МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Практикум з Основ комп’ютерних мереж

Дослідження мережних протоколів HTTP, HTTPS, SSL/TLS та DNS

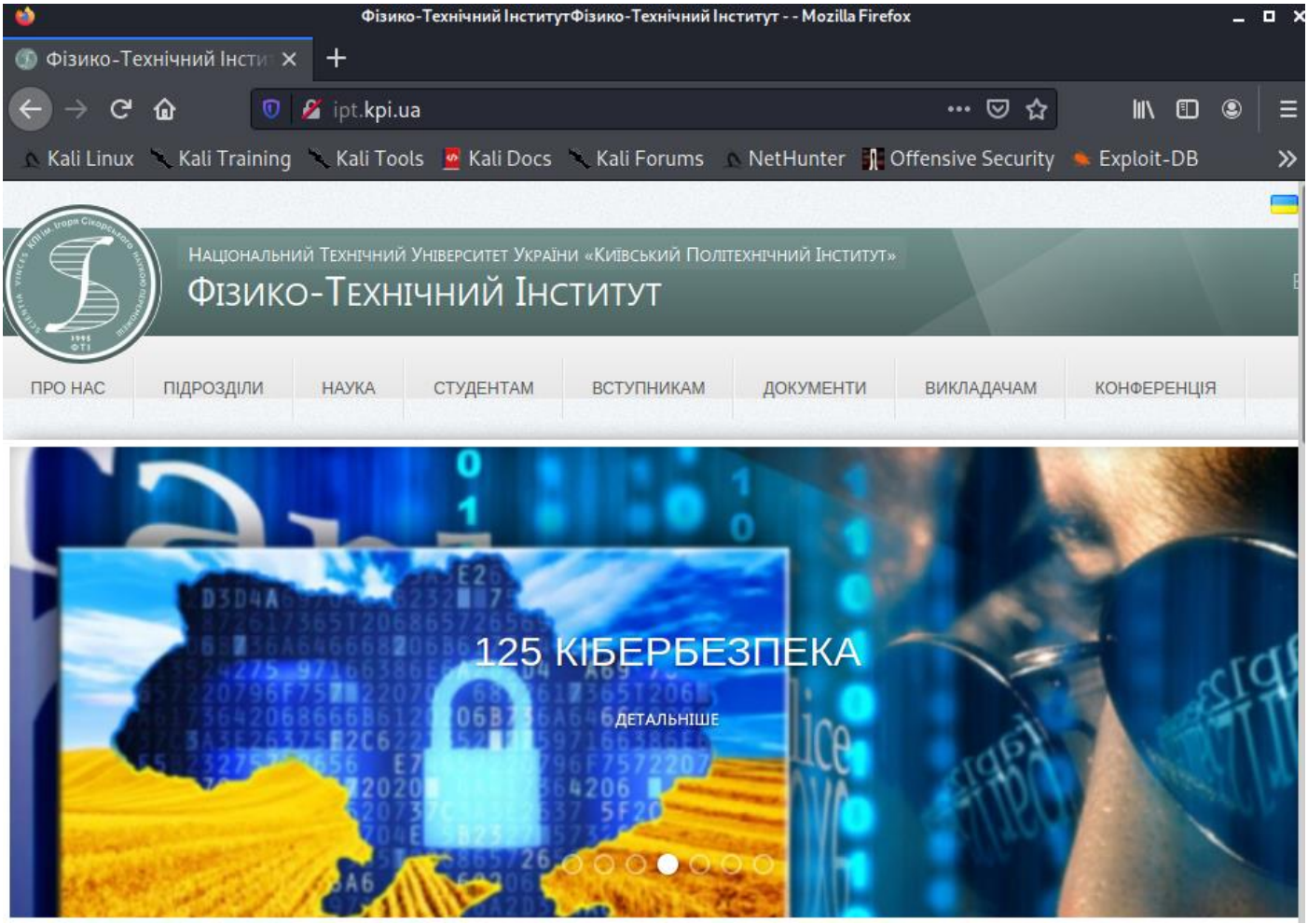
Перевірив:
_____

Виконав:
студент І курсу
групи ФБ-01
Сахній Н.Р.

