Міністерство освіти і науки України
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра програмування

Звіт
до лабораторної роботи №3
з теми
“Інтерфейс аналізатора пакетів Wireshark”

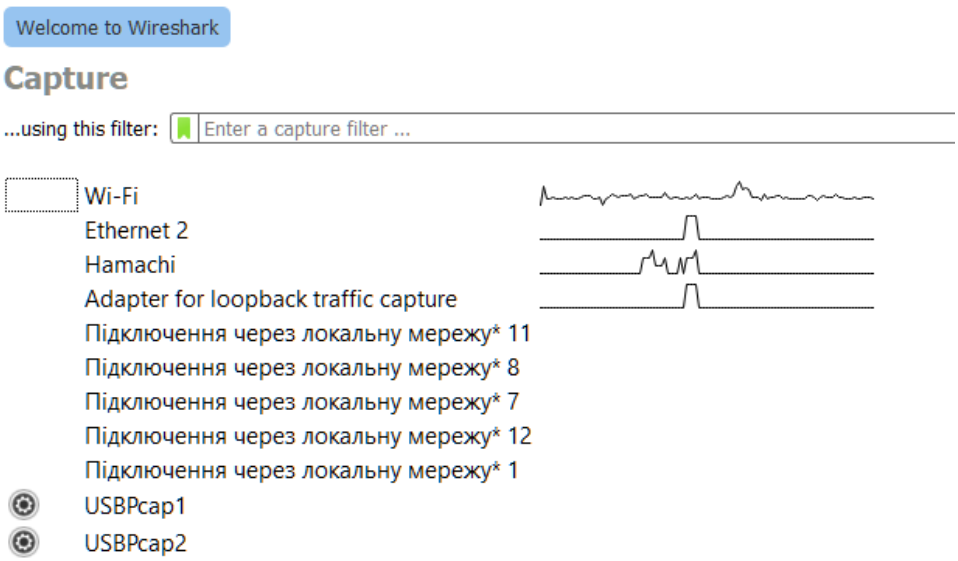
Підготував:
студент ПМІ-31
Процьків Назарій

Львів 2023

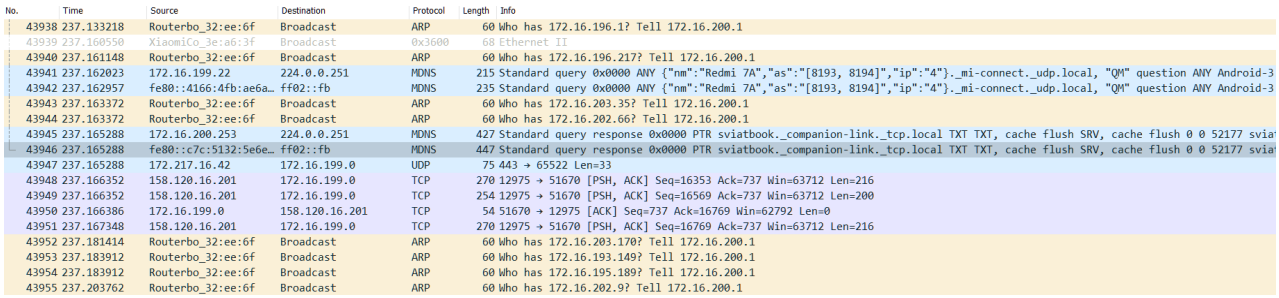
Мета: Отримати загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомитися з графічним інтерфейсом програми, навчитися захоплювати, сортувати і фільтрувати пакети.

Хід роботи

1. Для виконання цієї лабораторної інсталював аналізатор мережевих пакетів Wireshark та Npcap, драйвер для захоплення мережевого трафіку.
2. Відкрив його у режимі адміністратора:



   Обрав з переліку потрібний мережевий інтерфейс та почав процедуру захоплення пакетів.
3. Здійснив перехід на сайт у браузері.
4. Ознайомився з трьома основними елементами головного вікна програми.



