

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
Семіконь Я. В.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Wireshark, необхідними для дослідження мережевих протоколів.Начало форми

Хід виконання роботи

```
Germes-Air:~ some321user_34$ nslookup www.mit.edu
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
www.mit.edu      canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.96.143.80

Germes-Air:~ some321user_34$ █
```

```
=====

Germes-Air:~ some321user_34$ nslookup -type=NS mit.edu
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = use2.akam.net.

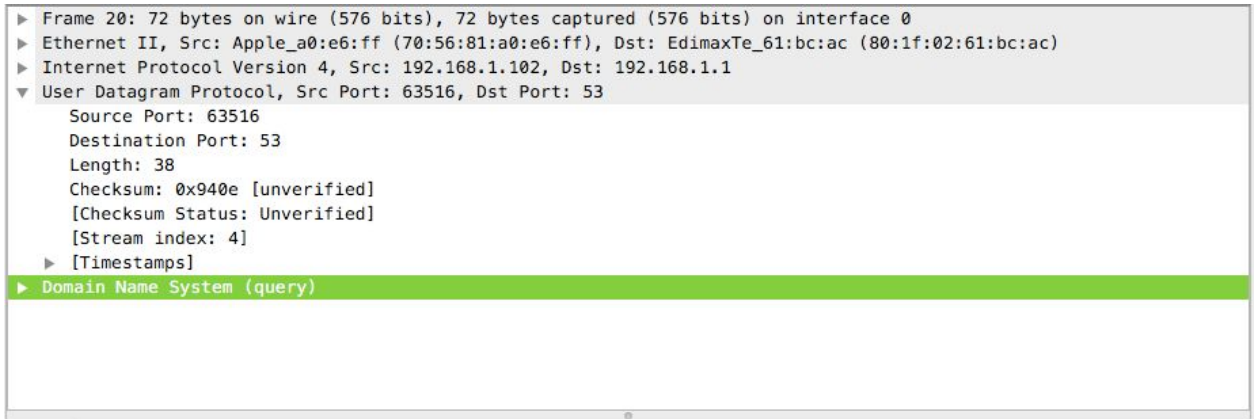
Authoritative answers can be found from:

Germes-Air:~ some321user_34$ █
```

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?

DNS використовує UDP.



Цільовий порт: 53

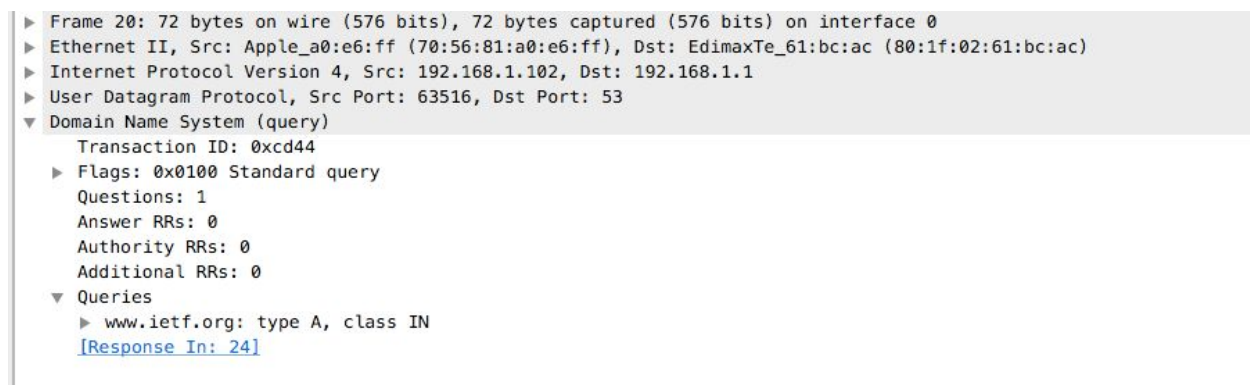
Вихідний порт: 63516

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

No.	Time	Source	Destination	Protocol	Length	Info
20	2.166444	192.168.1.102	192.168.1.1	DNS	72	Standard query 0xcd44 A www.ietf.org
24	2.221163	192.168.1.1	192.168.1.102	DNS	149	Standard query response 0xcd44 A www.ietf.org ...
1765	4.664370	192.168.1.102	192.168.1.1	DNS	80	Standard query 0x313c A speeddials.opera.com
1766	4.692432	192.168.1.1	192.168.1.102	DNS	190	Standard query response 0x313c A speeddials.op...

