Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

[Кафедра математичних методів системного аналізу](http://e-u.in.ua/ukr/?page=35)

**ЗВІТ**

про виконання лабораторних робіт

з дисципліни «Комп’ютерні мережі»

Виконав: студент групи ІС-зп92

**Чумаченко М.О.**

Прийняв: Кухарєв С.О.

Київ – 2020

|  |  |  |
| --- | --- | --- |
|  |  |  |

Лабораторна робота 1

**Мета роботи**: оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

**1. Хід роботи**

Необхідно виконати наступні дії:

1. Запустіть веб-браузер.

2. Запустіть Wireshark.

3. В Wireshark активуйте діалог вибору мережевого інтерфейсу для захоплення:

Capture >> Interfaces (або ж Ctrl + I).

4. Далі виберіть той інтерфейс, для якого відображається найбільша кількість

захоплених пакетів та натисніть кнопку Start навпроти нього.

5. Поки Wireshark захоплює пакети, відкрийте в браузері сторінку за наступною

адресою:

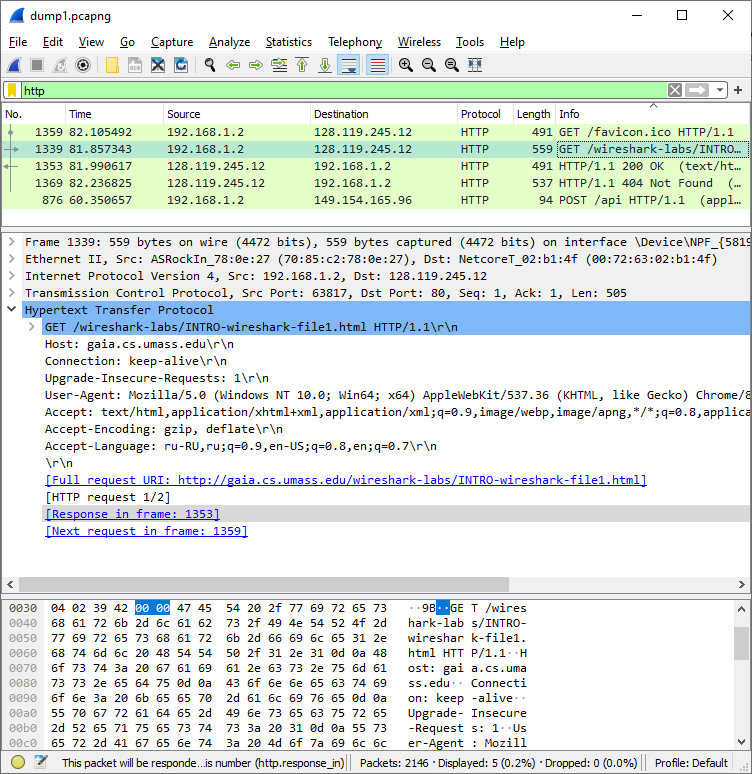
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.

6. Зупиніть захоплення пакетів за допомогою команди Capture >> Stop (або Ctrl + E).

7. Введіть текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу пакетів

мають залишитися тільки пакети, які були створені протоколом HTTP.



8. Виберіть перший пакет HTTP, який відображається в вікні лістингу, це має бути повідомлення GET протоколу HTTP. Також цей пакет має вміщувати інформації інших протоколів нижчих рівнів: TCP, IP, Ethernet.

9. У вікні деталей заголовків розкрийте деталі, пов’язані з протоколом HTTP та скрийте детальну інформацію про інші протоколи.

10. Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print.

11. Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та

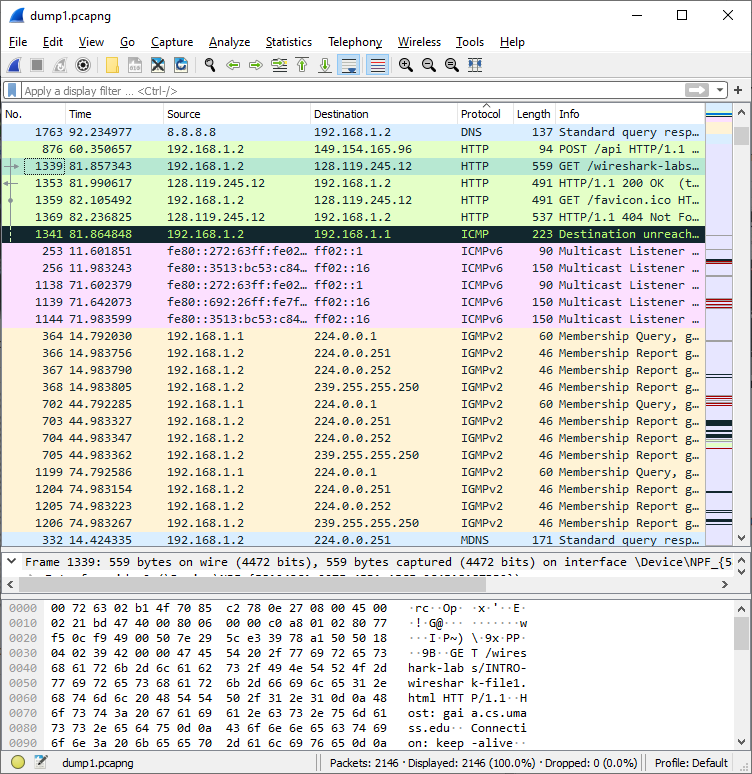
відображені необхідні для захисту протоколу.

12. Закрийте Wireshark.

**2. Контрольні запитання**

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?

Відповідь: UDP, TCP, TLSv1.2, TLSv1.3, SSL, ICMP, HTTP, IGMPv2, ICMPv6, DNS, MDNS.



2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?

Відповідь: [Protocols in frame: eth:ethertype:ip:tcp:http]

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до

отримання першого пакету з відповіддю сервера?

Відповідь: 0,133274 секунд.





4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

Запит: source – 192.168.1.2, destination – 128.119.245.12

Відповідь: source – 128.119.245.12, destination – 192.168.1.2

5. Яким був перший рядок запиту на рівні протоколу HTTP?



6. Яким був перший рядок відповіді на рівні протоколу HTTP?



Лабораторна робота 2

**Мета роботи**: аналіз деталей роботи протоколу HTTP.

**1. Хід роботи**

Необхідно виконати наступні дії:

1. Запустіть веб-браузер, очистіть кеш браузера.

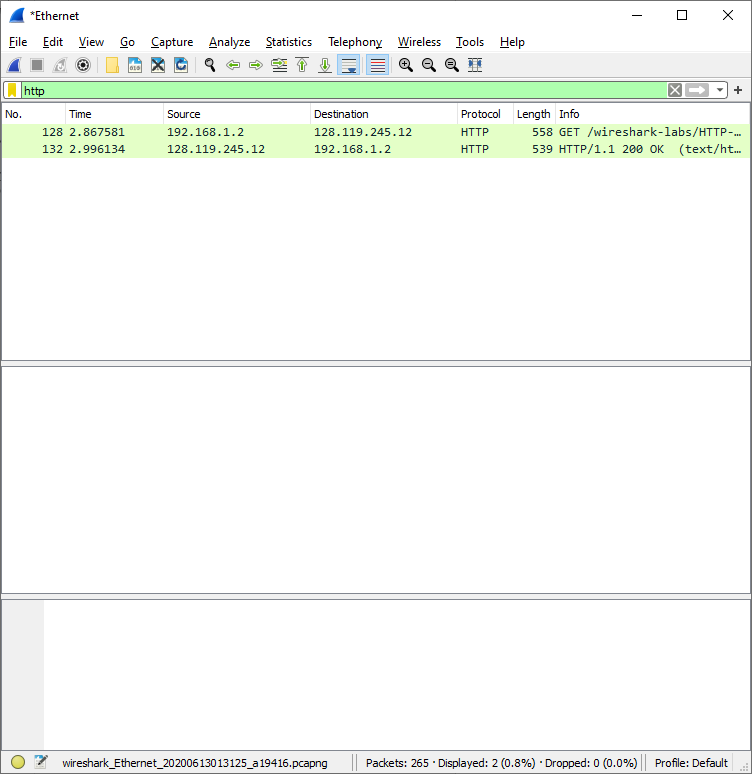
2. Запустіть Wireshark, введіть «http» в поле фільтрації, почніть захоплення пакетів.