No.	Time	Source	Destination	Protocol	Length	Info
43938	237.133218	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.196.1? Tell 172.16.200.1
43939	237.160550	XiaomiCo_3e:a6:3f	Broadcast	0x3600	68	Ethernet II
43940	237.161148	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.196.217? Tell 172.16.200.1
43941	237.162023	172.16.199.22	224.0.0.251	MDNS	215	Standard query 0x0000 ANY {"nm":"Redmi 7A","as":"[8193, 8194]","ip":"4"}._mi-connect._udp.local, "QM" question ANY Android-3
43942	237.162957	fe80::4166:4fb:ae6a…	ff02::fb	MDNS	235	Standard query 0x0000 ANY {"nm":"Redmi 7A","as":"[8193, 8194]","ip":"4"}._mi-connect._udp.local, "QM" question ANY Android-3
43943	237.163372	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.35? Tell 172.16.200.1
43944	237.163372	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.202.66? Tell 172.16.200.1
43945	237.165288	172.16.200.253	224.0.0.251	MDNS	427	Standard query response 0x0000 PTR sviatbook._companion-link._tcp.local TXT TXT, cache flush SRV, cache flush 0 0 52177 svia
43946	237.165288	fe80::c7c:5132:5e6e…	ff02::fb	MDNS	447	Standard query response 0x0000 PTR sviatbook._companion-link._tcp.local TXT TXT, cache flush SRV, cache flush 0 0 52177 svia
43947	237.165288	172.217.16.42	172.16.199.0	UDP	75	443 → 65522 Len=33
43948	237.166352	158.120.16.201	172.16.199.0	TCP	270	12975 → 51670 [PSH, ACK] Seq=16353 Ack=737 Win=63712 Len=216
43949	237.166352	158.120.16.201	172.16.199.0	TCP	254	12975 → 51670 [PSH, ACK] Seq=16569 Ack=737 Win=63712 Len=200
43950	237.166386	172.16.199.0	158.120.16.201	TCP	54	51670 → 12975 [ACK] Seq=737 Ack=16769 Win=62792 Len=0
43951	237.167348	158.120.16.201	172.16.199.0	TCP	270	12975 → 51670 [PSH, ACK] Seq=16769 Ack=737 Win=63712 Len=216
43952	237.181414	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.170? Tell 172.16.200.1
43953	237.183912	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.193.149? Tell 172.16.200.1
43954	237.183912	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.195.189? Tell 172.16.200.1
43955	237.203762	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.202.9? Tell 172.16.200.1

```
Frame 43946: 447 bytes on wire (3576 bits), 447 bytes captured (3576 bits) on interface \Device\NPF_{
    Section number: 1
    Interface id: 0 (\Device\NPF_{8B57350D-B6BD-4305-8E40-6D0F4C2B595C})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 19, 2023 15:22:47.381771000 Фінляндія (літо)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1695126167.381771000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 237.165288000 seconds]
    Frame Number: 43946
    Frame Length: 447 bytes (3576 bits)
    Capture Length: 447 bytes (3576 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:mdns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Apple_97:e9:a1 (9c:3e:53:97:e9:a1), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
```

```
0000  33 33 00 00 00 fb 9c 3e  53 97 e9 a1 86 dd 60 06   33·····> S·····`·
0010  01 00 01 89 11 ff fe 80  00 00 00 00 00 00 0c 7c   ····· ·····|
0020  51 32 5e 6e 4e 65 ff 02  00 00 00 00 00 00 00 00   Q2^nNe·· ·····
0030  00 00 00 00 00 fb 14 e9  14 e9 01 89 ee b7 00 00   ····· ·····
0040  84 00 00 00 00 02 00 00  00 06 0f 5f 63 6f 6d 70   ····· ···_comp
0050  61 6e 69 6f 6e 2d 6c 69  6e 6b 04 5f 74 63 70 05   anion-li nk·_tcp·
0060  6c 6f 63 61 6c 00 00 0c  00 01 00 00 11 94 00 0c   local··· ·····
0070  09 73 76 69 61 74 62 6f  6f 6b c0 0c 09 73 76 69   ·sviatbo ok···svi
0080  61 74 62 6f 6f 6b 0c 5f  64 65 76 69 63 65 2d 69   atbook·_ device-i
0090  6e 66 6f c0 1c 00 10 00  01 00 00 11 94 00 22 0d   nfo····· ·····"·
00a0  6d 6f 64 65 6c 3d 4d 61  63 31 34 2c 37 0a 6f 73   model=Ma c14,7·os
00b0  78 76 65 72 73 3d 32 32  08 69 63 6f 6c 6f 72 3d   xvers=22 ·icolor=
00c0  32 c0 32 00 10 80 01 00  00 11 94 00 7f 07 72 70   2·2····· ····rp
00d0  4d 61 63 3d 30 11 72 70  48 4e 3d 62 35 61 61 64   Mac=0·rp HN=b5aad
00e0  39 32 36 38 33 62 37 0c  72 70 46 6c 3d 30 78 32   92683b7· rpFl=0x2
00f0  30 30 30 30 11 72 70 48  41 3d 61 32 30 64 38 38   0000·rpH A=a20d88
0100  65 65 35 63 31 30 0a 72  70 56 72 3d 34 33 30 2e   ee5c10·r pVr=430.
0110  33 11 72 70 41 44 3d 64  64 35 62 66 38 32 30 65   3·rpAD=d d5bf820e
0120  36 65 66 11 72 70 48 49  3d 64 36 63 34 66 33 36   6ef·rpHI =d6c4f36
0130  32 35 64 36 39 16 72 70  42 41 3d 34 37 3a 41 41   25d69·rp BA=47:AA
0140  3a 39 44 3a 42 32 3a 37  36 3a 35 34 c0 32 00 21   :9D:B2:7 6:54·2·!
0150  80 01 00 00 00 78 00 12  00 00 00 00 cb d1 09 73   ·····x·· ·····s
```

5. Зберіг файл для подальшого аналізу.
6. Натиснувши кнопку пошуку та використовуючи спеціальний вираз **not ip**, знайшов пакети, які не стосуються протоколу IP:

not ip

No.	Time	Source	Destination	Protocol	Length	Info
43100	230.156514	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.196.174? Tell 172.16.200.1
43101	230.156514	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.202.66? Tell 172.16.200.1
43102	230.158153	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.196.217? Tell 172.16.200.1
43103	230.160057	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.35? Tell 172.16.200.1
43105	230.164661	fe80::1493:10e0:b28…	ff02::fb	MDNS	1507	Standard query 0x0000 PTR _companion-link._tcp.local,
43107	230.164661	fe80::1493:10e0:b28…	ff02::fb	MDNS	636	Standard query 0x0000 PTR _airplay._tcp.local, "QM" qu
43109	230.167650	AzureWav_f9:73:d9	Broadcast	ARP	60	Who has 172.16.197.245? Tell 172.16.204.214
43110	230.222688	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.21? Tell 172.16.200.1
43111	230.223585	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.202.242? Tell 172.16.200.1
43112	230.223585	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.199.56? Tell 172.16.200.1
43113	230.268703	8e:76:90:ee:86:09	Broadcast	ARP	60	ARP Announcement for 172.16.197.245
43114	230.269866	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.194.205? Tell 172.16.200.1
43115	230.270773	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.193.183? Tell 172.16.200.1
43116	230.270773	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.200.118? Tell 172.16.200.1
43120	230.315496	fe80::4d7:571f:325:…	ff02::fb	MDNS	463	Standard query response 0x0000 PTR D0880C7594DC@MacBoo
43121	230.315496	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.53? Tell 172.16.200.1
43122	230.315496	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.199.190? Tell 172.16.200.1
43124	230.316975	fe80::1c9b:277f:920…	ff02::fb	MDNS	432	Standard query response 0x0000 TXT, cache flush PTR _r
43125	230.318008	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.192.230? Tell 172.16.200.1