IP: 192.168.1.1 Так є.

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



Тип запиту – А . Вміщує.

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

```
▶ Frame 24: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
▶ Ethernet II, Src: EdimaxTe_61:bc:ac (80:1f:02:61:bc:ac), Dst: Apple_a0:e6:ff (70:56:81:a0:e6:ff)
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.102
▶ User Datagram Protocol, Src Port: 53, Dst Port: 63516
▼ Domain Name System (response)
  Transaction ID: 0xcd44
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.ietf.org: type A, class IN
  ▼ Answers
    ▶ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
    ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    [Request In: 20]
    [Time: 0.054719000 seconds]
```

3 відповіді.

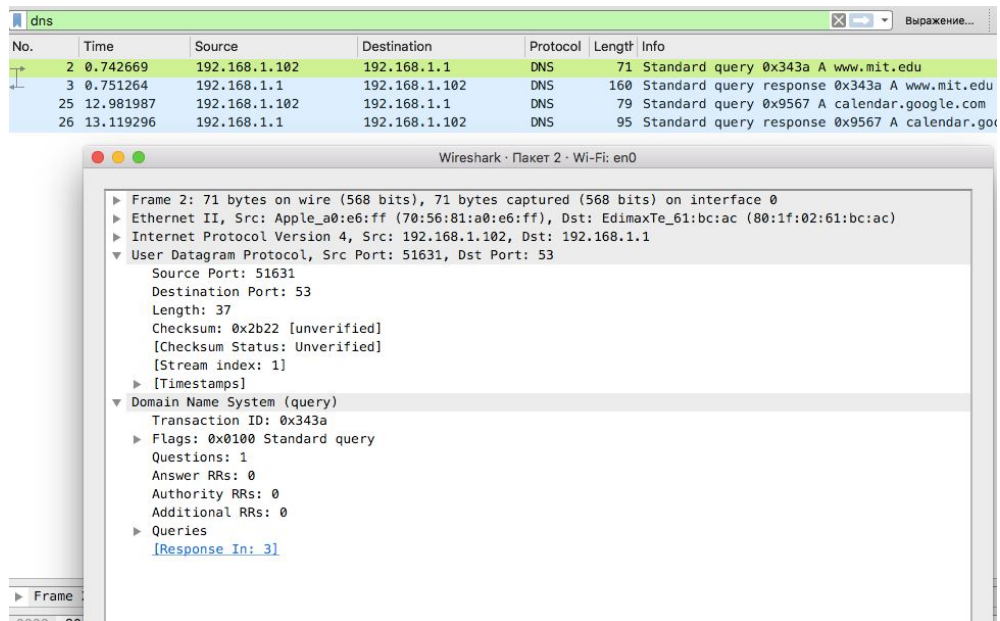
5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з однією із відповідей сервера DNS?

Так, співпадає.

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

Так виконує.

