

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №3

Інтерфейс аналізатора пакетів Wireshark

Виконав:

Студент групи ПМі-31

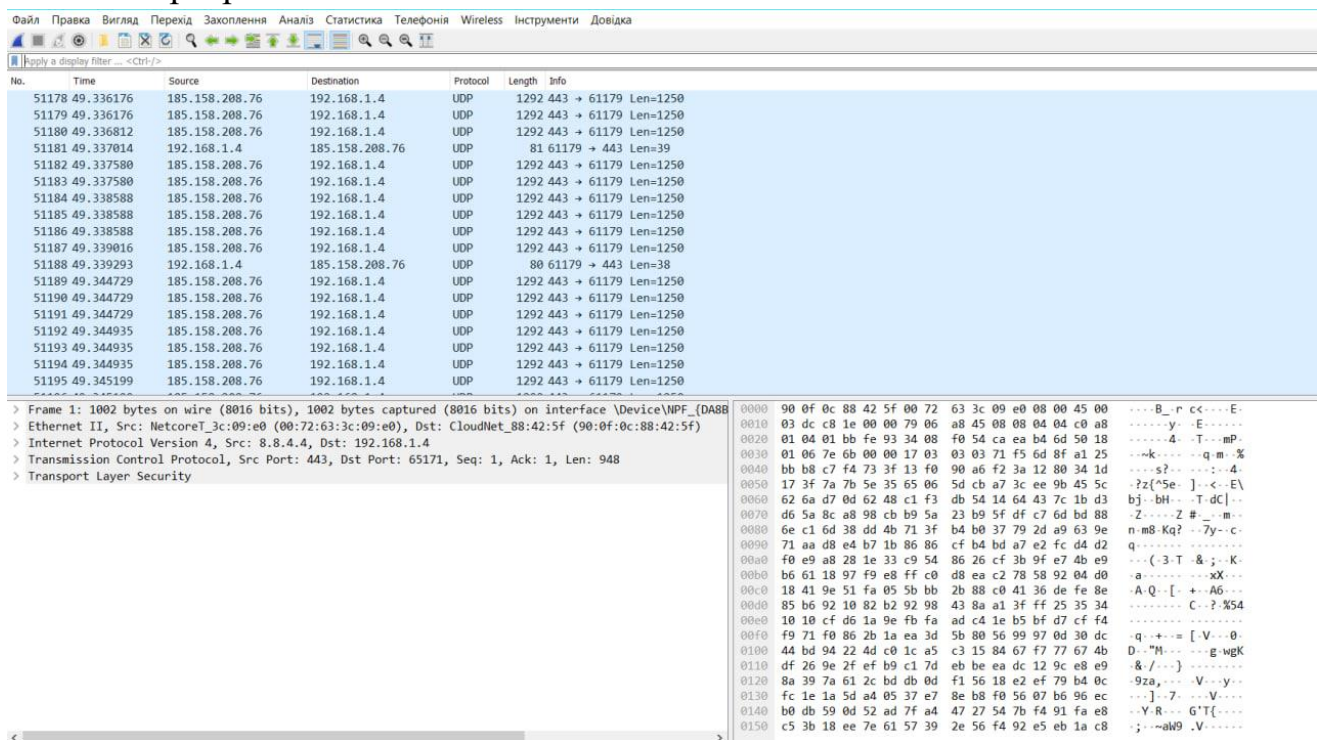
Яцуляк Андрій

2023

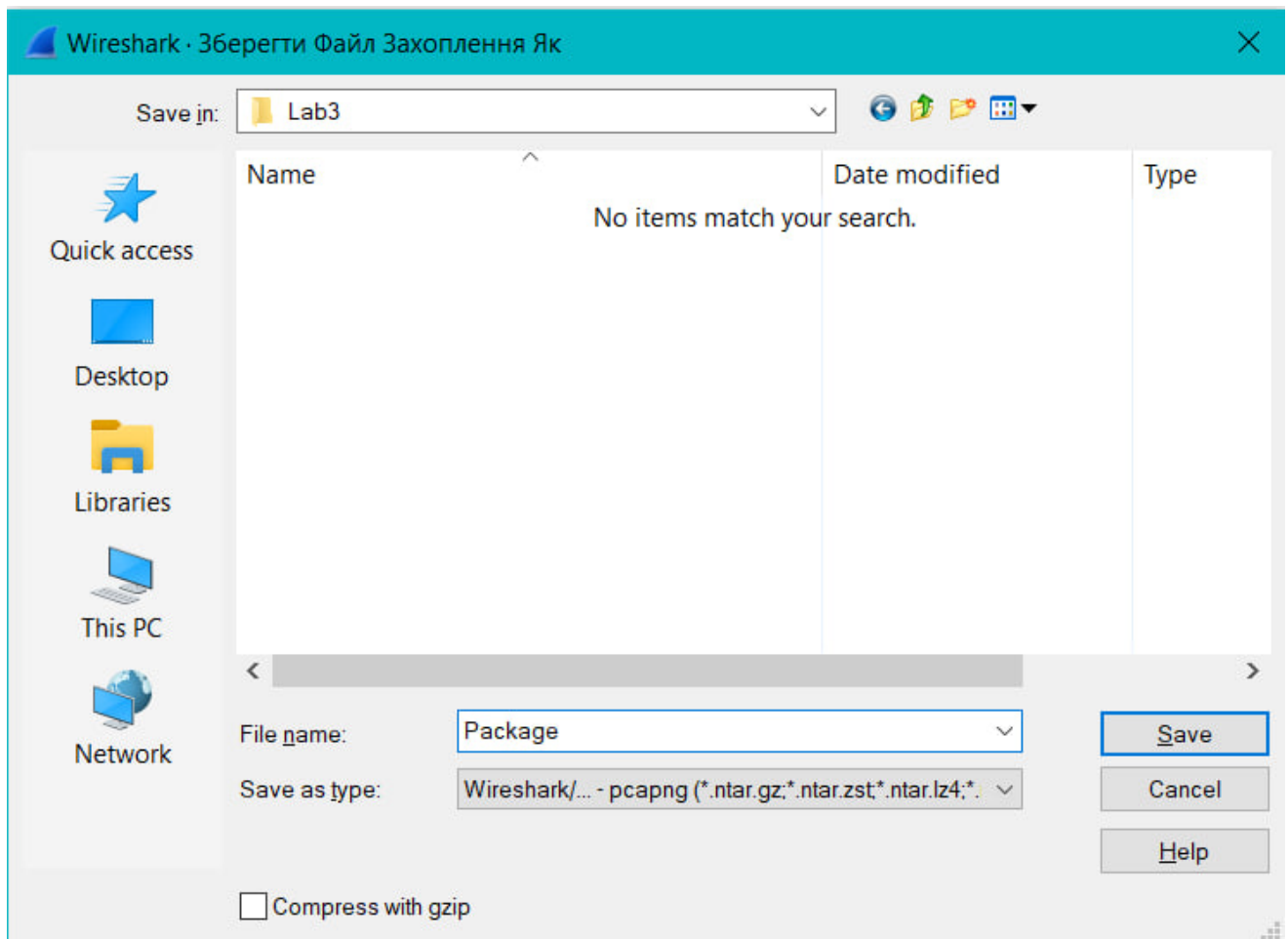
Мета: Отримати загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомитися з графічним інтерфейсом програми, навчитися захоплювати, сортувати та фільтрувати пакети.

Хід роботи

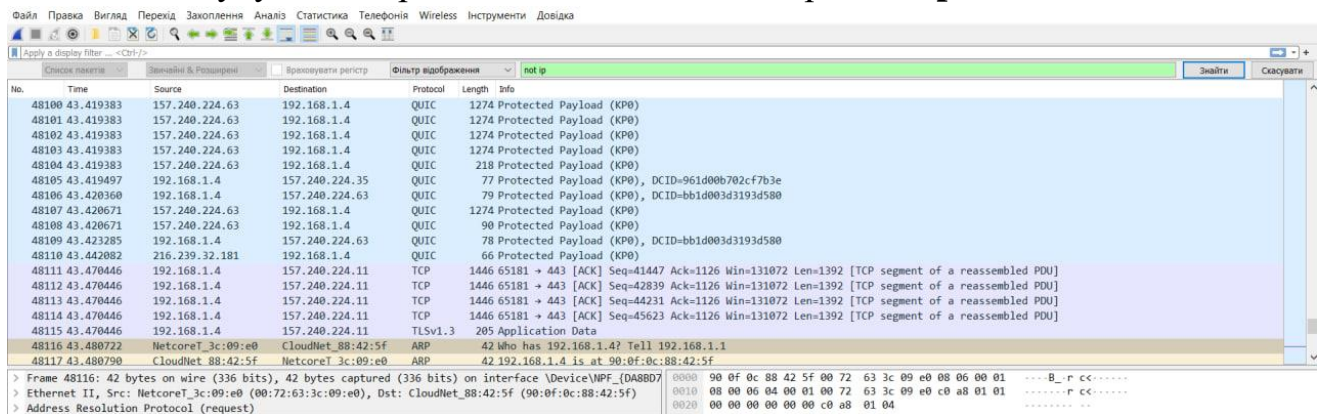
1. Опрацював теоретичний матеріал.
2. Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора.
3. Вибрав з переліку потрібний мережевий інтерфейс та почав процедуру.
4. Упродовж 60 секунд здійснив активність в браузері (перейшов на сайт, залогінився, скачав файл).
5. Зупинив процедуру захоплення пакетів.
6. Ознайомився з трьома основними елементами головного вікна програми:



7. Зберіг захоплені пакети у файл для подальшого аналізу:



8. Знайшов пакети, які не стосуються протоколу IP, натиснувши кнопку пошуку та використавши спеціальний вираз **not ip**:



9. Поекспериментував з різними виразами:

- `ip.addr == 192.168.1.4` – пакети, які були відправлені з мого IPv4 або отримані ним:

No.	Time	Source	Destination	Protocol	Length	Info
48099	43.419383	157.240.224.63	192.168.1.4	QUIC	1274	Protected Payload (KP0)
48100	43.419383	157.240.224.63	192.168.1.4	QUIC	1274	Protected Payload (KP0)
48101	43.419383	157.240.224.63	192.168.1.4	QUIC	1274	Protected Payload (KP0)
48102	43.419383	157.240.224.63	192.168.1.4	QUIC	1274	Protected Payload (KP0)
48103	43.419383	157.240.224.63	192.168.1.4	QUIC	1274	Protected Payload (KP0)
48104	43.419383	157.240.224.63	192.168.1.4	QUIC	218	Protected Payload (KP0)
48105	43.419497	192.168.1.4	157.240.224.35	QUIC	77	Protected Payload (KP0), DCID=961d00b702cf7b3e
48106	43.420360	192.168.1.4	157.240.224.63	QUIC	79	Protected Payload (KP0), DCID=bb1d003d3193d580
48107	43.420671	157.240.224.63	192.168.1.4	QUIC	1274	Protected Payload (KP0)
48108	43.420671	157.240.224.63	192.168.1.4	QUIC	90	Protected Payload (KP0)
48109	43.423285	192.168.1.4	157.240.224.63	QUIC	78	Protected Payload (KP0), DCID=bb1d003d3193d580
48110	43.442082	216.239.32.181	192.168.1.4	QUIC	66	Protected Payload (KP0)
48111	43.470446	192.168.1.4	157.240.224.11	TCP	1446	65181 + 443 [ACK] Seq=41447 Ack=1126 Win=131072 Len=1392 [TCP segment of a reassembled PDU]
48112	43.470446	192.168.1.4	157.240.224.11	TCP	1446	65181 + 443 [ACK] Seq=42839 Ack=1126 Win=131072 Len=1392 [TCP segment of a reassembled PDU]
48113	43.470446	192.168.1.4	157.240.224.11	TCP	1446	65181 + 443 [ACK] Seq=44231 Ack=1126 Win=131072 Len=1392 [TCP segment of a reassembled PDU]
48114	43.470446	192.168.1.4	157.240.224.11	TCP	1446	65181 + 443 [ACK] Seq=45623 Ack=1126 Win=131072 Len=1392 [TCP segment of a reassembled PDU]
48115	43.470446	192.168.1.4	157.240.224.11	TLSv1.3	205	Application Data
48118	43.483021	157.240.224.11	192.168.1.4	TCP	54	443 + 65181 [ACK] Seq=1126 Ack=42839 Win=156672 Len=0

> Frame 48115: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface \Device\NPF_{DA...}

> Ethernet II, Src: CloudNet_88:42:5f (90:0f:0c:88:42:5f), Dst: NetcoreT_3c:09:e0 (00:72:63:3c:09:e0)

> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 157.240.224.11

> Transmission Control Protocol, Src Port: 65181, Dst Port: 443, Seq: 47015, Ack: 1126, Len: 151

> [5 Reassembled TCP Segments (5719 bytes): #48111(1392), #48112(1392), #48113(1392), #48114(1392), #48115(1392)]

> Transport Layer Security

> TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

> Opaque Type: Application Data (23)

> Version: TLS 1.2 (0x0303)

> Length: 5714

> Encrypted Application Data: 1420e79ed9dbf69ca4776bf0e987675a02c4a5b09ceaad52ec51fd63e75c8f482baef [Application Data Protocol: Hypertext Transfer Protocol]

- `arp || udr.port == 53` – пакети, які були відправлені протоколом ARP або через UDP порт 53:

No.	Time	Source	Destination	Protocol	Length	Info
39522	24.631631	192.168.1.4	194.44.214.214	DNS	86	Standard query 0xd356 A config.teams.microsoft.com
39526	24.636109	194.44.214.214	192.168.1.4	DNS	244	Standard query response 0xd356 A config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams.config.sk...
39600	24.669052	192.168.1.4	194.44.214.40	DNS	86	Standard query 0xa800 AAAA config.teams.microsoft.com
39607	24.701847	194.44.214.40	192.168.1.4	DNS	256	Standard query response 0xa800 AAAA config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams.config...
39980	24.985834	194.44.214.214	192.168.1.4	DNS	256	Standard query response 0xa800 AAAA config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams.config...
39981	24.986075	192.168.1.4	194.44.214.214	ICMP	284	Destination unreachable (Port unreachable)
41651	31.423112	192.168.1.4	194.44.214.214	DNS	70	Standard query 0xdd1d HTTPS dns.google
41652	31.423172	192.168.1.4	194.44.214.214	DNS	146	Standard query 0x2aec A dns.google
41658	31.431588	194.44.214.214	192.168.1.4	DNS	182	Standard query response 0x2aec A dns.google A 8.8.8.8 A 8.8.4.4
42300	31.883168	194.44.214.214	192.168.1.4	DNS	146	Standard query response 0xdd1d HTTPS dns.google SOA ns1.zdns.google
42301	31.883251	192.168.1.4	194.44.214.214	ICMP	174	Destination unreachable (Port unreachable)
43762	37.486003	192.168.1.4	194.44.214.214	DNS	73	Standard query 0xbdd1 HTTPS meta.vcdn.biz
43764	37.486034	192.168.1.4	194.44.214.214	DNS	73	Standard query 0xb3de A meta.vcdn.biz
43765	37.497340	194.44.214.214	192.168.1.4	DNS	124	Standard query response 0xbdd1 HTTPS meta.vcdn.biz SOA ns1.vcdn.biz
43950	37.827632	194.44.214.214	192.168.1.4	DNS	137	Standard query response 0xb3de A meta.vcdn.biz A 195.182.7.95 A 193.187.76.107 A 195.182.7.92 A 193.187.76.106
47305	42.227481	192.168.1.4	194.44.214.214	DNS	82	Standard query 0x6fce A analytics.ff.avast.com
47315	42.234274	194.44.214.214	192.168.1.4	DNS	131	Standard query response 0x6fce A analytics.ff.avast.com CNAME analytics-prod-gcp.ff.avast.com A 34.117.223.223
48116	43.480722	NetcoreT_3c:09:e0	CloudNet_88:42:5f	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1