7. Знайшов пакети відправлені з мого локального IP або отримані ним:

ip.addr == 192.168.102.11

No.	Time	Source	Destination	Protocol	Length	Info
6251	17.046838	172.16.199.0	192.168.102.11	DNS	89	Standard query 0xdd59 A api.growingio.com
6518	17.339204	192.168.102.11	172.16.199.0	DNS	162	Standard query response 0xdd59 A api.growingio.com CNAME api.g
7928	23.529091	172.16.199.0	192.168.102.11	DNS	81	Standard query 0xfe0a A outlook.office365.com
7963	23.567947	192.168.102.11	172.16.199.0	DNS	214	Standard query response 0xfe0a A outlook.office365.com CNAME c
8247	24.881843	172.16.199.0	192.168.102.11	DNS	74	Standard query 0x951f A smtp.gmail.com
8263	24.898234	192.168.102.11	172.16.199.0	DNS	90	Standard query response 0x951f A smtp.gmail.com A 64.233.167.1
18488	80.039481	172.16.199.0	192.168.102.11	DNS	103	Standard query 0xf3bd AAAA espresso-pa.clients6.google.com
18492	80.041203	192.168.102.11	172.16.199.0	DNS	133	Standard query response 0xf3bd AAAA espresso-pa.clients6.googl
63345	368.213274	172.16.199.0	192.168.102.11	DNS	91	Standard query 0x6828 A emea.ng.msg.teams.microsoft.com
63357	368.240458	192.168.102.11	172.16.199.0	DNS	211	Standard query response 0x6828 A emea.ng.msg.teams.microsoft.c
92663	579.908138	172.16.199.0	192.168.102.11	DNS	101	Standard query 0xafb9 AAAA clientservices.googleapis.com
92809	580.922882	192.168.102.11	172.16.199.0	DNS	131	Standard query response 0xafb9 AAAA clientservices.googleapis.
6246	17.043474	172.16.199.0	192.168.102.11	TCP	62	62289 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
6248	17.046346	192.168.102.11	172.16.199.0	TCP	62	53 → 62289 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK
6249	17.046415	172.16.199.0	192.168.102.11	TCP	54	62289 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6250	17.046802	172.16.199.0	192.168.102.11	TCP	56	62289 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP segment
6253	17.047902	192.168.102.11	172.16.199.0	TCP	60	53 → 62289 [ACK] Seq=1 Ack=38 Win=64240 Len=0
6520	17.339664	172.16.199.0	192.168.102.11	TCP	54	62289 → 53 [FIN, ACK] Seq=38 Ack=109 Win=64132 Len=0
6526	17.350385	192.168.102.11	172.16.199.0	TCP	60	53 → 62289 [ACK] Seq=109 Ack=39 Win=64240 Len=0

8. Також знайшов пакети відправлені протоколом ARP або через UPD порт 80:

arp||udp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
702	4.293862	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.199.4? Tell 172.16.200.1
706	4.306194	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.204.175? Tell 172.16.200.1
713	4.407580	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.45? Tell 172.16.200.1
714	4.407580	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.21? Tell 172.16.200.1
717	4.407580	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.204.207? Tell 172.16.200.1
718	4.408150	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.197.123? Tell 172.16.200.1
719	4.421282	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.196.174? Tell 172.16.200.1
720	4.421282	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.201.38? Tell 172.16.200.1
721	4.421282	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.193.192? Tell 172.16.200.1
724	4.445636	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.201.95? Tell 172.16.200.1
725	4.446442	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.204.220? Tell 172.16.200.1
726	4.447342	Apple_bf:d2:e1	Broadcast	ARP	60	Who has 172.16.204.70? Tell 172.16.204.84
727	4.452819	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.203.176? Tell 172.16.200.1
730	4.480882	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.199.190? Tell 172.16.200.1
731	4.491893	IntelCor_bc:16:50	Broadcast	ARP	60	Who has 172.16.200.1? Tell 172.16.195.248
732	4.606433	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.195.19? Tell 172.16.200.1
737	4.610364	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.198.157? Tell 172.16.200.1
739	4.612354	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.204.223? Tell 172.16.200.1
741	4.716732	Routerbo_32:ee:6f	Broadcast	ARP	60	Who has 172.16.196.54? Tell 172.16.200.1

9. Пакети відправлені та отримані фізичною адресою мого адаптера:

eth.addr == 40-1C-83-E8-EA-0E

No.	Time	Source	Destination	Protocol	Length	Info
1213	6.817460	142.251.39.74	172.16.199.0	QUIC	1292	Initial, SCID=e1adea8940753ac8, PKN: 1, ACK, CRYPTO, PADDING
1214	6.825028	172.16.199.0	142.251.39.74	QUIC	1292	Initial, DCID=e1adea8940753ac8, PKN: 3, ACK, PADDING
1221	6.834541	142.251.39.74	172.16.199.0	QUIC	1292	Handshake, SCID=e1adea8940753ac8
1222	6.834541	142.251.39.74	172.16.199.0	QUIC	1292	Handshake, SCID=e1adea8940753ac8
1223	6.834876	142.251.39.74	172.16.199.0	QUIC	1292	Handshake, SCID=e1adea8940753ac8
1224	6.835045	142.251.39.74	172.16.199.0	QUIC	250	Protected Payload (KP0)
1225	6.835347	172.16.199.0	142.251.39.74	QUIC	81	Handshake, DCID=e1adea8940753ac8
1227	6.835918	172.16.199.0	142.251.39.74	QUIC	207	Protected Payload (KP0), DCID=e1adea8940753ac8
1229	6.836303	172.16.199.0	142.251.39.74	QUIC	569	Protected Payload (KP0), DCID=e1adea8940753ac8
1248	6.866476	142.251.39.74	172.16.199.0	QUIC	1024	Protected Payload (KP0)
1249	6.866784	142.251.39.74	172.16.199.0	QUIC	163	Protected Payload (KP0)
1250	6.866980	172.16.199.0	142.251.39.74	QUIC	74	Protected Payload (KP0), DCID=e1adea8940753ac8
1254	6.872060	142.251.39.74	172.16.199.0	QUIC	69	Protected Payload (KP0)
1269	6.898617	172.16.199.0	142.251.39.74	QUIC	74	Protected Payload (KP0), DCID=e1adea8940753ac8
1280	6.908618	142.251.39.74	172.16.199.0	QUIC	584	Protected Payload (KP0)
1281	6.908618	142.251.39.74	172.16.199.0	QUIC	163	Protected Payload (KP0)
1282	6.909046	172.16.199.0	142.251.39.74	QUIC	77	Protected Payload (KP0), DCID=e1adea8940753ac8
1294	6.934880	172.16.199.0	142.251.39.74	QUIC	74	Protected Payload (KP0), DCID=e1adea8940753ac8
1319	6.968380	142.251.39.74	172.16.199.0	QUIC	66	Protected Payload (KP0)

