Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Кафедра математичних методів системного аналізу

ЗВІТ

Про виконання лабораторних робіт

З дисципліни «Комп'ютерні мережі»

Виконав: ст. гр. ІС-ЗП91

Вдовенко А.М.

Прийняв: Кухарєв С.О.

Київ – 2020

Лабораторна робота 3

Хід роботи

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.

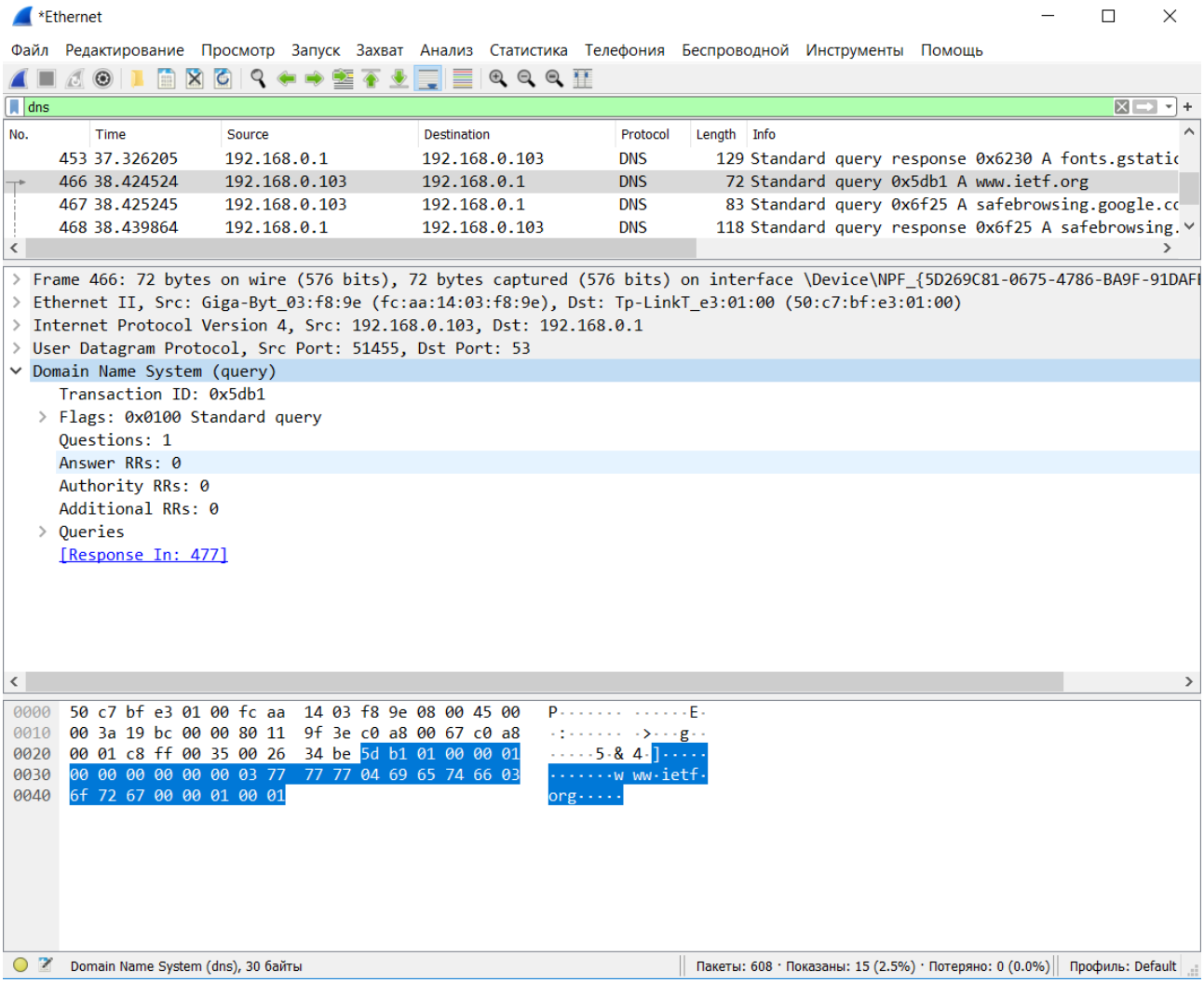


Рис. 1 – Результати запиту

8. Почніть захоплення пакетів

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

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

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

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

21. Закрийте Wireshark

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?