> Frame 47315: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_{DA...}

> Ethernet II, Src: NetcoreT_3c:09:e0 (00:72:63:3c:09:e0), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)

> Internet Protocol Version 4, Src: 194.44.214.214, Dst: 192.168.1.4

> User Datagram Protocol, Src Port: 53, Dst Port: 61129

> Domain Name System (response)

- `eth.addr == 90-0F-0C-88-42-5F` – пакети, які були відправлені або отримані фізичною адресою мого адаптеру:

No.	Time	Source	Destination	Protocol	Length	Info
47299	42.225666	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47300	42.225974	192.168.1.4	185.158.208.76	UDP	86	61179 + 443 Len=44
47301	42.226132	192.168.1.4	185.158.208.76	UDP	86	61179 + 443 Len=44
47302	42.226192	192.168.1.4	185.158.208.76	UDP	86	61179 + 443 Len=44
47303	42.226221	192.168.1.4	185.158.208.76	UDP	86	61179 + 443 Len=44
47304	42.226582	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47305	42.227481	192.168.1.4	194.44.214.214	DNS	82	Standard query 0x6fce A analytics.ff.avast.com
47306	42.227654	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47307	42.227654	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47308	42.227735	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47309	42.229794	192.168.1.4	185.158.208.76	UDP	87	61179 + 443 Len=45
47310	42.230184	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47311	42.230184	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47312	42.230246	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47313	42.230609	185.158.208.76	192.168.1.4	UDP	1292	443 + 61179 Len=1250
47314	42.233795	192.168.1.4	185.158.208.76	UDP	87	61179 + 443 Len=45
47315	42.234274	194.44.214.214	192.168.1.4	DNS	131	Standard query response 0x6fce A analytics.ff.avast.com CNAME analytics-prod-gcp.ff.avast.com A 34.117.223.223
47316	42.238055	185.158.208.76	192.168.1.4	UDP	1291	443 + 61179 Len=1249

> Frame 47315: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_{DA...}

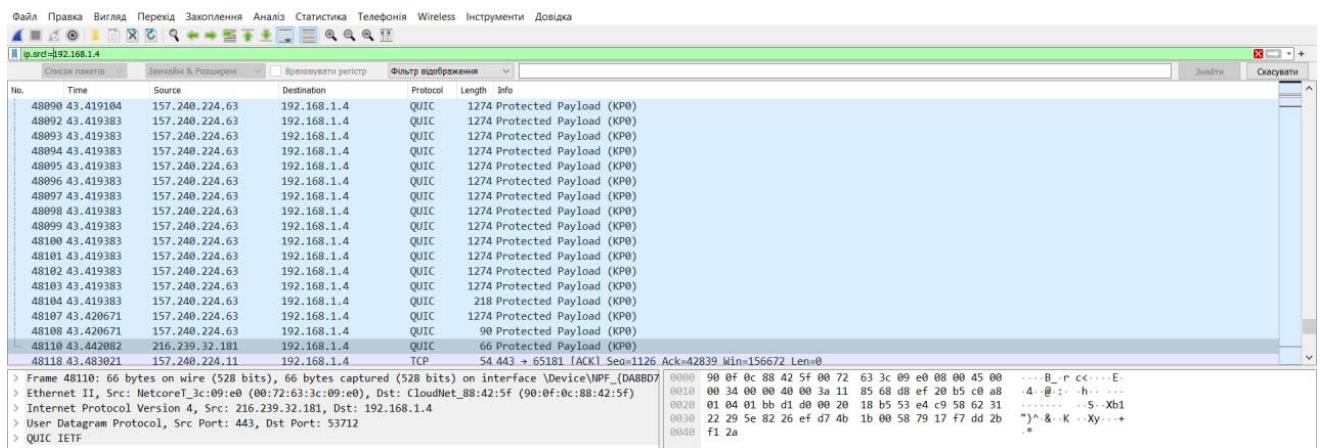
> Ethernet II, Src: NetcoreT_3c:09:e0 (00:72:63:3c:09:e0), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)

