Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

«Безпека комп'ютерних мереж»

Лабораторна робота №4
«Дослідження мережних протоколів HTTP, HTTPS, SSL/TLS та DNS»
Варіант 5.2

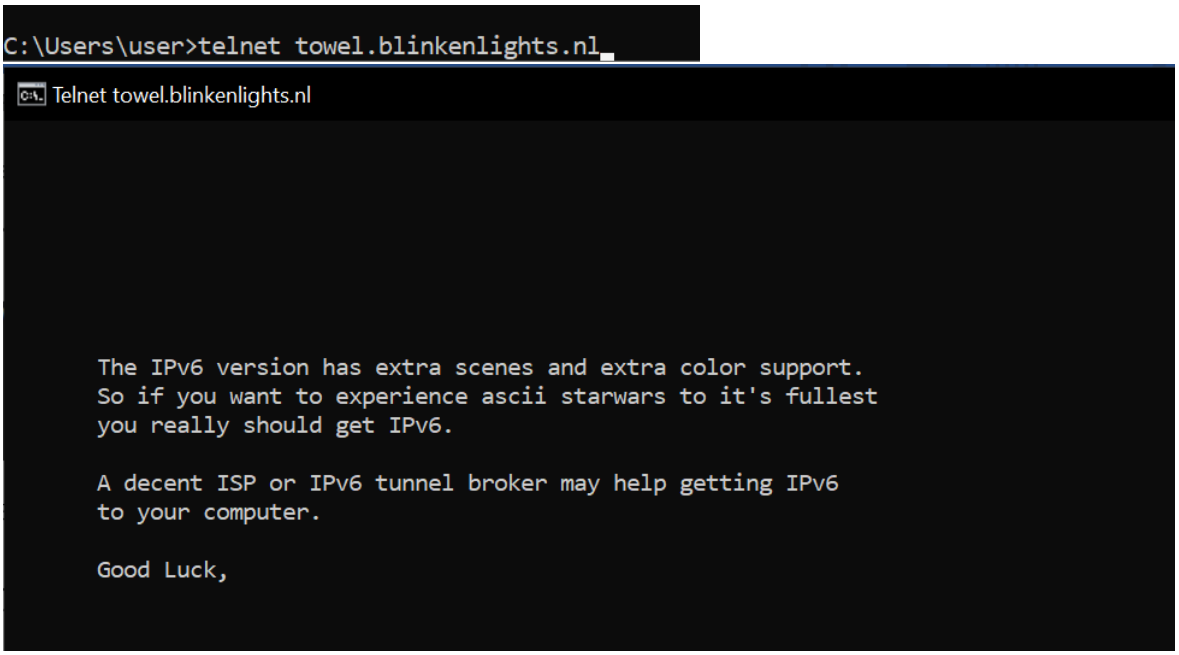
Виконала:
студентка групи ФБ-95
Гурджия Валерія Вахтангівна

