

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №4

Інтерфейс аналізатора пакетів Wireshark

Виконав:

Ст. Заречанський

Олексій

Група ПМІ-33

Оцінка

Прийняв:

ас. Жировецький В.В.

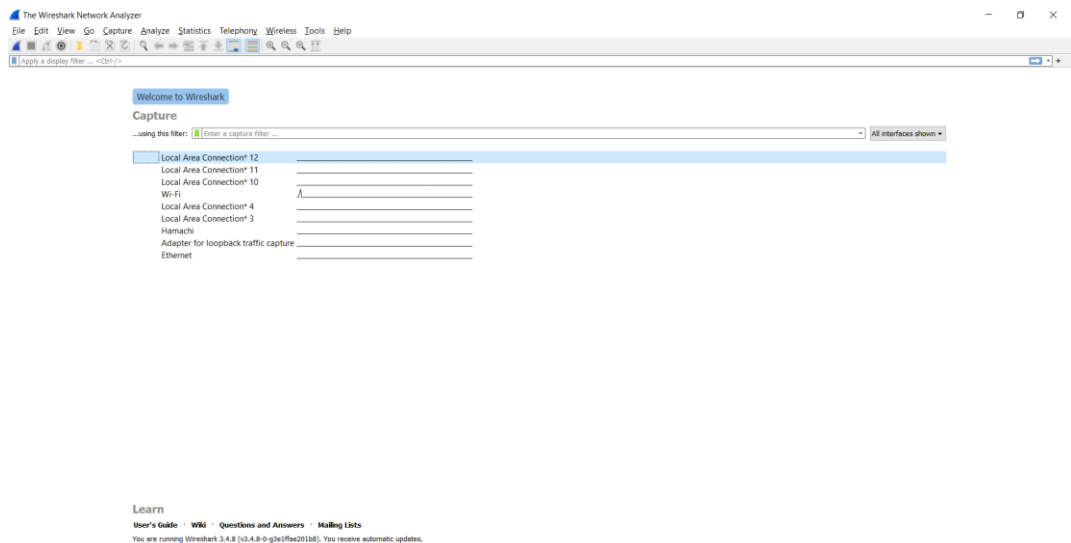
Тема

Інтерфейс аналізатора пакетів Wireshark.