- Використовує протокол UDP. Src:192.168.1.248, Dst:192.168.1.1

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

- Dst:192.168.1.1 – це локальний DNS сервер

3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи Вміщує цей запит деякі можливі компоненти «відповіді»?

- Має ссилку на відповідь. [Response In: 15]

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

- 3 відповіді, кожна має такі поля: Name, Type, Class, Time to live, Data length, Address;

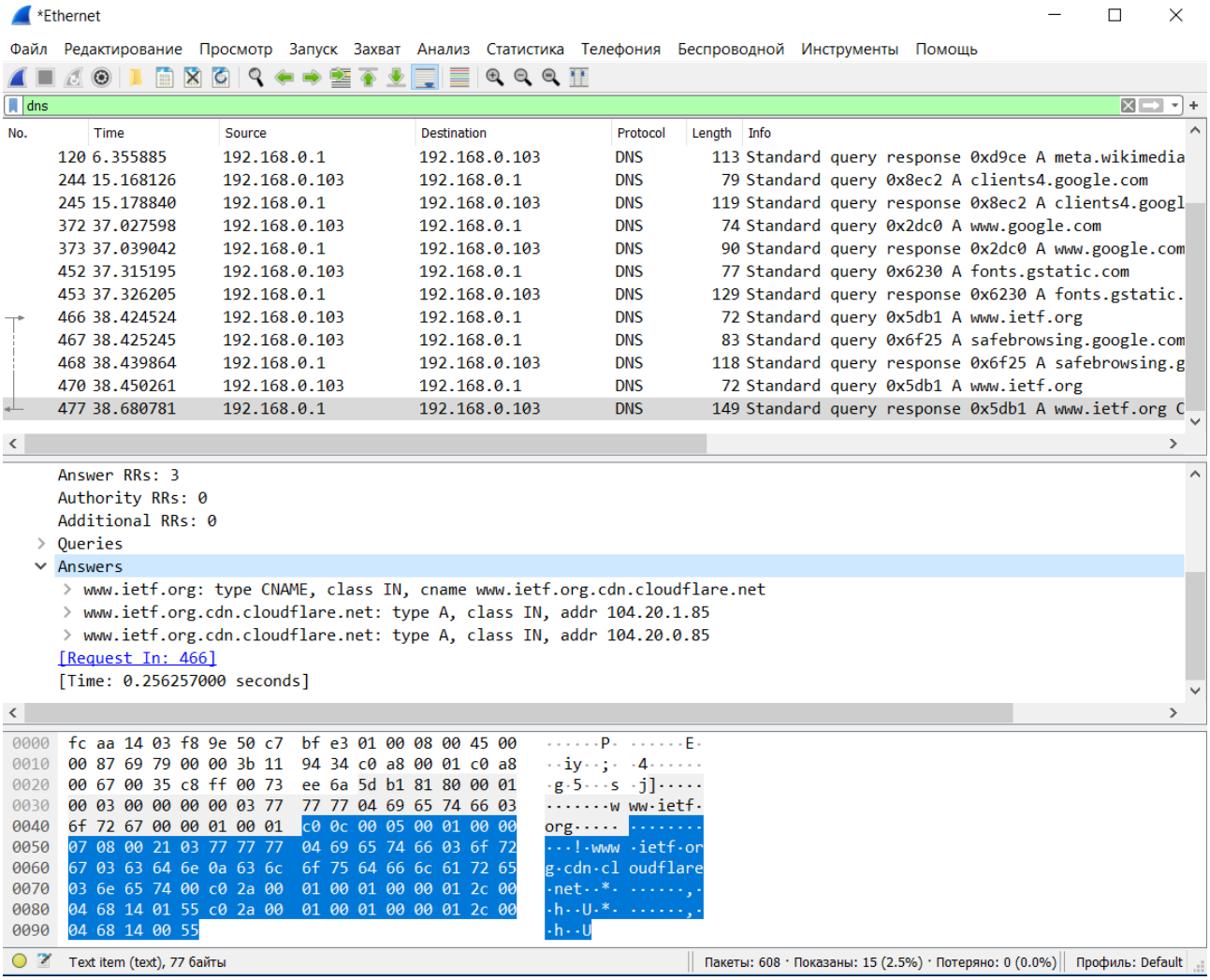


Рис. 2 – DNS Answers

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?