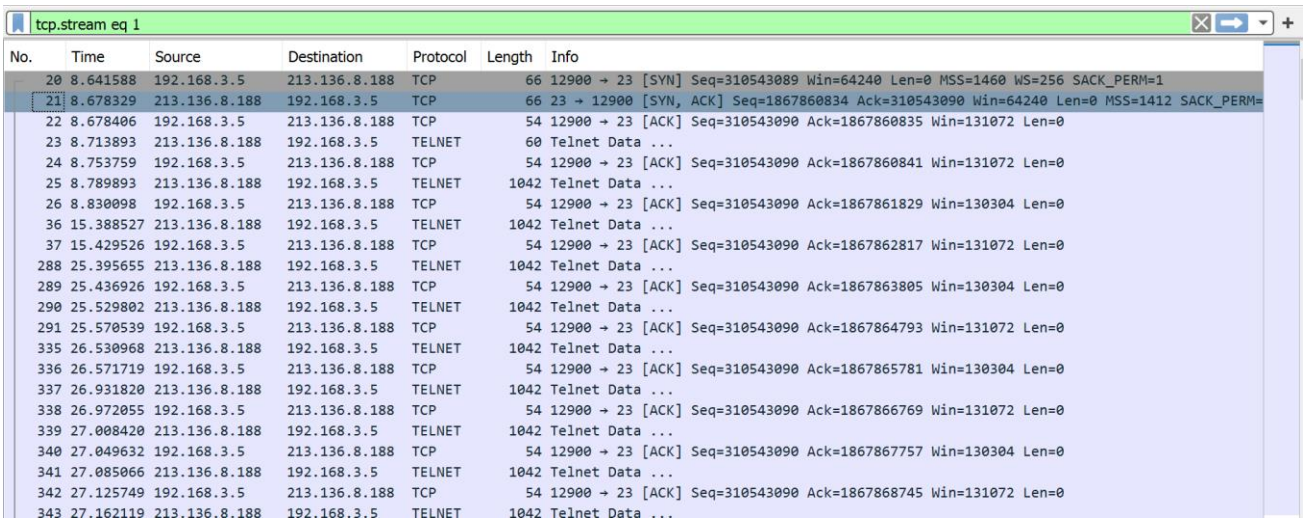
Київ-2022

1. Протокол HTTP

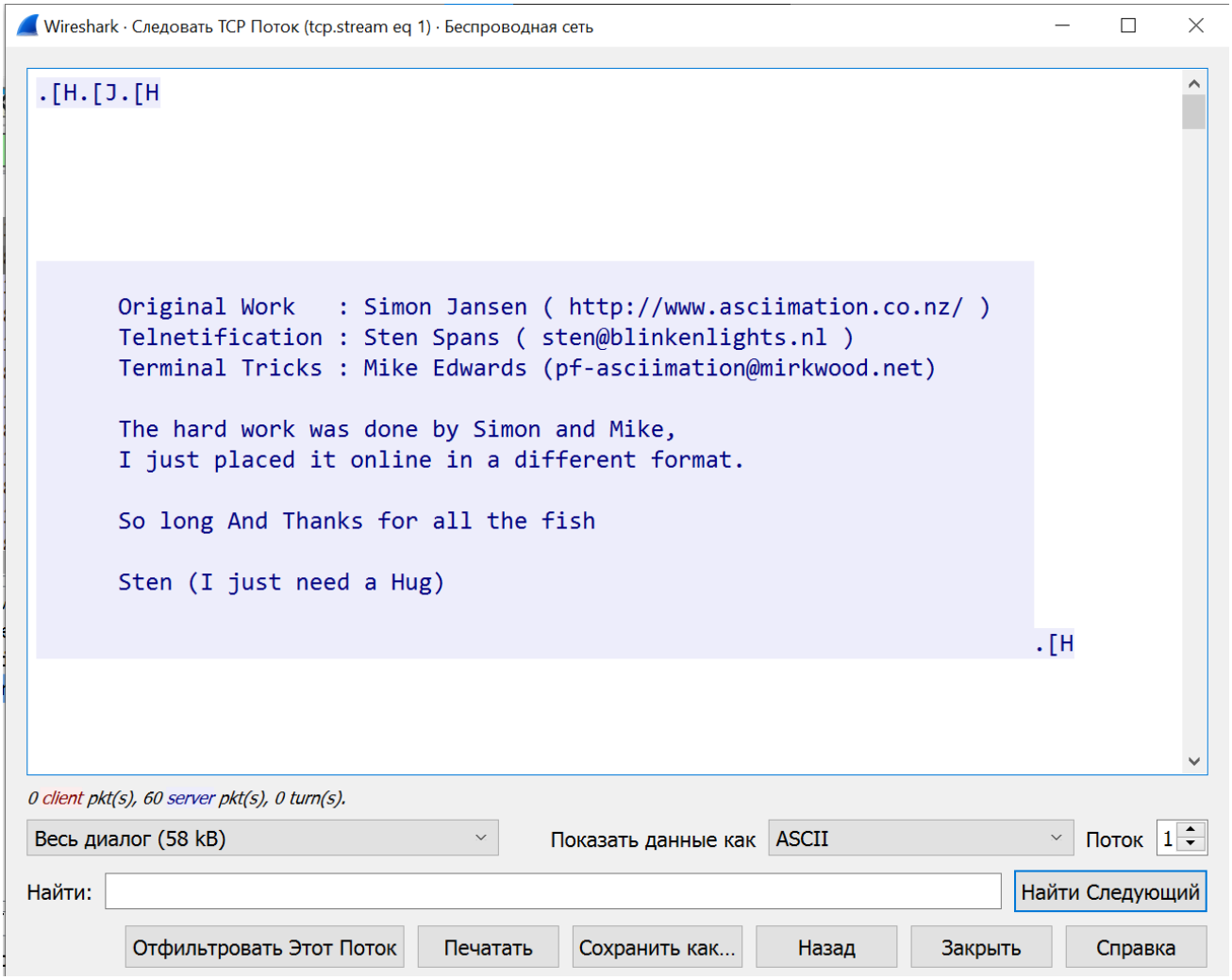
1.1

Виконаємо запит утілітою Telnet.





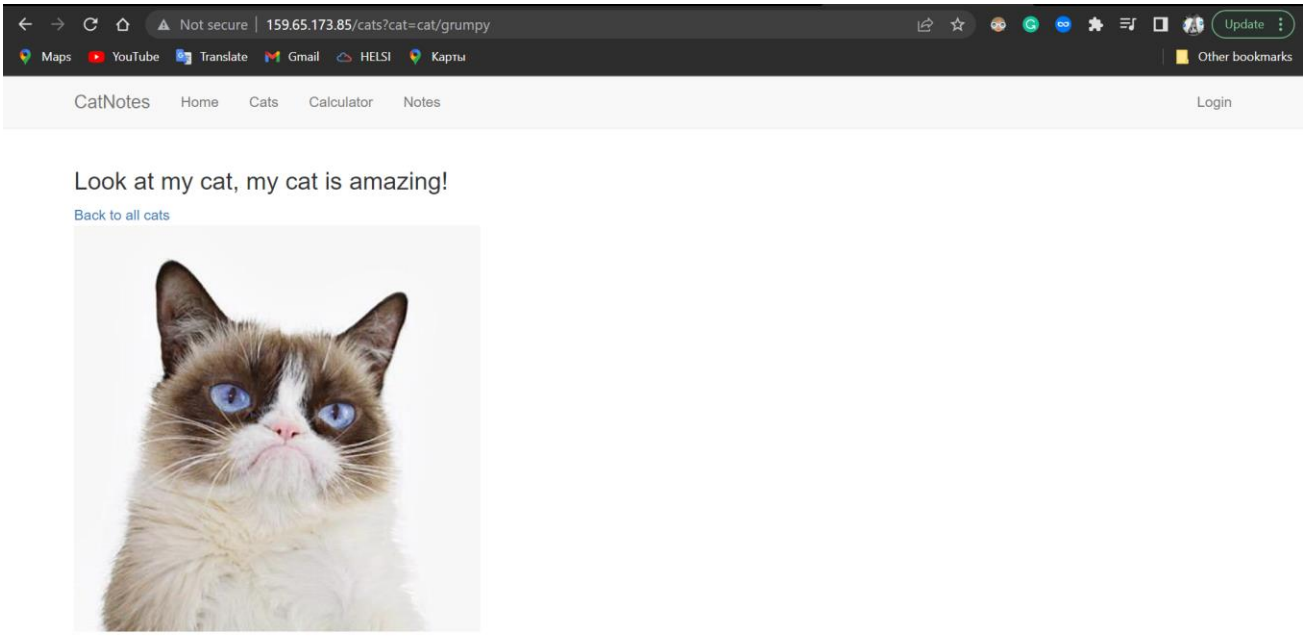
Після отримання відповіді сервера відновимо дані кожного TCP-з`єднання. Для цього виділимо один з пакетів з’єднання та виберемо пункт меню Analyse → Follow → TCP Stream.



1.2

Відкрили за протоколом HTTP Web-сторінку.

Вона містить картинки, css файли та js скрипти. Щоб отримати вкладений об’єкт браузер відправляє на HTTP сервер запит і отримує HTTP відповідь з потрібним об’єктом.