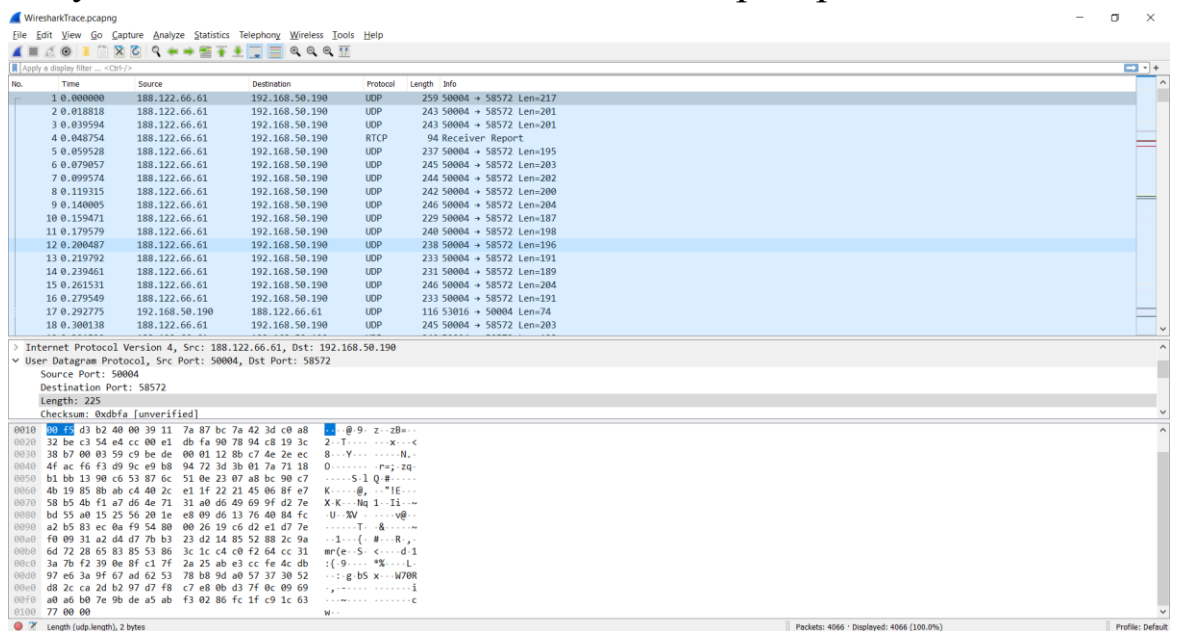
Мета роботи

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

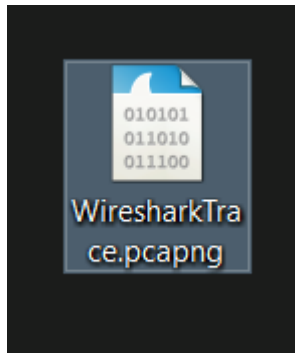
Звіт



Запускаємо Wireshark від імені адміністратора.



Лог.



Збережений лог в файлі.

WiresharkTrace.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

not ip

No.	Time	Source	Destination	Protocol	Length	Info
554	5.438825	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
933	6.462481	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
1012	7.383904	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
1632	9.429912	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
1633	9.431219	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
1873	10.454056	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
2198	11.491048	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
2199	11.491048	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
2322	13.525831	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
2485	14.447720	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
3020	15.387428	ASUSTekC_e6:13:70	IntelCor_69:03:0c	ARP	42	Who has 192.168.50.190? Tell 192.168.50.1
3021	15.387477	IntelCor_69:03:0c	ASUSTekC_e6:13:70	ARP	42	192.168.50.190 is at 98:2c:bc:69:03:0c
3094	15.472499	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
3169	15.575328	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
3384	16.495666	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
3668	17.622171	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
3838	19.465100	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
3850	19.567909	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232

> Frame 1873: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface [Device\NPF_{19DAAA47-2E3C-4C98-A05D-BE6A613C6EDB}, id 0
> Ethernet II, Src: Tvt_2d:f6:6e (00:18:ae:2d:f6:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

Пакети які не стосуються протоколу ір.

ip.addr == 192.168.50.190

No.	Time	Source	Destination	Protocol	Length	Info
7	0.099574	188.122.66.61	192.168.50.190	UDP	244	50004 → 58572 Len=202
8	0.119315	188.122.66.61	192.168.50.190	UDP	242	50004 → 58572 Len=200
9	0.140005	188.122.66.61	192.168.50.190	UDP	246	50004 → 58572 Len=204
10	0.159471	188.122.66.61	192.168.50.190	UDP	229	50004 → 58572 Len=187
11	0.179579	188.122.66.61	192.168.50.190	UDP	240	50004 → 58572 Len=198
12	0.200487	188.122.66.61	192.168.50.190	UDP	238	50004 → 58572 Len=196
13	0.219792	188.122.66.61	192.168.50.190	UDP	233	50004 → 58572 Len=191
14	0.239461	188.122.66.61	192.168.50.190	UDP	231	50004 → 58572 Len=189
15	0.261531	188.122.66.61	192.168.50.190	UDP	246	50004 → 58572 Len=204
16	0.279549	188.122.66.61	192.168.50.190	UDP	233	50004 → 58572 Len=191
17	0.292775	192.168.50.190	188.122.66.61	UDP	116	53016 → 50004 Len=74
18	0.300138	188.122.66.61	192.168.50.190	UDP	245	50004 → 58572 Len=203
19	0.321520	188.122.66.61	192.168.50.190	UDP	240	50004 → 58572 Len=198
20	0.323073	188.122.66.61	192.168.50.190	UDP	116	50004 → 53016 Len=74
21	0.340533	188.122.66.61	192.168.50.190	UDP	244	50004 → 58572 Len=202
22	0.361590	188.122.66.61	192.168.50.190	UDP	253	50004 → 58572 Len=211
23	0.380671	188.122.66.61	192.168.50.190	UDP	242	50004 → 58572 Len=200
24	0.400605	188.122.66.61	192.168.50.190	UDP	249	50004 → 58572 Len=207

Пакети відправлені з мого локального айпі або отримані ним.

