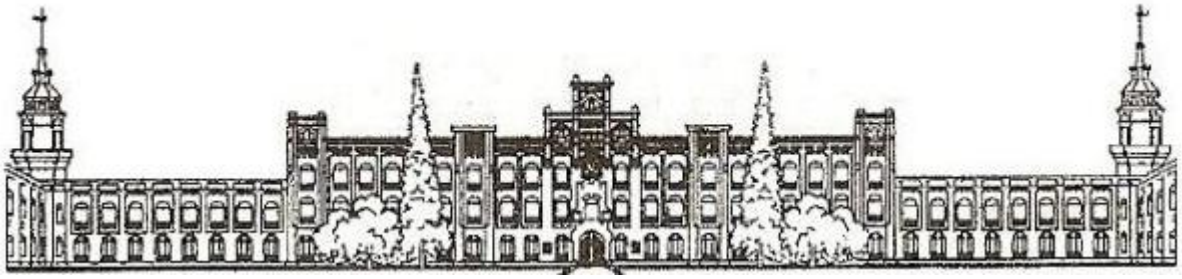


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Лабораторна робота № 3

З дисципліни: Комп'ютерні мережі

Протоколи DNS

Виконала:

Студентка III курсу

Групи КА-74

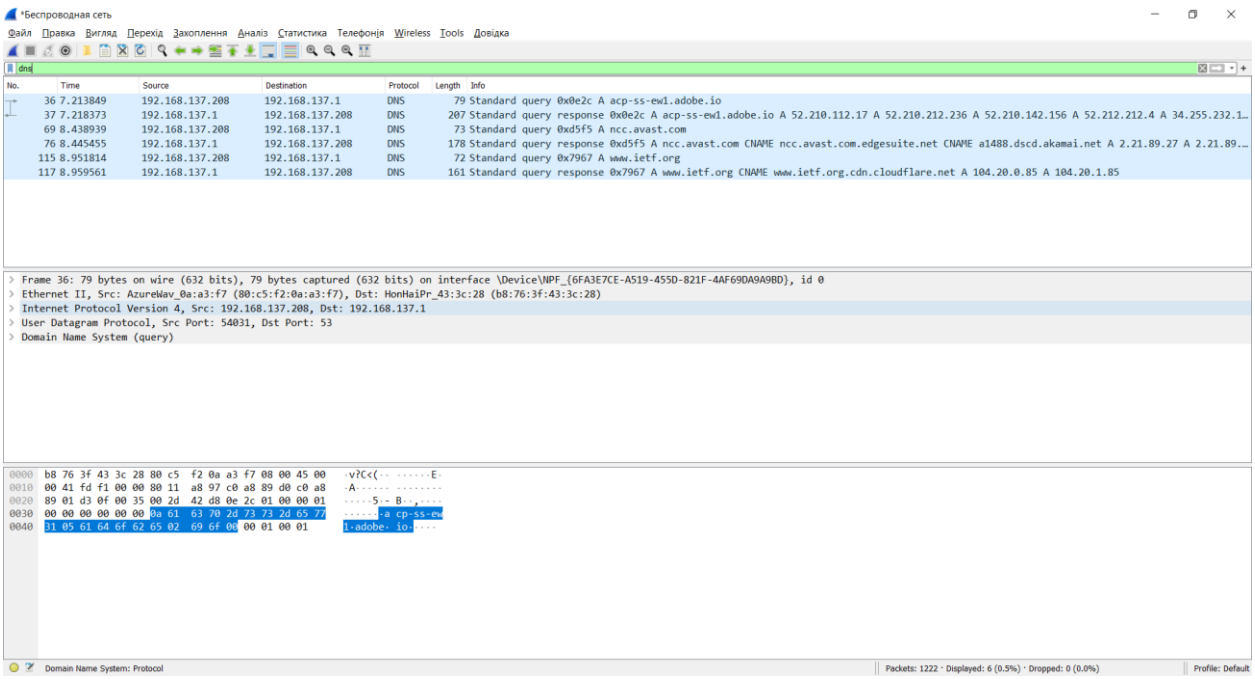
Соболь Н. О.

Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи



Контрольні питання

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?

```
> Ethernet II, Src: AzureWav_0a:a3:f7 (80:c5:f2:0a:a3:f7), Dst: HonHaiPr_43:3c:28 (b8:76:3f:43:3c:28)
> Internet Protocol Version 4, Src: 192.168.137.208, Dst: 192.168.137.1
> User Datagram Protocol, Src Port: 54031, Dst Port: 53
```

Цільовий - 53
Вихідний - 54031

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

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

```
Queries
 > acp-ss-ew1.adobe.io: type A, class IN
[Response In: 37]
```

Вміщує.

