

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»**  
**КАФЕДРА ММСА**

**Лабораторна робота № 3**  
**З дисципліни: Комп'ютерні мережі**

***Протоколи DNS***

**Виконав:**  
**Студент III курсу**  
**Групи КА-74**  
**Кришевич С.С**  
**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.

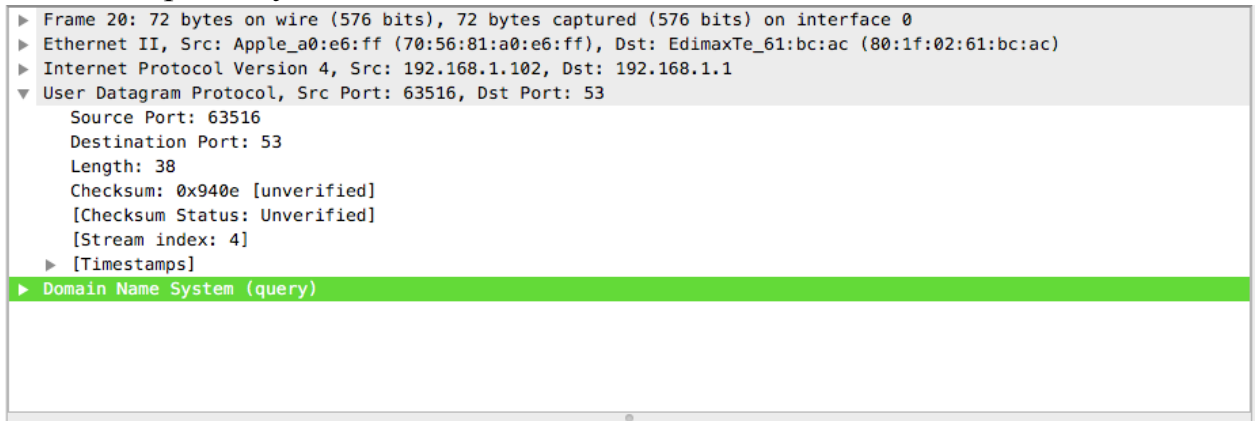
Authoritative answers can be found from:

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

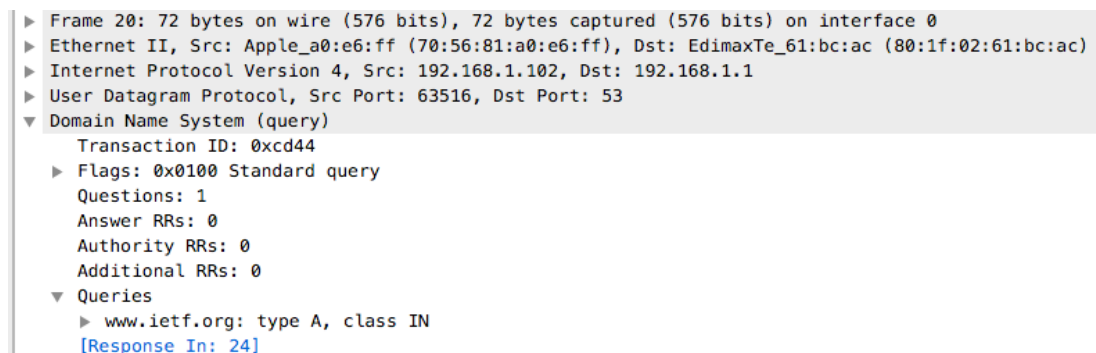
Вихідний порт: 63516

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?

The image shows two screenshots of Wireshark. The top screenshot is a packet list with the following data:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.742669	192.168.1.102	192.168.1.1	DNS	71	Standard query 0x343a A www.mit.edu
3	0.751264	192.168.1.1	192.168.1.102	DNS	160	Standard query response 0x343a A www.mit.edu
25	12.981987	192.168.1.102	192.168.1.1	DNS	79	Standard query 0x9567 A calendar.google.com
26	13.119296	192.168.1.1	192.168.1.102	DNS	95	Standard query response 0x9567 A calendar.google.com

The bottom screenshot shows the details of the selected packet (Frame 2), which is a DNS query. The details are as follows:

- Frame 2: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
- Ethernet II, Src: Apple\_a0:e6:ff (70:56:81:a0:e6:ff), Dst: EdimaxTe\_61:bc:ac (80:1f:02:61:bc:ac)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 51631, Dst Port: 53
  - Source Port: 51631
  - Destination Port: 53
  - Length: 37
  - Checksum: 0x2b22 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 1]
  - [Timestamps]
- Domain Name System (query)
  - Transaction ID: 0x343a
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - [Response In: 3]

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»?

```
▼ Queries
  ▼ www.mit.edu: type A, class IN
    Name: www.mit.edu
    [Name Length: 11]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 3]
```

Тип запиту - А. Вміщує.