arp || udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
3894	20.489722	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
3908	20.693776	Tvt_2d:f6:6e	Broadcast	ARP	60	ARP Announcement for 192.168.1.99
3976	21.410972	Tvt_2d:f6:6e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.99
3999	21.616954	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
4000	21.616954	Tvt_2d:f6:6e	Broadcast	ARP	60	ARP Announcement for 192.168.1.99
4009	21.717850	Tvt_2d:f6:6e	Broadcast	ARP	60	ARP Announcement for 192.168.1.99
4010	21.720276	Tvt_2d:f6:6e	Broadcast	ARP	60	ARP Announcement for 192.168.1.99
4011	21.720276	Tvt_2d:f6:6e	Broadcast	ARP	60	ARP Announcement for 192.168.1.99
4066	23.663623	SamsungE_1d:80:26	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.232
942	6.541294	192.168.50.190	192.168.50.1	DNS	76	Standard query 0xa376 A web.telegram.org
952	6.608899	192.168.50.190	192.168.50.1	DNS	76	Standard query 0xa376 A web.telegram.org
976	6.975202	192.168.50.1	192.168.50.190	DNS	92	Standard query response 0xa376 A web.telegram.org A 149.154.167.99
1021	7.480919	192.168.50.190	192.168.50.1	DNS	81	Standard query 0xd236 A zws2.web.telegram.org
1022	7.545825	192.168.50.190	192.168.50.1	DNS	81	Standard query 0xd236 A zws2.web.telegram.org
1024	7.572487	192.168.50.1	192.168.50.190	DNS	97	Standard query response 0xd236 A zws2.web.telegram.org A 149.154.167.99
1271	8.968013	192.168.50.190	192.168.50.1	DNS	75	Standard query 0x73c9 A www.gstatic.com
1272	8.970441	192.168.50.190	192.168.50.1	DNS	75	Standard query 0x674a A apis.google.com
1274	8.977633	192.168.50.190	192.168.50.1	DNS	86	Standard query 0xcfe0 A android.clients.google.com

Пакети відправлені протоколом ARP або через UDP порт 53.

eth.addr == 98-2C-BC-69-03-0C						
No.	Time	Source	Destination	Protocol	Length	Info
3555	16.963096	192.168.50.190	82.145.216.15	TLSv1.3	467	Application Data
3556	16.963140	192.168.50.190	82.145.216.15	TLSv1.3	123	Application Data
3609	17.030545	82.145.216.15	192.168.50.190	TLSv1.3	357	Application Data
3641	17.422346	192.168.50.190	149.154.167.99	TLSv1.3	171	Application Data
3643	17.423249	192.168.50.190	149.154.167.99	TLSv1.3	171	Application Data
3660	17.557828	149.154.167.99	192.168.50.190	TLSv1.3	167	Application Data
3895	20.489722	185.26.182.111	192.168.50.190	TLSv1.3	78	Application Data
3899	20.570906	192.168.50.190	149.154.167.99	TLSv1.3	171	Application Data
3900	20.571312	192.168.50.190	149.154.167.99	TLSv1.3	171	Application Data
3906	20.678428	149.154.167.99	192.168.50.190	TLSv1.3	167	Application Data
1	0.000000	188.122.66.61	192.168.50.190	UDP	259	50004 → 58572 Len=217
2	0.018818	188.122.66.61	192.168.50.190	UDP	243	50004 → 58572 Len=201
3	0.039594	188.122.66.61	192.168.50.190	UDP	243	50004 → 58572 Len=201
5	0.059528	188.122.66.61	192.168.50.190	UDP	237	50004 → 58572 Len=195
6	0.079057	188.122.66.61	192.168.50.190	UDP	245	50004 → 58572 Len=203
7	0.099574	188.122.66.61	192.168.50.190	UDP	244	50004 → 58572 Len=202
8	0.119315	188.122.66.61	192.168.50.190	UDP	242	50004 → 58572 Len=200
9	0.140005	188.122.66.61	192.168.50.190	UDP	246	50004 → 58572 Len=204

Пакети відправлені або отримані фізичною адресою мого адаптеру.

ip.src == 192.168.50.190				
No.	Time	Source	Destination	Protocol
2692	14.852517	192.168.50.190	151.101.85.164	TCP
2695	14.857111	192.168.50.190	151.101.85.164	TCP
2702	14.858560	192.168.50.190	151.101.85.164	TCP
2704	14.858784	192.168.50.190	151.101.85.164	TCP
2707	14.861219	192.168.50.190	151.101.85.164	TCP
2711	14.864214	192.168.50.190	151.101.85.164	TCP
2714	14.865699	192.168.50.190	151.101.85.164	TCP
2716	14.868557	192.168.50.190	151.101.85.164	TCP
2722	14.872145	192.168.50.190	151.101.85.164	TCP
2728	14.873423	192.168.50.190	151.101.85.164	TCP
2732	14.875524	192.168.50.190	151.101.85.164	TCP
2735	14.876891	192.168.50.190	151.101.85.164	TCP
2738	14.877672	192.168.50.190	151.101.85.164	TCP
2741	14.879478	192.168.50.190	151.101.85.164	TCP
2744	14.881230	192.168.50.190	151.101.85.164	TCP
2752	14.945164	192.168.50.190	151.101.85.164	TCP
2755	14.946922	192.168.50.190	151.101.85.164	TCP
2758	14.949115	192.168.50.190	151.101.85.164	TCP