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



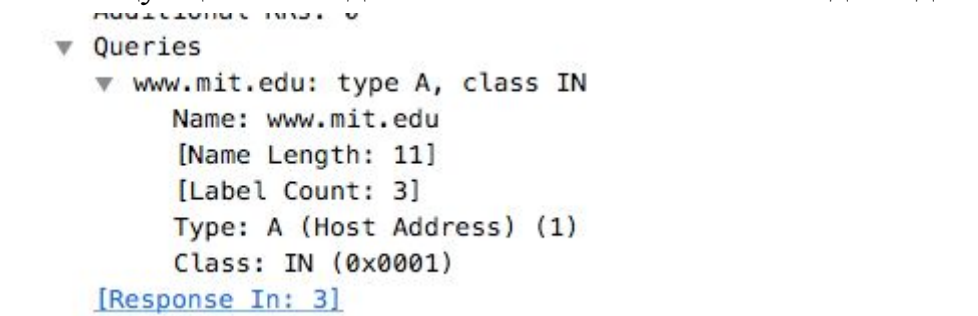
Цільовий: 53

Вихідний: 51631

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

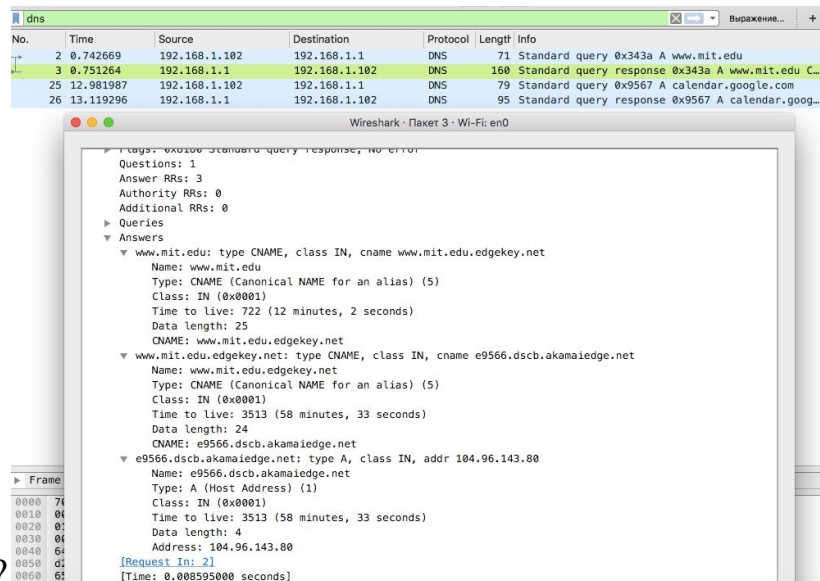
192.168.1.1. Так, є адресою локального сервера.

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



Тип запиту - A. Вміщує.

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



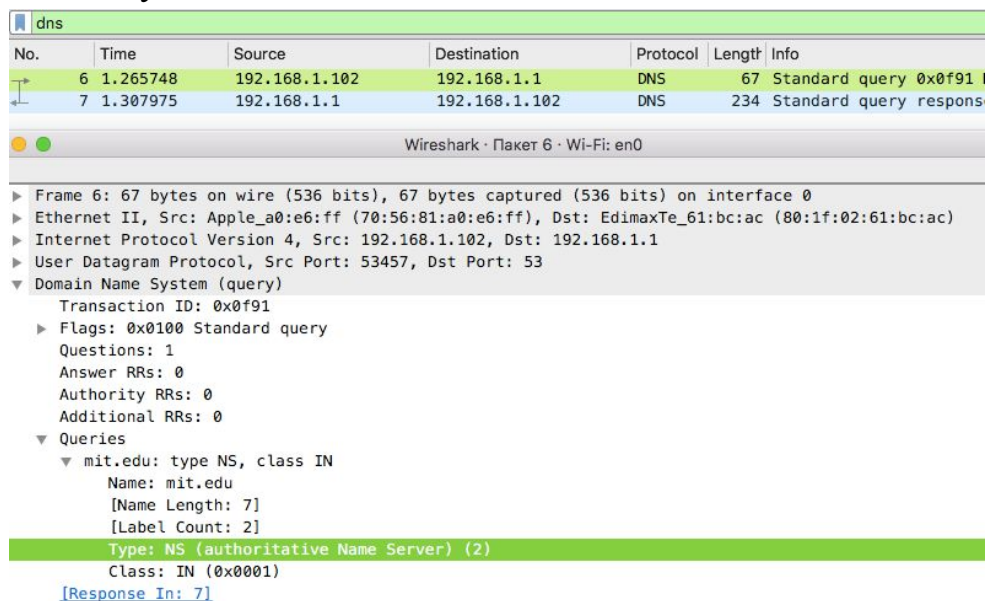
цих відповідей?

відповіді.

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

IP: 192.168.1.1. Так є.