3. Відкрийте за допомогою браузера одну із зазначених нижче адрес:

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

http://194.44.29.242/index.html

4. Зупиніть захоплення пакетів.



5. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей

пакету: згорніть деталі протоколів усіх рівнів крім HTTP (за допомогою знаків +/-).

6. Приготуйте відповіді на контрольні запитання 1-7, роздрукуйте необхідні для цього пакети.

7. Почніть захоплення пакетів.

8. Відкрийте у браузері ту ж саму сторінку, або ж просто натисніть F5 для її

повторного завантаження.

Якщо ви працюєте зі сторінкою на gaia.cs.umass.edu (ця сторінка регенерується

кожну хвилину) – почніть спочатку та виконайте кроки 1,2,3 та 8.

9. Зупиніть захоплення пакетів.

10. Приготуйте відповіді на контрольні запитання 8-11, роздрукуйте необхідні для

цього пакети.

11. Віберіть адрес деякого ресурсу (наприклад, зображення), розмір якого перевищує

8192 байти.

12. Почніть захоплення пакетів та очистіть кеш браузера.

13. Відкрийте обраний ресурс браузером.

14. Зупиніть захоплення пакетів.

15. Приготуйте відповіді на запитання 12-15. При необхідності роздрукуйте деякі

пакети з відповіді сервера.

16. Почніть захоплення пакетів.

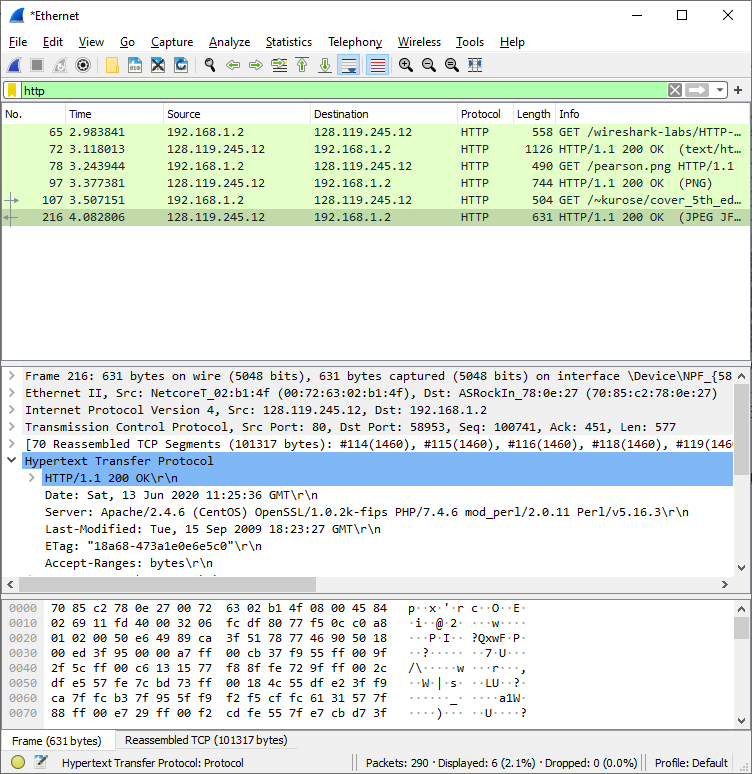
17. Відкрийте сторінку за адресою

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

також можна використати будь-яку нескладну сторінку з невеликою кількістю

зовнішніх ресурсів.

18. Зупиніть захоплення пакетів.



19. Приготуйте відповіді на запитання 16, 17. Роздрукуйте необхідні для цього пакети.

20. Закрийте Wireshark.

**2. Контрольні запитання**

1. Яку версію протоколу HTTP використовує ваш браузер (1.0 чи 1.1)? Яку версію

протоколу використовує сервер?

Відповідь: 1.1, 1.1





2. Які мови (якщо вказано) браузер може прийняти від сервера?

Відповідь: англійська, російська.