10. Пакети відправлені з мого локального IP:

ip.src == 192.168.102.11

No.	Time	Source	Destination	Protocol	Length	Info
6518	17.339204	192.168.102.11	172.16.199.0	DNS	162	Standard query response 0xdd59 A api.growingio.com CNAME api.g
7963	23.567947	192.168.102.11	172.16.199.0	DNS	214	Standard query response 0xfe0a A outlook.office365.com CNAME o
8263	24.898234	192.168.102.11	172.16.199.0	DNS	90	Standard query response 0x951f A smtp.gmail.com A 64.233.167.1
18492	80.041203	192.168.102.11	172.16.199.0	DNS	133	Standard query response 0xf3bd AAAA espresso-pa.clients6.googl
63357	368.240458	192.168.102.11	172.16.199.0	DNS	211	Standard query response 0x6828 A emea.ng.msg.teams.microsoft.c
6248	17.046346	192.168.102.11	172.16.199.0	TCP	62	53 → 62289 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK
6253	17.047902	192.168.102.11	172.16.199.0	TCP	60	53 → 62289 [ACK] Seq=1 Ack=38 Win=64240 Len=0
6526	17.350385	192.168.102.11	172.16.199.0	TCP	60	53 → 62289 [ACK] Seq=109 Ack=39 Win=64240 Len=0
6527	17.350385	192.168.102.11	172.16.199.0	TCP	60	53 → 62289 [FIN, ACK] Seq=109 Ack=39 Win=64240 Len=0
6650	17.650946	192.168.102.11	172.16.199.0	TCP	60	[TCP Retransmission] 53 → 62289 [FIN, ACK] Seq=109 Ack=39 Win=
18485	80.039353	192.168.102.11	172.16.199.0	TCP	62	53 → 62356 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK
18491	80.040616	192.168.102.11	172.16.199.0	TCP	60	53 → 62356 [ACK] Seq=1 Ack=52 Win=64240 Len=0
18497	80.043452	192.168.102.11	172.16.199.0	TCP	60	53 → 62356 [ACK] Seq=80 Ack=53 Win=64240 Len=0
18498	80.043806	192.168.102.11	172.16.199.0	TCP	60	53 → 62356 [FIN, ACK] Seq=80 Ack=53 Win=64240 Len=0

11. Пакети отримані моїм локальним IP:

ip.dst == 192.168.102.11

No.	Time	Source	Destination	Protocol	Length	Info
6251	17.046838	172.16.199.0	192.168.102.11	DNS	89	Standard query 0xdd59 A api.growingio.com
7928	23.529091	172.16.199.0	192.168.102.11	DNS	81	Standard query 0xfe0a A outlook.office365.com
8247	24.881843	172.16.199.0	192.168.102.11	DNS	74	Standard query 0x951f A smtp.gmail.com
18488	80.039481	172.16.199.0	192.168.102.11	DNS	103	Standard query 0xf3bd AAAA espresso-pa.clients6.google.com
63345	368.213274	172.16.199.0	192.168.102.11	DNS	91	Standard query 0x6828 A emea.ng.msg.teams.microsoft.com
92663	579.908138	172.16.199.0	192.168.102.11	DNS	101	Standard query 0xafb9 AAAA clientservices.googleapis.com
6246	17.043474	172.16.199.0	192.168.102.11	TCP	62	62289 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
6249	17.046415	172.16.199.0	192.168.102.11	TCP	54	62289 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6250	17.046802	172.16.199.0	192.168.102.11	TCP	56	62289 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP segment of a reassembled PDU]
6520	17.339664	172.16.199.0	192.168.102.11	TCP	54	62289 → 53 [FIN, ACK] Seq=38 Ack=109 Win=64132 Len=0
6528	17.350413	172.16.199.0	192.168.102.11	TCP	54	62289 → 53 [ACK] Seq=39 Ack=110 Win=64132 Len=0
6651	17.650971	172.16.199.0	192.168.102.11	TCP	54	[TCP ZeroWindow] 62289 → 53 [ACK] Seq=39 Ack=110 Win=0 Len=0
18484	80.038208	172.16.199.0	192.168.102.11	TCP	62	62356 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
18486	80.039397	172.16.199.0	192.168.102.11	TCP	54	62356 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
18487	80.039444	172.16.199.0	192.168.102.11	TCP	56	62356 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP segment of a reassembled PDU]
18493	80.041409	172.16.199.0	192.168.102.11	TCP	54	62356 → 53 [FIN, ACK] Seq=52 Ack=80 Win=64161 Len=0
18499	80.043817	172.16.199.0	192.168.102.11	TCP	54	62356 → 53 [ACK] Seq=53 Ack=81 Win=64161 Len=0
92659	579.893782	172.16.199.0	192.168.102.11	TCP	62	62522 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
92661	579.907769	172.16.199.0	192.168.102.11	TCP	54	62522 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0

12. Пакети http && ftp && arp:

http&&ftp&&arp

No.	Time	Source	Destination	Protocol	Length	Info

13. Пакети відправлені не з моєї локальної IP адреси:

ip.src != 192.168.102.11

No.	Time	Source	Destination	Protocol	Length	Info
6181	16.937977	172.16.199.0	74.125.133.155	TLSv1.3	152	Application Data
6182	16.938343	172.16.199.0	74.125.133.155	TLSv1.3	1021	Application Data
6183	16.938385	172.16.199.0	74.125.133.155	TLSv1.3	187	Application Data
6185	16.949165	140.82.112.25	172.16.199.0	TLSv1.3	127	Application Data
6190	16.969182	140.82.112.25	172.16.199.0	TLSv1.3	80	Application Data
6191	16.969182	140.82.112.25	172.16.199.0	TLSv1.3	78	Application Data
6196	16.981616	74.125.133.155	172.16.199.0	TLSv1.3	1028	Application Data, Application Data
6197	16.981761	74.125.133.155	172.16.199.0	TLSv1.3	85	Application Data
6200	16.981970	172.16.199.0	74.125.133.155	TLSv1.3	85	Application Data
6201	16.983619	74.125.133.155	172.16.199.0	TLSv1.3	400	Application Data
6202	16.983619	74.125.133.155	172.16.199.0	TLSv1.3	86	Application Data
6203	16.983619	74.125.133.155	172.16.199.0	TLSv1.3	85	Application Data
6204	16.983619	74.125.133.155	172.16.199.0	TLSv1.3	93	Application Data
6206	16.983858	74.125.133.155	172.16.199.0	TLSv1.3	123	Application Data
6207	16.984138	172.16.199.0	74.125.133.155	TLSv1.3	93	Application Data
6239	17.021794	172.16.199.0	216.239.36.181	TLSv1.3	594	Client Hello
6243	17.025560	172.16.199.0	106.75.109.179	TLSv1.3	624	Client Hello
6247	17.044003	172.16.199.0	142.251.39.67	TLSv1.3	571	Client Hello
6255	17.067997	216.239.36.181	172.16.199.0	TLSv1.3	1466	Server Hello, Change Cipher Spec

14. Ознайомився з пунктами у меню Statistics.
15. CaptureFileProperties – показує дані про пакети записані у файлі, час, та статистику пакетів.

Подробиці

Файл

Ім'я:	C:\Users\Admin\AppData\Local\Temp\wireshark_Wi-FiE9SOB2.pcapng
Розмір:	38 MB
Hash (SHA256):	e46b2750b4399da3fe32da5095bcfeef7048ed78a72926f24314dd794b7e7bdd
Hash (RIPEMD160):	b2f8940ed3f43f6749e0e5db978ff1c32df0f1a1
Hash (SHA1):	9c6491980c9be071fbb91abe65cf96efee65bc62
Формат:	Wireshark/... - pcapng
Інкапсуляція:	Ethernet

Час

Перший пакет:	2023-09-19 15:29:07
Останній пакет:	2023-09-19 15:45:38
Витрачено:	00:16:31

Захоплення

Апаратне забезпечення:	11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz (with SSE4.2)
ОС:	64-bit Windows 10 (22H2), build 19045
Застосунок:	Dumpcap (Wireshark) 4.0.8 (v4.0.8-0-g81696bb74857)

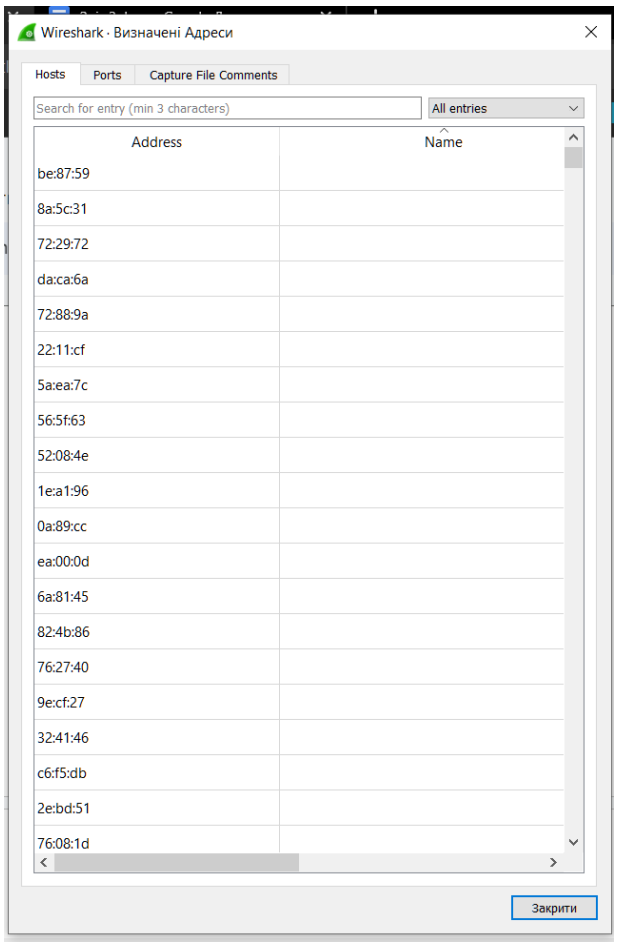
Інтерфейси

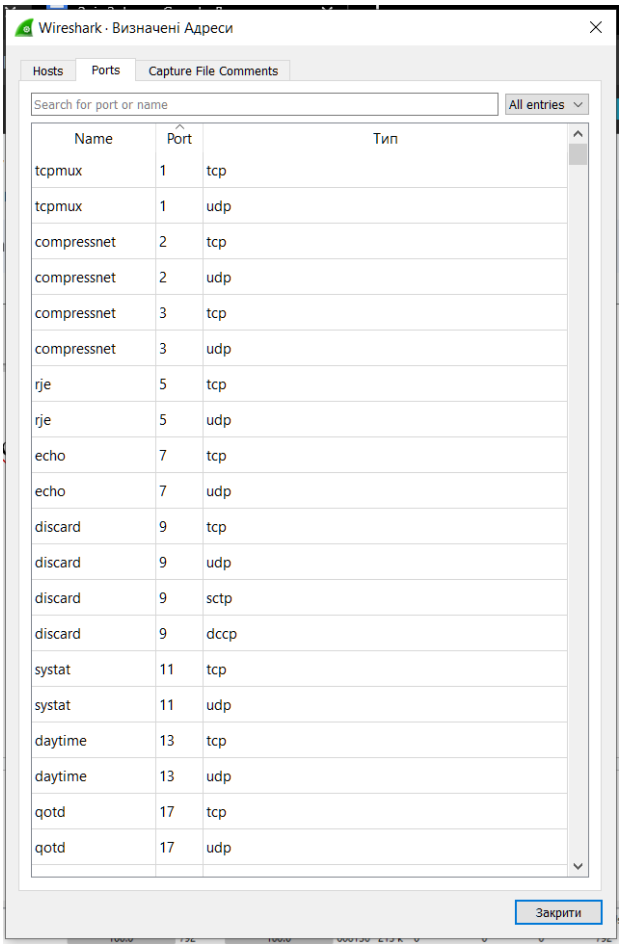
Інтерфейс	Відкинуті пакети	Фільтр захоплення	Тип з'єднання	Packet size limit (snaplen)
Wi-Fi	Невідомо	відсутній	Ethernet	262144 байтів

Статистика

Вимір	Захоплено	Відображено	Позначено
Пакетів	150228	58414 (38.9%)	—
Проміжок часу, с	991.642	991.642	—
Середнє пзс	151.5	58.9	—
Середній розмір пакету, Б	222	333	—
Байтів	33383030	19478602 (58.3%)	0
Байт/с (середнє значення)	33 k	19 k	—
біт/с (середнє значення)	269 k	157 k	—

16. ResolvedAddresses – має фізичні адреси, які отримували пакети або відправляли, а також порт та протокол за яким відправлено в другій вкладці.