- Так. В другій відповіді від DNS бачимо Address: 104.20.1.85 і в наступному запиті (рис 3) бачимо саме цю адресу.

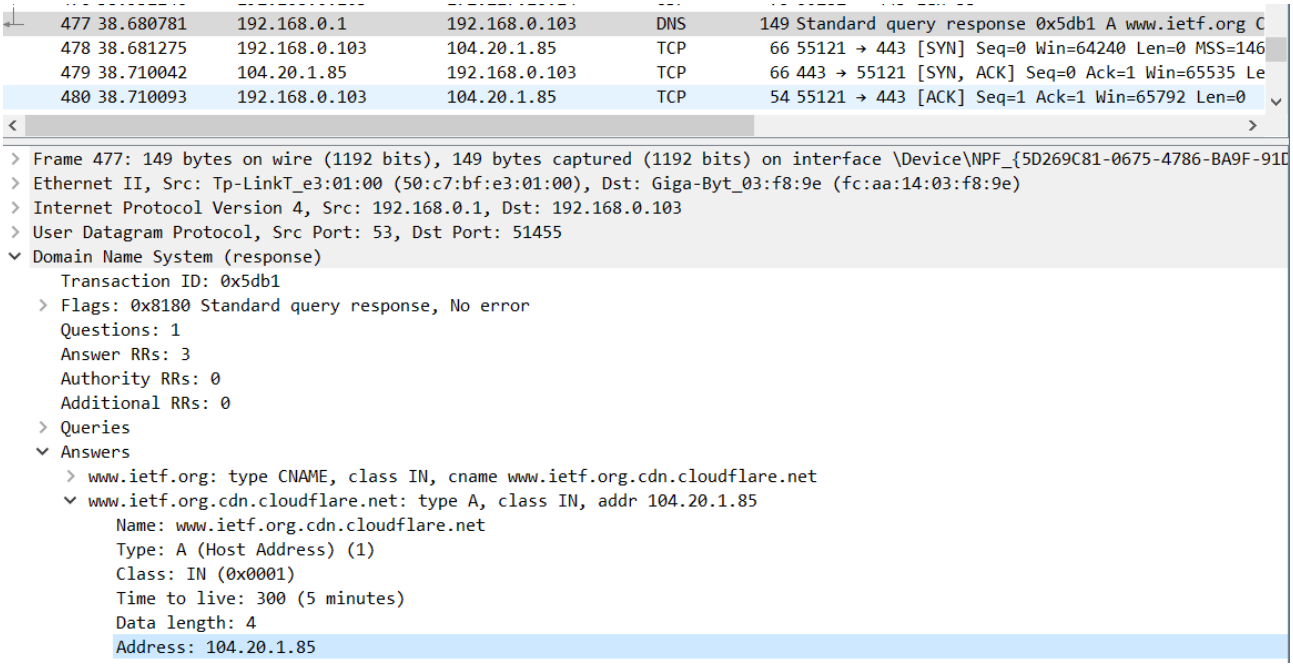


Рис. 3 – TCP source address

6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

- Так, був виконаний ще один запит

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

- Запит: Source Port: 61748 Destination Port: 53
- Відповідь: Source Port: 53 Destination Port: 61748

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

- Dst: 192.168.1.1 – адреса локального сервера за замовчанням

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

- Запит по UDP протоколу з посиланням на відповідь

10. Дослідить повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей

- 4 записи з відповідями, кожна складається з таких значень:
    - Name: www.mit.edu
    - Type: CNAME (Canonical NAME for an alias) (5)
    - Class: IN (0x0001)
    - Time to live: 1264 (21 minutes, 4 seconds)
    - Data length: 25
    - CNAME: www.mit.edu.edgekey.net