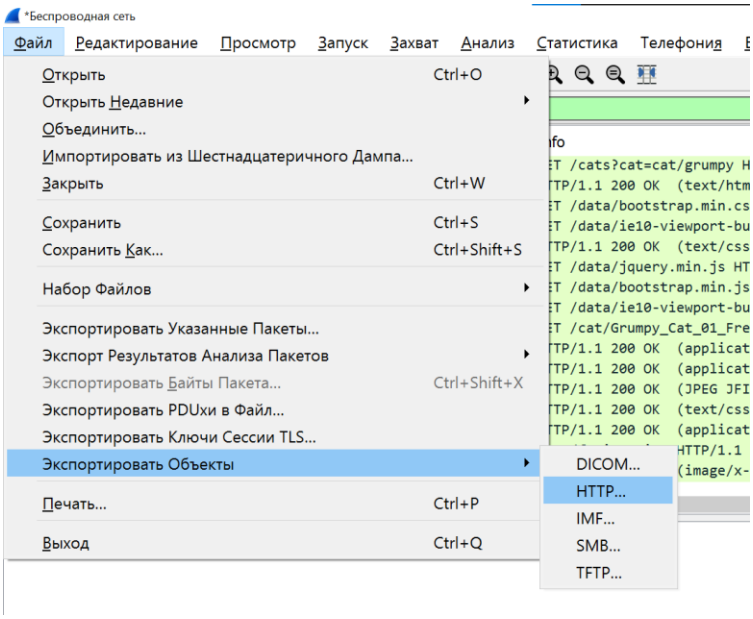


http

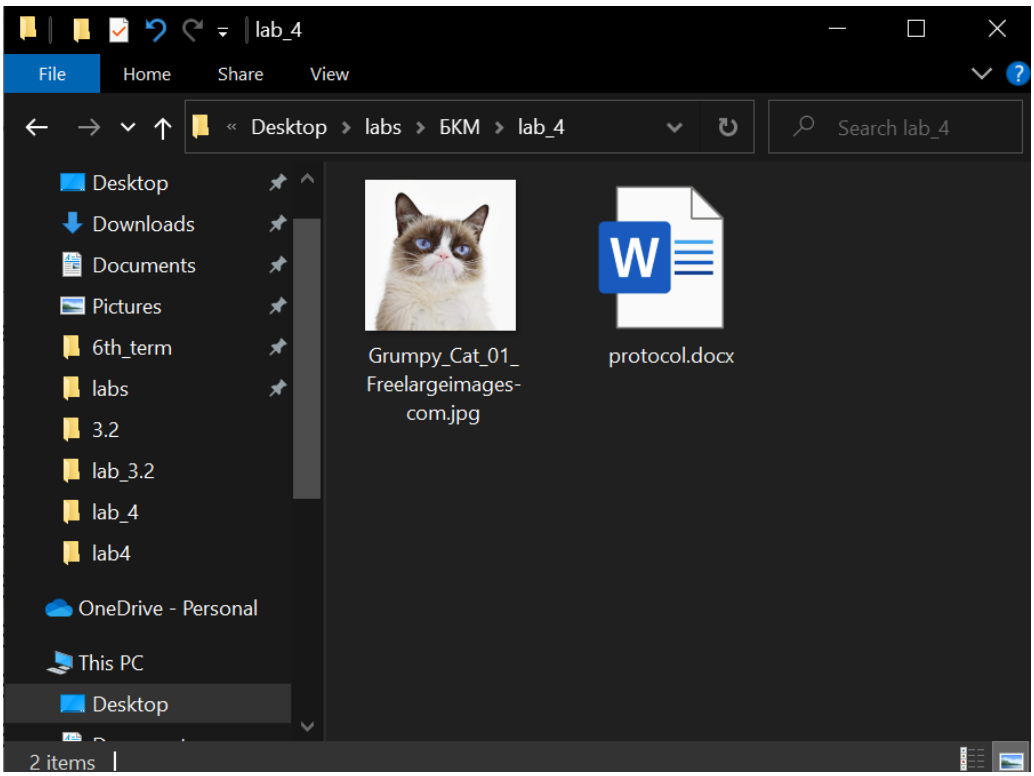
No.	Time	Source	Destination	Protocol	Length	Info
174	3.148680	192.168.3.5	159.65.173.85	HTTP	526	GET /cats?cat=cat/grumpy HTTP/1.1
181	3.269361	159.65.173.85	192.168.3.5	HTTP	1456	HTTP/1.1 200 OK (text/html)
182	3.298647	192.168.3.5	159.65.173.85	HTTP	433	GET /data/bootstrap.min.css HTTP/1.1
184	3.308232	192.168.3.5	159.65.173.85	HTTP	448	GET /data/ie10-viewport-bug-workaround.css HTTP/1.1
222	3.421330	159.65.173.85	192.168.3.5	HTTP	723	HTTP/1.1 200 OK (text/css)
225	3.421839	192.168.3.5	159.65.173.85	HTTP	414	GET /data/jquery.min.js HTTP/1.1
228	3.423357	192.168.3.5	159.65.173.85	HTTP	417	GET /data/bootstrap.min.js HTTP/1.1
229	3.423709	192.168.3.5	159.65.173.85	HTTP	432	GET /data/ie10-viewport-bug-workaround.js HTTP/1.1
234	3.424856	192.168.3.5	159.65.173.85	HTTP	498	GET /cat/Grumpy_Cat_01_Freelargeimages-com.jpg HTTP/1.1
299	3.532989	159.65.173.85	192.168.3.5	HTTP	945	HTTP/1.1 200 OK (application/javascript)
418	3.645739	159.65.173.85	192.168.3.5	HTTP	640	HTTP/1.1 200 OK (application/javascript)
424	3.650166	159.65.173.85	192.168.3.5	HTTP	75	HTTP/1.1 200 OK (JPEG JFIF image)
444	3.740193	159.65.173.85	192.168.3.5	HTTP	63	HTTP/1.1 200 OK (text/css)
485	3.754110	159.65.173.85	192.168.3.5	HTTP	1455	HTTP/1.1 200 OK (application/javascript)
488	3.849542	192.168.3.5	159.65.173.85	HTTP	468	GET /favicon.ico HTTP/1.1
494	3.958289	159.65.173.85	192.168.3.5	HTTP	1166	HTTP/1.1 200 OK (image/x-icon)

Для завантаження Web-сторінки повністю було встановлено 8 з`єднань.