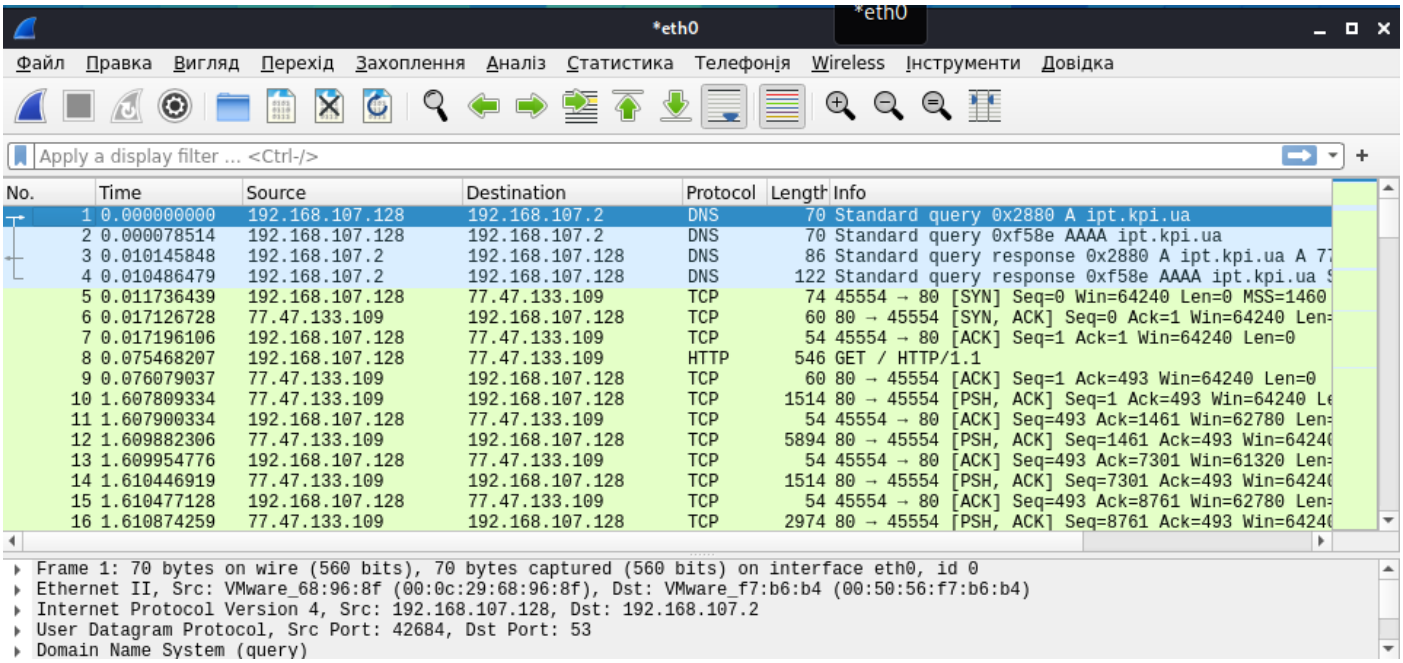
Київ 2021

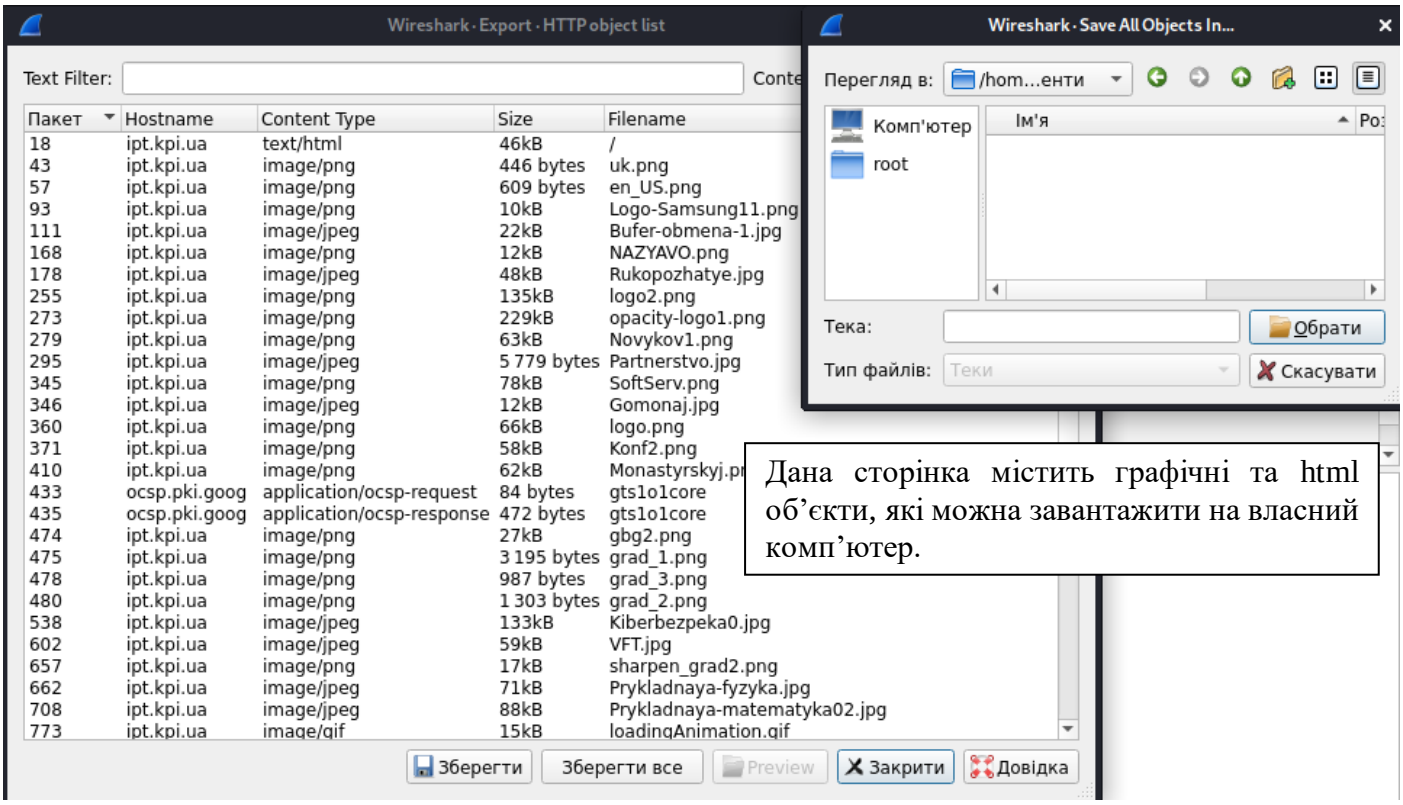
Протокол HTTP

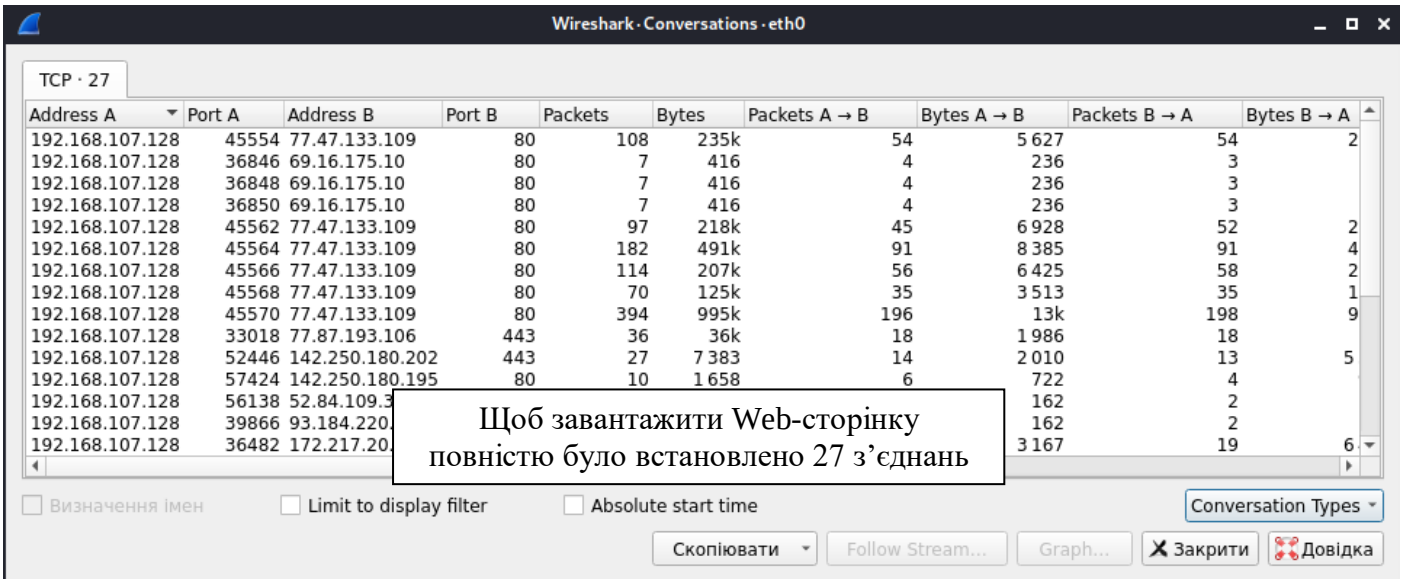
2. Тепер, послуговуючись браузером, відкрийте за протоколом HTTP деяку Web-сторінку. Які вкладені об`єкти вона містить? Із даних записаних пакетів збережіть окремим файлом деякий графічний об`єкт (картинку у форматі jpg, gif, png, тощо). Скільки було