VJEZBA 2: Osnovna analiza mrežnog prometa
Jan Šotić, David Rudar

PRIPREMA:

1) ARP je komunikacijski protokol kojim se dobiva fizicka adresa na lokalnoj mrezi iz poznate mrezne adrese.
2) ICMP je komunikacijski protokl koji je ugradjen u svaki IP modul da bi omogucio mreznim prolazima ili racunalima slanje kontrolnih poruka o greskama. Zaduzen je samo za prijavljivanje gresaka, ali ne ya njihovo ispravljanje.
3) Ping naredba je naredba naredbene naredbe koja se koristi za testiranje sposobnosti izvornog računala da dosegne određeno odredišno računalo. Ping naredba obično se koristi kao jednostavan način da se potvrdi da računalo može komunicirati preko mreže s drugim računalom ili mrežnim uređajem.

IZVOĐENJE VJEŽBE:

1. ...

2. ...

3. a) Uhvatilo je 25 Okvira kroz 25 redaka rada Wiresharka.

   b) Oznake protokola su : ARP, NBNS, MDNS, LLMNR.

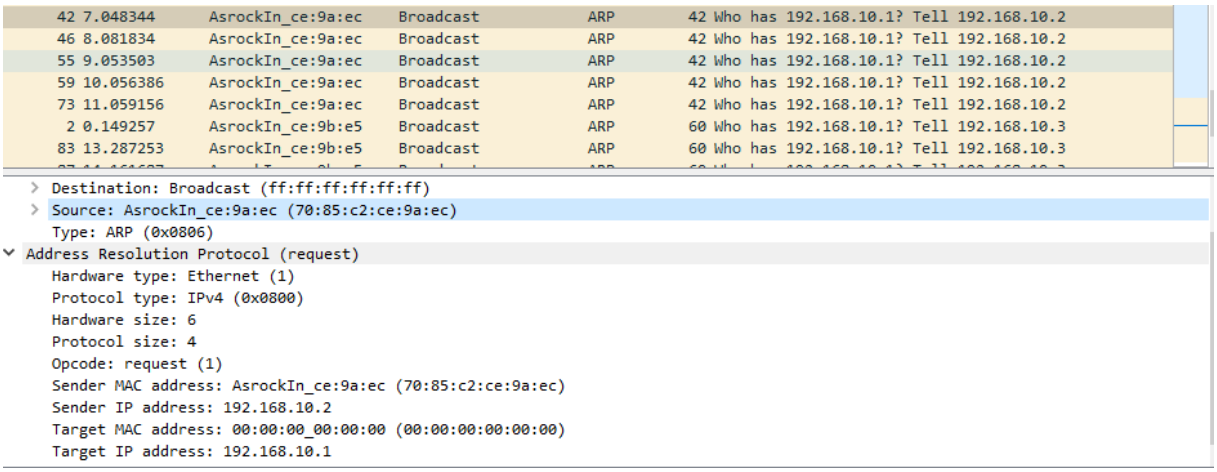
   c) ARP- pise u pripremi

   NBNS- protokol koji postoji da riješava imena na mreži bez potrebe za korištenje lokalnih host fileova ili DNS-a.

   MDNS- razrješava imena hostova u IP adrese unutar malih mreža koje ne uključuju lokalni poslužitelji naziva