> Internet Protocol Version 4, Src: 194.44.214.214, Dst: 192.168.1.4

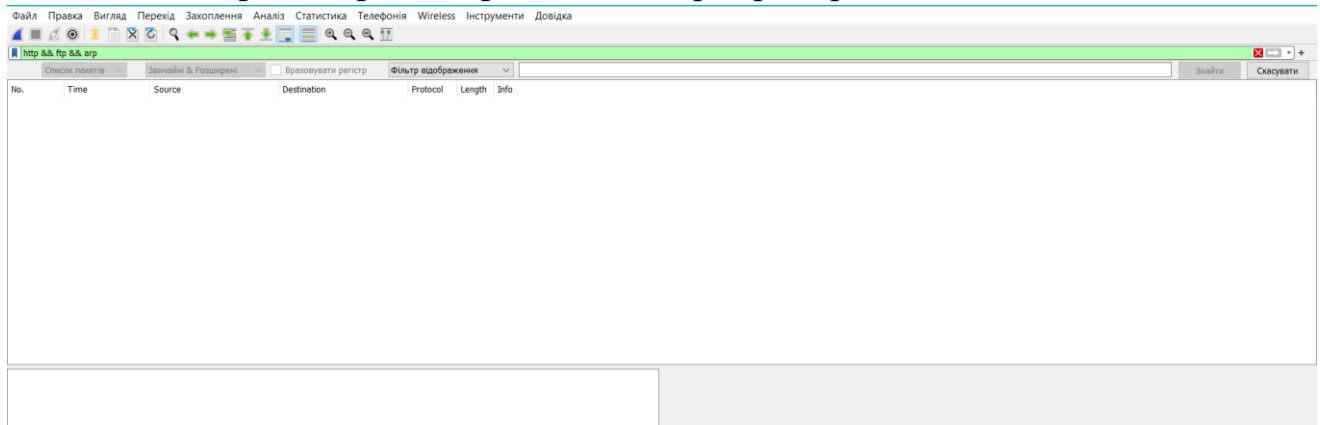
> User Datagram Protocol, Src Port: 53, Dst Port: 61129

> Domain Name System (response)

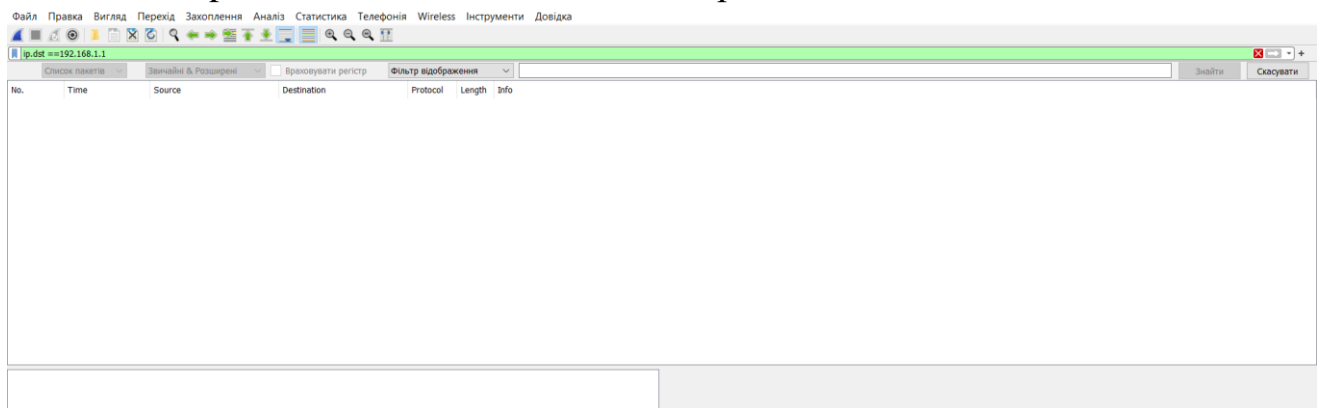
- `ip.src!=192.168.1.4` – пакети, які були відправлені НЕ з мого IPv4:



- http && ftp && arp – пакети http, ftp і arp:



- ip.dst == 192.168.1.1 – пакети, отримані моїм локальним IP:



10. У меню Statistics вибрав по черзі пункти Capture File Properties, Resolved Adresses, Protocol Hierarchy, Conversations, I/O Graph, IPv4 Statistics та ознайомився з інформацією:

- Capture file properties – показує дані про пакети записані у файлі, час, та статистику пакетів:

Wireshark · Властивості Файлу Захоплення · Package.pcapng

Подробиці

Файл

Ім'я: D:\Комп мережі\Lab3\Package.pcapng
 Розмір: 50 MB
 Hash (SHA256): 23e99ddbcbdad696aec45a7dc2ef2ba512d7927c3cf34c81359aacb9a37310786
 Hash (RIPEMD160): ffffce7fe92d246be38532ae902a86e83f142fa9
 Hash (SHA1): 4a89e3d00aaacd7d92964d3e0eb0dae582ee19b1
 Формат: Wireshark/... - pcapng
 Інкапсуляція: Ethernet