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

The image shows a Wireshark packet capture of DNS traffic. The packet list pane shows four packets: a query for www.mit.edu (No. 2), a response for www.mit.edu (No. 3), a query for calendar.google.com (No. 25), and a response for calendar.google.com (No. 26). The packet details pane for packet 3 shows the response structure: Questions: 1, Answer RRs: 3, Authority RRs: 0, Additional RRs: 0. The Answers section shows three records: 1. www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net. 2. www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net. 3. e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.143.80.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.742669	192.168.1.102	192.168.1.1	DNS	71	Standard query 0x343a A www.mit.edu
3	0.751264	192.168.1.1	192.168.1.102	DNS	160	Standard query response 0x343a A www.mit.edu C...
25	12.981987	192.168.1.102	192.168.1.1	DNS	79	Standard query 0x9567 A calendar.google.com
26	13.119296	192.168.1.1	192.168.1.102	DNS	95	Standard query response 0x9567 A calendar.goog...

Wireshark - Пакет 3 - Wi-Fi: en0

Packet 3 Details:

- Questions: 1
- Answer RRs: 3
- Authority RRs: 0
- Additional RRs: 0
- ▼ Queries
- ▼ Answers
  - www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    - Name: www.mit.edu
    - Type: CNAME (Canonical NAME for an alias) (5)
    - Class: IN (0x0001)
    - Time to Live: 722 (12 minutes, 2 seconds)
    - Data length: 25
    - CNAME: www.mit.edu.edgekey.net
  - www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    - Name: www.mit.edu.edgekey.net
    - Type: CNAME (Canonical NAME for an alias) (5)
    - Class: IN (0x0001)
    - Time to Live: 3513 (58 minutes, 33 seconds)
    - Data length: 24
    - CNAME: e9566.dscb.akamaiedge.net
  - e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.143.80
    - Name: e9566.dscb.akamaiedge.net
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to Live: 3513 (58 minutes, 33 seconds)
    - Data length: 4
    - Address: 104.96.143.80

[Request In: 2]  
[Time: 0.008595000 seconds]

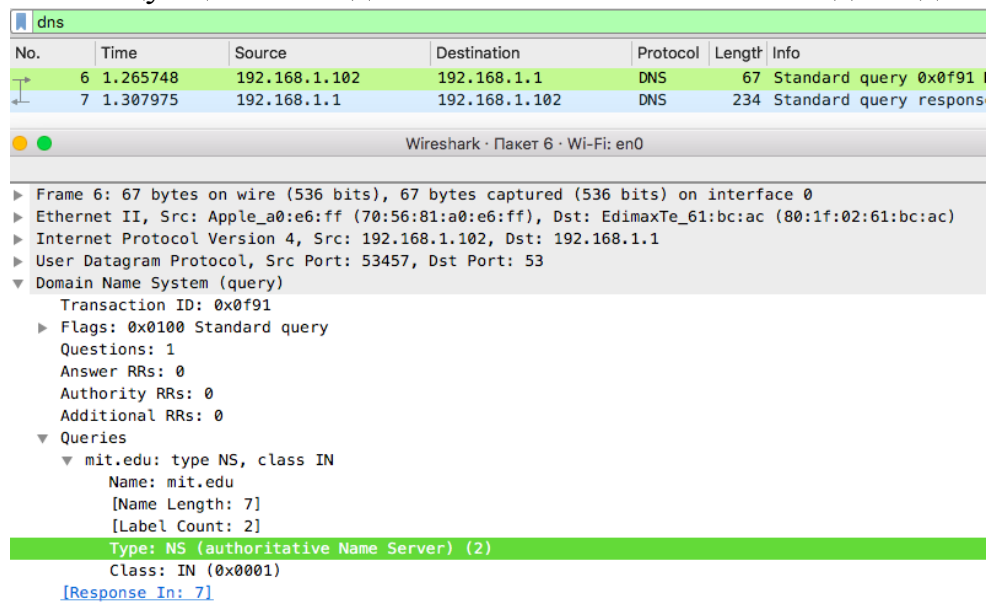
цих відповідей?