3. Які IP-адреси вашого комп’ютера та цільового веб-сервера?

Відповідь: мій – 192.168.1.2, сервера – 128.119.245.12



4. Який статусний код сервер повернув у відповіді вашому браузеру?

Відповідь: код 200.



5. Коли на сервері в останній раз був модифікований файл, який запитується браузером?



6. Скільки байт контенту повертається сервером?



7. Переглядаючи нерозібраний байтовий потік пакету, чи бачите ви деякі заголовки в потоці, які не відображаються у вікні деталей пакету? Якщо так, назвіть один з них.

Відповідь: ні.

8. Перевірте вміст першого запиту HTTP GET від вашого браузера до сервера. Чи є в

ньому заголовок IF-MODIFIED-SINCE?

Відповідь: ні.

9. Перевірте вміст першої відповіді сервера. Чи повернув сервер вміст файлу

безпосередньо у відповіді?

Відповідь: так.



10. Перевірте вміст другого запиту HTTP GET. Чи є в ньому заголовок IF-MODIFIED-SINCE? Якщо так, яке значення йому відповідає?



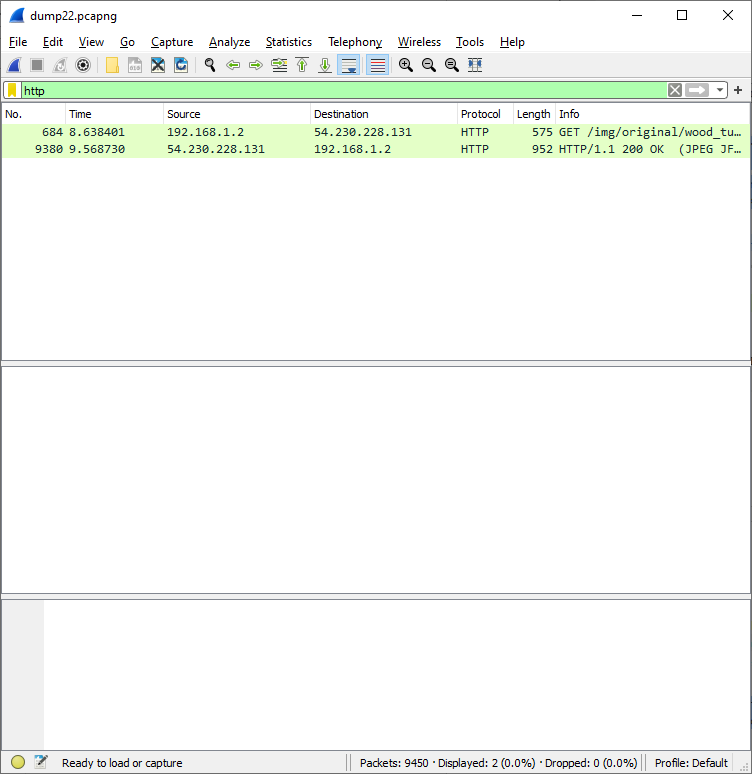
11. Який код та опис статусу другої відповіді сервера? Чи повернув сервер вміст файлу безпосередньо у відповіді?

Відповідь: не повернув.



12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

Відповідь: одне повідомлення.



13. Скільки пакетів TCP було необхідно для доставки одної відповіді HTTP-сервера?