Пакети відправлені з мого локального ір.

ip.dst == 192.168.50.190						
No.	ip.dst_host	Source	Destination	Protocol	Length	Info
96	1.660989	188.122.66.61	192.168.50.190	UDP	85	50004 → 58572 Len=43
98	2.133866	188.122.66.61	192.168.50.190	UDP	236	50004 → 58572 Len=194
99	2.154922	188.122.66.61	192.168.50.190	UDP	241	50004 → 58572 Len=199
100	2.173251	188.122.66.61	192.168.50.190	UDP	227	50004 → 58572 Len=185
101	2.197887	188.122.66.61	192.168.50.190	UDP	226	50004 → 58572 Len=184
102	2.211808	188.122.66.61	192.168.50.190	UDP	245	50004 → 58572 Len=203
103	2.234353	188.122.66.61	192.168.50.190	UDP	241	50004 → 58572 Len=199
104	2.256692	188.122.66.61	192.168.50.190	UDP	202	50004 → 58572 Len=160
106	2.273926	188.122.66.61	192.168.50.190	UDP	235	50004 → 58572 Len=193
107	2.297933	188.122.66.61	192.168.50.190	UDP	237	50004 → 58572 Len=195
112	2.313837	188.122.66.61	192.168.50.190	UDP	237	50004 → 58572 Len=195
113	2.331693	188.122.66.61	192.168.50.190	UDP	250	50004 → 58572 Len=208
114	2.354579	188.122.66.61	192.168.50.190	UDP	240	50004 → 58572 Len=198
115	2.374060	188.122.66.61	192.168.50.190	UDP	235	50004 → 58572 Len=193
116	2.397939	188.122.66.61	192.168.50.190	UDP	242	50004 → 58572 Len=200
121	2.414601	188.122.66.61	192.168.50.190	UDP	245	50004 → 58572 Len=203
122	2.432550	188.122.66.61	192.168.50.190	UDP	251	50004 → 58572 Len=209
123	2.456779	188.122.66.61	192.168.50.190	UDP	85	50004 → 58572 Len=43

Пакети отримані моїм локальним ір.

http && ftp && arp		
No.	Time	arp

Пакети http, ftp та arp.

Wireshark - Capture File Properties - WiresharkTrace.pcapng

Details

File

Name: C:\Users\mistel\Desktop\WiresharkTrace.pcapng
 Length: 2845k
 Hash (SHA256): 58f8102b79a7dccc74ce4888519a9f1a4e36d02ee18c965facc0f062b3bca6ef
 Hash (RIPEMD160): c13854dbb162166d3407386286324a9e786fc01e
 Hash (SHA1): fc9797108bfdce928d22ce2047cf6355afc24004
 Format: Wireshark/... - pcapng
 Encapsulation: Ethernet

Time

First packet: 2021-09-27 21:15:32
 Last packet: 2021-09-27 21:15:56
 Elapsed: 00:00:23

Capture

Hardware: Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz (with SSE4.2)
 OS: 64-bit Windows 10 (2009), build 19042
 Application: Dumpcap (Wireshark) 3.4.8 (v3.4.8-0-g3e1ffae201b8)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Wi-Fi	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	4066	4066 (100.0%)	—
Time span, s	23.664	23.664	—
Average pps	171.8	171.8	—
Average packet size, B	667	667	—
Bytes	2710168	2710168 (100.0%)	0
Average bytes/s	114k	114k	—
Average bits/s	916k	916k	—

