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-ЗП92

Дикун С.С.

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.

A screenshot of a social media post

Description automatically generated

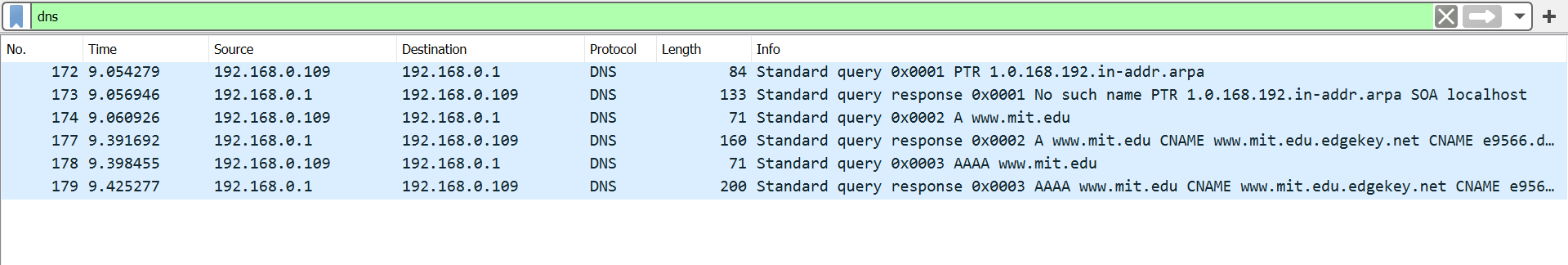
Мал. 1 – Результати запиту

8. Почніть захоплення пакетів

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

nslookup www.mit.edu

10. Зупиніть захоплення пакетів.



Мал. 2 – Результати запиту

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?

* Протокол UDP, Source Port: 62425, Destination Port: 53

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

* 192.168.0.1 – адреса локального DNS сервера

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

* Він містить посилання на рядок з відповіддю ([Response In: 57])

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;

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, співпадає

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

* Так, ще один запит - отримання IP-адреси analytics.ietf.org

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

* Запит: Source Port: 52021; Destination Port: 53
* Відповідь: Source Port: 53; Destination Port: 52021

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

* Dst: 192.168.0.1. Так, це 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: 1800 (30 minutes)Data length: 25
  + Data length: 25
  + CNAME: [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net)

Всі відповіді відображено на малюнку 3:

A screenshot of a cell phone

Description automatically generated

Мал. 2 – Результати запиту

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

* Відповідь: Destination: 192.168.0.1 – так, адреса мого 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 і він містить посилання на відповідь: [Response in: 94]

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?

* Було створено 8 записів, сервери запропоновані за допомогою доменного імені.

A screenshot of a social media post

Description automatically generated

Мал. 3 – Записи з адресами

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?

* На адресу 18.0.72.3

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

* UPD, Type: A (Host Address) (1)

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

* Немає дожної відповіді:

A screenshot of a cell phone

Description automatically generated

Мал. 4 – Таймаут