встановлено з`єднань для завантаження Web сторінки повністю?



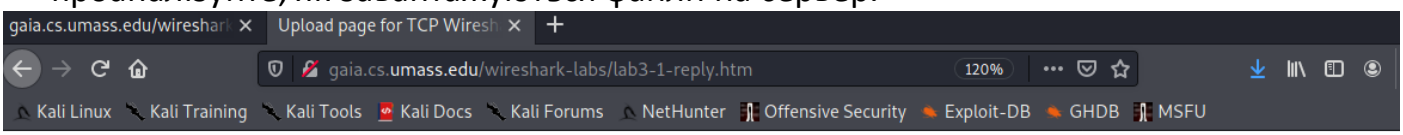
Відкривши Web-сторінку http://ipt.kpi.ua, перехопимо пакети у Wireshark





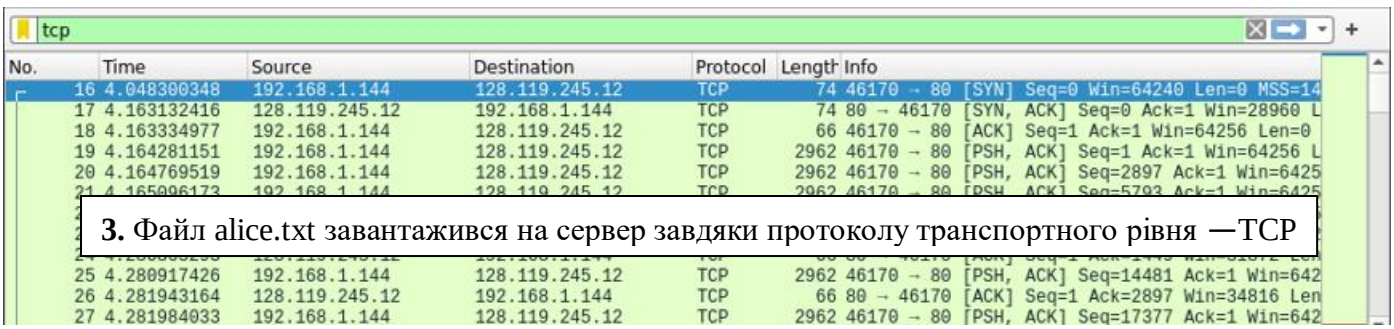


3. Знайдіть деяку Web-форму, що дозволяє передавати, файли та проаналізуйте, як завантажуються файли на сервер.



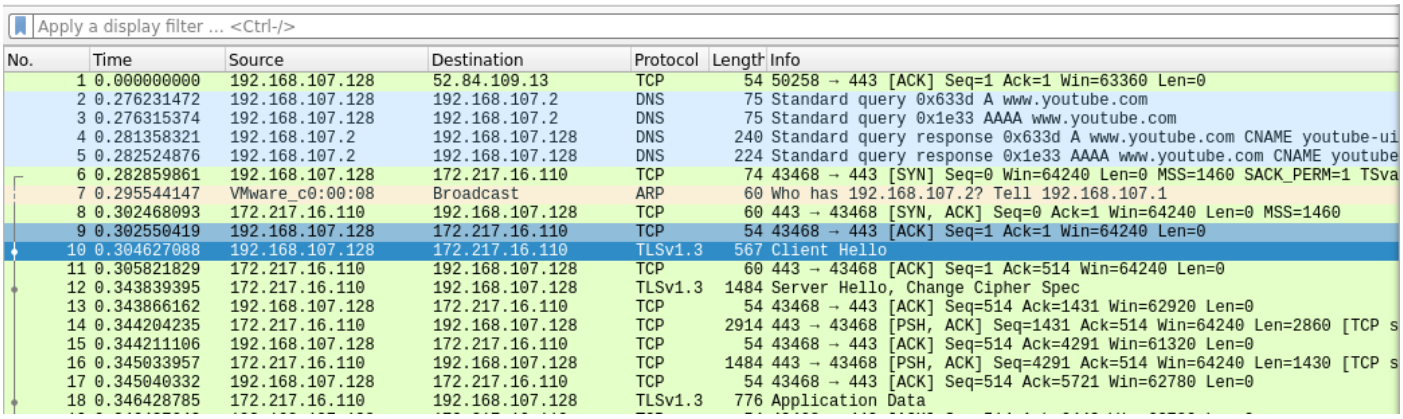
Congratulations!