Capture file comments

Refresh Save Comments Close Copy To Clipboard Help

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

Wireshark - Resolved Addresses

Hosts Ports Capture File Comments

Search for entry (min 3 characters) All entries

Address	Name
00:1b:c5:04:40:00	"RA
f8b5:68:e0:00:00	"RA
03:00:00:00:00:40	(OS/2-1.3-EE+Communications-Manager)
03:00:00:00:00:10	(OS/2-1.3-EE+Communications-Manager)
70:02:58	01Db-Metravib
7ccbre2:20:00:00	1000eyes
70b3:d5:7e:60:00	11811347
00:19:74	16063
38:b8:eb:10:00:00	1AConnec
6c:ce:44	1More
18:95:52	1More
9c:97:89	1More
78:a7:eb	1More
28:f5:37:80:00:00	1More
70b3:d5:14:d0:00	2-Observ
00:25:c3	21168
5c:85:7e:00:00:00	28Gorill
00:07:61	29530
3c:3f:51	2Crsi
00:16:a9	2Ei

Close

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

Wireshark · Protocol Hierarchy Statistics · WiresharkTrace.pcapng

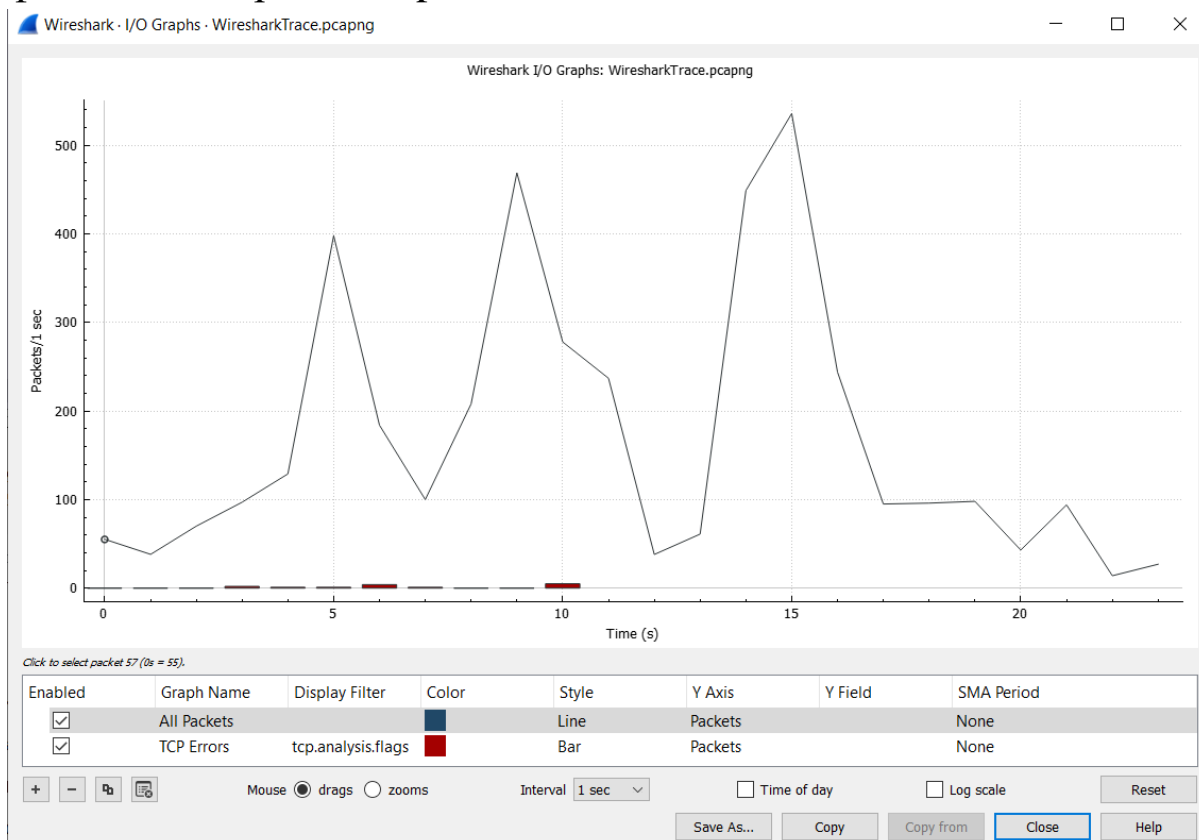
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	4066	100.0	2710168	916k	8	0	0
▼ Ethernet	99.8	4058	2.1	56812	19k	0	0	0
▼ Internet Protocol Version 4	99.0	4025	3.0	80516	27k	0	0	0
▼ User Datagram Protocol	70.4	2864	0.8	22912	7745	0	0	0
Real-time Transport Control Protocol	0.9	36	0.0	1136	384	36	1136	384
QUIC IETF	25.1	1019	29.2	791708	267k	996	773672	261k
▼ Domain Name System	0.7	27	0.1	3540	1196	23	1452	490
Malformed Packet	0.1	4	0.0	0	0	4	0	0
Data	44.4	1805	29.7	806008	272k	1805	806008	272k
▼ Transmission Control Protocol	28.4	1156	35.0	947873	320k	906	747922	252k
Transport Layer Security	6.3	257	34.4	932683	315k	249	898443	303k
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Internet Group Management Protocol	0.1	4	0.0	60	20	4	60	20
▼ Internet Control Message Protocol	0.0	1	0.0	162	54	0	0	0
Domain Name System	0.0	1	0.0	126	42	1	126	42
Address Resolution Protocol	0.8	33	0.1	1482	501	33	1482	501