Із даних записаних пакетів зберегли окремим файлом картинку у форматі jpg.



Пакет	Имя хоста	Тип Содержимого	Размер	Имя файла
181	159.65.173.85	text/html	2900 bytes	grumpy
222	159.65.173.85	text/css	433 bytes	ie10-viewport-bug-workaround.css
299	159.65.173.85	application/javascript	641 bytes	ie10-viewport-bug-workaround.js
418	159.65.173.85	application/javascript	37 kB	bootstrap.min.js
424	159.65.173.85	image/jpeg	18 kB	Grumpy_Cat_01_Freelargeimages-com.jpg
444	159.65.173.85	text/css	121 kB	bootstrap.min.css
485	159.65.173.85	application/javascript	97 kB	jquery.min.js
494	159.65.173.85	image/x-icon	6518 bytes	favicon.ico



1.4

Будемо використовувати сайт http://httpbin.org

Пакети процедури Base автентифікації

ip.addr==34.206.80.189

No.	Time	Source	Destination	Protocol	Length	Info
191	4.298060	192.168.3.5	34.206.80.189	HTTP	494	GET /basic-auth/user/123 HTTP/1.1
192	4.413302	34.206.80.189	192.168.3.5	HTTP	304	HTTP/1.1 401 UNAUTHORIZED
193	4.453999	192.168.3.5	34.206.80.189	TCP	54	9116 → 80 [ACK] Seq=3250000058 Ack=2324391689 Win=508 Len=0

Пакети процедури Digest автентифікації

ip.addr==44.195.242.112

No.	Time	Source	Destination	Protocol	Length	Info
41	5.217235	192.168.3.5	44.195.242.112	TCP	66	10079 → 80 [SYN] Seq=1443748927 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
43	5.334307	44.195.242.112	192.168.3.5	TCP	66	80 → 10079 [SYN, ACK] Seq=3374339558 Ack=1443748928 Win=26883 Len=0 MSS=1412
44	5.334473	192.168.3.5	44.195.242.112	TCP	54	10079 → 80 [ACK] Seq=1443748928 Ack=3374339559 Win=131072 Len=0
45	5.335020	192.168.3.5	44.195.242.112	HTTP	501	GET /digest-auth/auth/lera/1234 HTTP/1.1
46	5.459862	44.195.242.112	192.168.3.5	TCP	56	80 → 10079 [ACK] Seq=3374339559 Ack=1443749375 Win=28160 Len=0
47	5.464090	44.195.242.112	192.168.3.5	HTTP	555	HTTP/1.1 401 UNAUTHORIZED
48	5.503913	192.168.3.5	44.195.242.112	TCP	54	10079 → 80 [ACK] Seq=1443749375 Ack=3374340060 Win=130560 Len=0

2. Протокол HTTPS

Відкрили Web-сторінку (facebook.com) за протоколом HTTPS.

Використовується протокол версії TLSv1.3

ip.addr==31.13.81.36

No.	Time	Source	Destination	Protocol	Length	Info
91	2.191676	192.168.3.5	31.13.81.36	TCP	66	7549 → 443 [SYN] Seq=369825596 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
92	2.191878	192.168.3.5	31.13.81.36	TCP	66	7550 → 443 [SYN] Seq=2321456273 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
93	2.211548	31.13.81.36	192.168.3.5	TCP	66	443 → 7550 [SYN, ACK] Seq=2051215024 Ack=2321456274 Win=65535 Len=0 MSS=1392 SACK_PERM
94	2.211608	192.168.3.5	31.13.81.36	TCP	54	7550 → 443 [ACK] Seq=2321456274 Ack=2051215025 Win=132096 Len=0
95	2.211876	192.168.3.5	31.13.81.36	TLSv1.3	571	Client Hello
96	2.214443	31.13.81.36	192.168.3.5	TCP	66	443 → 7549 [SYN, ACK] Seq=1165636321 Ack=369825597 Win=65535 Len=0 MSS=1392 SACK_PERM=
98	2.214484	192.168.3.5	31.13.81.36	TCP	54	7549 → 443 [ACK] Seq=369825597 Ack=1165636322 Win=132096 Len=0
101	2.214817	192.168.3.5	31.13.81.36	TLSv1.3	571	Client Hello
102	2.232647	31.13.81.36	192.168.3.5	TCP	56	443 → 7550 [ACK] Seq=2051215025 Ack=2321456791 Win=66816 Len=0
103	2.232647	31.13.81.36	192.168.3.5	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
104	2.232726	31.13.81.36	192.168.3.5	TCP	56	443 → 7549 [ACK] Seq=1165636322 Ack=369826114 Win=66816 Len=0
106	2.232726	31.13.81.36	192.168.3.5	TLSv1.3	1446	Server Hello, Change Cipher Spec, Application Data
107	2.233032	192.168.3.5	31.13.81.36	TLSv1.3	118	Change Cipher Spec, Application Data
108	2.233345	192.168.3.5	31.13.81.36	TLSv1.3	146	Application Data
109	2.233552	192.168.3.5	31.13.81.36	TLSv1.3	542	Application Data
110	2.239223	31.13.81.36	192.168.3.5	TLSv1.3	1070	Application Data
111	2.239272	192.168.3.5	31.13.81.36	TCP	54	7549 → 443 [ACK] Seq=369826114 Ack=1165638730 Win=132096 Len=0
112	2.239836	192.168.3.5	31.13.81.36	TLSv1.3	118	Change Cipher Spec, Application Data
118	2.253773	31.13.81.36	192.168.3.5	TCP	56	443 → 7550 [ACK] Seq=2051215237 Ack=2321456855 Win=66816 Len=0
119	2.253773	31.13.81.36	192.168.3.5	TLSv1.3	225	Application Data
120	2.253773	31.13.81.36	192.168.3.5	TCP	56	443 → 7550 [ACK] Seq=2051215408 Ack=2321456947 Win=66816 Len=0
121	2.253773	31.13.81.36	192.168.3.5	TLSv1.3	85	Application Data

Клієнт встановлює TCP з’єднання з сервером. Браузер встановлює 2 з’єднання. Клієнт відправляє серверу 2 пакети з флагом SYN, потім отримує у відповідь 2 пакети з флагом SYN, ACK і відправляє 2 пакети з флагом ACK. Після цього починається процес встановлення з’єднання по протоколу TLS. Client Hello –

перший пакет для встановлення з’єднання TLS. Server Hello – відповідь від сервера. Change Cipher Spec – зміна типу шифрування. Application Data – передача даних.