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

```
Answers
  acp-ss-ew1.adobe.io: type A, class IN, addr 52.210.112.17
  acp-ss-ew1.adobe.io: type A, class IN, addr 52.210.212.236
  acp-ss-ew1.adobe.io: type A, class IN, addr 52.210.142.156
  acp-ss-ew1.adobe.io: type A, class IN, addr 52.212.212.4
  acp-ss-ew1.adobe.io: type A, class IN, addr 34.255.232.175
  acp-ss-ew1.adobe.io: type A, class IN, addr 52.17.96.151
  acp-ss-ew1.adobe.io: type A, class IN, addr 52.209.254.227
  acp-ss-ew1.adobe.io: type A, class IN, addr 52.210.118.87
[Request In: 36]
```

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, виконує.

```
DNS        79 Standard query 0x0e2c A acp-ss-ew1.adobe.io
DNS        72 Standard query 0x7967 A www.ietf.org
DNS        73 Standard query 0xd5f5 A ncc.avast.com
DNS       207 Standard query response 0x0e2c A acp-ss-ew1.adobe.io A 52.210.112.17 A 52.210.212.236 A 52.210.142.156 A 52.212.212.4 A 34.255.232.1…
DNS       161 Standard query response 0x7967 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85
DNS       178 Standard query response 0xd5f5 A ncc.avast.com CNAME ncc.avast.com.edgesuite.net CNAME a1488.dscd.akamai.net A 2.21.89.27 A 2.21.89.…
```

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

Запит Dst: 192.168.137.1

Відповідь 192.168.137.1

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

IP: 192.168.137.1. Так, є адресою локального сервера.

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

```
Queries
  www.mit.edu: type A, class IN
[Response In: 29]
```

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

```
Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.38.92.10
  [Request In: 28]
  [Time: 0.003918000 seconds]
```

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

IP: 192.168.137.1. Так, є адресою локального сервера.

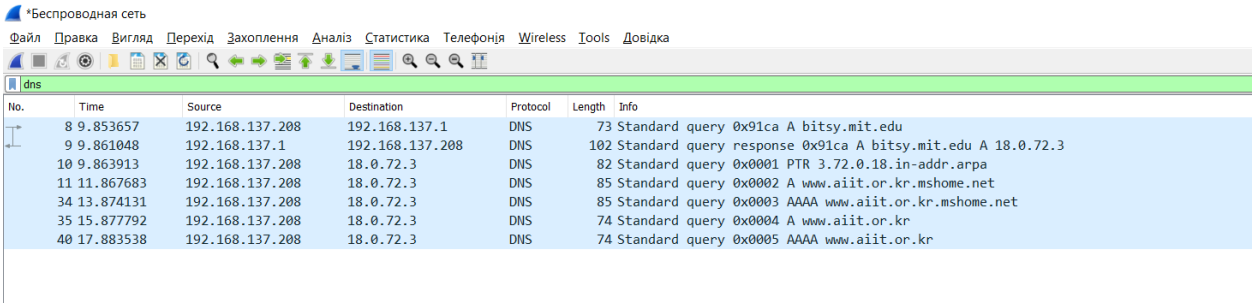
12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»? Вміщує.

```
Queries
  > 1.137.168.192.in-addr.arpa: type PTR, class IN
[Response In: 43]
```

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?

```
Answers
  > mit.edu: type NS, class IN, ns asia1.akam.net
  > mit.edu: type NS, class IN, ns use5.akam.net
  > mit.edu: type NS, class IN, ns eur5.akam.net
  > mit.edu: type NS, class IN, ns use2.akam.net
  > mit.edu: type NS, class IN, ns ns1-173.akam.net
  > mit.edu: type NS, class IN, ns asia2.akam.net
  > mit.edu: type NS, class IN, ns usw2.akam.net
  > mit.edu: type NS, class IN, ns ns1-37.akam.net
[Request In: 46]
[Time: 0.007270000 seconds]
```

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?

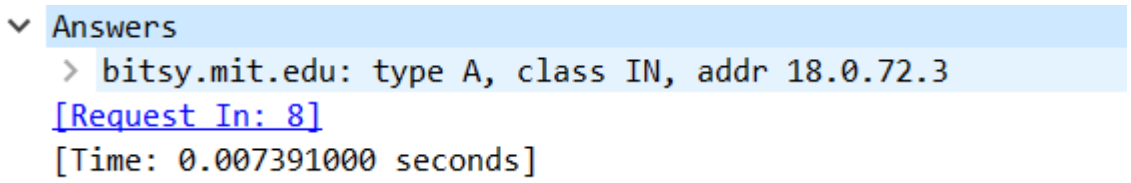


IP: 192.168.137.1. Так, є адресою локального сервера.

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

Тип запиту - A. Вміщує.

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



Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та було проведено аналіз деталей роботи даних протоколів.