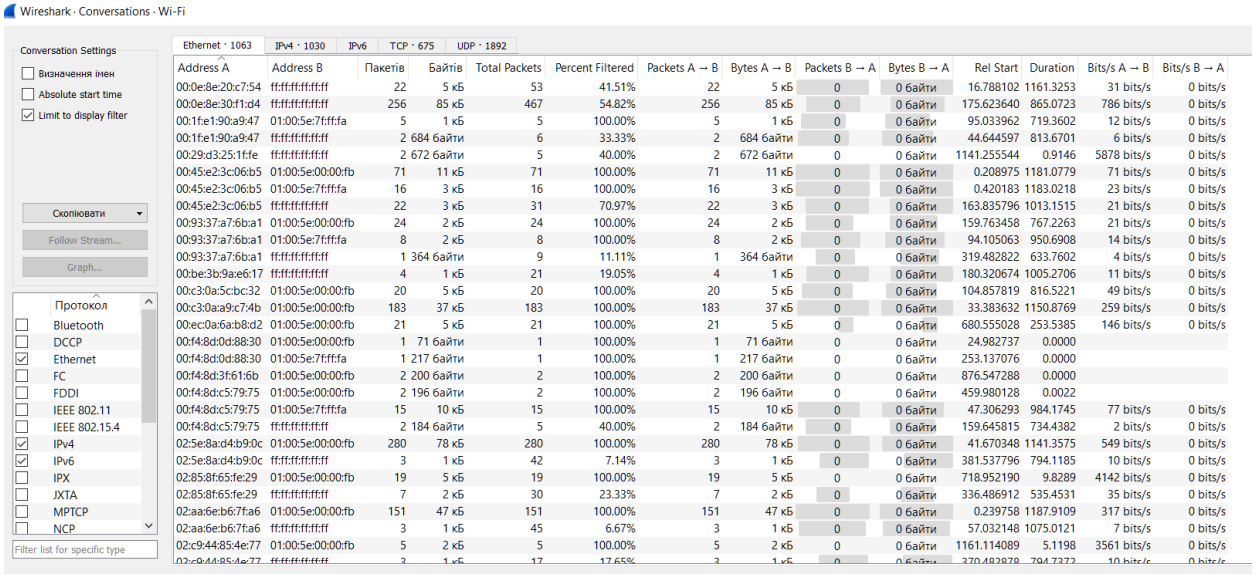


17. ProtocolHierarchy – показує ієрархію розподілення пакетів.

Wireshark · Protocol Hierarchy Statistics · Wi-Fi

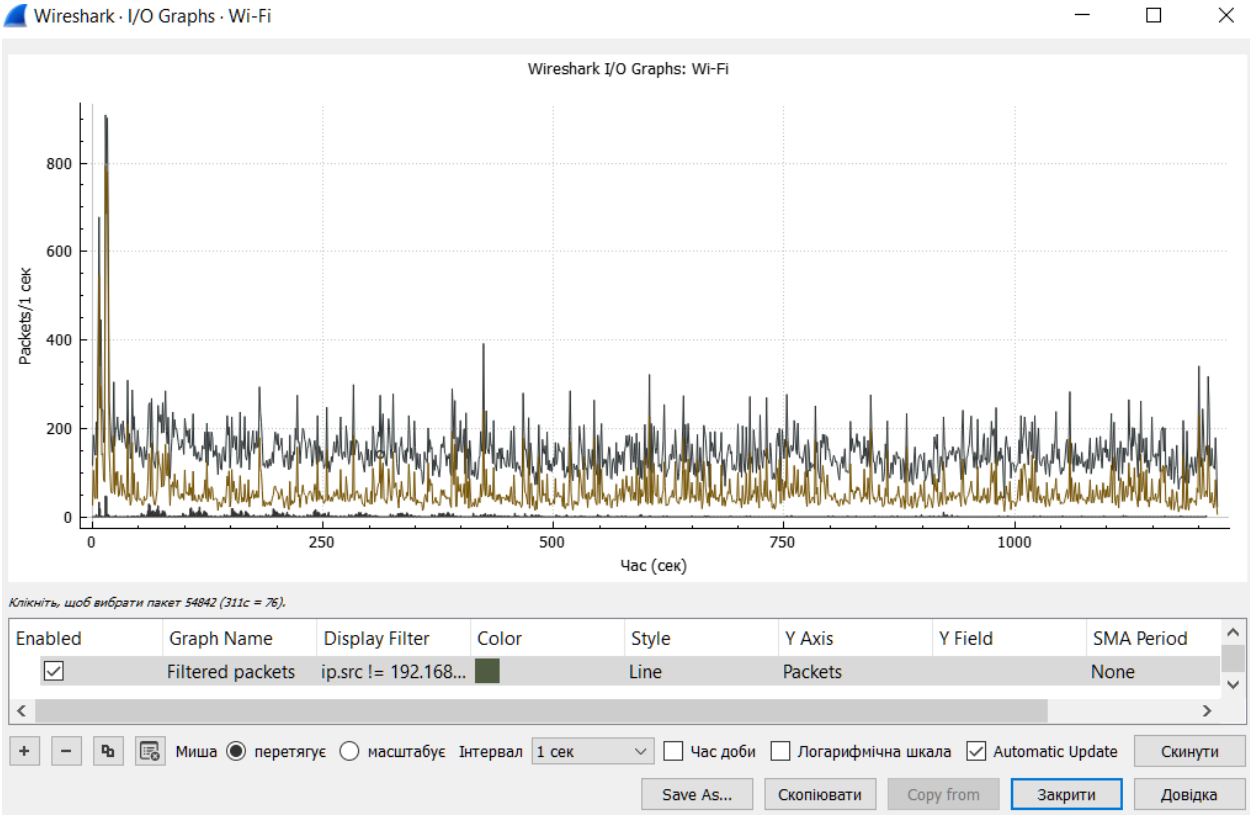
Протокол	Percent Packets	Пакетів	Percent Bytes	Байтів	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	67228	100.0	22316132	155 k	0	0	0	67228
Ethernet	100.0	67228	4.3	954028	6635	0	0	0	67228
Internet Protocol Version 4	100.0	67228	6.0	1344680	9353	0	0	0	67228
User Datagram Protocol	82.5	55460	2.0	443680	3086	0	0	0	55460
Steam In-Home Streaming Discovery Protocol	0.0	25	0.0	3933	27	25	3933	27	25
Simple Service Discovery Protocol	1.6	1074	0.8	186135	1294	1074	186135	1294	1074
QUIC IETF	8.1	5429	11.8	2641045	18 k	5429	2427047	16 k	5728
NetBIOS Name Service	0.7	496	0.1	26258	182	496	26258	182	496
NetBIOS Datagram Service	0.1	91	0.1	16647	115	0	0	0	91
SMB (Server Message Block Protocol)	0.1	91	0.0	9185	63	0	0	0	91
SMB MailSlot Protocol	0.1	91	0.0	2371	16	0	0	0	91
Microsoft Windows Browser Protocol	0.1	79	0.0	903	6	79	903	6	79
Multicast Domain Name System	55.9	37576	42.1	9389138	65 k	37574	9388742	65 k	37576
Malformed Packet	0.0	2	0.0	0	0	2	0	0	2
Mikrotik Neighbor Discovery Protocol	0.2	107	0.1	13417	93	107	13417	93	107
Link-local Multicast Name Resolution	0.1	73	0.0	2070	14	73	2070	14	73
Dynamic Host Configuration Protocol	2.8	1907	2.6	578195	4021	1907	578195	4021	1907
Dropbox LAN sync Discovery Protocol	3.3	2247	3.3	744526	5178	2247	744526	5178	2247
Domain Name System	0.2	103	0.1	21038	146	103	21038	146	103