You've now transferred a copy of alice.txt from your computer to gaia.cs.umass.edu. You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!



Протокол HTTPS

Відкрийте деяку Web-сторінку за протоколом HTTPS. Запишіть пакети цього з`єднання. По записаним пакетам ідентифікуйте версію протокол, що використовується, послідовність встановлення захищеного з`єднання та типи повідомлень, що передаються в процесі встановлення цього з`єднання.

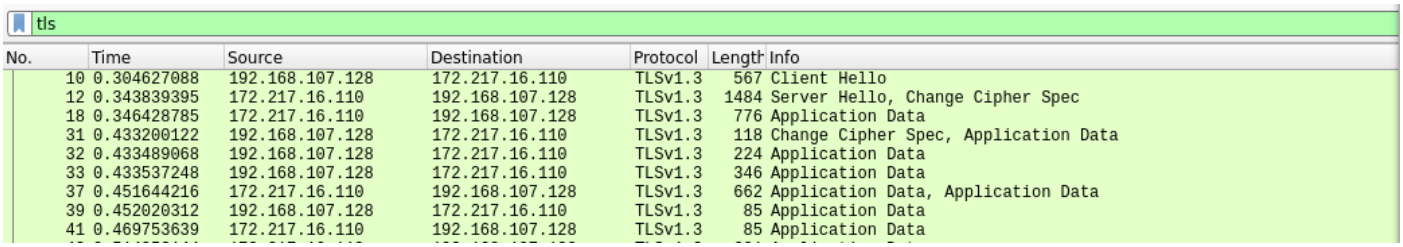


Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.107.128	52.84.109.13	TCP	54	50258 → 443 [ACK] Seq=1 Ack=1 Win=63360 Len=0
2	0.276231472	192.168.107.128	192.168.107.2	DNS	75	Standard query 0x633d A www.youtube.com
3	0.276315374	192.168.107.128	192.168.107.2	DNS	75	Standard query 0x1e33 AAAA www.youtube.com
4	0.281358321	192.168.107.2	192.168.107.128	DNS	240	Standard query response 0x633d A www.youtube.com CNAME youtube-ui
5	0.282524876	192.168.107.2	192.168.107.128	DNS	224	Standard query response 0x1e33 AAAA www.youtube.com CNAME youtube
6	0.282859861	192.168.107.128	172.217.16.110	TCP	74	43468 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
7	0.295544147	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.107.2? Tell 192.168.107.1
8	0.302468093	172.217.16.110	192.168.107.128	TCP	60	443 → 43468 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	0.302550419	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.304627088	192.168.107.128	172.217.16.110	TLSv1.3	567	Client Hello
11	0.305821829	172.217.16.110	192.168.107.128	TCP	60	443 → 43468 [ACK] Seq=1 Ack=514 Win=64240 Len=0
12	0.343839395	172.217.16.110	192.168.107.128	TLSv1.3	1484	Server Hello, Change Cipher Spec
13	0.343866162	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=514 Ack=1431 Win=62920 Len=0
14	0.344204235	172.217.16.110	192.168.107.128	TCP	2914	443 → 43468 [PSH, ACK] Seq=1431 Ack=514 Win=64240 Len=2860 [TCP s
15	0.344211106	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=514 Ack=4291 Win=61320 Len=0
16	0.345033957	172.217.16.110	192.168.107.128	TCP	1484	443 → 43468 [PSH, ACK] Seq=4291 Ack=514 Win=64240 Len=1430 [TCP s
17	0.345040332	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=514 Ack=5721 Win=62780 Len=0
18	0.346428785	172.217.16.110	192.168.107.128	TLSv1.3	776	Application Data

Окрім протоколів TCP, DNS та ARP, бачимо також TLS версії 1.3, що виконує захищене рукостискання, на відміну від TCP з'єднання.

↓Далі вказано типи повідомлень, що передаються, а саме клієнт посилає "Client Hello" → сервер відповідає "Server Hello", "Change Cipher Spec", "Application Data"→ клієнт посилає "Change Cipher Spec", "Application Data"→ далі починається обмін "Application Data"



tls

No.	Time	Source	Destination	Protocol	Length	Info
10	0.304627088	192.168.107.128	172.217.16.110	TLSv1.3	567	Client Hello
12	0.343839395	172.217.16.110	192.168.107.128	TLSv1.3	1484	Server Hello, Change Cipher Spec
18	0.346428785	172.217.16.110	192.168.107.128	TLSv1.3	776	Application Data
31	0.433200122	192.168.107.128	172.217.16.110	TLSv1.3	118	Change Cipher Spec, Application Data
32	0.433489068	192.168.107.128	172.217.16.110	TLSv1.3	224	Application Data
33	0.433537248	192.168.107.128	172.217.16.110	TLSv1.3	346	Application Data
37	0.451644216	172.217.16.110	192.168.107.128	TLSv1.3	662	Application Data, Application Data
39	0.452020312	192.168.107.128	172.217.16.110	TLSv1.3	85	Application Data
41	0.469753639	172.217.16.110	192.168.107.128	TLSv1.3	85	Application Data

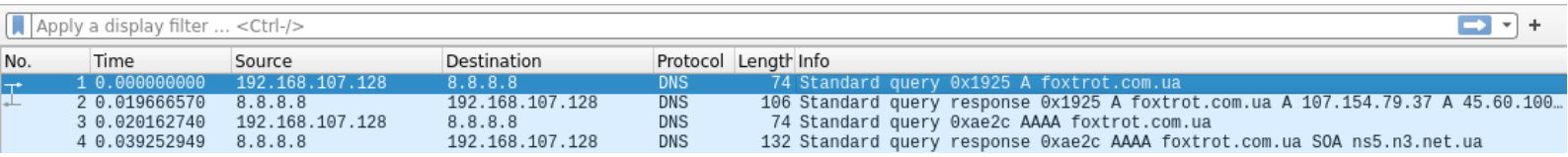
Служба DNS

Для тестування роботи служби DNS використовується утиліта nslookup.