3. Служба DNS

Сформувавши запис стосовно деякої символьної адреси, дізналися відповідну адресу

```
C:\Windows\system32>nslookup itc.ua
Server:  UnKnown
Address:  192.168.3.1

Non-authoritative answer:
Name:    itc.ua
Addresses:  2606:4700:3037::6815:5c0d
          2606:4700:3037::ac43:b87f
          104.21.92.13
          172.67.184.127
```

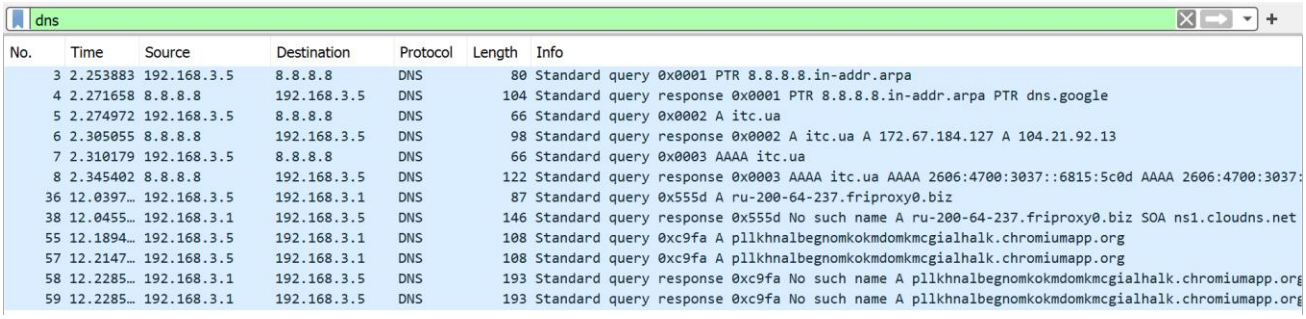
dns

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.3.5	192.168.3.1	DNS	75	Standard query 0xd479 A www.youtube.com
2	0.003958	192.168.3.1	192.168.3.5	DNS	285	Standard query response 0xd479 A www.youtube.com CNAME youtube-ui.l.google.com A 216.58.209.14
3	0.688702	192.168.3.5	192.168.3.1	DNS	89	Standard query 0x1209 A d27xxe7juh1us6.cloudfront.net
4	0.692967	192.168.3.1	192.168.3.5	DNS	153	Standard query response 0x1209 A d27xxe7juh1us6.cloudfront.net A 52.222.230.40 A 52.222.230.88
5	2.698962	192.168.3.5	192.168.3.1	DNS	87	Standard query 0x67b9 A ru-251-80-156.friproxy0.biz
6	2.703399	192.168.3.5	192.168.3.1	DNS	86	Standard query 0xd070 A ru-251-80-155.friproxy.biz
7	2.705370	192.168.3.5	192.168.3.1	DNS	83	Standard query 0x0328 A safebrowsing.google.com
8	2.708665	192.168.3.1	192.168.3.5	DNS	118	Standard query response 0x0328 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.16.14
9	2.715255	192.168.3.1	192.168.3.5	DNS	146	Standard query response 0x67b9 No such name A ru-251-80-156.friproxy0.biz SOA ns1.cloudns.net
10	2.728579	192.168.3.5	192.168.3.1	DNS	86	Standard query 0xd070 A ru-251-80-155.friproxy.biz
11	2.739991	192.168.3.1	192.168.3.5	DNS	145	Standard query response 0xd070 No such name A ru-251-80-155.friproxy.biz SOA ns1.cloudns.net
12	2.739991	192.168.3.1	192.168.3.5	DNS	145	Standard query response 0xd070 No such name A ru-251-80-155.friproxy.biz SOA ns1.cloudns.net
13	4.249098	192.168.3.5	192.168.3.1	DNS	84	Standard query 0x0001 PTR 1.3.168.192.in-addr.arpa
14	4.252334	192.168.3.1	192.168.3.5	DNS	84	Standard query response 0x0001 No such name PTR 1.3.168.192.in-addr.arpa
15	4.254469	192.168.3.5	192.168.3.1	DNS	66	Standard query 0x0002 A itc.ua
16	4.259152	192.168.3.1	192.168.3.5	DNS	98	Standard query response 0x0002 A itc.ua A 172.67.184.127 A 104.21.92.13
17	4.261996	192.168.3.5	192.168.3.1	DNS	66	Standard query 0x0003 AAAA itc.ua
18	4.263871	192.168.3.1	192.168.3.5	DNS	122	Standard query response 0x0003 AAAA itc.ua AAAA 2606:4700:3037::6815:5c0d AAAA 2606:4700:3037:

Запит направлений до DNS-сервера 8.8.8.8

```
C:\Windows\system32>nslookup itc.ua 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    itc.ua
Addresses:  2606:4700:3037::6815:5c0d
          2606:4700:3037::ac43:b87f
          172.67.184.127
          104.21.92.13
```



