

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ



Pokročilé komunikační techniky - MPC-PKT
2020/2021

Projekt

Analýza sieťovej komunikácie

Obsah

1	Zadanie	1
2	Analýza	1
2.1	Záznamy 1-22 - ECHO IPv4	1
2.2	Záznamy 23-46 - ECHO IPv6	2
2.3	Záznamy 47-82 - DNS (UDP + TCP)	5
2.4	Záznamy 83-104 - DNS (pokračovanie)	6
2.5	Záznamy 105-200 - ICMP	7
2.6	Záznamy 201-210 - komunikácia s webserverom - DNS, TCP	9
2.7	Záznamy 211-228 - komunikácia s webserverom - TCP, HTTP	10
2.8	Záznamy 229-238 - Protokol QUIC	12
2.9	Záznamy 239-439 - Protokol TCP	13
3	Záver	15

1 Zadanie

Zmyslom tohto projektu je samostatne analyzovať predložený .pcapng súbor, ktorý obsahuje zachytenú sieťovú komunikáciu.

2 Analýza

V tejto sekcii bude analyzovaná sieťová komunikácia súboru .pcapng. Sieťovú komunikáciu som rozdelil do logických celkov podľa druhov sieťového provozu. Celkovo sa tak analýza skladá z deviatich podkapitol. Celé zadanie projektu je možné nájsť na nasledujúcom odkaze¹.

2.1 Záznamy 1-22 - ECHO IPv4

Na nasledujúcom obrázku 1 je možné vidieť záznamy 1-22, ktoré budú analyzované v tejto sekcii.

No.	Time	Source	Destination	typ	Protocol	Length	Info
1	0.000000	00:00:00:00:00:01	Broadcast		ARP	64	Who has 172.16.1.4? Tell 172.16.1.1
2	0.000024	00:00:00:00:00:04	00:00:00:00:00:01		ARP	64	172.16.1.4 is at 00:00:00:00:00:04
3	0.000024	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0000)
4	0.000147	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0000)
5	0.000276	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0000)
6	0.992000	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0001) [Reassembled in #9]
7	0.992122	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0001) [Reassembled in #9]
8	0.992261	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0001) [Reassembled in #9]
9	0.992397	172.16.1.1	172.16.3.4		ECHO	606	Request
10	1.012904	00:00:00:00:00:04	Broadcast		ARP	64	Who has 172.16.1.1? Tell 172.16.1.4
11	1.012904	00:00:00:00:00:01	00:00:00:00:00:04		ARP	64	172.16.1.1 is at 00:00:00:00:00:04
12	1.013046	172.16.3.4	172.16.1.1		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0000)
13	1.013180	172.16.3.4	172.16.1.1		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0000)
14	1.013312	172.16.3.4	172.16.1.1		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0000)
15	1.992000	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0002) [Reassembled in #18]
16	1.992122	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0002) [Reassembled in #18]
17	1.992250	172.16.1.1	172.16.3.4		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0002) [Reassembled in #18]
18	1.992379	172.16.1.1	172.16.3.4		ECHO	606	Request
19	2.006995	172.16.3.4	172.16.1.1		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0001) [Reassembled in #22]
20	2.009399	172.16.3.4	172.16.1.1		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0001) [Reassembled in #22]
21	2.011802	172.16.3.4	172.16.1.1		IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0001) [Reassembled in #22]
22	2.012673	172.16.3.4	172.16.1.1		ECHO	606	Response

Obr. 1: Záznamy 1-22

- V tejto komunikácii figuruje sieťový protokol **IPv4**, transportný protokol **UDP**, linkový protokol **ARP** a sieťový protokol **ICMP**.
- Z ukážky vyplýva, že sa jedná o komunikáciu medzi dvoma zariadeniami. Zariadenie **00:00:00:00:00:01** vyslala správu typu **ARP Broadcast** zo zdrojovou IP adresou **172.16.1.1** s požiadavkou na zistenie IP adresy zariadenia **172.16.1.4** veľkosť paketu predstavuje **64 B** (štandardná veľkosť ethernet paketu) a typ zapuzdrenia je **Ethernet**.
- V druhom pakete zariadenie s MAC adresou **00:00:00:00:00:04** odpovedá, že disponuje s hľadanou IP adresou **172.16.1.4**. V tomto prípade sa nejedná o **ARP Broadcast** odpoveď ale práve o unicast. Hľadané zariadenie odpovedá len tazateľovi. Veľkosť paketu znovu predstavuje **64 B** a typ zapuzdrenia je **Ethernet**.
- V prípade paketov **3-9** je z wiresharku možné vyčítať, že **proto = UDP 17**², z ktorého vyplýva, že sa jedná o fragmentovaný **UDP** provoz. S najväčšou pravdepodobnosťou prebehla snaha o ping zo siete LAN na inú sieť, kde sa nachádza zariadenie **172.16.3.4**. Fragmentáciu rovnako naznačujú aj príznaky (flags) v jednotlivých paketoch (...1. = More fragments: Set). K fragmentácii mohlo dôjsť z dôvodu veľkosti daných paketov. Z wiresharku je možné vidieť, že veľkosť paketov predstavuje **1518 B** čo podľa zdroja³ predstavuje maximálnu veľkosť ethernetového paketu, avšak **MTU** niektorej

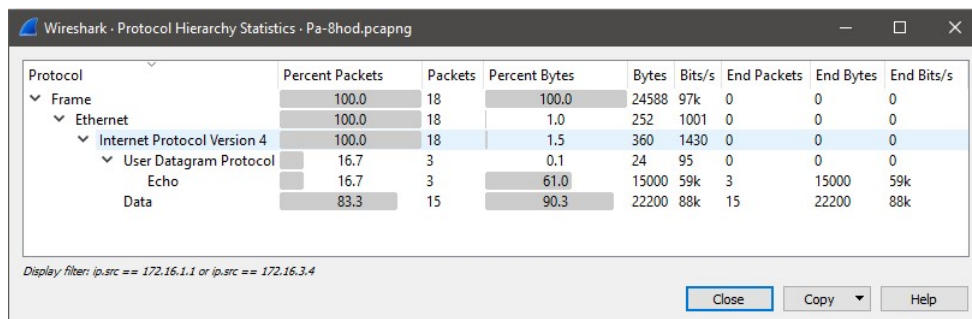
¹<https://bit.ly/3s9qhNs>

²<https://bit.ly/3daY1WB>

³<https://bit.ly/3d51iGJ>

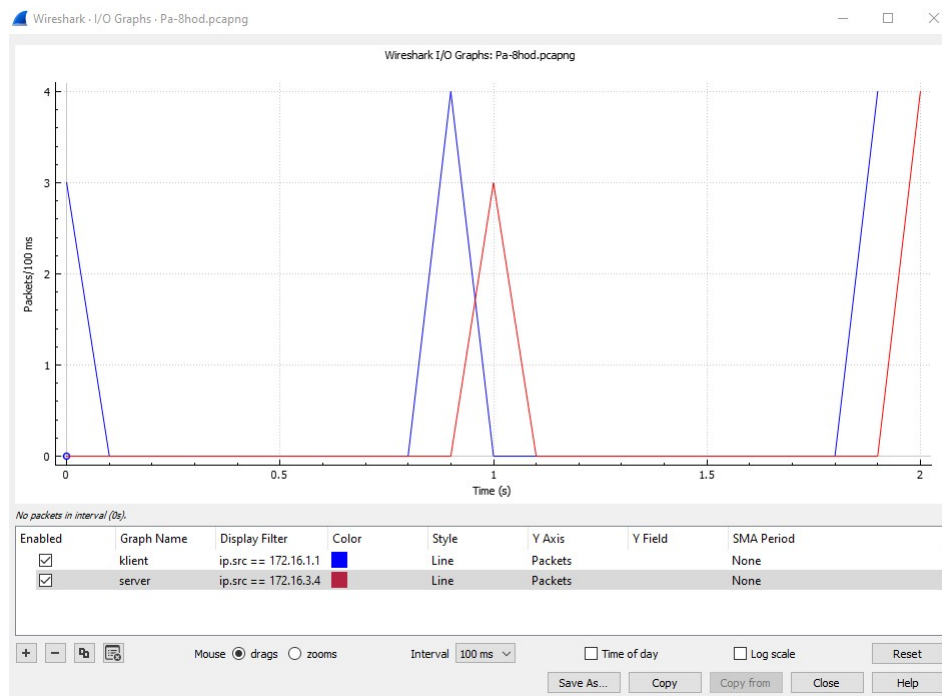
linky na sieť môže byť nastavené na štandardnú hodnotu **1500 B**, čo v konečnom dôsledku zapríčini fragmentáciu jednotlivých paketov. Rovnako veľkosť ECHO paketu dátovej časti je **5008 B**.

- V paketoch 10 a 11 sa znovu jedná o **ARP request** a **ARP reply**. Rovnako nastáva fragmentácia z dôvodu veľkej dátovej časti ECHO request paketu



Obr. 2: Protocol Hierarchy Statistics IPv4

- Z ukážky 2 vyplýva, že boli prenesené **3 ECHO** pakety avšak vďaka fragmentovanému stavu ich celkovo bolo **18**.
- Veľkosť ECHO paketov bola dohromady 15 000 B = **15 kB**.
- Prenášané dáta neboli žiadnym spôsobom zabezpečené.
- Rýchlosti prenosu je možné vidieť na grafe 3.

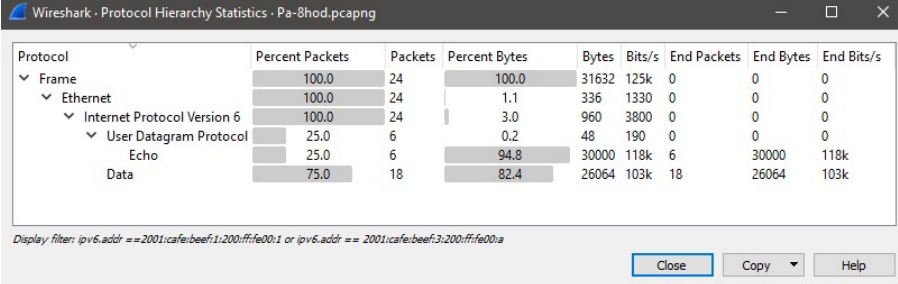


Obr. 3: I/O Graphs IPv4

2.2 Záznamy 23-46 - ECHO IPv6

Na nasledujúcom obrázku 4 je možné vidieť záznamy 23-46, ktoré budú analyzované v tejto sekcii.

- Objem dát predstavuje 6 prenesených ECHO paketov, ktoré boli celkovo fragmentované na 24 paketov vid' 6.



Wireshark - Protocol Hierarchy Statistics - Pa-8hod.pcapng

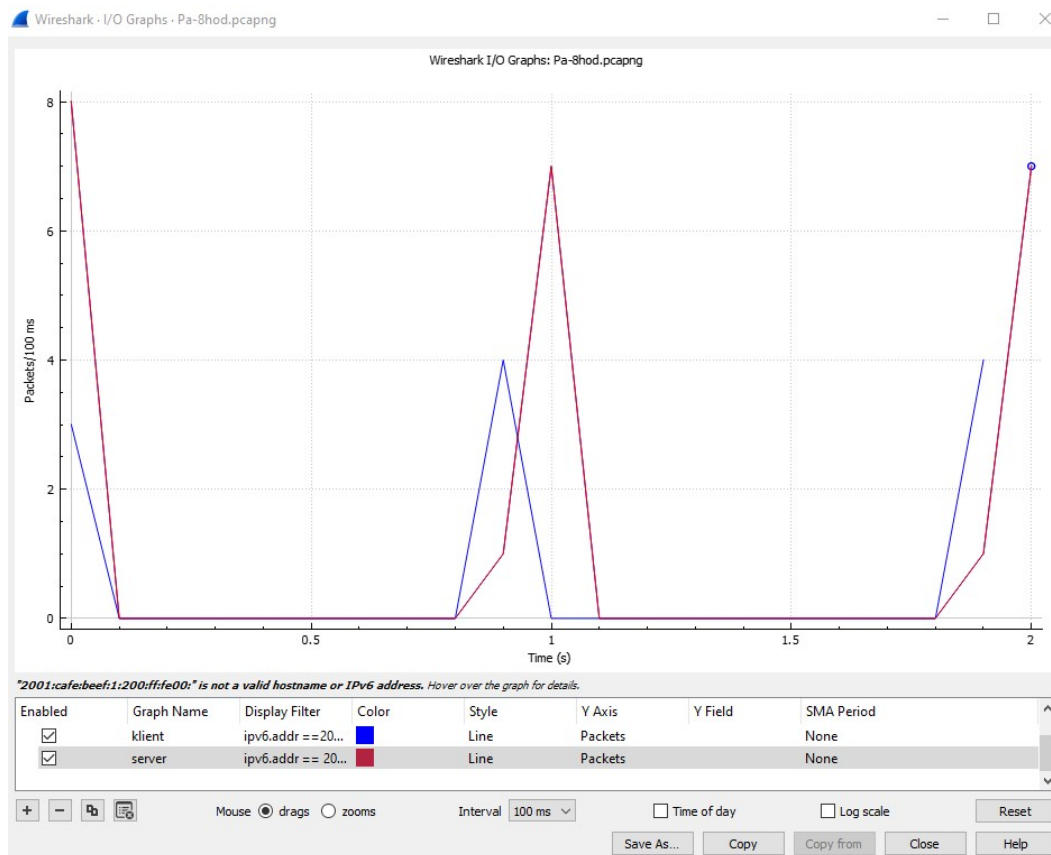
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	24	100.0	31632	125k	0	0	0
Ethernet	100.0	24	1.1	336	1330	0	0	0
Internet Protocol Version 6	100.0	24	3.0	960	3800	0	0	0
User Datagram Protocol	25.0	6	0.2	48	190	0	0	0
Echo	25.0	6	94.8	30000	118k	6	30000	118k
Data	75.0	18	82.4	26064	103k	18	26064	103k

Display filter: ipv6.addr == 2001:cafe:beef:1:200:ff:fe00:1 or ipv6.addr == 2001:cafe:beef:3:200:ff:fe00:a

Buttons: Close, Copy, Help

Obr. 6: Protocol Hierarchy Statistics IPv6

- Prenosová rýchlosť je znázornená na grafe 7.



Obr. 7: I/O Graphs IPv6

- Dáta rovnako ako v prípade IPv4 nie sú zabezpečené.
- Obsah dátovej časti v prípade ECHO Requestu činí **5000 B** a je fragmentovaná na 3 pakety 23-25 vid' 5. V prípade ECHO Response nastáva podobný jav.

2.3 Záznamy 47-82 - DNS (UDP + TCP)

Na nasledujúcom obrázku 8 je možné vidieť záznamy 47-82, ktoré budú analyzované v tejto sekcii.

47	*REF*	10.0.2.15	9.9.9.9	DNS	81 Standard query 0x0000 A airbnb.com OPT
48	0.503260	9.9.9.9	10.0.2.15	DNS	129 Standard query response 0x0000 A airbnb.com A 54.82.106.203 A 52.202.116.246 A 34.193.147.255 OPT
49	4.934543	10.0.2.15	9.9.9.9	DNS	81 Standard query 0x0000 RRSIG airbnb.com OPT
50	4.960608	9.9.9.9	10.0.2.15	DNS	150 Standard query response 0x0000 RRSIG airbnb.com SOA ns1.p74.dyneet.net OPT
51	7.714297	10.0.2.15	9.9.9.9	DNS	81 Standard query 0x0000 DNSKEY airbnb.com OPT
52	7.882571	9.9.9.9	10.0.2.15	DNS	146 Standard query response 0x0000 DNSKEY airbnb.com SOA dns1.p08.nsone.net OPT
53	12.547987	10.0.2.15	9.9.9.9	TCP	66 50181 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
54	12.576450	9.9.9.9	10.0.2.15	TCP	60 53 → 50181 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
55	12.576517	10.0.2.15	9.9.9.9	TCP	54 50181 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
56	12.576711	10.0.2.15	9.9.9.9	DNS	95 Standard query 0x0000 DNSKEY airbnb.com OPT
57	12.576875	9.9.9.9	10.0.2.15	TCP	60 53 → 50181 [ACK] Seq=1 Ack=42 Win=65535 Len=0
58	12.747022	9.9.9.9	10.0.2.15	DNS	160 Standard query response 0x0000 DNSKEY airbnb.com SOA dns1.p08.nsone.net OPT
59	12.747124	10.0.2.15	9.9.9.9	TCP	54 50181 → 53 [FIN, ACK] Seq=42 Ack=107 Win=64134 Len=0
60	12.747346	9.9.9.9	10.0.2.15	TCP	60 53 → 50181 [ACK] Seq=107 Ack=43 Win=65535 Len=0
61	12.776268	9.9.9.9	10.0.2.15	TCP	60 53 → 50181 [FIN, ACK] Seq=107 Ack=43 Win=65535 Len=0
62	12.776310	10.0.2.15	9.9.9.9	TCP	54 50181 → 53 [ACK] Seq=43 Ack=108 Win=64134 Len=0
63	15.036140	10.0.2.15	9.9.9.9	TCP	66 50182 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
64	15.066385	9.9.9.9	10.0.2.15	TCP	60 53 → 50182 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
65	15.066459	10.0.2.15	9.9.9.9	TCP	54 50182 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
66	15.066581	10.0.2.15	9.9.9.9	DNS	95 Standard query 0x0000 RRSIG airbnb.com OPT
67	15.066702	9.9.9.9	10.0.2.15	TCP	60 53 → 50182 [ACK] Seq=1 Ack=42 Win=65535 Len=0
68	15.078357	9.9.9.9	10.0.2.15	DNS	160 Standard query response 0x0000 RRSIG airbnb.com SOA dns1.p08.nsone.net OPT
69	15.078452	10.0.2.15	9.9.9.9	TCP	54 50182 → 53 [FIN, ACK] Seq=42 Ack=107 Win=64134 Len=0
70	15.078634	9.9.9.9	10.0.2.15	TCP	60 53 → 50182 [ACK] Seq=107 Ack=43 Win=65535 Len=0
71	15.096605	9.9.9.9	10.0.2.15	TCP	60 53 → 50182 [FIN, ACK] Seq=107 Ack=43 Win=65535 Len=0
72	15.096670	10.0.2.15	9.9.9.9	TCP	54 50182 → 53 [ACK] Seq=43 Ack=108 Win=64134 Len=0
73	18.025827	10.0.2.15	9.9.9.9	TCP	66 50183 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
74	18.056331	9.9.9.9	10.0.2.15	TCP	60 53 → 50183 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
75	18.056412	10.0.2.15	9.9.9.9	TCP	54 50183 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
76	18.056554	10.0.2.15	9.9.9.9	DNS	95 Standard query 0x0000 A airbnb.com OPT
77	18.056705	9.9.9.9	10.0.2.15	TCP	60 53 → 50183 [ACK] Seq=1 Ack=42 Win=65535 Len=0
78	18.224889	9.9.9.9	10.0.2.15	DNS	143 Standard query response 0x0000 A airbnb.com A 34.193.147.255 A 54.82.106.203 A 52.202.116.246 OPT
79	18.225089	10.0.2.15	9.9.9.9	TCP	54 50183 → 53 [FIN, ACK] Seq=42 Ack=90 Win=64151 Len=0
80	18.225143	9.9.9.9	10.0.2.15	TCP	60 53 → 50183 [ACK] Seq=90 Ack=43 Win=65535 Len=0
81	18.246301	9.9.9.9	10.0.2.15	TCP	60 53 → 50183 [FIN, ACK] Seq=90 Ack=43 Win=65535 Len=0
82	18.246356	10.0.2.15	9.9.9.9	TCP	54 50183 → 53 [ACK] Seq=43 Ack=91 Win=64151 Len=0

Obr. 8: Záznamy 47-82

- V tejto komunikácii figuruje aplikačný protokol **DNS**, transportný protokol **TCP** a **UDP**.
- Protokol UDP (DNS) využíva pri komunikácii na strane klienta dynamické porty z rozsahu 49152-65535. Príklad na tento port je **55848** (klient, paket 48). Na strane serveru je to port **53**, ktorý zodpovedá službe DNS⁵.
- V prípade TCP klient využíva dynamický port **50181** (paket 53), server využíva port **53** (štandardný port pre DNS rovnako ako v prípade UDP komunikácie⁶).
- **IPv4 adresy** komunikujúcich strán:
 - **Klient:** 10.0.2.15 → MAC 08:00:27:08:94:4e
 - **Server:** 9.9.9.9 → MAC 52:54:00:12:35:02
- **Priebeh komunikácie:** Komunikácia prebieha pomocou protokolov TCP a UDP.
 - **UDP:**
 - * Klient 10.0.2.15 odošle DNS dotaz typu **A** (Dotazuje sa na IP adresu) na DNS server 9.9.9.9. Konkrétne sa dotazuje na IP adresu webovej stránky **airbnb.com**.
 - * Následne server odpovedá a zasiela ako odpoveď IP adresy webu **airbnb.com**.
 - * V ďalšom kroku znovu prebehne komunikácia medzi klientom a serverom, len s tým rozdielom, že komunikácia je zašifrovaná (Resource Record Signature - **RRSIG**).
 - * Posledným dotazom je dotaz **DNSKEY**, v ktorom sa klient pýta serveru na verejný kľúč. Server následne odpovie a zašle potrebné informácie.
 - **TCP**
 - * Komunikácia prebieha obdobným spôsobom, len s tým rozdielom, že v prípade TCP pred DNS dotazom nastane **3-way handshake**, rovnako pri ukončení spojenia **4-way handshake**.
 - * Rovnako TCP komunikácia obsahuje aj potvrdzovacie **ACK** pakety.

⁵<https://bit.ly/3sdmLl0>

⁶<https://bit.ly/3mHJ51D> → služba DNS využíva transportný protokol ako **TCP** tak aj **UDP**

2.4 Záznamy 83-104 - DNS (pokračovanie)

Na nasledujúcom obrázku 9 je možné vidieť záznamy 83-104, ktoré budú analyzované v tejto sekcii.

83 *REF*	135.76.93.254	135.76.186.134	DNS	70 Standard query 0xc1f A airbnb.com
84 0.031081	135.76.93.254	135.76.1.134	DNS	70 Standard query 0xc1f A airbnb.com
85 0.160010	135.76.186.134	135.76.93.254	DNS	118 Standard query response 0xc1f A airbnb.com A 54.82.106.203 A 34.193.147.255 A 52.202.116.246
86 0.174675	135.76.1.134	135.76.93.254	DNS	118 Standard query response 0xc1f A airbnb.com A 34.193.147.255 A 52.202.116.246 A 54.82.106.203
87 0.174701	135.76.93.254	135.76.1.134	ICMP	146 Destination unreachable (Port unreachable)
88 0.530489	135.76.93.254	135.76.186.134	DNS	74 Standard query 0xf17d A www.airbnb.com
89 0.561938	135.76.93.254	135.76.1.134	DNS	74 Standard query 0xf17d A www.airbnb.com
90 0.715777	135.76.186.134	135.76.93.254	DNS	230 Standard query response 0xf17d A www.airbnb.com CNAME san1.airbnb.com.edgekey.net CNAME e111434.a.akamaiedge.net A
91 0.804393	135.76.1.134	135.76.93.254	DNS	230 Standard query response 0xf17d A www.airbnb.com CNAME san1.airbnb.com.edgekey.net CNAME e111434.a.akamaiedge.net A
92 0.804069	135.76.93.254	135.76.186.134	DNS	80 Standard query 0x91e6 AAAA pxyapp.proxy.att.com
93 0.834701	135.76.93.254	135.76.1.134	DNS	80 Standard query 0x91e6 AAAA pxyapp.proxy.att.com
94 0.840836	135.76.186.134	135.76.93.254	DNS	179 Standard query response 0x91e6 AAAA pxyapp.proxy.att.com CNAME lbv-135-28-13-12.pmttr.west.att.com SOA ns0.sldc.sbc.
95 0.842145	135.76.93.254	135.76.186.134	DNS	83 Standard query 0x28b6 AAAA operations.intl.att.com
96 0.872780	135.76.93.254	135.76.1.134	DNS	83 Standard query 0x28b6 AAAA operations.intl.att.com
97 0.877679	135.76.1.134	135.76.93.254	DNS	179 Standard query response 0x91e6 AAAA pxyapp.proxy.att.com CNAME lbv-135-28-13-12.pmttr.west.att.com SOA ns0.sldc.sbc.
98 0.877679	135.76.93.254	135.76.1.134	ICMP	207 Destination unreachable (Port unreachable)
99 0.877891	135.76.186.134	135.76.93.254	DNS	138 Standard query response 0x28b6 AAAA operations.intl.att.com SOA bebrxdc01.intl.att.com
100 0.116859	135.76.1.134	135.76.93.254	DNS	138 Standard query response 0x28b6 AAAA operations.intl.att.com SOA defradc15.intl.att.com
101 0.229790	135.76.93.254	135.76.186.134	DNS	76 Standard query 0x212e A www.airbnb.co.uk
102 0.261171	135.76.93.254	135.76.1.134	DNS	76 Standard query 0x212e A www.airbnb.co.uk
103 0.415612	135.76.186.134	135.76.93.254	DNS	232 Standard query response 0x212e A www.airbnb.co.uk CNAME san1.airbnb.com.edgekey.net CNAME e111434.a.akamaiedge.net
104 0.420806	135.76.1.134	135.76.93.254	DNS	232 Standard query response 0x212e A www.airbnb.co.uk CNAME san1.airbnb.com.edgekey.net CNAME e111434.a.akamaiedge.net

Obr. 9: Záznamy 47-82

- V tejto komunikácii figuruje aplikačný protokol **DNS**, transportný protokol **UDP** a sieťový protokol **ICMP**.
- Rovnako ako v predošlom prípade 2.3 DNS na strane klienta využíva dynamické porty z rozsahu 49125-65535. Na strane serveru využíva dobre známy port **53** (štandardný port pre službu DNS).
- **IPv4 adresy** komunikujúcich strán:
 - **Klient:** 135.76.93.254 → MAC 00:05:9a:3c:7a:00
 - **Server-1:** 135.76.186.134 → MAC 00:11:22:33:44:55
 - **Server-2:** 135.76.1.134 → MAC 00:11:22:33:44:55
- **Priebeh komunikácie:**
 - Klient **135.76.93.254** odošle 2 DNS dotazy typu **A** na serveri **135.76.186.134** a **135.76.1.134**, kde sa dotazuje na IPv4 webovej stránky **airbnb.com**.
 - Následne mu serveri odpovedajú a poskytujú radu IP adries, ktoré patria dotazovanej webovej stránke.
 - Následne server **135.76.1.134** prestane odpovedať *Destination unreachable (Port unreachable)*
 - Pakety **88-91** opakujú celý proces znovu.
 - V ďalšom kroku klient odošle znovu dotaz na oba serveri, avšak tento raz sa jedná o dotaz typu **AAAA**. V tomto dotaze sa snaží zistiť **IPv6** adresu pre webovú stránku **pxyapp.proxy.att.com**.
 - Server znovu *unreachable* a proces sa opakuje znovu (ďalšie DNS dotazy na **airbnb.co.uk**).
- Celkovo v komunikácii prebehlo 22 paketov, komunikácia nebola nijakým spôsobom šifrovaná.

2.5 Záznamy 105-200 - ICMP

Na nasledujúcom obrázku 10 je možné vidieť záznamy 105-152, a na obrázku 11 sú zobrazené záznamy 153-200, ktoré budú analyzované v tejto sekcii.

105 "REF"	192.168.1.108	147.229.2.90	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e870)
106 8.985804	192.168.1.108	147.229.2.90	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e871)
107 13.835107	192.168.1.108	147.229.2.90	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e872)
108 18.835948	192.168.1.108	147.229.2.90	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e873)
109 23.834876	192.168.1.108	147.229.2.90	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e874)
110 35.620689	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=180/46808, ttl=128 (reply in 111)
111 35.628288	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=180/46808, ttl=54 (request in 110)
112 36.631365	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=181/46336, ttl=128 (reply in 113)
113 36.630860	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=181/46336, ttl=54 (request in 112)
114 37.646917	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=182/46592, ttl=128 (reply in 115)
115 37.654587	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=182/46592, ttl=54 (request in 114)
116 38.662517	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=183/46848, ttl=128 (reply in 117)
117 38.670120	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=183/46848, ttl=54 (request in 116)
118 39.678171	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=184/47104, ttl=128 (reply in 119)
119 39.685713	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=184/47104, ttl=54 (request in 118)
120 40.693786	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=185/47360, ttl=128 (reply in 121)
121 40.701368	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=185/47360, ttl=54 (request in 120)
122 41.709503	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=186/47616, ttl=128 (reply in 123)
123 41.717062	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=186/47616, ttl=54 (request in 122)
124 42.725060	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=187/47872, ttl=128 (reply in 125)
125 42.732633	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=187/47872, ttl=54 (request in 124)
126 43.740662	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=188/48128, ttl=128 (reply in 127)
127 43.748312	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=188/48128, ttl=54 (request in 126)
128 44.756287	192.168.1.108	147.229.2.90	ICMP	43 Echo (ping) request id=0x0001, seq=189/48384, ttl=128 (reply in 129)
129 44.764153	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=189/48384, ttl=54 (request in 128)
130 58.403658	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=190/48640, ttl=1 (no response found!)
131 58.403916	192.168.1.1	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
132 58.404496	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=191/48896, ttl=1 (no response found!)
133 58.404925	192.168.1.1	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
134 58.405256	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=192/49152, ttl=1 (no response found!)
135 58.405501	192.168.1.1	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
136 58.408997	192.168.1.1	192.168.1.108	ICMP	120 Destination unreachable (Port unreachable)
137 59.923781	192.168.1.1	192.168.1.108	ICMP	120 Destination unreachable (Port unreachable)
138 61.439296	192.168.1.1	192.168.1.108	ICMP	120 Destination unreachable (Port unreachable)
139 63.971849	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=193/49408, ttl=2 (no response found!)
140 63.973164	192.168.1.108	147.229.2.90	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
141 63.974607	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=194/49664, ttl=2 (no response found!)
142 63.975387	100.125.139.2	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
143 63.976434	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=195/49920, ttl=2 (no response found!)
144 63.977227	100.125.139.2	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
145 64.987477	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=196/50176, ttl=3 (no response found!)
146 64.988066	83.240.3.13	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
147 64.990438	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=197/50432, ttl=3 (no response found!)
148 64.991554	83.240.3.13	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
149 64.992777	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=198/50688, ttl=3 (no response found!)
150 64.993892	83.240.3.13	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
151 66.003108	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=199/50944, ttl=4 (no response found!)
152 66.007531	83.240.2.38	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

Obr. 10: Záznamy 105-152

153 66.009472	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=200/51200, ttl=4 (no response found!)
154 66.015886	83.240.2.38	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
155 66.018140	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=201/51456, ttl=4 (no response found!)
156 66.022301	83.240.2.38	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
157 67.034264	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=202/51712, ttl=5 (no response found!)
158 67.039729	83.240.2.37	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
159 67.041023	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=203/51968, ttl=5 (no response found!)
160 67.046083	83.240.2.37	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
161 67.047823	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=204/52224, ttl=5 (no response found!)
162 67.051972	83.240.2.37	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
163 68.005669	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=205/52480, ttl=6 (no response found!)
164 68.071710	91.210.16.191	192.168.1.108	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
165 68.073971	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=206/52736, ttl=6 (no response found!)
166 68.079867	91.210.16.191	192.168.1.108	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
167 68.081856	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=207/52992, ttl=6 (no response found!)
168 68.088525	91.210.16.191	192.168.1.108	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
169 69.097013	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=208/53248, ttl=7 (no response found!)
170 69.104842	195.113.157.161	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
171 69.107162	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=209/53504, ttl=7 (no response found!)
172 69.115168	195.113.157.161	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
173 69.117280	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=210/53760, ttl=7 (no response found!)
174 69.125893	195.113.157.161	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
175 70.128169	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=211/54016, ttl=8 (no response found!)
176 70.135487	213.195.192.106	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
177 70.137782	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=212/54272, ttl=8 (no response found!)
178 70.145179	213.195.192.106	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
179 70.147213	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=213/54528, ttl=8 (no response found!)
180 70.154521	213.195.192.106	192.168.1.108	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
181 71.159342	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=214/54784, ttl=9 (no response found!)
182 71.159788	147.229.253.236	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
183 71.170063	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=215/55040, ttl=9 (no response found!)
184 71.178235	147.229.253.236	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
185 71.180800	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=216/55296, ttl=9 (no response found!)
186 71.188852	147.229.253.236	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
187 72.221927	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=217/55552, ttl=10 (no response found!)
188 72.230239	147.229.253.96	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
189 72.232452	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=218/55808, ttl=10 (no response found!)
190 72.240519	147.229.253.96	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
191 72.242684	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=219/56064, ttl=10 (no response found!)
192 72.250815	147.229.253.96	192.168.1.108	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
193 73.268881	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=220/56320, ttl=11 (reply in 194)
194 73.276379	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=220/56320, ttl=54 (request in 193)
195 73.278624	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=221/56576, ttl=11 (reply in 196)
196 73.286108	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=221/56576, ttl=54 (request in 195)
197 73.288081	192.168.1.108	147.229.2.90	ICMP	106 Echo (ping) request id=0x0001, seq=222/56832, ttl=11 (reply in 198)
198 73.295777	147.229.2.90	192.168.1.108	ICMP	60 Echo (ping) reply id=0x0001, seq=222/56832, ttl=54 (request in 197)
199 157.012471	192.168.1.108	103.248.176.78	ICMP	1042 Echo (ping) request id=0x0001, seq=223/57088, ttl=128 (reply in 200)
200 157.295425	103.248.176.78	192.168.1.108	ICMP	1042 Echo (ping) reply id=0x0001, seq=223/57088, ttl=46 (request in 199)

Obr. 11: Záznamy 153-200

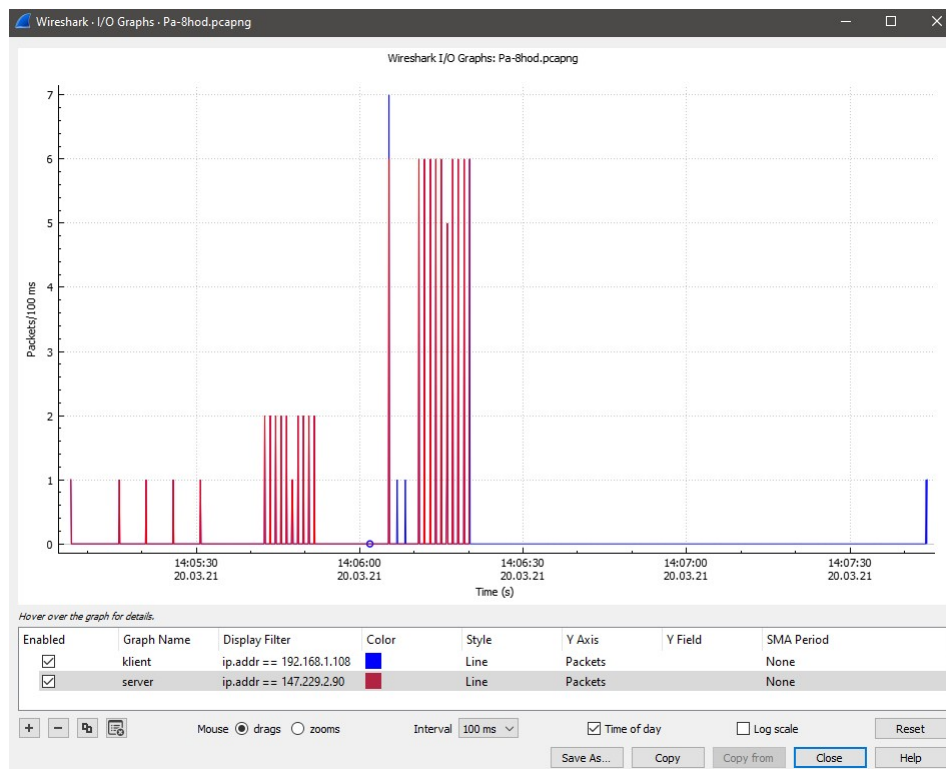
- V tejto komunikácii nefiguruje žiadny aplikačný ani transportný protokol, iba sieťový protokol ICMP a IPv4.

- **IPv4 adresy komunikujúcich strán:**

- **Klient:** 192.168.1.108 → 50:e5:49:38:9d:8f
- **Server:** 147.229.2.90 → d8:58:d7:00:4f:80

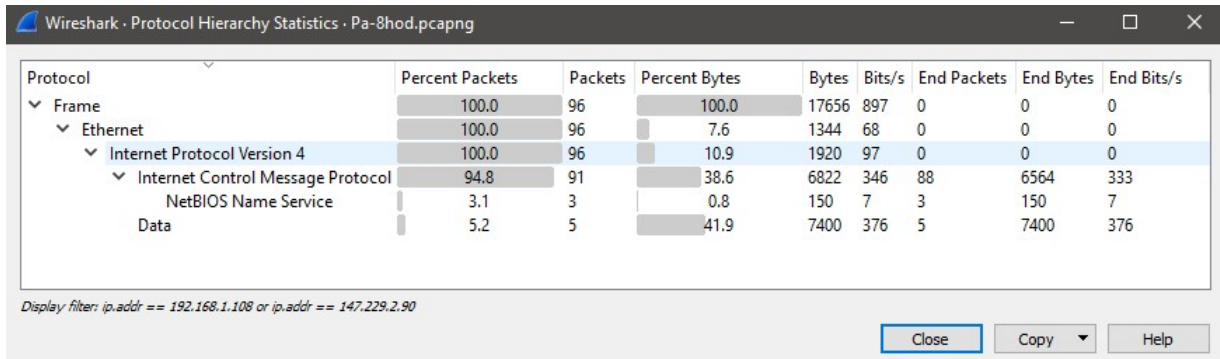
- **Priebeh komunikácie:**

- Úvod komunikácie tvorí fragmentovaný IPv4 provoz, fragmentácia nastala z dôvodu príliš veľkej veľkosti paketu (1514 B), ktorá prekračuje maximálne povolené MTU v sieti.
 - Následne pakety 110-129 tvoria štandardný ICMP Request/Reply provoz. Za povšimnutie stojí aj hodnota **TTL**, ktorá je v prípade **ECHO Request 128** a v prípade **ECHO Reply je 53**.
 - V prípade paketu **130** došlo k zmene, hodnota TTL už nie je 128 ale **1**. Čo má za následok, že ICMP request sa nedostane za router do siete.
 - Tento jav opísaný v predošlom bode je vidieť na paketoch **131, 133 a 134**, ktoré sa nemôže dostať z lokálnej siete vďaka nastavenej hodnote **TTL=1**.
 - Pakety **136-138** značia, že lokálny router, ktorého adresa default gateway je 192.168.1.1 nevie kontaktovať cieľovú stanicu.
 - Následne na paketoch **139-192** môžeme pozorovať postupné navyšovanie hodnoty **TTL** (z hodnoty 2 na hodnotu 10).
 - Na záver v paketoch **193-157** sa táto hodnota navýši na hodnotu **TTL = 11** a následné ICMP ECHO Request/Reply komunikácia medzi klientom a serverom prebiehajú bez problémov.
- Rýchlosť prenášania paketov je vidieť na grafe 12. Rovnako je vidieť aj „hluchú“ časť komunikácie, keď hodnota $TTL < 11$ a následne sa ku koncu komunikácie prenosová rýchlosť obnovila pre **TTL = 11**.



Obr. 12: I/O Graphs ICMP

- Objem dát a rýchlosť prenosu je možné vidieť na obrázku 13.
- Je možné vidieť, že bolo celkovo prenesených 96 paketov o veľkosti **17 656 B**.



Obr. 13: Protocol Hierarchy Statistics ICMP

2.6 Záznamy 201-210 - komunikácia s webserverom - DNS, TCP

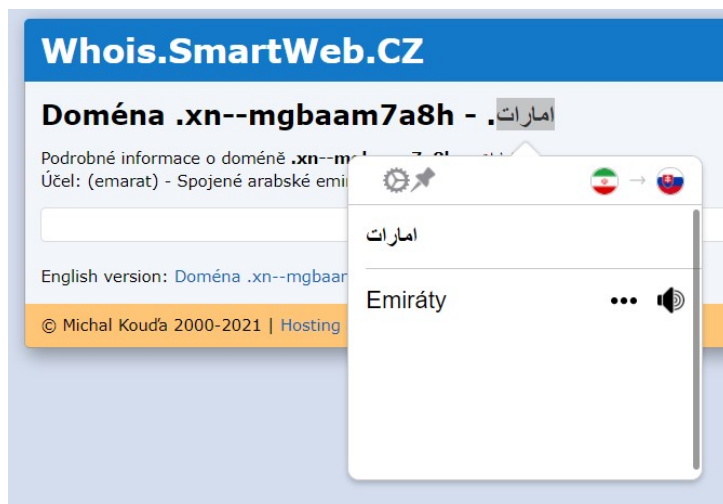
Na nasledujúcom obrázku 14 je možné vidieť záznamy 201-210, ktoré budú analyzované v tejto sekcii.

201 *REF*	192.168.110.142	146.230.254.16	TCP	66 52297 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
202 0.191498	146.230.254.16	192.168.110.142	TCP	60 53 → 52297 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
203 0.191581	192.168.110.142	146.230.254.16	TCP	54 52297 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
204 0.191842	192.168.110.142	146.230.254.16	DNS	99 Standard query 0x850c A xn--mgbam7a8h OPT
205 0.191936	146.230.254.16	192.168.110.142	TCP	60 53 → 52297 [ACK] Seq=1 Ack=46 Win=64240 Len=0
206 0.384256	146.230.254.16	192.168.110.142	DNS	99 Standard query response 0x850c Server failure A xn--mgbam7a8h OPT
207 0.384477	192.168.110.142	146.230.254.16	TCP	54 52297 → 53 [FIN, ACK] Seq=46 Ack=46 Win=64195 Len=0
208 0.384664	146.230.254.16	192.168.110.142	TCP	60 53 → 52297 [ACK] Seq=46 Ack=47 Win=64239 Len=0
209 0.575904	146.230.254.16	192.168.110.142	TCP	60 53 → 52297 [FIN, PSH, ACK] Seq=46 Ack=47 Win=64239 Len=0
210 0.575947	192.168.110.142	146.230.254.16	TCP	54 52297 → 53 [ACK] Seq=47 Ack=47 Win=64195 Len=0

Obr. 14: Záznamy 201-210

- V tejto komunikácii figuruje aplikačný protokol **DNS** a transportný protokol **TCP**.
- **IPv4 adresy** komunikujúcich strán:
 - **Klient:** 192.168.110.142 → MAC: 00:0c:29:fb:b6:1f
 - **Server:** 146.230.254.16 → MAC: 00:50:56:fa:12:6a
- Na strane **klienta** sú využívané dynamické porty z rozsahu **49125-65535**. Na strane **serveru** štandardný port pre **DNS 53**.
- **Priebeh komunikácie:**
 - V prípade TCP prenosu sa komunikácia nadväzuje štandardným **3-way handshake** procesom⁷.
 - Paket **204** žiada DNS dotazom (dotaz typu **A**) server o IP adresu hosta **xn--mgbam7a8h**.
 - Paket **205** je **TCP ACK** správa zo strany serveru klientovi.
 - Nasleduje odpoveď zo strany serveru, že daného hosta nepozná
 - V poslednom kroku sa ukončí TCP spojenie pomocou **4-way handshake**.
 - Hľadané doménové meno **xn--mgbam7a8h** zodpovedá arabskému znaku (neviem ho vysádzať), po preklade do slovenského jazyka naberá význam **Emiráty**.

⁷<https://bit.ly/3g8Xw18>



Obr. 15: .xn--mgbam7a8h

2.7 Záznamy 211-228 - komunikácia s webserverom - TCP, HTTP

Na nasledujúcom obrázku 16 je možné vidieť záznamy 211-228, ktoré budú analyzované v tejto sekcii.

211	*REF*	192.168.1.169	147.229.71.65	TCP	66 63184 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
212	0.000002	192.168.1.169	147.229.71.65	TCP	66 63185 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
213	0.031980	147.229.71.65	192.168.1.169	TCP	68 80 → 63185 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
214	0.031981	147.229.71.65	192.168.1.169	TCP	68 80 → 63184 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
215	0.032128	192.168.1.169	147.229.71.65	TCP	54 63185 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
216	0.032203	192.168.1.169	147.229.71.65	TCP	54 63184 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
217	0.033480	192.168.1.169	147.229.71.65	HTTP	472 GET /~xstodu07/ HTTP/1.1
218	0.043888	147.229.71.65	192.168.1.169	HTTP	649 HTTP/1.1 200 OK (text/html)
219	0.043962	192.168.1.169	147.229.71.65	TCP	54 63185 → 80 [ACK] Seq=419 Ack=596 Win=261376 Len=0
220	0.188550	192.168.1.169	147.229.71.65	TCP	66 63186 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
221	0.188879	192.168.1.169	147.229.71.65	TCP	66 63187 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
222	0.211867	147.229.71.65	192.168.1.169	TCP	68 80 → 63186 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
223	0.211867	147.229.71.65	192.168.1.169	TCP	68 80 → 63187 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
224	0.211995	192.168.1.169	147.229.71.65	TCP	54 63186 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
225	0.212087	192.168.1.169	147.229.71.65	TCP	54 63187 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
226	0.212396	192.168.1.169	147.229.71.65	HTTP	406 GET /favicon.ico HTTP/1.1
227	0.224457	147.229.71.65	192.168.1.169	HTTP	667 HTTP/1.1 404 Not Found (text/html)
228	0.224574	192.168.1.169	147.229.71.65	TCP	54 63186 → 80 [ACK] Seq=353 Ack=614 Win=261376 Len=0

Obr. 16: Záznamy 221-228

- V tejto komunikácii figuruje aplikačný protokol **HTTP** a transportný protokol **TCP**.
- Na strane **klienta** sú využívané dynamické porty z rozsahu **49125-65535**. Na strane **serveru** štandardný port pre HTTP **80**.
- **IPv4 adresy** komunikujúcich strán:
 - **Klient:** 192.168.1.169 → MAC: 10:02:b5:54:8f:c1
 - **Server:** 147.229.71.65 → MAC: 50:d4:f7:ca:f4:00
- **Priebeh komunikácie:**
 - Komunikácia sa v prípade transportného protokolu TCP zaháji štandardne pomocou **3-way handshake** procesu. Sú odoslané dva SYN pakety na server, následne klient obdrží dva SYN, ACK. V poslednom kroku klient odošle na server dva SYN pakety čím otvára spojenie.
 - V pakete **217** klient odošle na server **HTTP GET** požiadavku. Detail tejto požiadavky je možné vidieť na obrázku 17

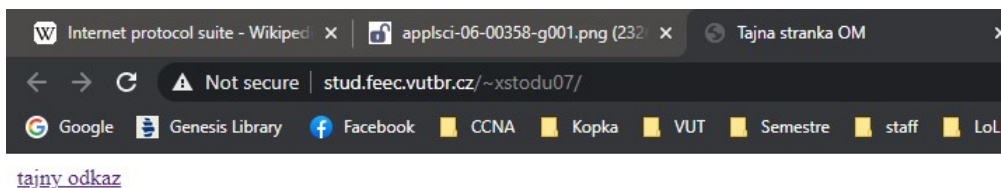
```

Hypertext Transfer Protocol
  GET /~xstodu07/ HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /~xstodu07/ HTTP/1.1\r\n]
      [GET /~xstodu07/ HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /~xstodu07/
    Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US,en;q=0.7,cs;q=0.3\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; ATT-IE11; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate, peerdist\r\n
    Host: www.stud.feec.vutbr.cz\r\n
    Connection: Keep-Alive\r\n
    X-P2P-PeerDist: Version=1.1\r\n
    X-P2P-PeerDistEx: MinContentInformation=1.0, MaxContentInformation=2.0\r\n
    \r\n
    [Full request URI: http://www.stud.feec.vutbr.cz/~xstodu07/]
    [HTTP request 1/1]
    [Response in frame: 218]

```

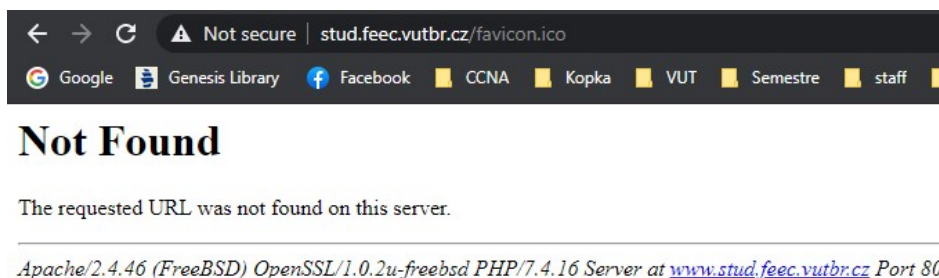
Obr. 17: Detail HTTP GET

- V GET requeste sa nachádzajú detaily požiadavky na server.
- Je možné vidieť aj **Full request URI**: `http://www.stud.feec.vutbr.cz/~xstodu07/`.
- Po otvorení tohto URI nastane presmerovanie na „tajnú“ stránku vid' 18.



Obr. 18: Tajná stránka

- na tejto stránke sa nachádza odkaz na formulár⁸ za bonusové body ☺.
- Paketom **218** server potvrdzuje požiadavku (200 OK).
- Paket **226** predstavuje GET request na prvok **favicon.ico**. URI na tento prvok⁹ sa nachádza opäť v detailoch paketu.
- * Otvorenie tohto odkazu je zamietnuté (404 Not Found), avšak ako vidieť na obrázku 19, odhaľuje verziu *Apache* a verziu *PHP*, ktorá je nainštalovaná na serveri - jedná sa o bezpečnostné riziko.



Obr. 19: Potenciálne bezpečnostné riziko

⁸<https://bit.ly/2RofSRc>

⁹<https://bit.ly/3tjW9QP>

2.8 Záznamy 229-238 - Protokol QUIC

Na nasledujúcom obrázku 20 je možné vidieť záznamy 229-238, ktoré budú analyzované v tejto sekcii.

229 *REF*	10.0.2.15	216.58.201.67	Long Header	QUIC	1392 Initial, DCID=fdeda346e620e2b0, PKN: 1, CRYPTO, PADDING
230 0.000427	10.0.2.15	216.58.201.67	Long Header	QUIC	121 0-RTT, DCID=fdeda346e620e2b0
231 0.023875	216.58.201.67	10.0.2.15	Long Header	QUIC	1392 Initial, SCID=fdeda346e620e2b0, PKN: 1, ACK, CRYPTO, PADDING
232 0.024080	216.58.201.67	10.0.2.15	Long Header	QUIC	278 Handshake, SCID=fdeda346e620e2b0
233 0.024080	216.58.201.67	10.0.2.15	Short Header	QUIC	103 Protected Payload (KP0)
234 0.024523	10.0.2.15	216.58.201.67	Long Header	QUIC	120 Handshake, DCID=fdeda346e620e2b0
235 0.024693	216.58.201.67	10.0.2.15	Short Header	QUIC	654 Protected Payload (KP0)
236 0.025222	10.0.2.15	216.58.201.67	Short Header	QUIC	75 Protected Payload (KP0), DCID=fdeda346e620e2b0
237 0.030802	216.58.201.67	10.0.2.15	Short Header	QUIC	124 Protected Payload (KP0)
238 0.063644	10.0.2.15	216.58.201.67	Short Header	QUIC	75 Protected Payload (KP0), DCID=fdeda346e620e2b0

Obr. 20: Záznamy 229-238

- V tejto komunikácii figuruje aplikačný protokol **QUIC** a transportný protokol **UDP**.
- Na strane **klienta** sú využívané dynamické porty z rozsahu **49125-65535**. Na strane **serveru** štandardný port pre **HTTPS 443**.
- **IPv4 adresy** komunikujúcich strán:
 - **Klient:** 10.0.2.15 → MAC: 08:00:27:08:94:4e
 - **Server:** 216.58.201.57 → MAC: 52:54:00:12:35:02
- **Priebeh komunikácie:**
 - Komunikácia prebieha štandardne pre protokol QUIC.
 - V prvom rade bolo pomocou paketov typu **Long Header** naviazané spojenie a prebehol handshake.
 - Následne po naviazaní spojenia klient začne komunikovať pomocou **Short Header** paketov.
- Objem dát a rýchlosť prenosu je možné vidieť na obrázku 21.
 - Celkovo bolo prenesených 10 paketov rýchlosťou 544 kbit/s. Podiel QUIC pri komunikácii tvorí **3914 B**

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	10	100.0	4334	544k	0	0	0
▼ Ethernet	100.0	10	3.2	140	17k	0	0	0
▼ Internet Protocol Version 4	100.0	10	4.6	200	25k	0	0	0
▼ User Datagram Protocol	100.0	10	1.8	80	10k	0	0	0
QUIC IETF	100.0	10	90.3	3914	491k	10	3914	491k

Display filter: udp.port == 443

Close Copy Help

Obr. 21: Protokol Hierarchy Statistics QUIC

- **Bezpečnosť prenášaných dát:** Všetky prenášané dáta sú zašifrované symetrickou blokovou šifrou AES vid'. 22.
- **Obsah dátovej časti:** V programe nie je možné zobrazíť dátovú časť, práve z dôvodu, že wireshark zachytáva už zašifrované dáta. Ak by bolo potrebné zachytiť nešifrovanú komunikáciu je to možné pomocou nástroja net-export.



Obr. 22: Handshake Protocol

2.9 Záznamy 239-439 - Protokol TCP

Na nasledujúcom obrázku 23 je možné vidieť snippet zo záznamov 239-439, ktoré budú analyzované v tejto sekcii.

239	*REF*	192.168.204.130	192.168.204.1	TCP	66 49732 → 5201 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
240	0.000448	192.168.204.1	192.168.204.130	TCP	66 5201 → 49732 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
241	0.000506	192.168.204.130	192.168.204.1	TCP	54 49732 → 5201 [ACK] Seq=1 Ack=1 Win=262656 Len=0
242	0.000645	192.168.204.130	192.168.204.1	TCP	91 49732 → 5201 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=37
243	0.002920	192.168.204.1	192.168.204.130	TCP	1514 5201 → 49732 [ACK] Seq=1 Ack=38 Win=1051136 Len=1460
244	0.002920	192.168.204.1	192.168.204.130	TCP	1514 5201 → 49732 [ACK] Seq=1461 Ack=38 Win=1051136 Len=1460
245	0.002920	192.168.204.1	192.168.204.130	TCP	1514 5201 → 49732 [ACK] Seq=2921 Ack=38 Win=1051136 Len=1460
246	0.002920	192.168.204.1	192.168.204.130	TCP	1514 5201 → 49732 [ACK] Seq=4381 Ack=38 Win=1051136 Len=1460
247	0.002920	192.168.204.1	192.168.204.130	TCP	1514 5201 → 49732 [ACK] Seq=5841 Ack=38 Win=1051136 Len=1460
248	0.002920	192.168.204.1	192.168.204.130	TCP	1514 5201 → 49732 [ACK] Seq=7301 Ack=38 Win=1051136 Len=1460
249	0.002920	192.168.204.1	192.168.204.130	TCP	1514 5201 → 49732 [ACK] Seq=8761 Ack=38 Win=1051136 Len=1460

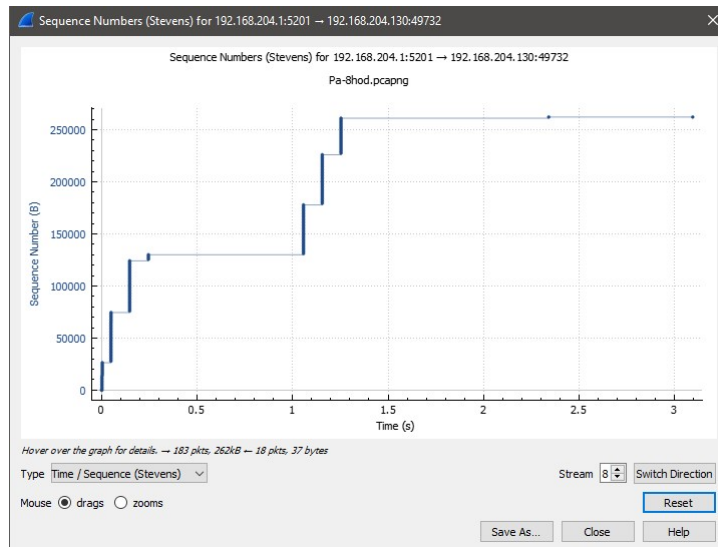
Obr. 23: Záznamy 239-249

- V tejto komunikácii figuruje transportný protokol **TCP**.
- Na strane **klienta** sú využívané dynamické porty z rozsahu 49125-65535 konkrétne **49 732**. Na strane serveru je využívaný port **5201**, ktorý podľa zdroja¹⁰ patrí aplikácii *Iperf*¹¹.
- **IPv4 adresy** komunikujúcich strán:
 - **Klient:** 192.168.204.130 → MAC: 00:0c:29:6f:52:b6
 - **Server:** 192.168.204.130 → MAC: 00:50:56:c0:00:08
- **Priebeh komunikácie:**
 - Pakety **239-242** pomocou 3-way handshake procesu sa otvorí spojenie.
 - Komunikácia sa javí byť bezproblémová, server pravidelne bez retransmisií posíla pakety klientovi, ktorý mu v pravidelných intervaloch odpovedá **ACK** správou.
 - Na grafe 24 je možné vidieť ako sa postupne zvyšovali hodnoty sekvenčných čísel. Nárast je viacmenej **lineárny** bez strát.
 - Na grafe 25 je možné vidieť priepustnosť linky. Z grafu je možné konštatovať, že hodnota je konštantná. Prípadné kolísania sú zapríčinené ACK paketmi zo strany klienta. Postupné utlmenie vidíme v čase $t = 2$ s, keď dochádza k ukončeniu spojenia zo strany klienta pomocou **4-way handshake** mechanizmu.

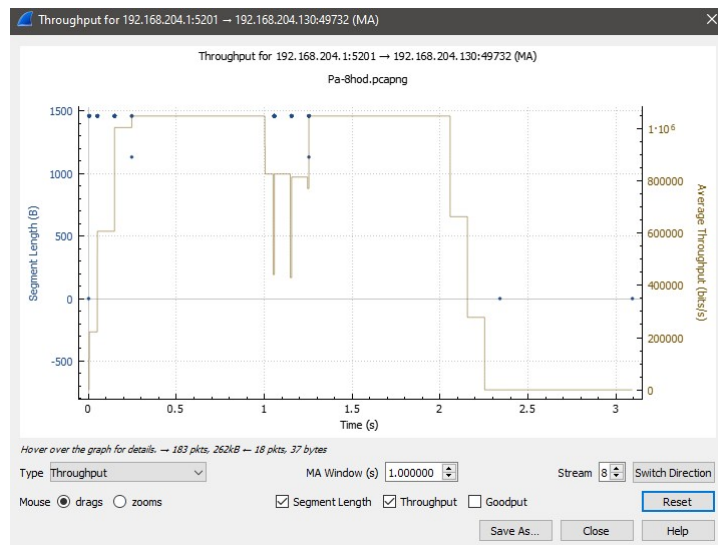
¹⁰<https://bit.ly/2Q19vDa>

¹¹<https://bit.ly/3a5ydJt>

- Na grafe 26 je možné vidieť celkový objem prenesených dát a rýchlosť prenosu. Celkovo bolo prenesených 201 paketov, rýchlosťou 706 kbit/s o celkovej veľkosti **273 071 B**.
- Sieťová komunikácia nie je šifrovaná, veľkosť dátovej časti jednotlivých paketov je **1460 B**.



Obr. 24: Graf nárastu sekvenčných čísel



Obr. 25: Throughput

Wireshark - Protocol Hierarchy Statistics - Pa-8hod.pcapng								
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	201	100.0	273071	706k	0	0	0
▼ Ethernet	100.0	201	1.0	2814	7276	0	0	0
▼ Internet Protocol Version 4	100.0	201	1.5	4020	10k	0	0	0
▼ Transmission Control Protocol	100.0	201	97.5	266225	688k	20	424	1096
Data	90.0	181	96.0	262181	677k	181	262181	677k

Display filter: tcp.stream eq 8

Close Copy Help

Obr. 26: Protocol Hierarchy Statistics - TCP

3 Záver

V tomto projekte bol analyzovaný súbor .pcapng. Súbor bol rozdelený do logických na seba nadväzujúcich celkov, ktoré sú uvedené ako podkapitoly v tejto projektovej dokumentácii. V podkapitole 2.1 boli analyzované pakety 1-22, jednalo sa o ECHO IPv4 komunikáciu. V podkapitole 2.2 boli analyzované pakety 23-46, jednalo sa o ECHO IPv6 komunikáciu. V podkapitole 2.3 boli analyzované pakety 47-82, jednalo sa o DNS komunikáciu, kde figurovalo ako UDP tak aj TCP. V podkapitole 2.4 boli analyzované pakety 83-104, jednalo sa o ďalší typ DNS komunikácie. V podkapitole 2.5 boli analyzované pakety 105-200, jednalo sa o ICMP komunikáciu. V podkapitole 2.6 boli analyzované pakety 201-210, jednalo sa o komunikáciu so serverom pomocou transportného protokolu TCP. Bolo potrebné zistiť význam arabského symbolu, ktorý našiel využitie v ďalšej podkapitole. V podkapitole 2.7 boli analyzované pakety 211-228, jednalo sa o ďalší typ komunikácie so serverom, v tomto prípade figurovali protokoly TCP a HTTP. V tejto podkapitole bolo možné objaviť tajný odkaz z formulárom. V podkapitole 2.8 boli analyzované pakety 229-238, jednalo sa o sieťový protokol transportnej vrstvy - QUIC. V podkapitole 2.9 boli analyzované pakety 239-439, jednalo sa o komunikáciu TCP. Výstupom každej kapitoly sú komentáre, grafy, obrázky a štatistiky. Bola taktiež splnená bonusová úloha, ktorá bola popísaná v podkapitolách 2.6 a 2.7.