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

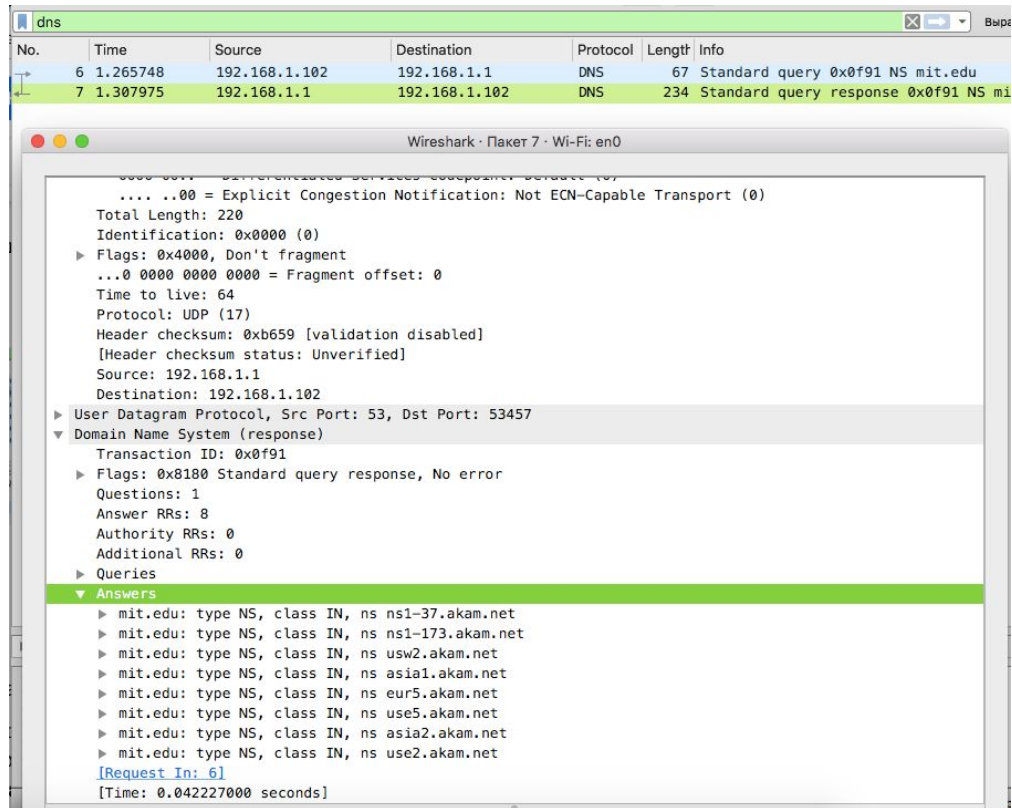


Тип запиту - NS. Так вміщує.

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

- 3

доменного імені, адреси IP або й того й іншого?



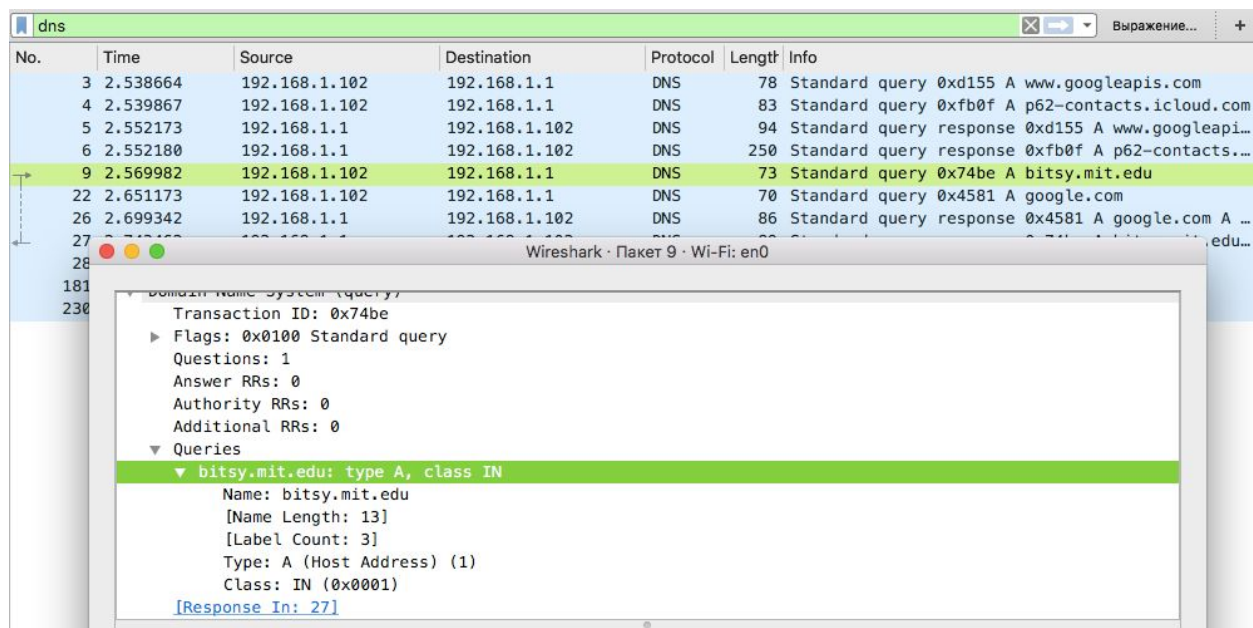
8 записів із відповіддю.