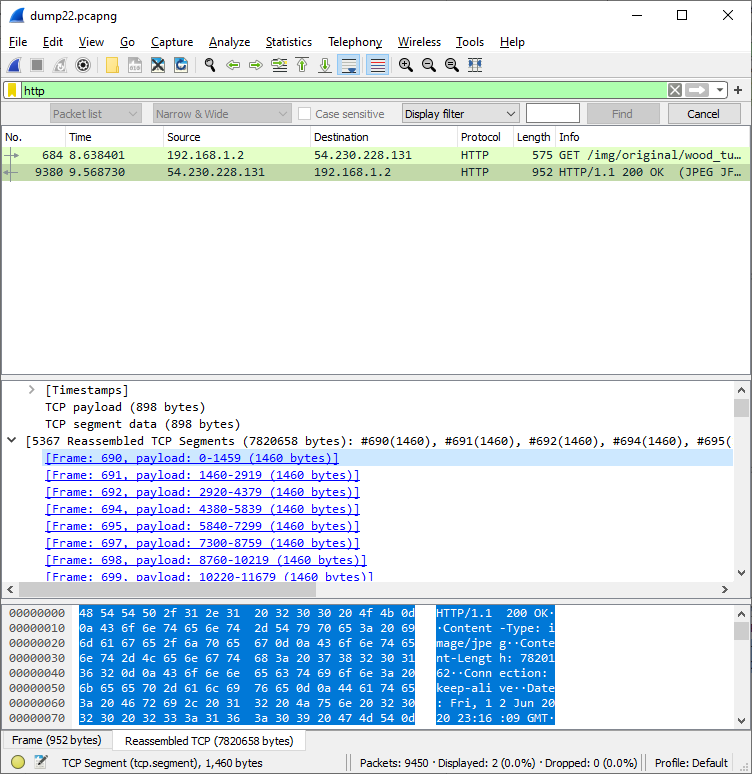
14. Який код та опис статусу був у відповіді сервера?



15. Чи зустрічаються у даних пакетів-продовжень протоколу TCP стрічки з кодом та

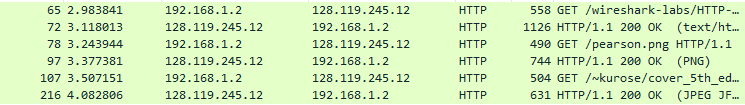
описом статусу відповіді, або ж якісь заголовки протоколу HTTP?

Відповідь: зустрічаються у першому фреймі, в байтах 9-14.



16. Скільки запитів HTTP GET було відправлено вашим браузером? Якими були цільові IP-адреси запитів?

Відповідь: три запити, цільові IP-адреси – 128.119.245.12



17. Чи можете ви встановити, чи були ресурси отримані паралельно чи послідовно?

Яким чином?

Відповідь: ресурси були отримані послідовно, адже кожен запит на новий ресурс відбувався після отримання попереднього. Також, можна було візуально спостерігати завантаження кожного ресурсу на сторінці.

Лабораторна робота 3

**Мета роботи**: аналіз деталей роботи протоколу DNS.

**1. Хід роботи**

Необхідно виконати наступні дії:

1. Очистіть кеш DNS-записів.

2. Запустіть веб-браузер, очистіть кеш браузера.

3. Запустіть Wireshark, почніть захоплення пакетів.

4. Відкрийте за допомогою браузера одну із зазначених нижче адрес:

http://www.ietf.org

5. Зупиніть захоплення пакетів.

6. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей

пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).

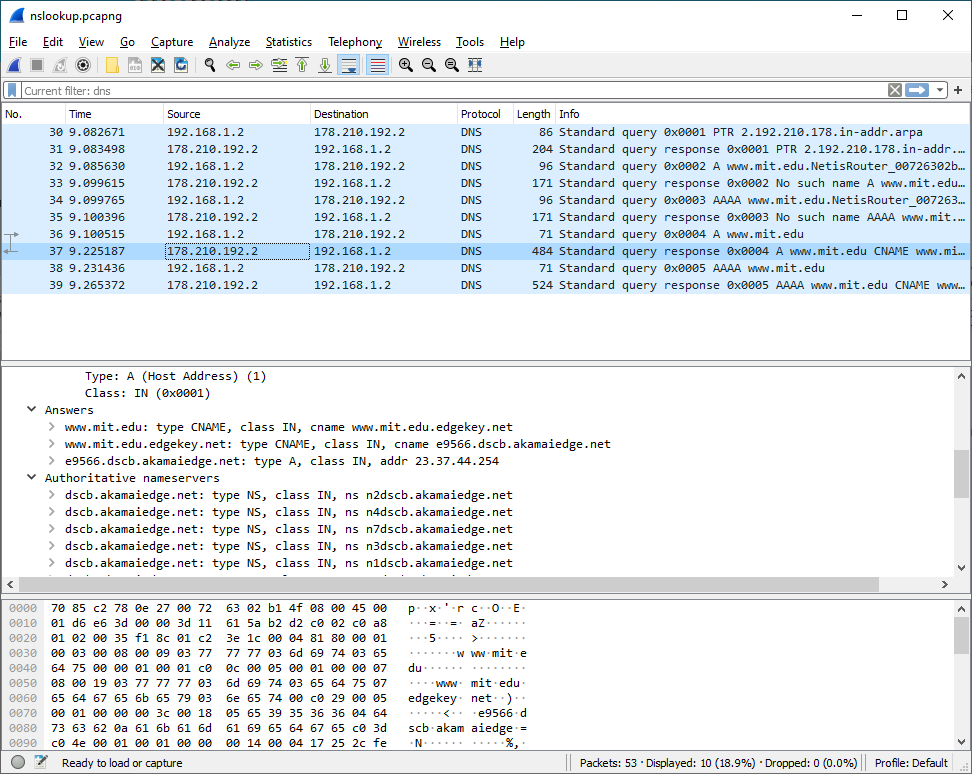
7. Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.