Сформуйте запит стосовно деякої символьної адреси до вашого звичайного сервера DNS або до деякого публічного DNS-сервера (наприклад, DNS сервера Google з IP адресою 8.8.8.8) та запишіть пакети запитів до DNS та відповідей на них.

```
┌──(snz24㉿cybernaz)-[~]
└─$ nslookup foxtrot.com.ua 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   foxtrot.com.ua
Address: 107.154.79.37
Name:   foxtrot.com.ua
Address: 45.60.100.37
```



Apply a display filter ... <Ctrl-/>

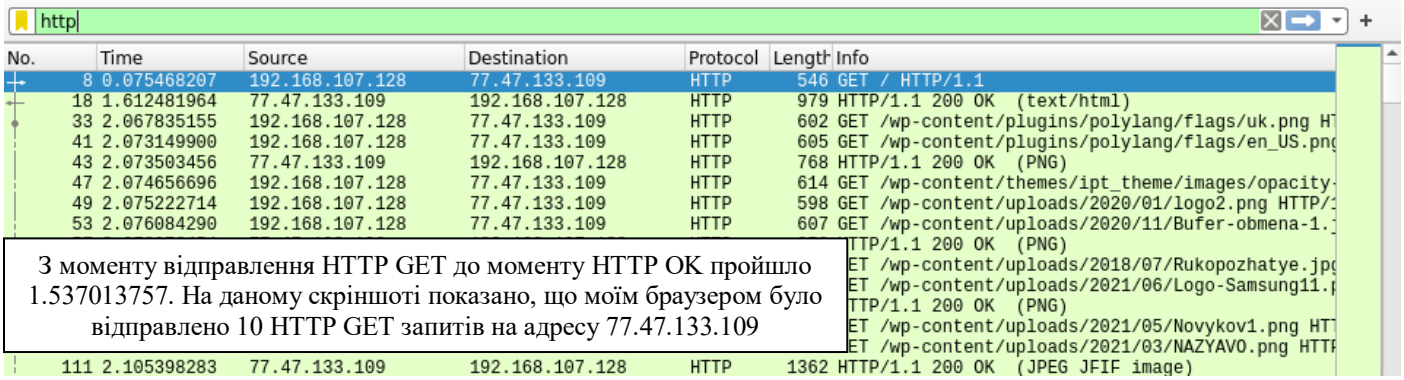
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.107.128	8.8.8.8	DNS	74	Standard query 0x1925 A foxtrot.com.ua
2	0.019666570	8.8.8.8	192.168.107.128	DNS	106	Standard query response 0x1925 A foxtrot.com.ua A 107.154.79.37 A 45.60.100…
3	0.020162740	192.168.107.128	8.8.8.8	DNS	74	Standard query 0xae2c AAAA foxtrot.com.ua
4	0.039252949	8.8.8.8	192.168.107.128	DNS	132	Standard query response 0xae2c AAAA foxtrot.com.ua SOA ns5.n3.net.ua

На прикладі перехоплених пакетів дайте відповідь на наступні питання:

HTTP:

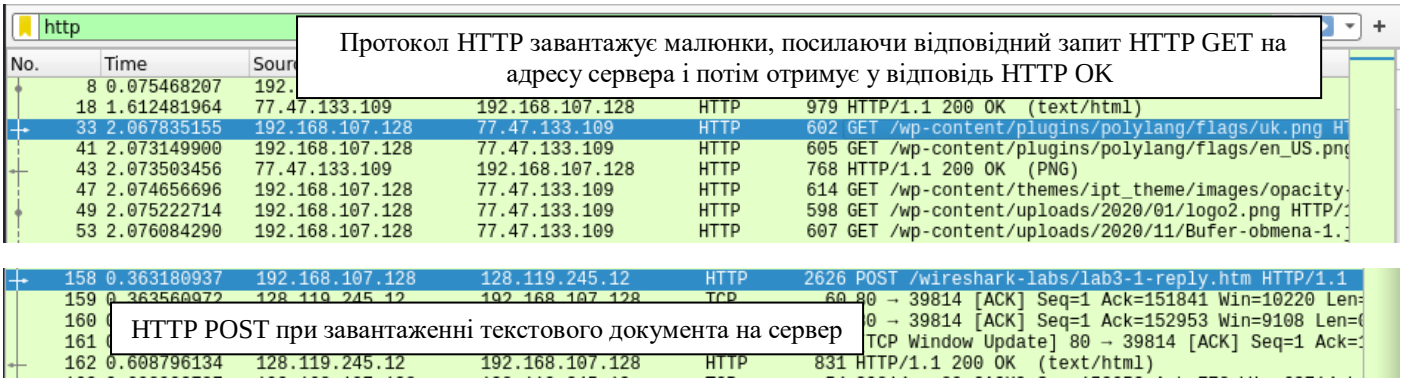
1. *Перехопіть з'єднання з Web-сервером і відновіть повідомлення, що містять запит і відповідь, а також інші об`єкти, що передаються в рамках даного з'єднання.*

2. *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?*



З моменту відправлення HTTP GET до моменту HTTP OK пройшло 1.537013757. На даному скріншоті показано, що моїм браузером було відправлено 10 HTTP GET запитів на адресу 77.47.133.109

3. *Як протокол HTTP завантажує малюнки. Продемонструйте пакети HTTP POST.*



Протокол HTTP завантажує малюнки, посилаючи відповідний запит HTTP GET на адресу сервера і потім отримує у відповідь HTTP OK

HTTP POST при завантаженні текстового документа на сервер

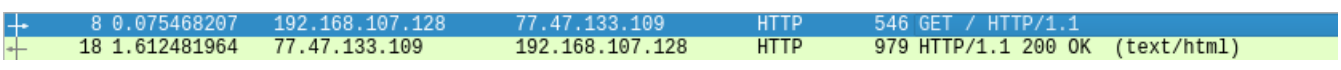
4. *Як протокол HTTP захищає при автентифікації значення login і password, що передаються.*