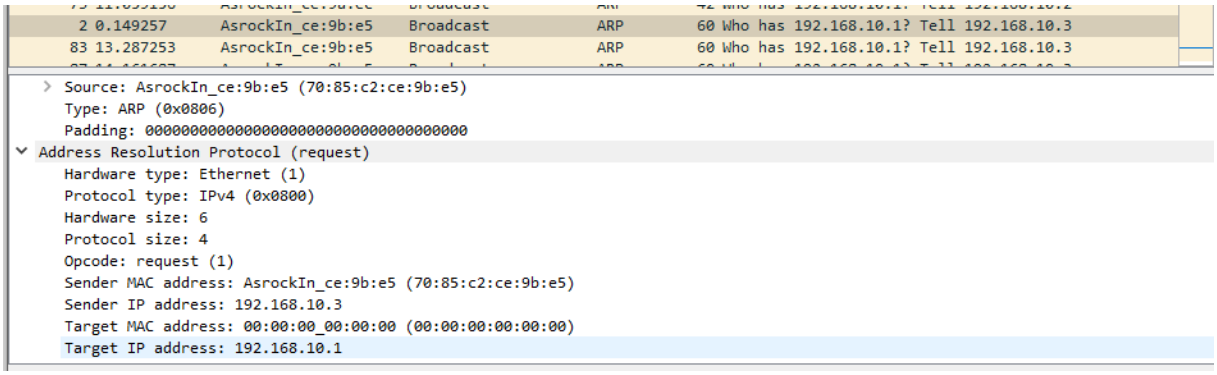
   LLMNR- protokol temeljen na formatu paketa Domain Name System koji omogučuje i IPv4 i IPv6 hostovima da izvrše razrješenje imena za hostove na istoj lokalnoj vezi.

d) ARP REQUEST:



odredišna IP adresa: 192.168.10.1
ishodišna IP adresa: 192.168.10.2
odredišna MAC adresa: 00:00:00:00:00:00
ishodišna MAC adresa: 70:85:c2:ce:9a:ec

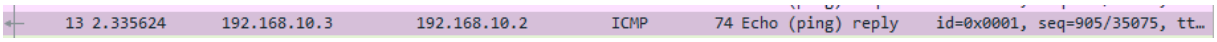
ARP REPLY:



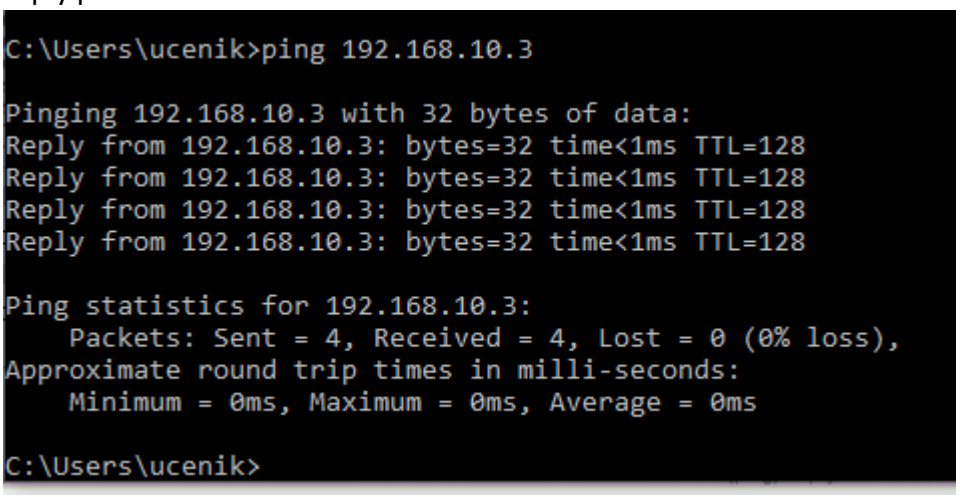
ishodišna IP adresa: 192.168.10.3
odredišna IP adresa: 192.168.10.1
ishodišna MAC adresa: 70:85:c2:ce:9b:e5
odredišna MAC adresa: 00:00:00:00:00:00

e) ff:ff:ff:ff:ff:ff zato što je to brodcast adresa preko koje se šalje ARP zahtjev svim uređajima u mreži

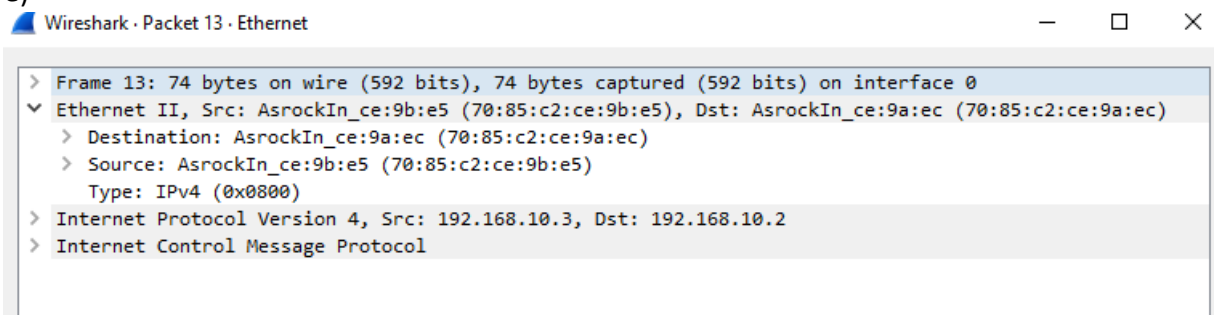
4. a)



ICMP Echo: 74
reply paketa: 4

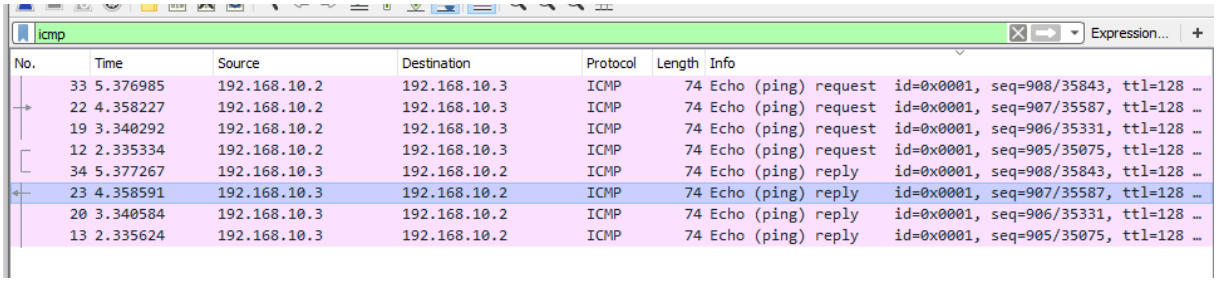


b) Protokol koji pokreće naredba ping je ICMP
c) ICMP protokol je sastavni dio IP protokola
d) U Ethernet okvir
e)



Polazišna IP adresa je: 192.168.10.3
f) Odredišna IP adresa je: 192.168.10.2
g) MAC adresa polazišnog računala je 70:85:c2:ce:9b:35
h) MAC adresa odredišnog računala je 70:85:c2:ce:9a:ec
i) 0x0800 – indicira ARP datagram
j) IP adresa: 60 bitova
MAC adresa: 48 bitova
k) 60 bitova
l) 20 bitova

m)

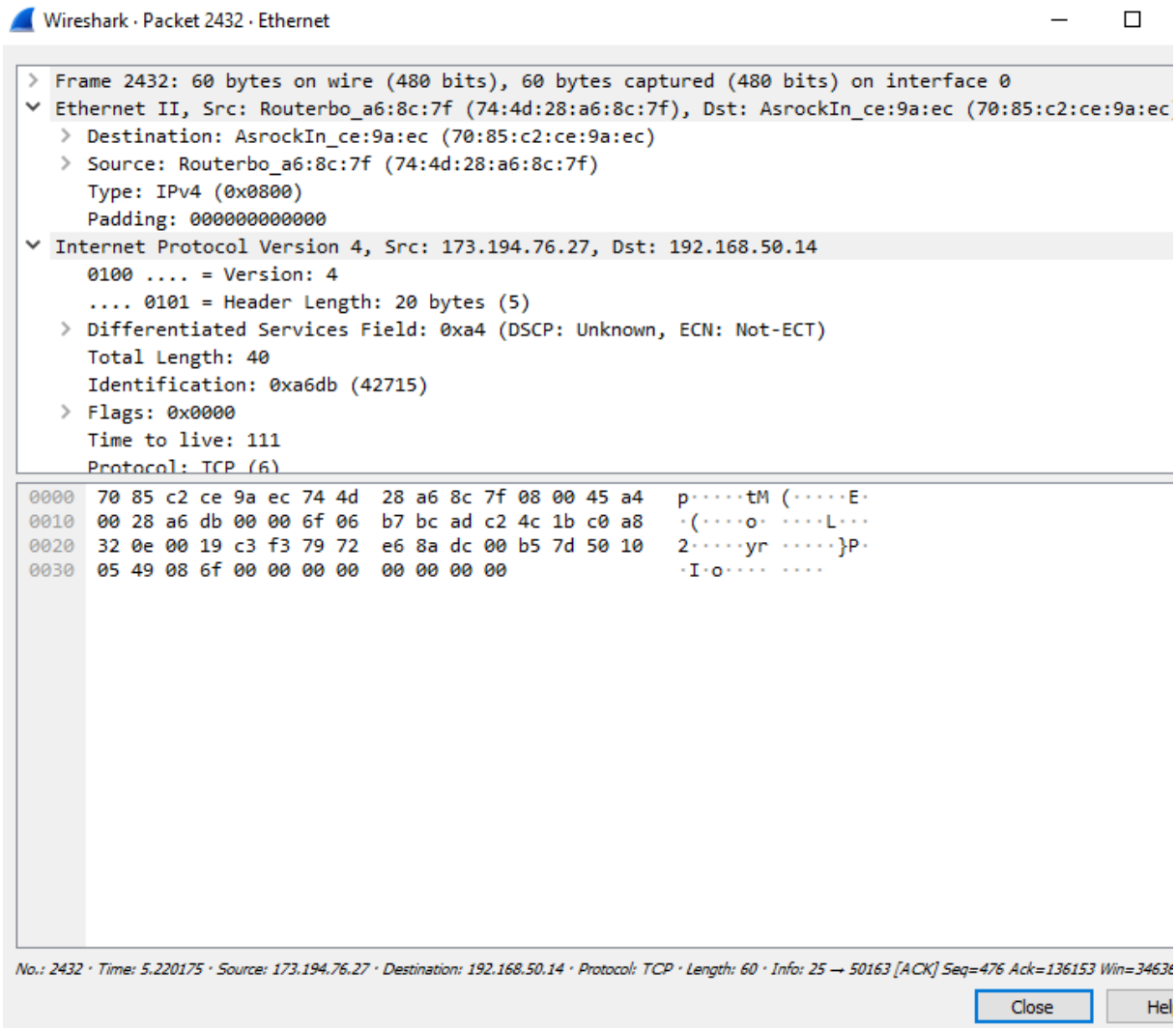


icmp

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
33	5.376985	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=908/35843, ttl=128 …
22	4.358227	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=907/35587, ttl=128 …
19	3.340292	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=906/35331, ttl=128 …
12	2.335334	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=905/35075, ttl=128 …
34	5.377267	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=908/35843, ttl=128 …
23	4.358591	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=907/35587, ttl=128 …
20	3.340584	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=906/35331, ttl=128 …
13	2.335624	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=905/35075, ttl=128 …

5.



7120	9.233610	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7486	9.317686	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7487	9.317686	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7488	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7489	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7490	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7491	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7492	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7493	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7494	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7495	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7496	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7497	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7498	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7499	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7500	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7501	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7502	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7503	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7504	9.319622	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200

7088	9.225960	192.168.50.14	104.16.125.63	UDP	1399 61786 → 443 Len=1357
7167	9.251644	192.168.50.14	104.16.125.63	UDP	94 61786 → 443 Len=52
7168	9.251668	192.168.50.14	104.16.125.63	UDP	94 61786 → 443 Len=52
7142	9.242306	192.168.50.14	104.16.125.63	UDP	96 61786 → 443 Len=54
7117	9.232880	192.168.50.14	104.16.125.63	UDP	97 61786 → 443 Len=55
7231	9.261947	192.168.50.14	104.16.125.63	UDP	120 61786 → 443 Len=78
7230	9.261923	192.168.50.14	104.16.125.63	UDP	130 61786 → 443 Len=88
7244	9.263853	192.168.50.14	104.16.125.63	UDP	137 61786 → 443 Len=95
7256	9.264248	192.168.50.14	104.16.125.63	UDP	137 61786 → 443 Len=95
7448	9.300504	192.168.50.14	104.16.125.63	UDP	137 61786 → 443 Len=95