Час

Перший пакет: 2023-09-22 12:49:40
 Останній пакет: 2023-09-22 12:50:32
 Витрачено: 00:00:52

Захоплення

Апаратне забезпечення: AMD Ryzen 5 4600H with Radeon Graphics (with SSE4.2)
 ОС: 64-bit Windows 10 (22H2), build 19045
 Застосунок: Dumpcap (Wireshark) 4.0.8 (v4.0.8-0-g81696bb74857)

Інтерфейси

Інтерфейс	Відкинута пакети	Фільтр захоплення	Тип з'єднання	Packet size limit (snaplen)
Беспроводная сеть 2	0 (0.0%)	відсутній	Ethernet	262144 байтів

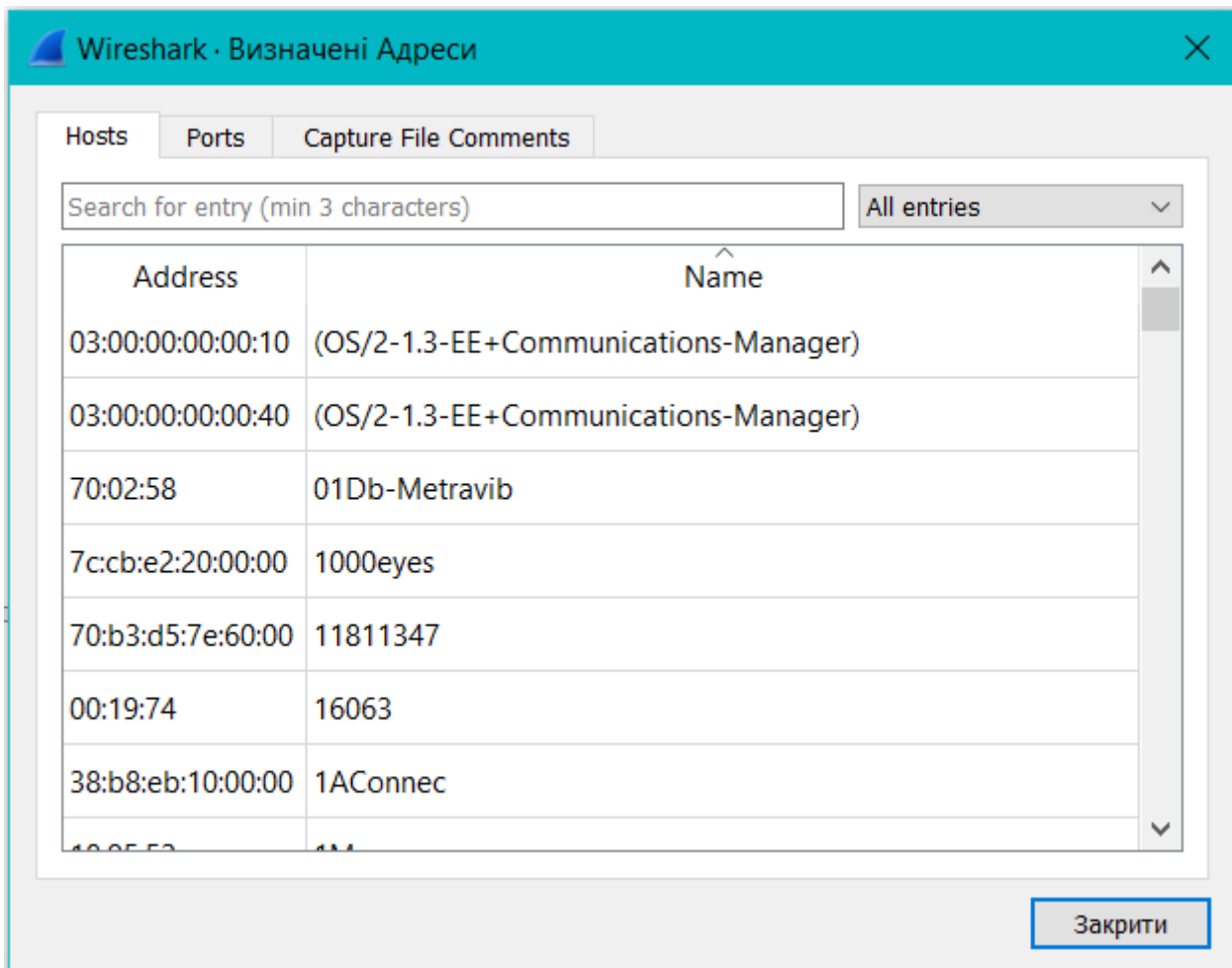
Статистика

Вимір	Захоплено	Відображено	Позначено
Пакетів	51596	—	—
Проміжок часу, с	52.286	—	—
Середнє пзс	986.8	—	—
Середній розмір пакету, Б	942	—	—
Байтів	48588651	0	0
Байт/с (середнє значення)	929 k	—	—
біт/с (середнє значення)	7434 k	—	—