Protocol hierarchy показує ієрархію розподілення пакетів по протоколам.

Wireshark · Conversations · WiresharkTrace.pcapng

Ethernet · 5		IPv4 · 42		IPv6		TCP · 26		UDP · 35			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:18:ae:2d:f6:6e	ff:ff:ff:ff:ff:ff	19	1140	19	1140	0	0	0.418907	21.3014	428	0
01:00:5e:00:00:16	98:2c:bc:69:03:0c	3	162	0	0	3	162	8.327767	6.9873	0	0
98:2c:bc:69:03:0c	f0:2f:74:e6:13:70	4,019	2706k	947	229k	3,072	2477k	0.000000	23.5205	78k	0
e4:7d:bd:1d:80:26	ff:ff:ff:ff:ff:ff	16	1028	16	1028	0	0	1.340290	22.3233	368	0
f0:2f:74:e6:13:70	ff:ff:ff:ff:ff:ff	1	102	1	102	0	0	2.672065	0.0000	—	0

Conversations показує сумарні дані передачі даних між фізичними адресами, ір тощо.



Графік отриманих та відправлених пакетів.

Wireshark · All Addresses · WiresharkTrace.pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ All Addresses	4025				0,1711	100%	1,8000	9,135
91.198.174.208	5				0,0002	0,12%	0,0500	13,803
82.145.216.15	16				0,0007	0,40%	0,1100	16,873
65.9.91.132	2				0,0001	0,05%	0,0200	11,857
64.233.161.188	3				0,0001	0,07%	0,0300	10,961
54.77.143.119	3				0,0001	0,07%	0,0300	3,416
52.84.197.22	2				0,0001	0,05%	0,0200	13,590
52.111.231.4	2				0,0001	0,05%	0,0200	19,962
3.124.35.138	2				0,0001	0,05%	0,0100	18,736
3.124.118.104	2				0,0001	0,05%	0,0100	21,242
224.0.0.22	3				0,0001	0,07%	0,0100	8,328
224.0.0.1	1				0,0000	0,02%	0,0100	7,844
216.58.215.110	18				0,0008	0,45%	0,1100	14,109
216.58.209.4	822				0,0349	20,42%	1,6500	9,135
216.58.209.2	18				0,0008	0,45%	0,1300	9,909
216.58.209.14	285				0,0121	7,08%	0,6700	4,273
216.58.209.214	240				0,0145	8,45%	1,0600	5,551

Display filter:

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

АНАЛІЗ ПОВІДОМЛЕНЬ КАНАЛЬНОГО РІВНЯ ЗАСОБАМИ WIRESHARK

- Опишіть на основі опрацьованого теоретичного матеріалу формат кадру Ethernet II (порядок полів, їх розмір та призначення).

Заголовок			Дані (+ поле заповнення)	Кінцевик
DA	SA	T	Data (+ Padding)	FCS
6	6	2	46-1500 байт	4
64-1518 байт				

Кадр Ethernet 2 складається:

- Першим йде заголовок, в ньому вказано:
 - 6 Байтів адреса призначення
 - 6 Байтів адреса відправника
 - 2 Байти вказують протокол кадру
- Далі йде поле даних, в якому є мінімум 46 байтів, максимум 1500, якщо обсягу даних недостатньо для заповнення 46 байтів, то вони заповнюються паддингом.

3) 4 Байти контрольна сума, яка показує наскільки “битим” доходить кадр.

2. Запускаю аналізатор пакетів Wireshark від імені адміністратора, та перехоплюю пакети на протязі 30 секунд.