18. Conversations показує сумарні дані фізичними адресами, ip.

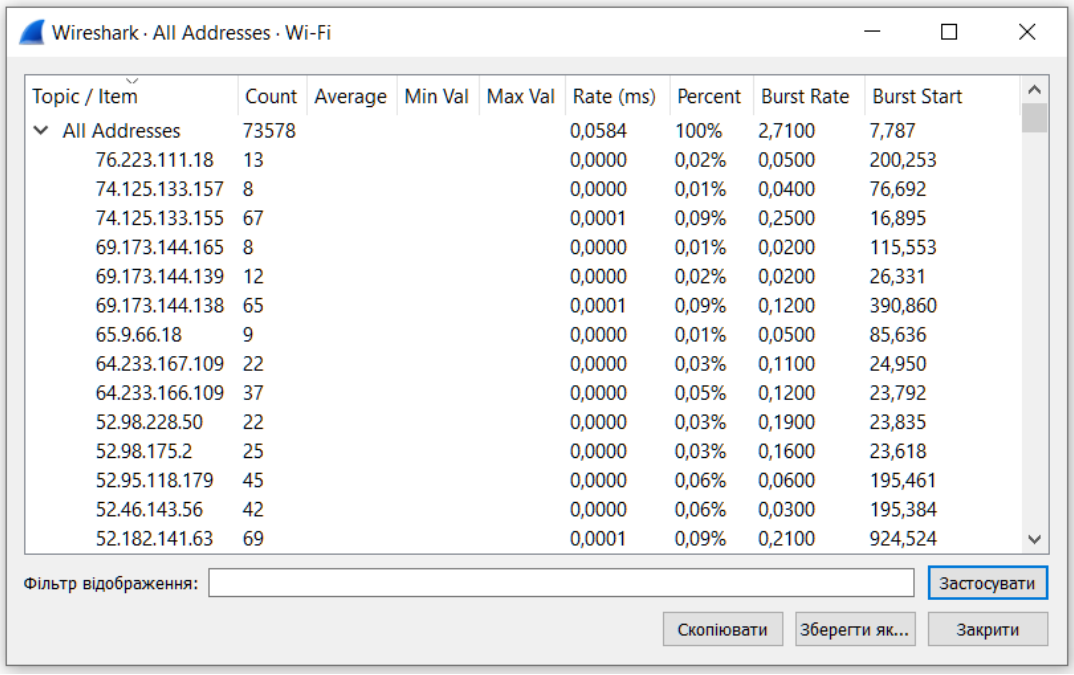


Address A	Address B	Пакетів	Байтів	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:0e:8e:20:c7:54	ff:ff:ff:ff:ff:ff	22	5 кБ	53	41.51%	22	5 кБ	0	0 байти	16.788102	1161.3253	31 bits/s	0 bits/s
00:0e:8e:30:f1:d4	ff:ff:ff:ff:ff:ff	256	85 кБ	467	54.82%	256	85 кБ	0	0 байти	175.623640	865.0723	786 bits/s	0 bits/s
00:1f:e1:90:a9:47	01:00:5e:7f:ff:fa	5	1 кБ	5	100.00%	5	1 кБ	0	0 байти	95.033962	719.3602	12 bits/s	0 bits/s
00:1f:e1:90:a9:47	ff:ff:ff:ff:ff:ff	2	684 байти	6	33.33%	2	684 байти	0	0 байти	44.644597	813.6701	6 bits/s	0 bits/s
00:29:d3:25:1f:fe	ff:ff:ff:ff:ff:ff	2	672 байти	5	40.00%	2	672 байти	0	0 байти	1141.255544	0.9146	5878 bits/s	0 bits/s
00:45:e2:3c:06:b5	01:00:5e:00:00:fb	71	11 кБ	71	100.00%	71	11 кБ	0	0 байти	0.208975	1181.0779	71 bits/s	0 bits/s
00:45:e2:3c:06:b5	01:00:5e:7f:ff:fa	16	3 кБ	16	100.00%	16	3 кБ	0	0 байти	0.420183	1183.0218	23 bits/s	0 bits/s
00:45:e2:3c:06:b5	ff:ff:ff:ff:ff:ff	22	3 кБ	31	70.97%	22	3 кБ	0	0 байти	163.835796	1013.1515	21 bits/s	0 bits/s
00:93:37:a7:6b:a1	01:00:5e:00:00:fb	24	2 кБ	24	100.00%	24	2 кБ	0	0 байти	159.763458	767.2263	21 bits/s	0 bits/s
00:93:37:a7:6b:a1	01:00:5e:7f:ff:fa	8	2 кБ	8	100.00%	8	2 кБ	0	0 байти	94.105063	950.6908	14 bits/s	0 bits/s
00:93:37:a7:6b:a1	ff:ff:ff:ff:ff:ff	1	364 байти	9	11.11%	1	364 байти	0	0 байти	319.482822	633.7602	4 bits/s	0 bits/s
00:be:3b:9a:e6:17	ff:ff:ff:ff:ff:ff	4	1 кБ	21	19.05%	4	1 кБ	0	0 байти	180.320674	1005.2706	11 bits/s	0 bits/s
00:c3:0a:5c:bc:32	01:00:5e:00:00:fb	20	5 кБ	20	100.00%	20	5 кБ	0	0 байти	104.857819	816.5221	49 bits/s	0 bits/s
00:c3:0a:a9:c7:4b	01:00:5e:00:00:fb	183	37 кБ	183	100.00%	183	37 кБ	0	0 байти	33.383632	1150.8769	259 bits/s	0 bits/s
00:ec:0a:6a:b8:d2	01:00:5e:00:00:fb	21	5 кБ	21	100.00%	21	5 кБ	0	0 байти	680.555028	253.5385	146 bits/s	0 bits/s
00:f4:8d:0d:88:30	01:00:5e:00:00:fb	1	71 байти	1	100.00%	1	71 байти	0	0 байти	24.982737	0.0000		
00:f4:8d:0d:88:30	01:00:5e:7f:ff:fa	1	217 байти	1	100.00%	1	217 байти	0	0 байти	253.137076	0.0000		
00:f4:8d:3f:61:6b	01:00:5e:00:00:fb	2	200 байти	2	100.00%	2	200 байти	0	0 байти	876.547288	0.0000		
00:f4:8d:c5:79:75	01:00:5e:00:00:fb	2	196 байти	2	100.00%	2	196 байти	0	0 байти	459.980128	0.0022		