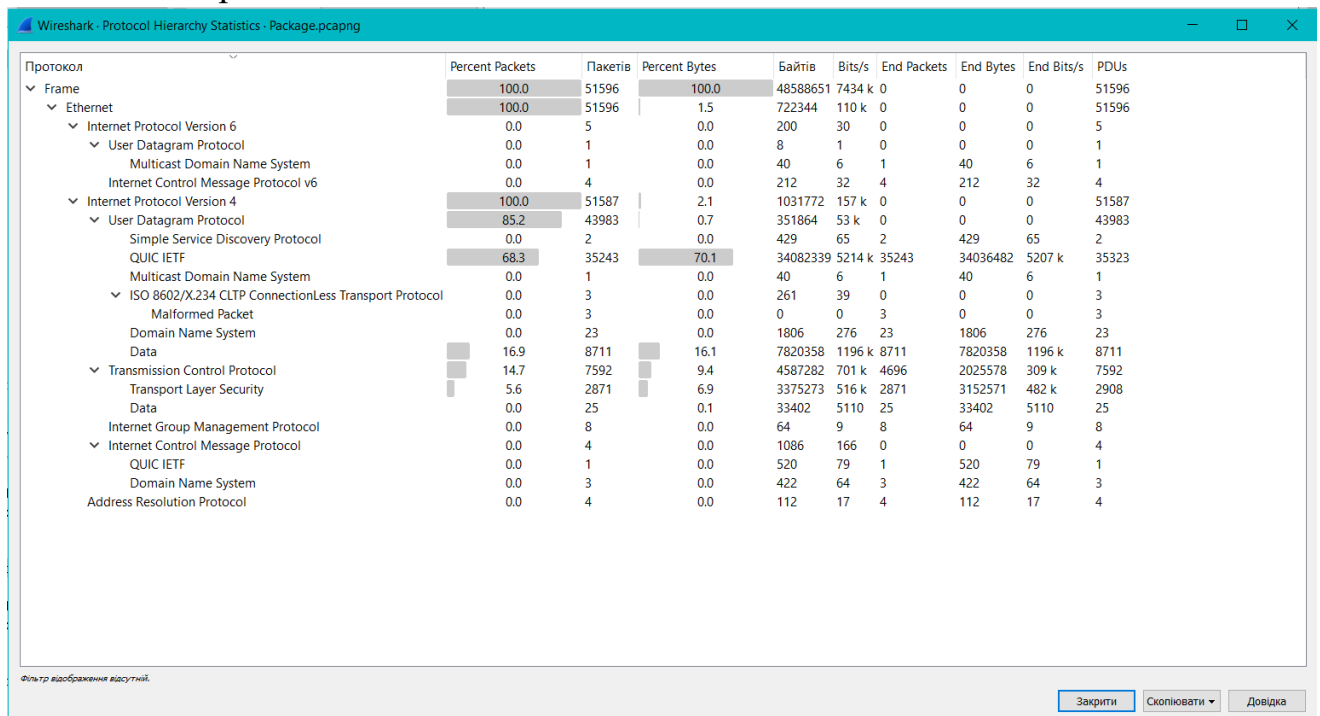
Коментарі файлу захоплення

Оновити Зберегти Коментарі Закрити Скопіювати До Буферу Обміну Довідка

- Resolved addresses має фізичні адреси, які отримували пакети або відправляли, а також порт та протокол за яким відправлено в другій вкладці:



- Protocol hierarchy показує ієрархію розподілення пакетів по протоколах:



- Conversations показує сумарні дані передачі даних між фізичними адресами, IP, тощо:

Wireshark - Conversations - Package.pcapng

Conversation Settings

- ☐ Визначення імен
- ☐ Absolute start time
- ☐ Limit to display filter

Скопіювати

Follow Stream...

Graph...