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?

No.	Time	Source	Destination	Protocol	Length	Info
3	2.538664	192.168.1.102	192.168.1.1	DNS	78	Standard query 0xd155 A www.googleap
4	2.539867	192.168.1.102	192.168.1.1	DNS	83	Standard query 0xfb0f A p62-contacts
5	2.552173	192.168.1.1	192.168.1.102	DNS	94	Standard query response 0xd155 A www
6	2.552180	192.168.1.1	192.168.1.102	DNS	250	Standard query response 0xfb0f A p62
9	2.569982	192.168.1.102	192.168.1.1	DNS	73	Standard query 0x74be A bitsy.mit.ed
22	2.651173	192.168.1.102	192.168.1.1	DNS	70	Standard query 0x4581 A google.com
26	2.699342	192.168.1.1	192.168.1.102	DNS	86	Standard query response 0x4581 A goo
27	2.743462	192.168.1.1	192.168.1.102	DNS	89	Standard query response 0x74be A bit
28	2.746512	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.or.
181	7.748548	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.or.
230	12.753708	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.or.

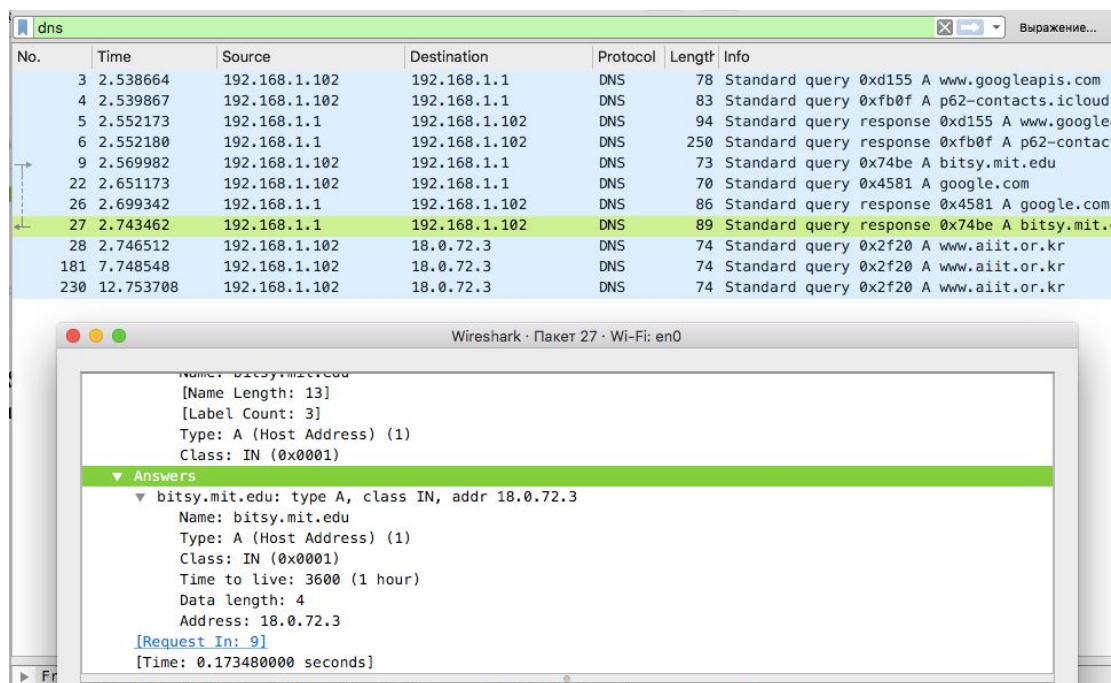
IP: 192.168.1.1. Є адресою локального сервера.

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



Тип запиту - А. Вміщує.

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



Була отримана одна відповідь.

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.