8. Почніть захоплення пакетів.

9. Виконайте nslookup для домену www.mit.edu за допомогою команди

a. nslookup www.mit.edu

10. Зупиніть захоплення пакетів.



11. Приготуйте відповіді на контрольні запитання 7-10, роздрукуйте необхідні для

цього пакети. Утиліта nslookup відправляє три запити та отримує три відповіді,

така поведінка є специфічною, тому слід ігнорувати перші два запити та перші дві

відповіді.

12. Почніть захоплення пакетів.

13. Виконайте nslookup для домену www.mit.edu за допомогою команди

a. nslookup –type=NS mit.edu

14. Зупиніть захоплення пакетів.

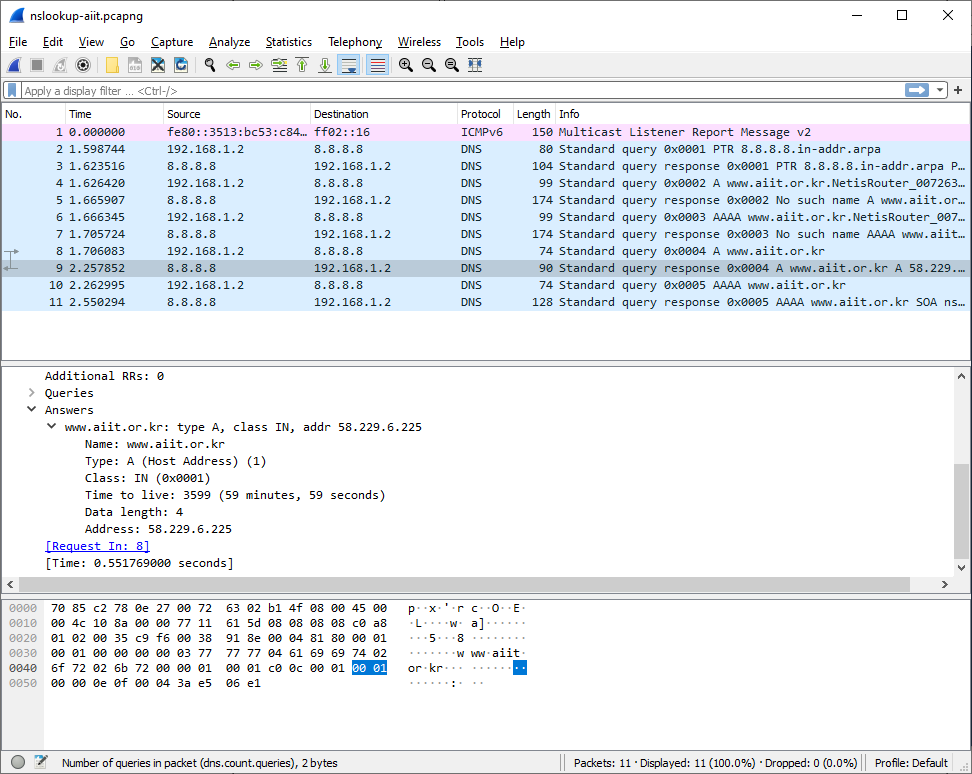
15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі

захоплені пакети.