00:f4:8d:c5:79:75	01:00:5e:7f:ff:fa	15	10 кБ	15	100.00%	15	10 кБ	0	0 байти	47.306293	984.1745	77 bits/s	0 bits/s
00:f4:8d:c5:79:75	ff:ff:ff:ff:ff:ff	2	184 байти	5	40.00%	2	184 байти	0	0 байти	159.645815	734.4382	2 bits/s	0 bits/s
02:5e:8a:d4:b9:0c	01:00:5e:00:00:fb	280	78 кБ	280	100.00%	280	78 кБ	0	0 байти	41.670348	1141.3575	549 bits/s	0 bits/s
02:5e:8a:d4:b9:0c	ff:ff:ff:ff:ff:ff	3	1 кБ	42	7.14%	3	1 кБ	0	0 байти	381.537796	794.1185	10 bits/s	0 bits/s
02:85:8f:65:fe:29	01:00:5e:00:00:fb	19	5 кБ	19	100.00%	19	5 кБ	0	0 байти	718.952190	9.8289	4142 bits/s	0 bits/s
02:85:8f:65:fe:29	ff:ff:ff:ff:ff:ff	7	2 кБ	30	23.33%	7	2 кБ	0	0 байти	336.486912	535.4531	35 bits/s	0 bits/s
02:aa:6e:b6:7f:a6	01:00:5e:00:00:fb	151	47 кБ	151	100.00%	151	47 кБ	0	0 байти	0.239758	1187.9109	317 bits/s	0 bits/s
02:aa:6e:b6:7f:a6	ff:ff:ff:ff:ff:ff	3	1 кБ	45	6.67%	3	1 кБ	0	0 байти	57.032148	1075.0121	7 bits/s	0 bits/s
02:c9:44:85:4e:77	01:00:5e:00:00:fb	5	2 кБ	5	100.00%	5	2 кБ	0	0 байти	1161.114089	5.1198	3561 bits/s	0 bits/s
02:c9:44:85:4e:77	ff:ff:ff:ff:ff:ff	3	1 кБ	17	17.65%	3	1 кБ	0	0 байти	370.482878	794.7372	10 bits/s	0 bits/s

19. I/OGraph – графік отриманих та відправлених пакетів.



20. IPv4Statistics – показує всі адреси ipv4, які є у файлі та статистичні дані про них.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	73578				0,0584	100%	2,7100	7,787
76.223.111.18	13				0,0000	0,02%	0,0500	200,253
74.125.133.157	8				0,0000	0,01%	0,0400	76,692
74.125.133.155	67				0,0001	0,09%	0,2500	16,895
69.173.144.165	8				0,0000	0,01%	0,0200	115,553
69.173.144.139	12				0,0000	0,02%	0,0200	26,331
69.173.144.138	65				0,0001	0,09%	0,1200	390,860
65.9.66.18	9				0,0000	0,01%	0,0500	85,636
64.233.167.109	22				0,0000	0,03%	0,1100	24,950
64.233.166.109	37				0,0000	0,05%	0,1200	23,792
52.98.228.50	22				0,0000	0,03%	0,1900	23,835
52.98.175.2	25				0,0000	0,03%	0,1600	23,618
52.95.118.179	45				0,0000	0,06%	0,0600	195,461
52.46.143.56	42				0,0000	0,06%	0,0300	195,384
52.182.141.63	69				0,0001	0,09%	0,2100	924,524

Висновок: отримав загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомився з графічним інтерфейсом програми, навчився захоплювати, сортувати та фільтрувати пакети.