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»?



The image shows a Wireshark packet capture of a DNS query. The packet list at the top shows two packets: packet 6 is a DNS standard query from 192.168.1.102 to 192.168.1.1, and packet 7 is the corresponding response. The packet details pane for packet 6 is expanded, showing the Domain Name System (query) section. The transaction ID is 0xf91. The flags indicate a standard query. The query section shows a single query for mit.edu, type NS, class IN. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
6	1.265748	192.168.1.102	192.168.1.1	DNS	67	Standard query 0xf91
7	1.307975	192.168.1.1	192.168.1.102	DNS	234	Standard query response

Wireshark · Пакет 6 · Wi-Fi: en0

Frame 6: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0

Ethernet II, Src: Apple\_a0:e6:ff (70:56:81:a0:e6:ff), Dst: EdimaxTe\_61:bc:ac (80:1f:02:61:bc:ac)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 53457, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xf91

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

mit.edu: type NS, class IN

Name: mit.edu

[Name Length: 7]

[Label Count: 2]

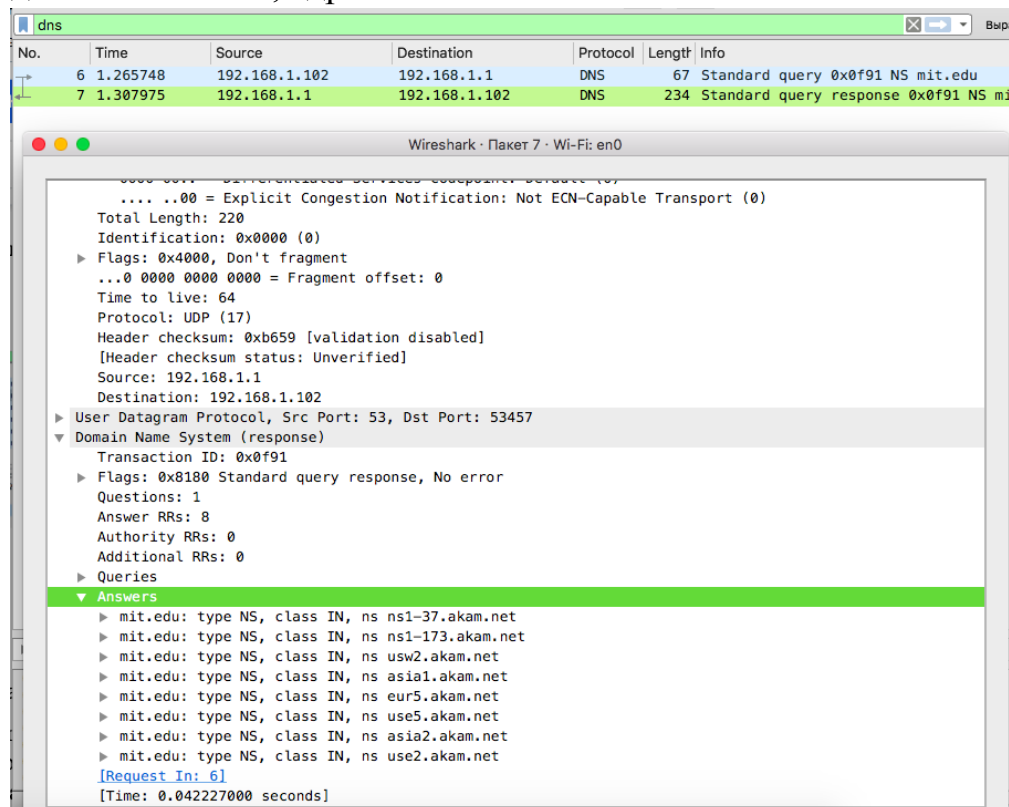
Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

[Response In: 7]

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 доменного імені, адреси IP або й того й іншого?