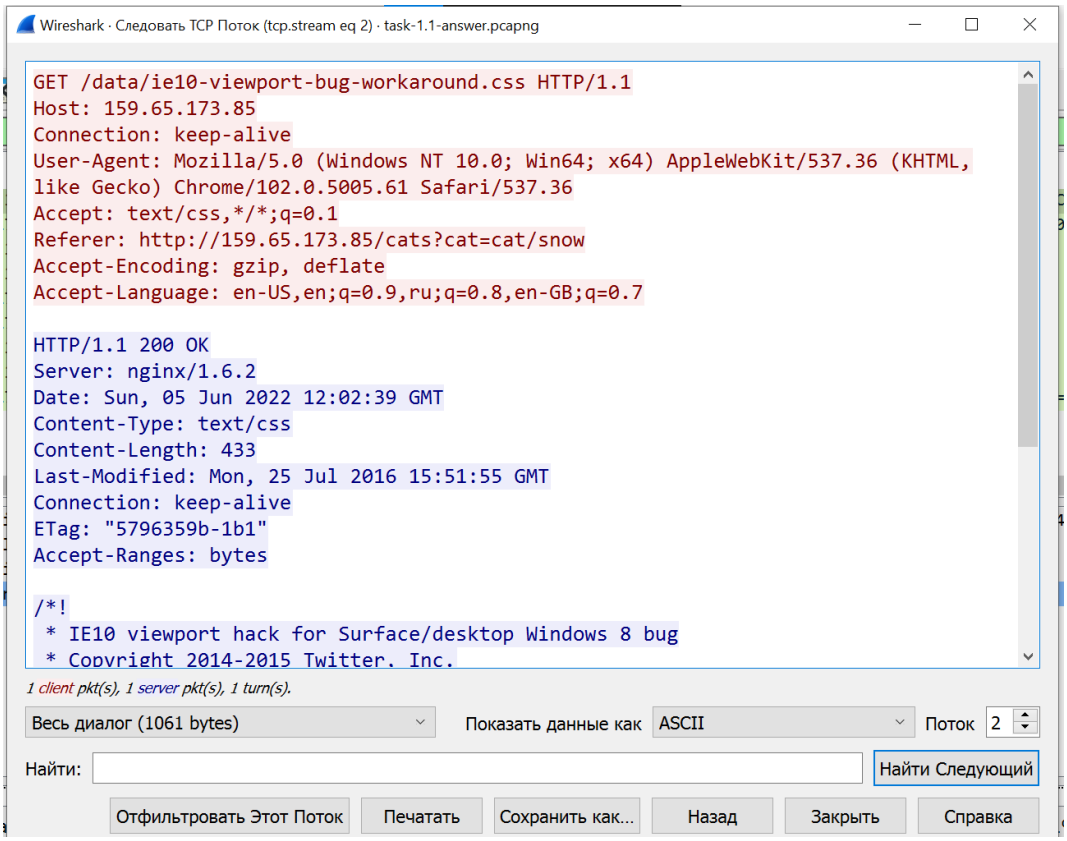
dns

No.	Time	Source	Destination	Protocol	Length	Info
3	2.253883	192.168.3.5	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
4	2.271658	8.8.8.8	192.168.3.5	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
5	2.274972	192.168.3.5	8.8.8.8	DNS	66	Standard query 0x0002 A itc.ua
6	2.305055	8.8.8.8	192.168.3.5	DNS	98	Standard query response 0x0002 A itc.ua A 172.67.184.127 A 104.21.92.13
7	2.310179	192.168.3.5	8.8.8.8	DNS	66	Standard query 0x0003 AAAA itc.ua
8	2.345402	8.8.8.8	192.168.3.5	DNS	122	Standard query response 0x0003 AAAA itc.ua AAAA 2606:4700:3037::6815:5c0d AAAA 2606:4700:3037:
36	12.0397…	192.168.3.5	192.168.3.1	DNS	87	Standard query 0x555d A ru-200-64-237.friproxy0.biz
38	12.0455…	192.168.3.1	192.168.3.5	DNS	146	Standard query response 0x555d No such name A ru-200-64-237.friproxy0.biz SOA ns1.cloudns.net
55	12.1894…	192.168.3.5	192.168.3.1	DNS	108	Standard query 0xc9fa A pllkhnalbegnomkokmdomkmcgialhalk.chromiumapp.org
57	12.2147…	192.168.3.5	192.168.3.1	DNS	108	Standard query 0xc9fa A pllkhnalbegnomkokmdomkmcgialhalk.chromiumapp.org
58	12.2285…	192.168.3.1	192.168.3.5	DNS	193	Standard query response 0xc9fa No such name A pllkhnalbegnomkokmdomkmcgialhalk.chromiumapp.org
59	12.2285…	192.168.3.1	192.168.3.5	DNS	193	Standard query response 0xc9fa No such name A pllkhnalbegnomkokmdomkmcgialhalk.chromiumapp.org

Відповідь на питання:

1. **HTTP:**

Перехопіть з'єднання з Web-сервером і відновіть повідомлення, що містять запит і відповідь, а також інші об`єкти, що передаються в рамках даного з'єднання.



Знайдіть повідомлення HTTP GET. Скільки часу займає процес з моменту відправлення повідомлення HTTP GET до моменту отримання відповіді HTTP OK. Скільки запитів HTTP GET було відправлено браузером для отримання однієї Web - сторінки. На які Інтернет адреси були відправлені ці GET запити?