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

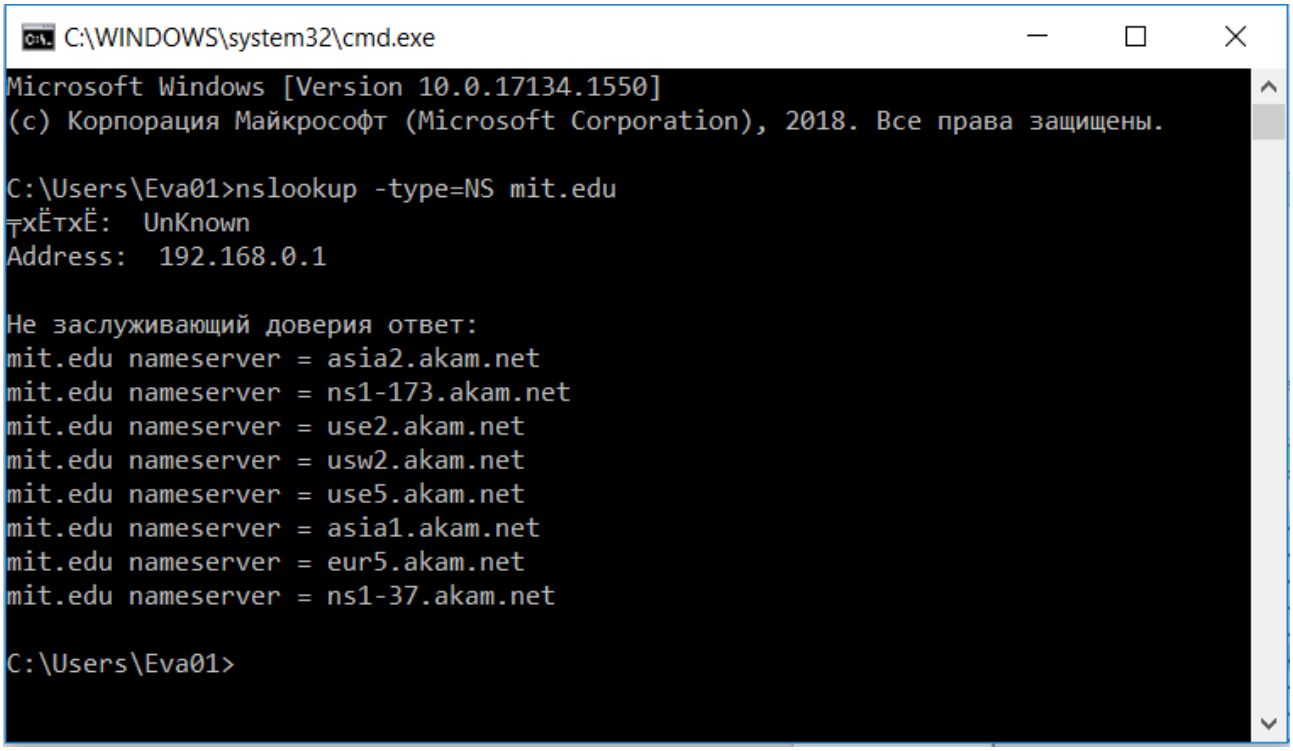
- Відповідь: Destination: 192.168.1.1 – це є адреса локального сервера DNS за замовчанням

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

- Відповідь: Це був запит по UDP протоколу. Так, цей запит вміщує ссилку на відповідь: [Response in: 16]

13. Дослідить 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?

- 8 записів з відповідями, сервери запропоновані за допомогою доменного імені



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?

- Запит було відправлено на 18.0.72.3 що не є адресою локального серверу за замовченням, адреса відповідає доменному імені
    - Name: www.aiit.or.kr

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

Тип запиту A, вміщує посилання на відповідь

16. Дослідить повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

- 1 відповідь що вміщує такі дані
    - Name: bitsy.mit.edu
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to live: 1025 (17 minutes, 5 seconds)
    - Data length: 4

- Address: 18.0.72.3