The image shows a Wireshark packet capture of a DNS response. The packet list at the top shows two packets: packet 6 is a DNS standard query from 192.168.1.102 to 192.168.1.1, and packet 7 is the corresponding response. The packet details pane for packet 7 is expanded, showing the Domain Name System (response) section. The transaction ID is 0xf91. The flags indicate a standard query response with no error. The response section shows 8 answer records for mit.edu, type NS, class IN. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
6	1.265748	192.168.1.102	192.168.1.1	DNS	67	Standard query 0xf91 NS mit.edu
7	1.307975	192.168.1.1	192.168.1.102	DNS	234	Standard query response 0xf91 NS mi

Wireshark · Пакет 7 · Wi-Fi: en0

.... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 220

Identification: 0x0000 (0)

Flags: 0x4000, Don't fragment

... 0 0000 0000 0000 = Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0xb659 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.1

Destination: 192.168.1.102

User Datagram Protocol, Src Port: 53, Dst Port: 53457

Domain Name System (response)

Transaction ID: 0xf91

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 0

Queries

Answers

mit.edu: type NS, class IN, ns ns1-37.akam.net

mit.edu: type NS, class IN, ns ns1-173.akam.net

mit.edu: type NS, class IN, ns usw2.akam.net

mit.edu: type NS, class IN, ns asia1.akam.net

mit.edu: type NS, class IN, ns eur5.akam.net

mit.edu: type NS, class IN, ns use5.akam.net

mit.edu: type NS, class IN, ns asia2.akam.net

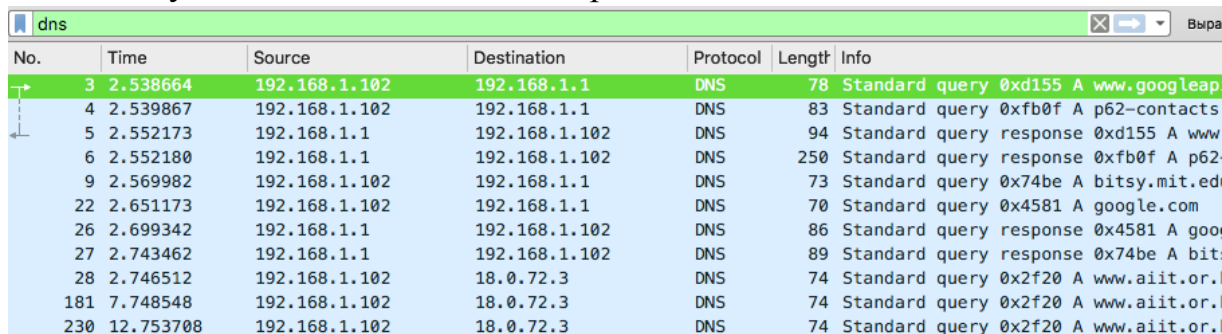
mit.edu: type NS, class IN, ns use2.akam.net

[Request In: 6]

[Time: 0.042227000 seconds]

8 записів із відповіддю.

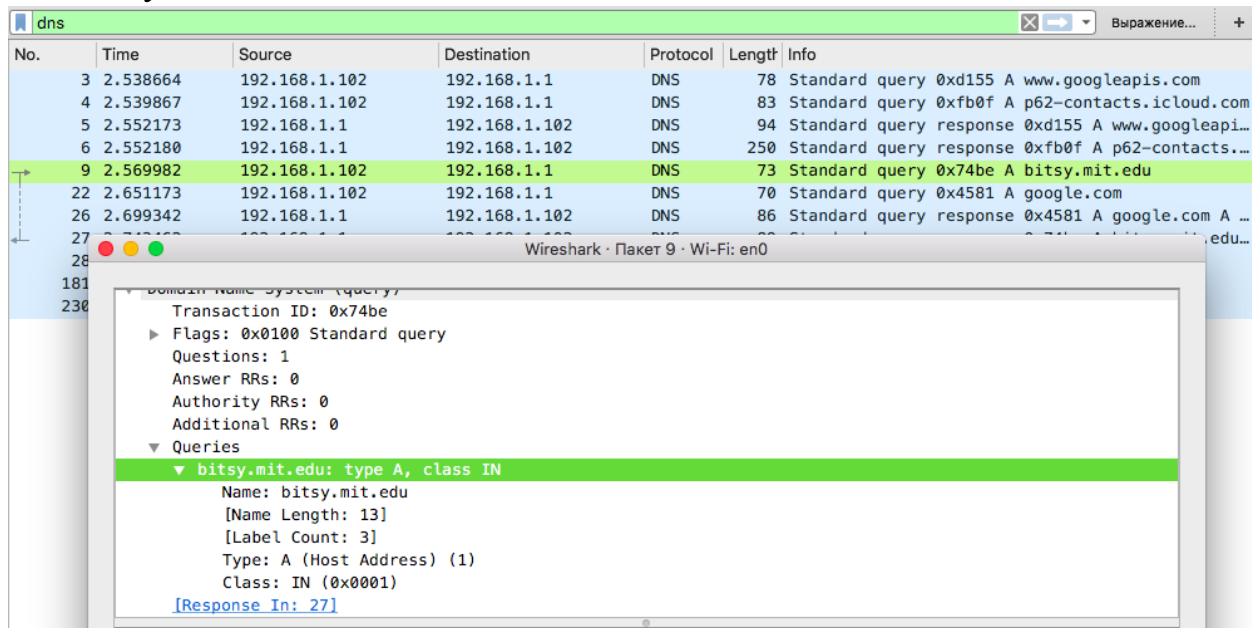
14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?