16. Почніть захоплення пакетів.

17. Виконайте nslookup для домену www.mit.edu за допомогою команди

a. nslookup www.aiit.or.kr bitsy.mit.edu



18. Зупиніть захоплення пакетів.

19. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі

захоплені пакети.

20. Закрийте Wireshark.

**2. Контрольні запитання**

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або

TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта

відповіді DNS?

Відповідь: UDP, цільовий порт – 53, вихідний – 56053.



2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

Відповідь: на адресу 8.8.8.8, це безкоштовний публічний DNS-сервер Google.

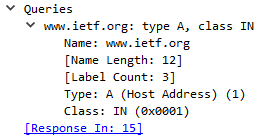




3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує

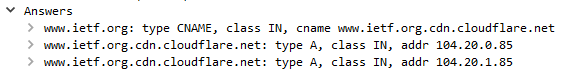
цей запит деякі можливі компоненти «відповіді»?

Відповідь: Type A, посилання на відповідь



4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

Відповідь: 3 відповіді, перша містить CNAME ідентифікатор, дві інші – IP-адреси.



5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після

отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

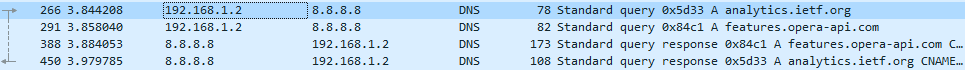
Відповідь: так, повідомлення було надіслане на першу адресу.



6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які

використовує документ, що отримав браузер?

Відповідь: так, був зроблений ще один запит.



7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт

повідомлення із відповіддю DNS?

Відповідь: цільовий порт запита – 53, вихідний порт відповіді – 53.





8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого

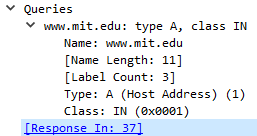
локального сервера DNS за замовчанням?

Відповідь: 178.210.192.2, це адреса мого локального сервера DNS.



9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

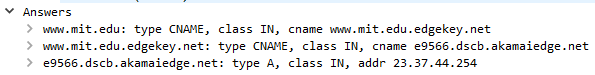
Відповідь: запит типу А, вміщує посилання на відповідь.



10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було

запропоновано сервером? З чого складається кожна із цих відповідей?

Відповідь: 3 відповіді, перші дві з CNAME ідентифікаторами, остання з IP-адресою.



11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого

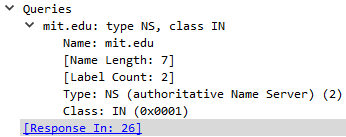
локального сервера DNS за замовчанням?

Відповідь: запит був направлений на адресу 8.8.8.8, вона є публічним сервером Google.



12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Відповідь: тип NS, вміщує посилання на відповідь.

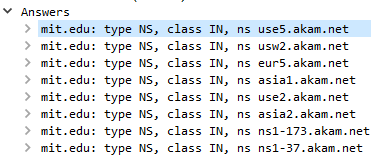


13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було

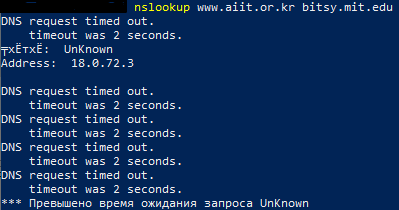
запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери

були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

Відповідь: було запропоновано 8 відповідей, сервери були запропоновані за доменним ім’ям.



Так, як наведений DNS виявився недосяжним, використовувався запит nslookup www.aiit.or.kr 8.8.8.8



14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого

локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені

відповідає ця IP-адреса?

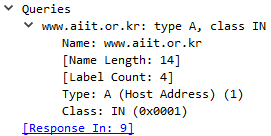
Відповідь: на адресу 8.8.8.8. Це адреса безкоштовного публічного DNS Google під назвою dns.google





15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Відповідь: запит типу А, вміщує посилання на відповідь.



16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було

запропоновано сервером? З чого складається кожна з цих відповідей?

Відповідь: сервером була запропонована одна відповідь з IP-адресою.

