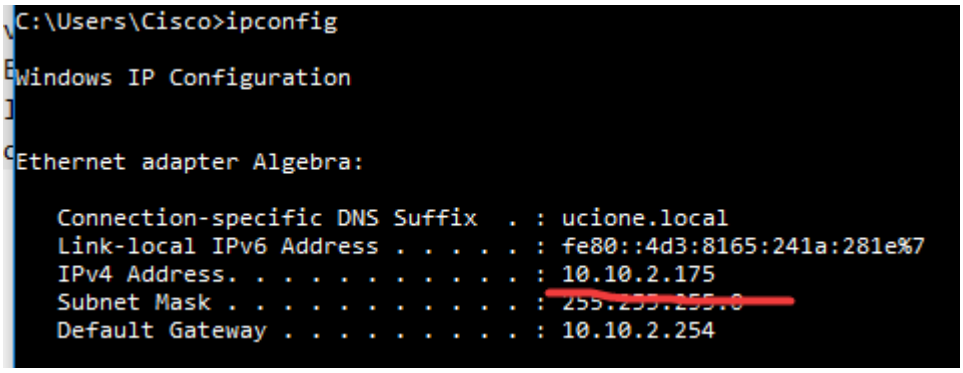
Ili klikanjem na kartice:



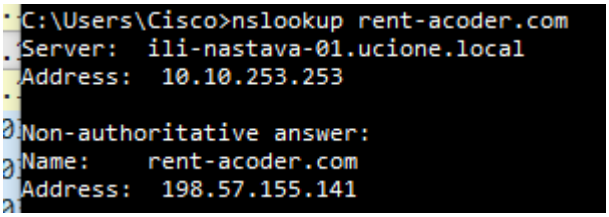
Nadalje mozemo pratiti kretanje određenog streama tako da desnim klikom odaberemo stavku -> follow -> [udp/tcp] stream

Appendix B: provjere

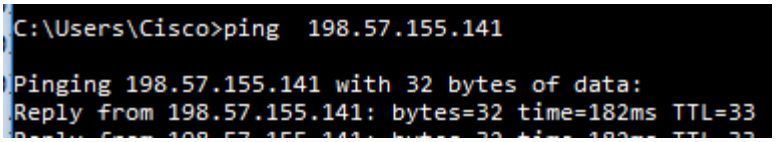
Svoju ip adresu mozemo dobiti komandom ipconfig iz CMD-a.



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



Komandom ping mozemo provjeriti dali je server online:



Komandom netstat mozemo vidjeti trenutno aktivne konekcije: