Niko Marinović, Borna Margetić, 3.G

Vježba 2: Osnovna analiza mrežnog prometa

Priprema:

1. **Što je i čemu služi protokol ARP?**

ARP (Address Resolution Protocol) je protokol koji služi za otkrivanje MAC adresa iz poznatih IP adresa spojenih računala.

2. **Što je i čemu služi protokol ICMP?**

ICMP (Internet Control Message Protocol) je protokol kojim uređaji u mreži mogu kominicirati o problemima sa prijenosom podataka.

3. **Što znaš o naredbi ping?**

Naredba ping nam služi kako bi provjerili ispravnost veze između računala.

Zadatci:

3.

a) Koliko je točno okvira Wireshark „uhvatio“?
Wireshark je „uhvatio“ točno 127 okvira.

b) Koje su oznake protokola na tim okvirima?

Oznake protokola na okvirima su ARP i ICMP.

b) Koristeći dostupne informacije sa predavanja/Interneta opiši kratko funkcije tih protokola.

ARP protokol koji služi za otkrivanje MAC adresa spojenih računala, a ICMP protokol je protokol kojim uređaji u mreži mogu komunicirati o problemima s prijenosom podataka.

c) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

- polazišnu MAC adresu

04:7C:16:C7:52:F1

- odredišnu MAC adresu

04:7C:16:C7:53:2A

- polazišnu IP adresu

192.168.10.3

- odredišnu IP adresu

192.168.10.2

ARP paket (protokol) – reply te ispiši:

- polazišnu MAC adresu

04:7C:16:C7:53:2A

- odredišnu MAC adresu

04:7C:16:C7:52:F1

- Kolika je veličina svake od ovih adresa?

MAC adresa(48bit), IP(32bit)

- polazišnu IP adresu

192.168.10.2

- odredišnu IP adresu

192.168.10.3

e) Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?

Ona glasi ff:ff:ff:ff:ff:ff, zato što računalo još nije saznalo MAC adresu računala sa IP adresom 192.168.10.2

4.

a) Koliko je ICMP echo i reply paketa?

8 paketa.

b) Koji protokol pokreće naredba ping?

Naredba ping pokreće ICMP protokol.

c) Sastavni dio kojeg protokola je ICMP protokol?

IP protokola.

d) U koji okvir je enkapsuliran IP paket?
U Ethernet 2 okvir.

e) Koja je polazišna IP adresa?

192.168.10.3

f) Koja je odredišna IP adresa?

192.168.10.2

g) Koja je MAC adresa polazišnog uređaja?

04:7C:16:C7:52:F1

h) Koja je MAC adresa odredišnog uređaja?

04:7C:16:C7:53:2A

i) Koja je oznaka vrste podataka u Ethernet okviru?

IPv4 (0x0800).

j) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?

IP adrese je 32 bita (4B), a MAC adrese 48 bita (6B).

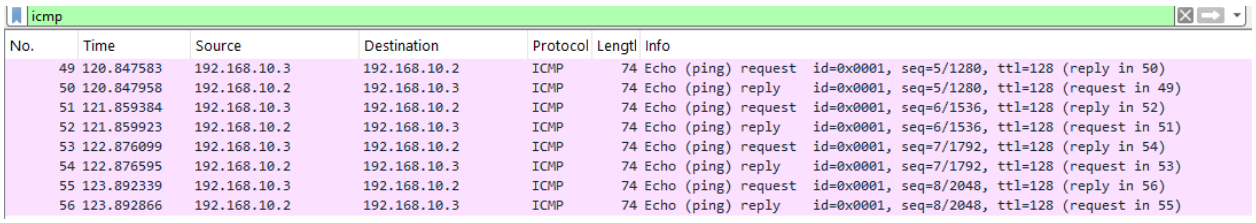
k) Koja je veličina IP paketa kod ICMP protokola?

60 B.

l) Koja je veličina podataka u IP paketu kod ICMP protokola?

40 B.

m) Postavi filter da se prati samo ICMP protokol.


icmp

No.	Time	Source	Destination	Protocol	Lengtl	Info
49	120.847583	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 50)
50	120.847958	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 (request in 49)
51	121.859384	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 52)
52	121.859923	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 (request in 51)
53	122.876099	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 54)
54	122.876595	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=128 (request in 53)
55	123.892339	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 56)
56	123.892866	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=128 (request in 55)

n) Koliko je ICMP echo i reply paketa?

4 echo request i 4 echo reply paketa.

o) Koji protokol pokreće naredba ping?

ICMP protokol.

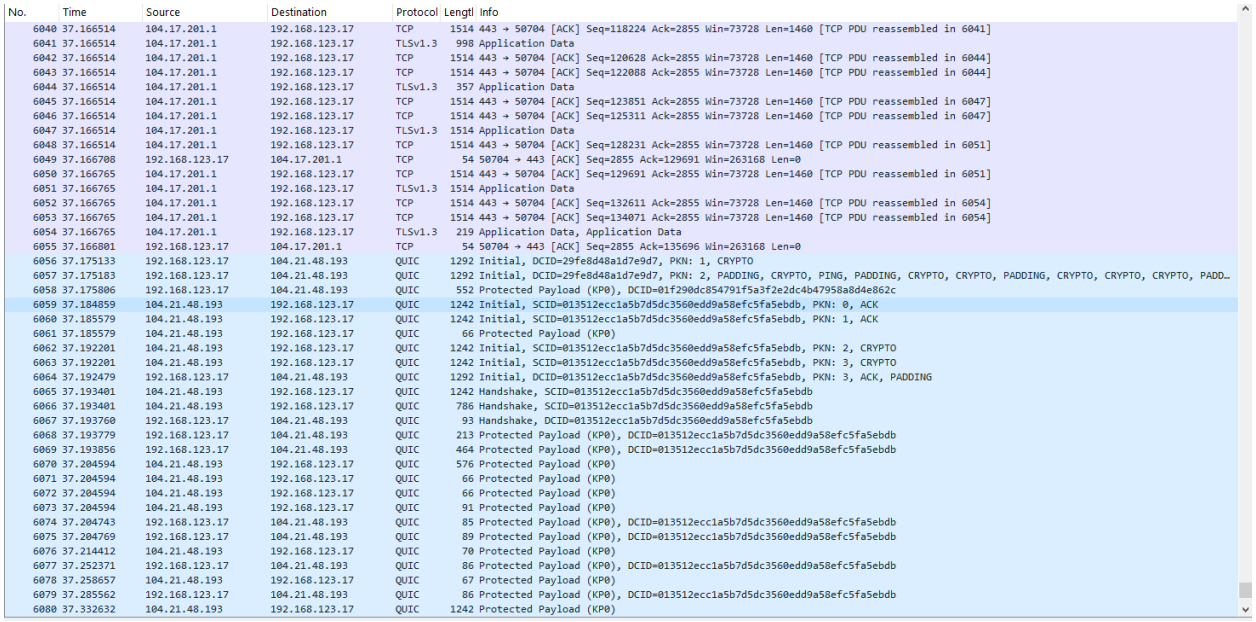
p) Sastavni dio kojeg protokola je protokol ICMP?

IP protokola.

q) U koji okvir je enkapsuliran IP paket?

U Ethernet 2 okvir.

5.



No.	Time	Source	Destination	Protocol	Lengtl	Info
6040	37.166514	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=118224 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6041]
6041	37.166514	104.17.201.1	192.168.123.17	TLSv1.3	998	Application Data
6042	37.166514	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=120628 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6044]
6043	37.166514	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=122088 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6044]
6044	37.166514	104.17.201.1	192.168.123.17	TLSv1.3	357	Application Data
6045	37.166514	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=123851 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6047]
6046	37.166514	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=125311 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6047]
6047	37.166514	104.17.201.1	192.168.123.17	TLSv1.3	1514	Application Data
6048	37.166514	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=128231 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6051]
6049	37.166708	192.168.123.17	104.17.201.1	TCP	54	50704 → 443 [ACK] Seq=2855 Ack=129691 Win=263168 Len=0
6050	37.166765	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=129691 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6051]
6051	37.166765	104.17.201.1	192.168.123.17	TLSv1.3	1514	Application Data
6052	37.166765	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=132611 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6054]
6053	37.166765	104.17.201.1	192.168.123.17	TCP	1514	443 → 50704 [ACK] Seq=134071 Ack=2855 Win=73728 Len=1460 [TCP PDU reassembled in 6054]
6054	37.166765	104.17.201.1	192.168.123.17	TLSv1.3	219	Application Data, Application Data
6055	37.166801	192.168.123.17	104.17.201.1	TCP	54	50704 → 443 [ACK] Seq=2855 Ack=135696 Win=263168 Len=0
6056	37.175133	192.168.123.17	104.21.48.193	QUIC	1292	Initial, DCID=29fe8d48a1d7e9d7, PKN: 1, CRYPTO
6057	37.175183	192.168.123.17	104.21.48.193	QUIC	1292	Initial, DCID=29fe8d48a1d7e9d7, PKN: 2, PADDING, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PADD…
6058	37.175806	192.168.123.17	104.21.48.193	QUIC	552	Protected Payload (KP0), DCID=01f290dc854791f5a3f2e2dc4b47958a8d4e862c
6059	37.184859	104.21.48.193	192.168.123.17	QUIC	1242	Initial, SCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb, PKN: 0, ACK
6060	37.185579	104.21.48.193	192.168.123.17	QUIC	1242	Initial, SCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb, PKN: 1, ACK
6061	37.185579	104.21.48.193	192.168.123.17	QUIC	66	Protected Payload (KP0)
6062	37.192201	104.21.48.193	192.168.123.17	QUIC	1242	Initial, SCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb, PKN: 2, CRYPTO
6063	37.192201	104.21.48.193	192.168.123.17	QUIC	1242	Initial, SCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb, PKN: 3, CRYPTO
6064	37.192479	192.168.123.17	104.21.48.193	QUIC	1292	Initial, DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb, PKN: 3, ACK, PADDING
6065	37.193401	104.21.48.193	192.168.123.17	QUIC	1242	Handshake, SCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6066	37.193401	104.21.48.193	192.168.123.17	QUIC	786	Handshake, SCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6067	37.193760	192.168.123.17	104.21.48.193	QUIC	93	Handshake, DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6068	37.193779	192.168.123.17	104.21.48.193	QUIC	213	Protected Payload (KP0), DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6069	37.193856	192.168.123.17	104.21.48.193	QUIC	464	Protected Payload (KP0), DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6070	37.204594	104.21.48.193	192.168.123.17	QUIC	576	Protected Payload (KP0)
6071	37.204594	104.21.48.193	192.168.123.17	QUIC	66	Protected Payload (KP0)
6072	37.204594	104.21.48.193	192.168.123.17	QUIC	66	Protected Payload (KP0)
6073	37.204594	104.21.48.193	192.168.123.17	QUIC	91	Protected Payload (KP0)
6074	37.204743	192.168.123.17	104.21.48.193	QUIC	85	Protected Payload (KP0), DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6075	37.204769	192.168.123.17	104.21.48.193	QUIC	89	Protected Payload (KP0), DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6076	37.214412	104.21.48.193	192.168.123.17	QUIC	70	Protected Payload (KP0)
6077	37.252371	192.168.123.17	104.21.48.193	QUIC	86	Protected Payload (KP0), DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6078	37.258657	104.21.48.193	192.168.123.17	QUIC	67	Protected Payload (KP0)
6079	37.285562	192.168.123.17	104.21.48.193	QUIC	86	Protected Payload (KP0), DCID=013512ecc1a5b7d5dc3560edd9a58efc5fa5ebdb
6080	37.332632	104.21.48.193	192.168.123.17	QUIC	1242	Protected Payload (KP0)