No.	Time	Source	Destination	Protocol	Length	Info
57	3.282540	192.168.3.5	159.65.173.85	HTTP	481	GET /cat/cat-188088_960_720.jpg HTTP/1.1
21	2.995752	192.168.3.5	159.65.173.85	HTTP	524	GET /cats?cat=cat/snow HTTP/1.1
25	3.155917	192.168.3.5	159.65.173.85	HTTP	431	GET /data/bootstrap.min.css HTTP/1.1
52	3.281004	192.168.3.5	159.65.173.85	HTTP	415	GET /data/bootstrap.min.js HTTP/1.1
26	3.163053	192.168.3.5	159.65.173.85	HTTP	446	GET /data/ie10-viewport-bug-workaround.css HTTP/1.1
56	3.281773	192.168.3.5	159.65.173.85	HTTP	430	GET /data/ie10-viewport-bug-workaround.js HTTP/1.1
33	3.275067	192.168.3.5	159.65.173.85	HTTP	412	GET /data/jquery.min.js HTTP/1.1
456	3.853192	192.168.3.5	159.65.173.85	HTTP	466	GET /favicon.ico HTTP/1.1
453	3.817084	159.65.173.85	192.168.3.5	HTTP	62	HTTP/1.1 200 OK (JPEG JFIF image)
125	3.414405	159.65.173.85	192.168.3.5	HTTP	945	HTTP/1.1 200 OK (application/javascript)
198	3.536742	159.65.173.85	192.168.3.5	HTTP	640	HTTP/1.1 200 OK (application/javascript)
328	3.623551	159.65.173.85	192.168.3.5	HTTP	1455	HTTP/1.1 200 OK (application/javascript)
488	3.970376	159.65.173.85	192.168.3.5	HTTP	1166	HTTP/1.1 200 OK (image/x-icon)
48	3.280386	159.65.173.85	192.168.3.5	HTTP	723	HTTP/1.1 200 OK (text/css)
348	3.656651	159.65.173.85	192.168.3.5	HTTP	63	HTTP/1.1 200 OK (text/css)
24	3.115390	159.65.173.85	192.168.3.5	HTTP	1452	HTTP/1.1 200 OK (text/html)

З моменту відправки запиту HTTP GET до отримки відповіді HTTP OK пройшло 0.119638 с

Всього відправилось 8 GET-запитів.

GET-запити були відправлені на адресу Web-сторінки.

Як протокол HTTP завантажує малюнки. Продемонструйте пакети HTTP POST.

Окремими запитами

```
 21 2.995752  192.168.3.5     159.65.173.85  HTTP         524 GET /cats?cat=cat/snow HTTP/1.1
 453 3.817084  159.65.173.85   192.168.3.5    HTTP          62 HTTP/1.1 200 OK  (JPEG JFIF image)

456 3.853192  192.168.3.5     159.65.173.85  HTTP          466 GET /favicon.ico HTTP/1.1
 488 3.970376  159.65.173.85   192.168.3.5    HTTP        1166 HTTP/1.1 200 OK  (image/x-icon)
```

Як протокол HTTP захищає при автентифікації значення login і пароль, що передаються.

Ніяк не захищає


```
HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "_username" = "lera"
  > Form item: "_password" = "1234"
```

Ваш браузер використовує версію HTTP 1.0, 1.1 чи 2.0? Яку версію використовує сервер?

Сервер та браузер використовують версію HTTP 1.1

В якому мовному кодуванні (якщо таке є) ваш браузер має можливість приймати інформацію від сервера?

UTF-8

Яку відповідь дає сервер (код статусу та кодова фраза) на початкове повідомлення HTTP GET вашого браузера?

```
HTTP/1.1 200 OK\r\n
```

Код статусу – 200, кодова фраза – OK

Чи є якісь рядки статусу в HTTP, що пов'язані з розбивкою повідомлення на декілька TCP сегментів?

```
▾ HTTP chunked response
```

```
[27 Reassembled TCP Segments (37298 bytes): #103(1412), #104(1412), #105(1412), #106(1412), #107(1
```

Скільки знадобилося TCP сегментів, щоб передати звичайну HTTP відповідь?

27

Який був останній час модифікації HTML файлу, що ви отримали?

```
Last-Modified: Mon, 25 Jul 2016 15:51:55 GMT\r\n
```

Скільки байтів інформації було передано браузеру?

```
File Data: 37045 bytes
```

Чи були малюнки завантажені вашим браузером послідовно, чи вони завантажувалися з двох web сайтів паралельно? Поясніть.

Послідовно, час пакетів відрізняється

```
453 3.817084  159.65.173.85   192.168.3.5    HTTP        62 HTTP/1.1 200 OK  (JPEG JFIF image)
125 3.414405  159.65.173.85   192.168.3.5    HTTP       945 HTTP/1.1 200 OK  (application/javascript)
198 3.536742  159.65.173.85   192.168.3.5    HTTP       640 HTTP/1.1 200 OK  (application/javascript)
328 3.623551  159.65.173.85   192.168.3.5    HTTP      1455 HTTP/1.1 200 OK  (application/javascript)
488 3.970376  159.65.173.85   192.168.3.5    HTTP      1166 HTTP/1.1 200 OK  (image/x-icon)
```

Коли ваш браузер відправив HTTP GET повідомлення вдруге, яке нове поле було додано?

Вперше

```
GET /cats?cat=cat/snow HTTP/1.1\r\n
Host: 159.65.173.85\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,ru;q=0.8,en-GB;q=0.7\r\n
\r\n
```

Вдруге

```
GET /data/bootstrap.min.css HTTP/1.1\r\n
Host: 159.65.173.85\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
Accept: text/css,*/*;q=0.1\r\n
Referer: http://159.65.173.85/cats?cat=cat/snow\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,ru;q=0.8,en-GB;q=0.7\r\n
\r\n
[Full request URI: http://159.65.173.85/data/bootstrap.min.css]
[HTTP request 2/2]
```

З’явилося поле Referer

2. SSL/TLS:

Для кожного з перших восьми Ethernet фреймів визначте джерело повідомлення (сервер чи клієнт), визначте номер SSL запису, що вставлений у фрейм, і складіть список типів SSL повідомлень.