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.googleapis.com
4	2.539867	192.168.1.102	192.168.1.1	DNS	83	Standard query 0xfb0f A p62-contacts.icloud.com
5	2.552173	192.168.1.1	192.168.1.102	DNS	94	Standard query response 0xd155 A www.googleapis.com
6	2.552180	192.168.1.1	192.168.1.102	DNS	250	Standard query response 0xfb0f A p62-contacts.icloud.com
9	2.569982	192.168.1.102	192.168.1.1	DNS	73	Standard query 0x74be A bitsy.mit.edu
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 google.com
27	2.743462	192.168.1.1	192.168.1.102	DNS	89	Standard query response 0x74be A bitsy.mit.edu
28	2.746512	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.org
181	7.748548	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.org
230	12.753708	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.org

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»?



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.googleapis.com
4	2.539867	192.168.1.102	192.168.1.1	DNS	83	Standard query 0xfb0f A p62-contacts.icloud.com
5	2.552173	192.168.1.1	192.168.1.102	DNS	94	Standard query response 0xd155 A www.googleapis.com
6	2.552180	192.168.1.1	192.168.1.102	DNS	250	Standard query response 0xfb0f A p62-contacts.icloud.com
9	2.569982	192.168.1.102	192.168.1.1	DNS	73	Standard query 0x74be A bitsy.mit.edu
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 google.com
27	2.743462	192.168.1.1	192.168.1.102	DNS	89	Standard query response 0x74be A bitsy.mit.edu
28	2.746512	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.org
181	7.748548	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.org
230	12.753708	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.org

Transaction ID: 0x74be
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
bitsy.mit.edu: type A, class IN
Name: bitsy.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 27]

Тип запиту - А. Вміщує.

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

цих відповідей?

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.googleapis.com
4	2.539867	192.168.1.102	192.168.1.1	DNS	83	Standard query 0xfb0f A p62-contacts.icloud
5	2.552173	192.168.1.1	192.168.1.102	DNS	94	Standard query response 0xd155 A www.google
6	2.552180	192.168.1.1	192.168.1.102	DNS	250	Standard query response 0xfb0f A p62-contac
9	2.569982	192.168.1.102	192.168.1.1	DNS	73	Standard query 0x74be A bitsy.mit.edu
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 google.com
27	2.743462	192.168.1.1	192.168.1.102	DNS	89	Standard query response 0x74be A bitsy.mit.
28	2.746512	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.or.kr
181	7.748548	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.or.kr
230	12.753708	192.168.1.102	18.0.72.3	DNS	74	Standard query 0x2f20 A www.aiit.or.kr

Wireshark · Пакет 27 · Wi-Fi: en0	
[Name Length: 13] [Label Count: 3] Type: A (Host Address) (1) Class: IN (0x0001)	
▼ Answers	
bitsy.mit.edu: type A, class IN, addr 18.0.72.3	
Name: bitsy.mit.edu	
Type: A (Host Address) (1)	
Class: IN (0x0001)	
Time to live: 3600 (1 hour)	
Data length: 4	
Address: 18.0.72.3	
<a href="#">[Request In: 9]</a>	
[Time: 0.173480000 seconds]	

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.