Протокол

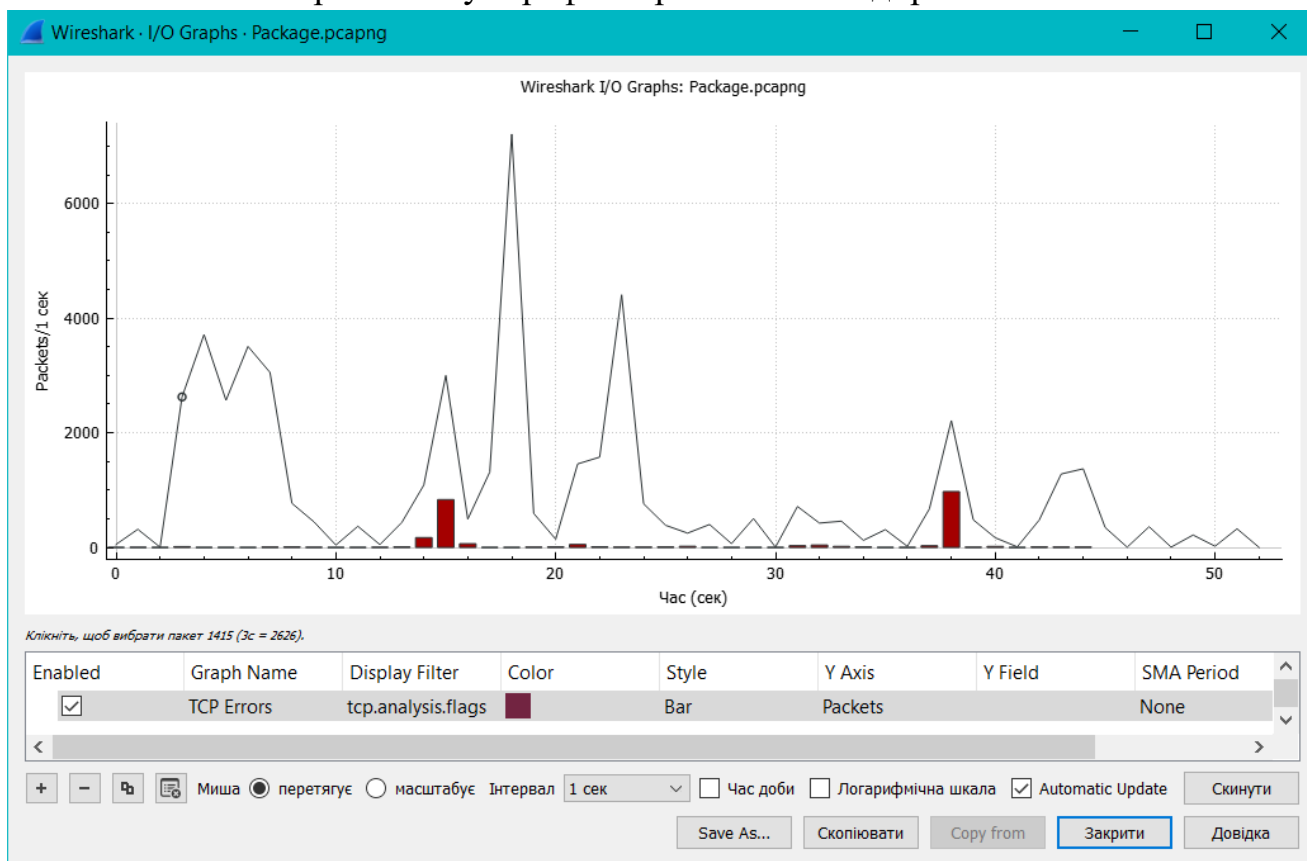
- ☐ Bluetooth
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☐ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA
- ☐ MPTCP
- ☐ NCP

Filter list for specific type

Address A	Address B	Пакейти	Байти	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:72:63:3c:09:e0	90:0f:0c:88:42:5f	51 584	49 MБ	38 404	47 MБ	13 180	2 MБ	0.000000	52.2860	7146 kbps	287 kbps
90:0f:0c:88:42:5f	01:00:5e:00:00:fb	2	92 байти	2	92 байти	0	0 байти	20.223490	29.9938	24 bits/s	0 bits/s
90:0f:0c:88:42:5f	01:00:5e:00:00:fc	2	92 байти	2	92 байти	0	0 байти	20.223398	29.9938	24 bits/s	0 bits/s
90:0f:0c:88:42:5f	01:00:5e:7fff:fa	3	271 байти	3	271 байти	0	0 байти	1.330066	48.8873	44 bits/s	0 bits/s
90:0f:0c:88:42:5f	33:33:00:00:00:16	1	150 байти	1	150 байти	0	0 байти	46.724263	0.0000	72 bits/s	0 bits/s
ec:2e:98:5d:d6:aa	90:0f:0c:88:42:5f	4	404 байти	4	404 байти	0	0 байти	1.871211	44.7145	72 bits/s	0 bits/s

Закрити Довідка

- I/O Graphs показує графік отриманих та відправлених пакетів:



- IPv4 Statistics показує всі адреси ipv4, які є у файлі та статистичні дані про них:

Wireshark · All Addresses · Package.pcapng								
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ All Addresses	51587				0,9866	100%	10,3700	18,265
91.214.126.237	28				0,0005	0,05%	0,2200	38,462
91.214.126.234	46				0,0009	0,09%	0,2500	34,640
91.214.126.205	29				0,0006	0,06%	0,1900	34,639
91.214.126.202	70				0,0013	0,14%	0,1800	33,001
8.8.8.8	127				0,0024	0,25%	0,2500	3,337
8.8.4.4	799				0,0153	1,55%	0,6200	31,647
74.125.131.188	2				0,0000	0,00%	0,0200	11,164
74.125.131.156	63				0,0012	0,12%	0,3100	32,916
54.211.227.8	24				0,0005	0,05%	0,1000	7,977
52.123.128.14	45				0,0009	0,09%	0,3300	22,964
52.114.77.97	5				0,0001	0,01%	0,0300	21,718
52.114.75.169	3				0,0001	0,01%	0,0300	27,242
52.113.194.132	216				0,0041	0,42%	0,7200	26,541
51.83.200.186	46				0,0009	0,09%	0,1300	32,621

Фільтр відображення: Застосувати

Скопіювати Зберегти як... Закрити

Висновок. Під час виконання лабораторної роботи я отримав загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомився з графічним інтерфейсом програми, навчився захоплювати, сортувати та фільтрувати пакети.