3. Вибираю кадр для аналізу:

19	1.328509	192.168.50.190	192.168.50.1	DNS	75 Standard query 0x861e A ssl.gstatic.com
21	1.340259	192.168.50.1	192.168.50.190	DNS	91 Standard query response 0x861e A ssl.gstatic.com A 172.217.16.35
22	1.341004	192.168.50.190	172.217.16.35	QUIC	1392 Initial, DCID=6f9e8823eb9d9ab6, PKN: 1, CRYPTO, PADDING
23	1.341176	192.168.50.190	172.217.16.35	QUIC	115 0-RTT, DCID=6f9e8823eb9d9ab6
24	1.341308	192.168.50.190	172.217.16.35	QUIC	487 0-RTT, DCID=6f9e8823eb9d9ab6

> Frame 19: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{19DAAA47-2E3C-4C98-A05D-BE6A613C6EDB}, id 0
> Ethernet II, Src: IntelCor_69:03:0c (98:2c:bc:69:03:0c), Dst: ASUSTekC_e6:13:70 (f0:2f:74:e6:13:70)
> Internet Protocol Version 4, Src: 192.168.50.190, Dst: 192.168.50.1
> User Datagram Protocol, Src Port: 63611, Dst Port: 53
> Domain Name System (query)

- Кадр 19.
- Розмір 75 байт.

```
✓ Frame 19: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{19DAAA47-2E3C-4C98-A05D-BE6A613C6EDB}, id 0
  > Interface id: 0 (\Device\NPF_{19DAAA47-2E3C-4C98-A05D-BE6A613C6EDB})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 18, 2021 20:12:25.856515000 FLE Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1634577145.856515000 seconds
    [Time delta from previous captured frame: 0.150093000 seconds]
    [Time delta from previous displayed frame: 0.150093000 seconds]
    [Time since reference or first frame: 1.328509000 seconds]
    Frame Number: 19
    Frame Length: 75 bytes (600 bits)
    Capture Length: 75 bytes (600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

- Час захоплення: 18 жовтня 2021, 20:12:25
- Ієрархія протоколів: Ethernet кадр – Ір-пакет – Udp-сегмент – DNS-повідомлення.

```
> Destination: ASUSTekC_e6:13:70 (f0:2f:74:e6:13:70)
> Source: IntelCor_69:03:0c (98:2c:bc:69:03:0c)
Type: IPv4 (0x0800)
```

- Заголовок – перші 14 байтів повідомлення.
 - Отримувач: маршрутизатор (f0:2f:74:e6:13:70)
 - Відправник: моя мережева плата (98:2c:bc:69:03:0c)
 - Протокол: IPv4

4. За першою половиною MAC адреси перевіряю виробника:

- Для відправника:



Визначення виробника по MAC-адресі

Введіть mac-адресу для перевірки

98:2c:bc

ПЕРЕВІРИТИ

Виробником пристрою з mac-адресою 98:2c:bc є компанія:

Ім'я компанії:	Intel Corp
Адреса компанії:	Lot 8, Jalan Hi-Tech 2/3 Kulim Kedah 09000 MY
Країна:	 MY
Приватний:	Hi
Унікальний ідентифікатор організації:	98:2C:BC
Розмір діапазону:	MA-L 
Створено діапазон:	01 лип. 2019
Оновлено діапазон:	01 лип. 2019

- Для одержувача:



Визначення виробника по MAC-адресі

Введіть mac-адресу для перевірки

f0:2f:74

ПЕРЕВІРИТИ

Виробником пристрою з mac-адресою f0:2f:74 є компанія:

Ім'я компанії:	ASUSTek Computer Inc
Адреса компанії:	15,Li-Te Rd., Peitou, Taipei 112, Taiwan Taipei Taiwan 112 TW
Країна:	 TW
Приватний:	Hi
Унікальний ідентифікатор організації:	F0:2F:74
Розмір діапазону:	MA-L 
Створено діапазон:	29 вер. 2020
Оновлено діапазон:	29 вер. 2020

5. Знаходимо кадри з протоколу ARP:

[illegible]

Поле Padding потрібно для внесення додаткових нулів, щоб наш ір-заголовок був кратним 32 бітам, якщо він кратний сам по собі, то падінгу не буде.

Кінцевик відсутній, він використовується для перевірки успішності передачі даних, так як перевірка була успішно пройдена, то він нам не потрібен, бо корисної інформації не несе.