Найбільш серйозним недоліком базової автентифікації є те, що протокол HTTP не захищає значення *login* і *password*, тому це призводить до фактично відкритої передачі тексту пароля користувача фізичної мережі. Наприклад:

http://test_server.kiev.ua/program.php?user=guest&pass=rock

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

Мій браузер та сервер використовують версію HTTP 1.1



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

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    Host: ipt.kpi.ua\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

У мовному кодуванні en-US, en; q=0.5 мій браузер має можливість приймати інформацію від сервера

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

`HTTP/1.1 200 OK` - відповідь на перший HTTP GET

8. *Який код статусу та кодова фраза міститься у HTTP відповіді? Які ще значення можуть зустрітися? Чи є якісь рядки статусу в HTTP, що пов'язані з розбивкою повідомлення на декілька TCP сегментів.*

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

Код статусу: 200

Кодова фраза: OK

Можуть зустрітися такі HTTP відповіді:

Інформаційні	Успішні операції	Перенаправлення	Помилки клієнта	Помилки сервера
100: Continue	200: OK	303: See Other	400: Bad Request	501: Not Implemented
101: Switching Protocol	202: Created	304: Not Modified	403: Forbidden	502: Bad Gateway
102: Processing	204: No Contest	305: Use Proxy	409: Conflict	503: Service Unavailable

9. *Скільки знадобилося TCP сегментів, щоб передати звичайну HTTP відповідь?*

```
[5 Reassembled TCP Segments (12605 bytes): #10(1460), #12(5840), #14(1460), #16(2920), #18(925)]
    [Frame: 10, payload: 0-1459 (1460 bytes)]
    [Frame: 12, payload: 1460-7299 (5840 bytes)]
    [Frame: 14, payload: 7300-8759 (1460 bytes)]
    [Frame: 16, payload: 8760-11679 (2920 bytes)]
    [Frame: 18, payload: 11680-12604 (925 bytes)]
    [Segment count: 5]
    [Reassembled TCP length: 12605]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205361742c203139204a756e2032…]
```

Знадобилося 5 TCP-сегментів, щоб передати звичайну HTTP відповідь

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

```
Last-Modified: Tue, 24 May 2016 16:43:04 GMT\r\n
```

11. *Скільки байтів інформації було передано браузеру?*

```
Content-Length: 11851\r\n
```

- передано разом із першою HTTP відповіддю

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

http

No.	Time	Source	Destination	Protocol	Length	Info
8	0.075468207	192.168.107.128	77.47.133.109	HTTP	546	GET / HTTP/1.1
18	1.612481964	77.47.133.109	192.168.107.128	HTTP	979	HTTP/1.1 200 OK (text/html)
33	2.067835155	192.168.107.128	77.47.133.109	HTTP	602	GET /wp-content/plugins/polylang/flags/uk.png HTTP/1.1
41	2.073149900	192.168.107.128	77.47.133.109	HTTP	605	GET /wp-content/plugins/polylang/flags/en_US.png HTTP/1.1
43					768	HTTP/1.1 200 OK (PNG)
47					614	GET /wp-content/themes/ipt_theme/images/opacity-logo1.png HTTP/1.1
49					598	GET /wp-content/uploads/2020/01/logo2.png HTTP/1.1
53					607	GET /wp-content/uploads/2020/11/Bufer-obmena-1.jpg HTTP/1.1
57					958	HTTP/1.1 200 OK (PNG)
59					605	GET /wp-content/uploads/2018/07/Rukopozhatye.jpg HTTP/1.1
61	2.079861221	192.168.107.128	77.47.133.109	HTTP	607	GET /wp-content/uploads/2021/06/Logo-Samsung11.png HTTP/1.1

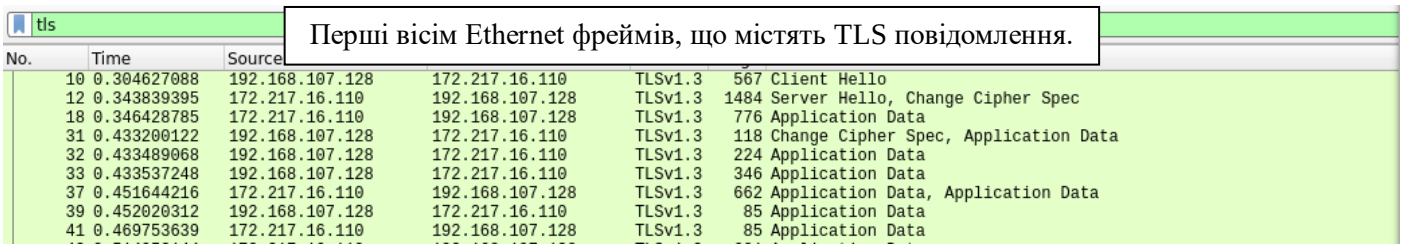
Малюнки були завантажені моїм браузером паралельно, адже два різних HTTP GET пакети отримали дві різні HTTP OK відповіді