No.	Time	Source	Destination	Protocol	Length	Info
95	2.211876	192.168.3.5	31.13.81.36	TLSv1.3	571	Client Hello
101	2.214817	192.168.3.5	31.13.81.36	TLSv1.3	571	Client Hello
103	2.232647	31.13.81.36	192.168.3.5	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
106	2.232726	31.13.81.36	192.168.3.5	TLSv1.3	1446	Server Hello, Change Cipher Spec, Application Data
107	2.233032	192.168.3.5	31.13.81.36	TLSv1.3	118	Change Cipher Spec, Application Data
108	2.233345	192.168.3.5	31.13.81.36	TLSv1.3	146	Application Data
109	2.233552	192.168.3.5	31.13.81.36	TLSv1.3	542	Application Data
110	2.239223	31.13.81.36	192.168.3.5	TLSv1.3	1070	Application Data

Бачимо такі повідомлення:

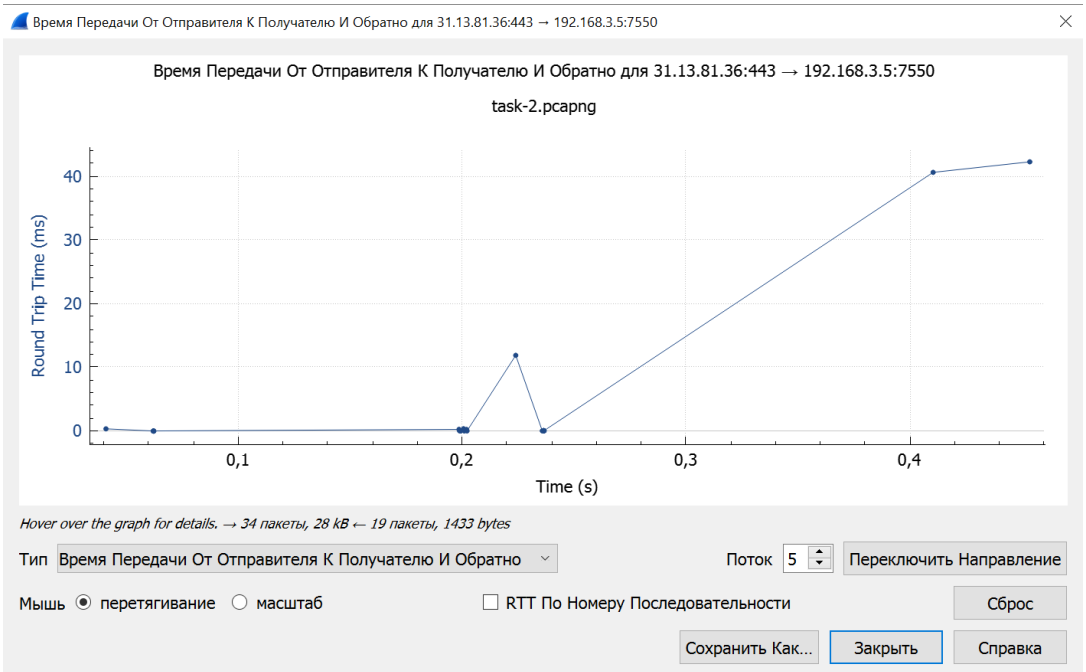
. Client Hello – перший пакет для встановлення з’єднання TLS.
. Server Hello – відповідь від сервера.
. Change Cipher Spec – сервер та клієнт починають використовувати шифрування.
. Application Data – передача даних.

Інші типи SSL-повідомлень:

. Certificate – містить цифровий сертифікат сервера.
. ServerKeyExchange – передаються необхідні дані, якщо переданих сервером даних недостатньо для вироблення спільного симетричного секретного ключа в рамках вибраного шифронабору.
. ServerHelloDone – ідентифікує закінчення першого раунду встановлення з'єднання.
. ClientKeyExchange - містить клієнтську частину протоколу Діффі-Хеллмана.

. Finished - містить хеш і MAC, що згенеровані на основі попередніх повідомлень процедури підтвердження зв'язку

Складіть часову діаграму передавання SSL пакетів між клієнтом та сервером.



Кожен SSL запис починається з однакових трьох полів (можливо, з різними значеннями). Одне з цих полів - це “content type”, яке має розмір в один байт. Випишіть всі три поля та їхній розмір.

Content Type – 1 байт

Version – 2 байти

Length – 2 байти

Де передається цифровий сертифікат.

В SSL повідомленні Certificate

3. DNS:

Відшукайте пакети запитів до DNS. Вони переслані за допомогою UDP чи TCP?

UDP

Який номер порту призначення у відправленому пакеті DNS запиту? Який номер порту призначення у пакеті DNS відповіді?

Запит

```
User Datagram Protocol, Src Port: 60180, Dst Port: 53
    Source Port: 60180
    Destination Port: 53
```

Відповідь

```
User Datagram Protocol, Src Port: 53, Dst Port: 60180
    Source Port: 53
    Destination Port: 60180
```

На яку IP адресу був відправлений DNS запит?

Source	Destination	Protocol	Length	Info
192.168.3.5	192.168.3.1	DNS	75	Standard query 0xd479 A www.youtube.com

Послуговуючись утилітою ipconfig, визначіть IP адреси вашого локального DNS серверу.

```
Wireless LAN adapter Беспроводная сеть:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Physical Address. . . . . . . . . : 00-E1-8C-AD-2F-4B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d036:6970:743d:9e4c%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.3.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : суббота, 4 июня 2022 г. 20:55:30
   Lease Expires . . . . . . . . . . : вторник, 7 июня 2022 г. 15:48:25
   Default Gateway . . . . . . . . . : 192.168.3.1
   DHCP Server . . . . . . . . . . . : 192.168.3.1
   DHCPv6 IAID . . . . . . . . . . . : 50389388
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-C2-41-AF-00-E1-8C-AD-2F-4B
   DNS Servers . . . . . . . . . . . : 192.168.3.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Дослідіть пакети DNS запитів. Що означає поле “Type” в ньому?

```
Queries
    www.youtube.com: type A, class IN
        Name: www.youtube.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Типи запитань DNS - поля типу, які використовуються в запитах і відповідях DNS, вказують тип запису ресурсу, для якого призначений запит або відповідь.

Чи повідомлення містить якесь поле “Answers”?

Поле “Answers” містять лише повідомлення-відповіді, а не запити.

Дослідіть повідомлення DNS відповіді. Скільки “відповідей” було отримано?

12 відповідей.

Що кожна з цих відповідей містить?

```
▾ www.youtube.com: type CNAME, class IN, cname youtube-ui.l.google.com
      Name: www.youtube.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 229 (3 minutes, 49 seconds)
      Data length: 22
      CNAME: youtube-ui.l.google.com
```

Якщо на Web сторінці містяться малюнки, то чи надсилає ваш хост нові DNS запити перед завантаженням кожного з цих малюнків?

Ні