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

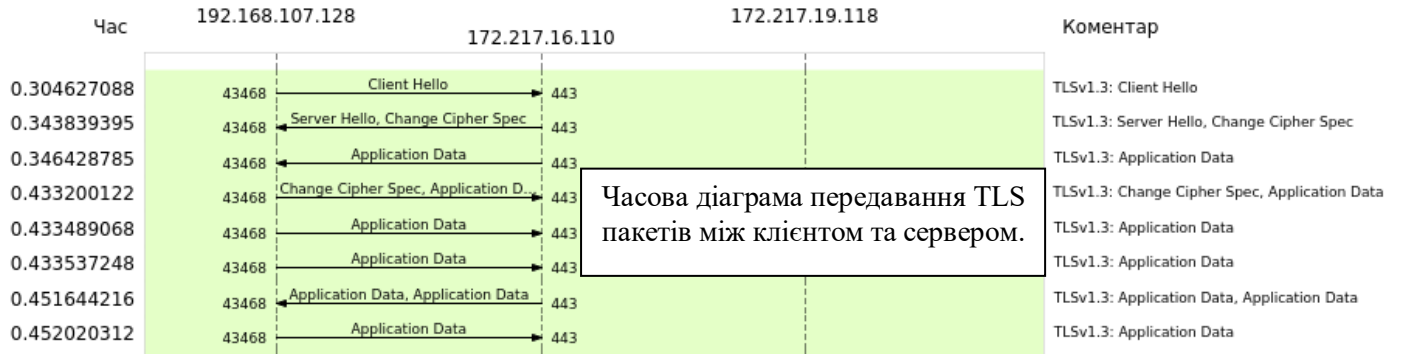
```
Referer: http://ipt.kpi.ua/\r\n
```

SSL/TLS:

1. Для кожного з перших восьми Ethernet фреймів визначте джерело повідомлення (сервер чи клієнт), визначте номер TLS запису, що вставлений у фрейм, і складіть список типів TLS повідомлень. Складіть часову діаграму передавання TLS пакетів між клієнтом та сервером.



Номер фрейму	Сервер/клієнт	Номер TLS запису	TLS повідомлення
10	Клієнт	1	Client Hello
12	Сервер	2	Server Hello, Change Cipher Spec
18	Сервер	1	Application Data
31	Клієнт	2	Change Cipher Spec, Application Data
32	Клієнт	1	Application Data
33	Клієнт	1	Application Data
37	Сервер	2	Application Data, Application Data
39	Клієнт	1	Application Data



2. Кожен TLS 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.

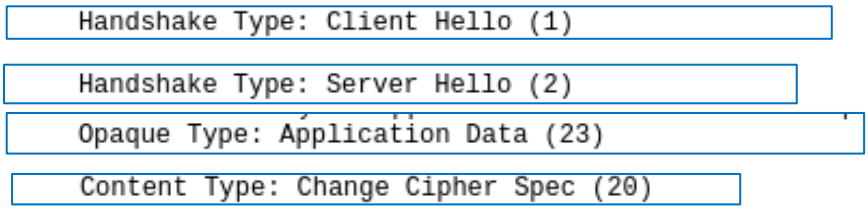
```
▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)   1 байт
    Version: TLS 1.0 (0x0301)      2 байти
    Length: 508                    2 байти
```

3. *Як шифруються дані прикладного рівня? Чи записи, які містять дані прикладного рівня, містять ще й значення хешу MAC (Message Authentication Code)? Чи Wireshark розмежовує дані прикладного рівня та хеш MAC?*

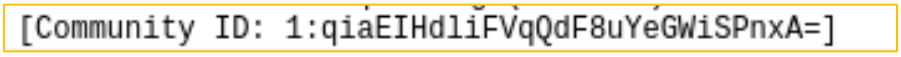
Перед тим, як розпочати захищений обмін інформацією, клієнт та сервер мають узгодити алгоритм шифрування та відповідний ключ. Це відбувається під час процедури “рукостискання” – відкриття сеансу зв’язку. Наступні алгоритми можуть бути використані для цього завдання: Криптографічна система RSA, Протокол Діффі-Геллмана, короткочасні (ефемерні) ключі Діффі-Геллмана, Протокол Діффі-Геллмана на еліптичних кривих, короткочасні ключі за протоколом Діффі-Геллмана на еліптичних кривих, анонімний протокол Діффі-Геллмана, попередньо узгоджений ключ та Secure Remote Password

TLS забезпечує відправку кожного повідомлення з кодом MAC (Message Authentication Code), алгоритм створення якого - одностороння криптографічний функція хешування (фактично - контрольна сума), ключі якої відомі обом учасникам зв'язку. Wireshark не відрізняє зашифровані дані прикладного рівня та хеш MAC

4. *а) Які типи TLS повідомлень зустрічаються в перехопленні?*



б) Який ідентифікатор даної TLS сесії?



в) Які набори алгоритмів захисту підтримують клієнт і сервер?

Криптографічна система RSA, Протокол Діффі-Геллмана, короткочасні (ефемерні) ключі Діффі-Геллмана, Протокол Діффі-Геллмана на еліптичних кривих, короткочасні ключі за протоколом Діффі-Геллмана на еліптичних кривих, анонімний протокол Діффі-Геллмана, попередньо узгоджений ключ та Secure Remote Password

г) Де передається цифровий сертифікат?

Сервер стверджує версію використовуваного протоколу, вибирає спосіб шифрування з наданого списку, і відправляє відповідь клієнту, прикріпивши свій цифровий сертифікат разом із відповіддю “Server Hello”.

DNS:

1. *Ознайомтесь с форматом DNS запиту і відповіді.*

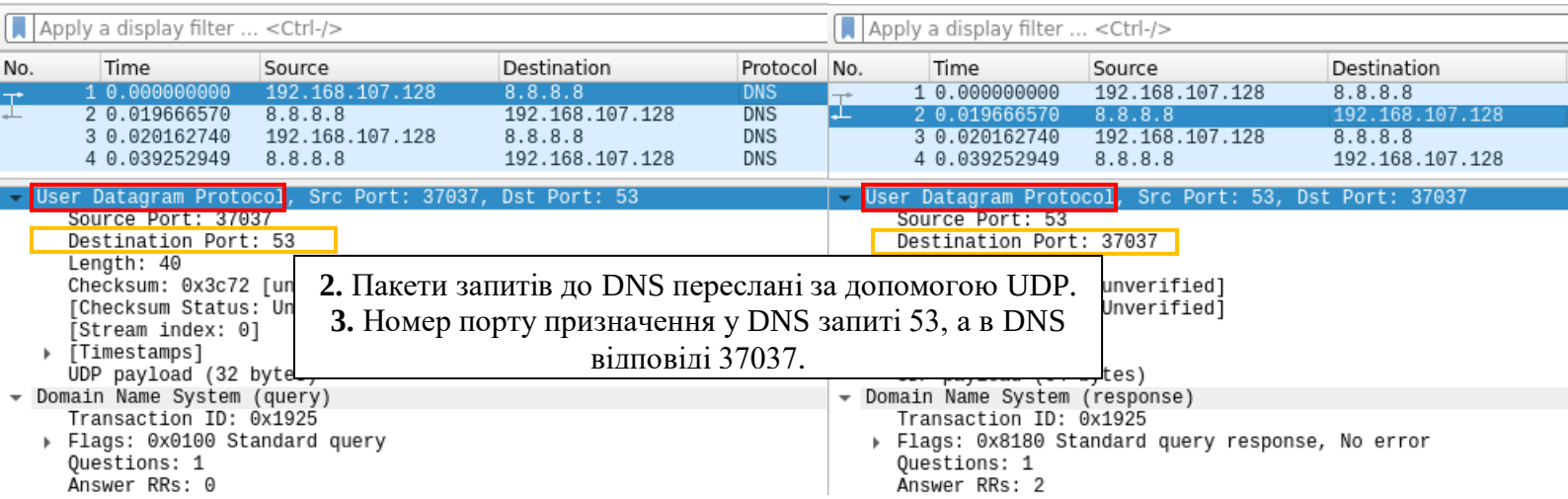
Формат *DNS запиту* дуже простий, містить ім'я, тип і клас запису.

Ім'я
Тип запису
Клас запису

Формат *DNS відповіді* складніший, перші три поля точно такі ж ім'я, тип запису і клас запису. Потім вказується час життя, це час на який запис можна зберегти в кеші DNS resolver, потім вказується довжина даних і власне дані відповіді.

Ім'я
Тип запису
Клас запису
Час життя (TTL)
Довжина даних
Дані

2. *Відшукайте пакети запитів до DNS. Вони переслані за допомогою UDP чи TCP?*
3. *Який номер порту призначення у відправленому пакеті DNS запиту? Який номер порту призначення у пакеті DNS відповіді?*



2. Пакети запитів до DNS переслані за допомогою UDP.
3. Номер порту призначення у DNS запиті 53, а в DNS відповіді 37037.

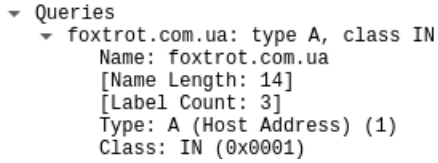
4. *На яку IP адресу був відправлений DNS запит? Послуговуючись утилітою nslookup, визначіть IP адреси вашого локального DNS серверу.*

DNS запит був відправлений на публічний DNS-сервер Google з IP адресою 8.8.8.8

```
C:\Users\user>nslookup
Default Server:  router.asus.com
Address:  192.168.1.1
```

5. *Дослідіть пакети DNS запитів. Що означає поле "Type" в ньому? Чи повідомлення містить якесь поле "Answers"?*

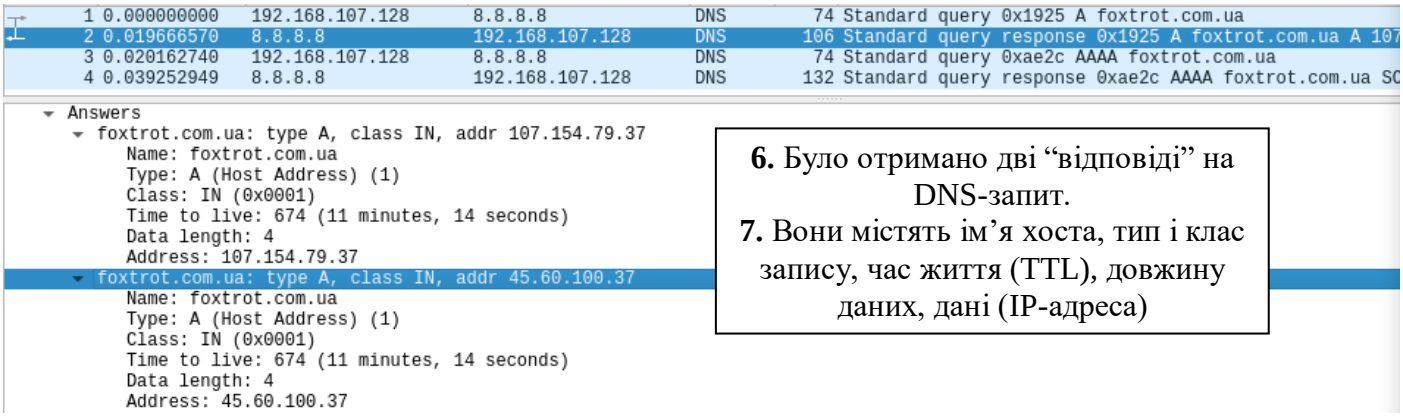
TYPE (Тип) — визначає формат і призначення цього ресурсного запису



Запис A (address record) — запис адреси — пов'язує ім'я хосту з адресою протоколу IPv4

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

7. *Що кожна з цих відповідей містить?*



6. Було отримано дві “відповіді” на DNS-запит.
7. Вони містять ім’я хоста, тип і клас запису, час життя (TTL), довжину даних, дані (IP-адреса)

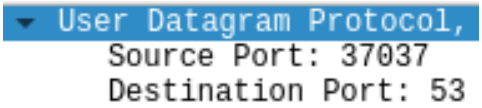
8. *Якщо на Web сторінці містяться малюнки, то чи надсилає ваш хост нові DNS запити перед завантаженням кожного з цих малюнків?*

Ні, не надсилає.

9. *На прикладах перехоплених пакетів опишіть роботу системи DNS. Який з протоколів (TCP або UDP) використовує DNS. Які номери портів мають повідомлення DNS.*

Протокол DNS (порт 53) може використовувати для роботи TCP або UDP, проте традиційно запити та відповіді відправляються у вигляді однієї UDP дейтаграми, а TCP використовується для AXFR-запитів.

DNS-запит



DNS-відповідь