

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

Лабораторна робота № 3
З дисципліни: Комп'ютерні мережі

Протокол DNS

Виконав:
Студент III курсу
Групи КА-72
Третьяков М.Ю.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

Перша частина

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The packet list pane displays a list of captured packets, with the selected packet (No. 9) highlighted. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw hex and ASCII data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
9	4.530186	192.168.0.103	8.8.8.8	DNS	72	Standard query 0xaa70 A www.ietf.org
12	4.568603	8.8.8.8	192.168.0.103	DNS	149	Standard query response 0xaa70 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85
1266	5.686109	192.168.0.103	8.8.8.8	DNS	78	Standard query 0x2611 A analytics.ietf.org
1444	5.747590	8.8.8.8	192.168.0.103	DNS	108	Standard query response 0x2611 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1528	9.209647	192.168.0.103	8.8.8.8	DNS	75	Standard query 0xf55e A ssl.gstatic.com
1529	9.232360	8.8.8.8	192.168.0.103	DNS	91	Standard query response 0xf55e A ssl.gstatic.com A 172.217.20.163

Frame 9: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6A04B65AB4DF}, id 0
Ethernet II, Src: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac), Dst: Tp-LinkT_72:eb:50 (18:d6:c7:72:eb:50)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 41838, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xaa70
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
0000 18 d6 c7 72 eb 50 70 f1 a1 e9 5f ac 08 00 45 00E
0010 00 3a 67 0f 00 00 00 11 02 85 c0 a8 00 67 08 08g
0020 08 08 a3 6e 00 35 00 26 be 29 aa 70 01 00 00 01n-5&)p
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03w ww.ietf
0040 6f 72 67 00 00 01 00 01org

Request:

No.	Time	Source	Destination	Protocol	Length	Info
532	2.594504	192.168.0.102	192.168.0.1	DNS	78	Standard query 0xd07e A analytics.ietf.org

Frame 532: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0
Ethernet II, Src: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd), Dst: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 52699, Dst Port: 53
Source Port: 52699
Destination Port: 53
Length: 44
Checksum: 0x7bdf [unverified]
[Checksum Status: Unverified]
[Stream index: 7]
[Timestamps]
Domain Name System (query)
Transaction ID: 0xd07e
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 533]

Response:

No.	Time	Source	Destination	Protocol	Length	Info
533	2.596023	192.168.0.1	192.168.0.102	DNS	94	Standard query response 0xd07e A analytics.ietf.org

A 4.31.198.44
Frame 533: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0
Ethernet II, Src: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8), Dst: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102
User Datagram Protocol, Src Port: 53, Dst Port: 52699
 Source Port: 53
 Destination Port: 52699
 Length: 60
 Checksum: 0x6cdf [unverified]
 [Checksum Status: Unverified]
 [Stream index: 7]
 [Timestamps]
Domain Name System (response)
 Transaction ID: 0xd07e
 Flags: 0x8580 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 Queries
 Answers
 [Request In: 532]
 [Time: 0.001519000 seconds]

Друга частина

```
C:\Users\Maks>nslookup www.mit.edu
ПхЕтхЕ:  UnKnown
Address:  192.168.0.1

Не заслуживающий доверия ответ:
Ль :      e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:132:382::255e
           2a02:26f0:132:3a6::255e
           23.61.218.91
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

*Беспроводная сеть						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
dns						
No.	Time	Source	Destination	Protocol	Length	Info
727	4.955122	192.168.0.102	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
731	4.983906	192.168.0.1	192.168.0.102	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
733	4.993328	192.168.0.102	192.168.0.1	DNS	89	Standard query 0x0002 A www.mit.edu.www.tendawifi.com
736	5.016652	192.168.0.1	192.168.0.102	DNS	89	Standard query response 0x0002 No such name A www.mit.edu.www.tendawifi.com
737	5.017610	192.168.0.102	192.168.0.1	DNS	89	Standard query 0x0003 AAAA www.mit.edu.www.tendawifi.com
738	5.020961	192.168.0.1	192.168.0.102	DNS	89	Standard query response 0x0003 No such name AAAA www.mit.edu.www.tendawifi.com
740	5.021832	192.168.0.102	192.168.0.1	DNS	85	Standard query 0x0004 A www.mit.edu.tendawifi.com
745	5.051068	192.168.0.1	192.168.0.102	DNS	85	Standard query response 0x0004 No such name A www.mit.edu.tendawifi.com
746	5.051839	192.168.0.102	192.168.0.1	DNS	85	Standard query 0x0005 AAAA www.mit.edu.tendawifi.com
747	5.054478	192.168.0.1	192.168.0.102	DNS	85	Standard query response 0x0005 No such name AAAA www.mit.edu.tendawifi.com
748	5.055238	192.168.0.102	192.168.0.1	DNS	71	Standard query 0x0006 A www.mit.edu
784	5.289720	192.168.0.1	192.168.0.102	DNS	160	Standard query response 0x0006 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.61.218.91
787	5.301968	192.168.0.102	192.168.0.1	DNS	71	Standard query 0x0007 AAAA www.mit.edu
794	5.365761	192.168.0.1	192.168.0.102	DNS	232	Standard query response 0x0007 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:132:382...

Request:

```

No.      Time      Source      Destination      Protocol Length Info
 737 5.017610    192.168.0.102    192.168.0.1      DNS           89      Standard query 0x0003 AAAA www.mit.edu.www.tendawifi.com
Frame 737: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0
Ethernet II, Src: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd), Dst: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 58696, Dst Port: 53
  Source Port: 58696
  Destination Port: 53
  Length: 55
  Checksum: 0x8bc6 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  [Timestamps]
Domain Name System (query)
  Transaction ID: 0x0003
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
  [Response In: 738]
```

Response:

No.	Time	Source	Destination	Protocol	Length	Info
738	5.020961	192.168.0.1	192.168.0.102	DNS	89	Standard query response 0x0003 No such name

AAAA www.mit.edu.www.tendawifi.com

Frame 738: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0

Ethernet II, Src: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8), Dst: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102

User Datagram Protocol, Src Port: 53, Dst Port: 58696

Source Port: 53

Destination Port: 58696

Length: 55

Checksum: 0x0b43 [unverified]

[Checksum Status: Unverified]

[Stream index: 3]

[Timestamps]

Domain Name System (response)

Transaction ID: 0x0003

Flags: 0x8183 Standard query response, No such name

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Request In: 737]

[Time: 0.003351000 seconds]

Третья часть

```
C:\Users\Maks>nslookup -type=NS mit.edu
DNS request timed out.
    timeout was 2 seconds.
*~xËTxË: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net

mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net
```

Wireshark - Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
905	5.374798	192.168.0.102	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
906	5.377946	192.168.0.1	192.168.0.102	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
908	5.384007	192.168.0.102	192.168.0.1	DNS	85	Standard query 0x0002 NS mit.edu.www.tendawifi.com
920	5.415147	192.168.0.1	192.168.0.102	DNS	85	Standard query response 0x0002 No such name NS mit.edu.www.tendawifi.com
921	5.415450	192.168.0.102	192.168.0.1	DNS	81	Standard query 0x0003 NS mit.edu.tendawifi.com
947	5.485994	192.168.0.1	192.168.0.102	DNS	81	Standard query response 0x0003 No such name NS mit.edu.tendawifi.com
948	5.486956	192.168.0.102	192.168.0.1	DNS	67	Standard query 0x0004 NS mit.edu
949	5.491724	192.168.0.1	192.168.0.102	DNS	346	Standard query response 0x0004 NS mit.edu NS ns1-37.akam.net NS asia2.akam.net NS ns1-173.akam.net NS use5.akam.net NS use2.akam.net

> Frame 905: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-AA49-49C317EF7C40}, id 0
 > Ethernet II, Src: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd), Dst: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8)
 > Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
 > User Datagram Protocol, Src Port: 52827, Dst Port: 53
 Source Port: 52827
 Destination Port: 53
 Length: 50
 Checksum: 0x22c6 [unverified]
 [Checksum Status: Unverified]

0000 04 95 e6 00 c4 e8 cc b0 da 0e 89 dd 08 00 45 00E.
 0010 00 46 64 cf 00 00 80 11 54 20 c0 a8 00 66 c0 a8 ..Fd....T...f..
 0020 00 01 ce 5b 00 35 00 32 22 c6 00 01 01 00 00 01 ...[-5-2".....
 0030 00 00 00 00 00 01 31 01 30 03 31 36 38 03 311 0.168.1
 0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92-in-addr-arpa-
 0050 00 0c 00 01

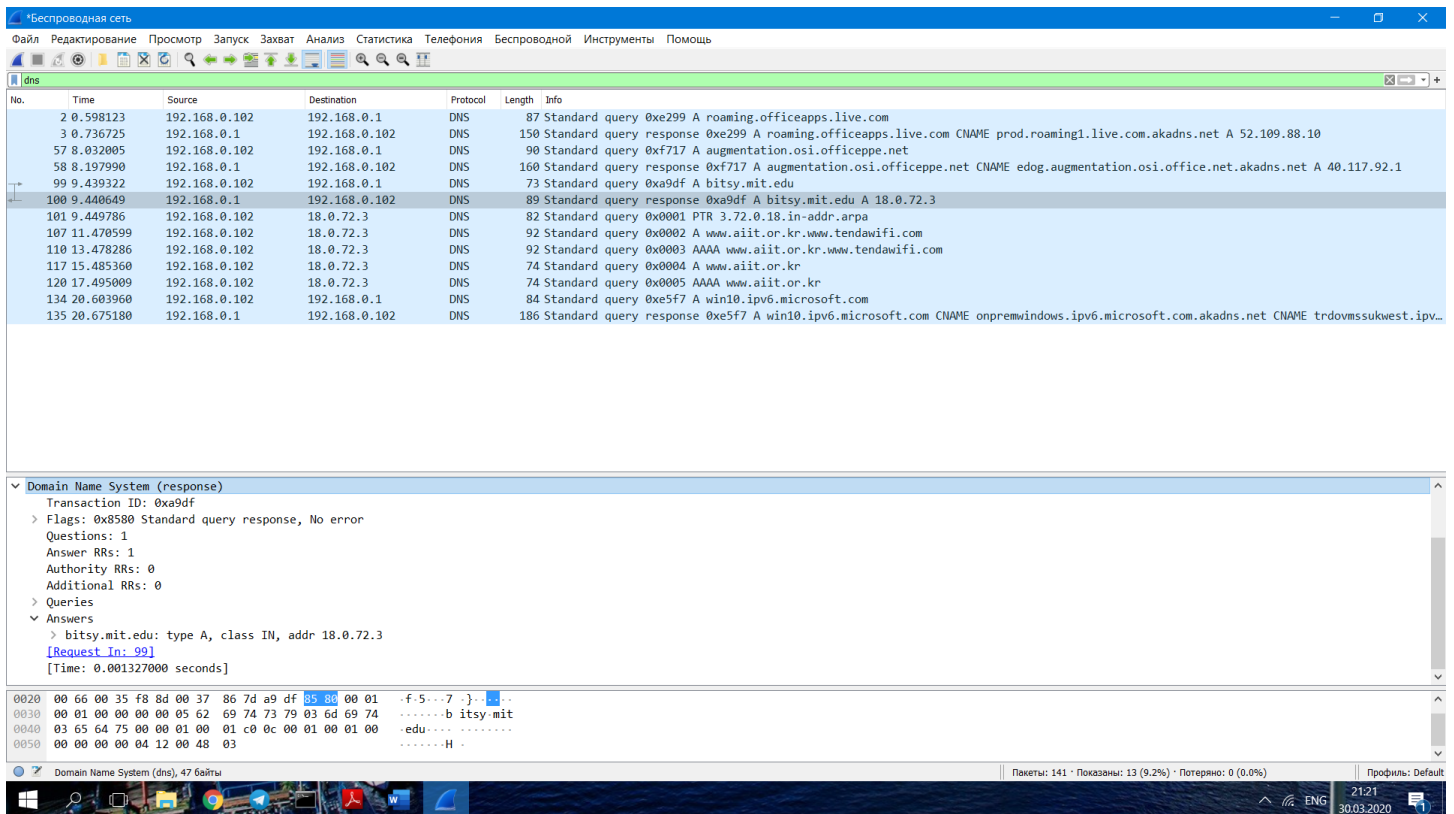
Wireshark - Беспроводная сеть_20200330202113_804968.pcapng | Пакеты: 1466 - Показаны: 8 (0.5%) | Профиль: Default

2025 30.03.2020

Четверта часть

```
C:\Users\Maks>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
*~xÈtxÈ: UnKnown
Address: 18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Превышено время ожидания запроса UnKnown
```



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?

Вони використовують протокол UDP. Порт 53.

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

192.168.0.1. Так.

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

Тип А.

3 відповіді

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

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

Три відповіді. Містять name, type, class, ttl, data length, answer (cname або addr).

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.

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

Так.

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

Порт 53

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

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

PTR, A, AAAA.

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

Чотири відповіді. Містять name, type, class, ttl, data length, answer (cname або addr).

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

1. 104.74.143.40. Ні.

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

PTR, A, AAAA

Типу NS. Всі компоненти блоку Queries

13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді?

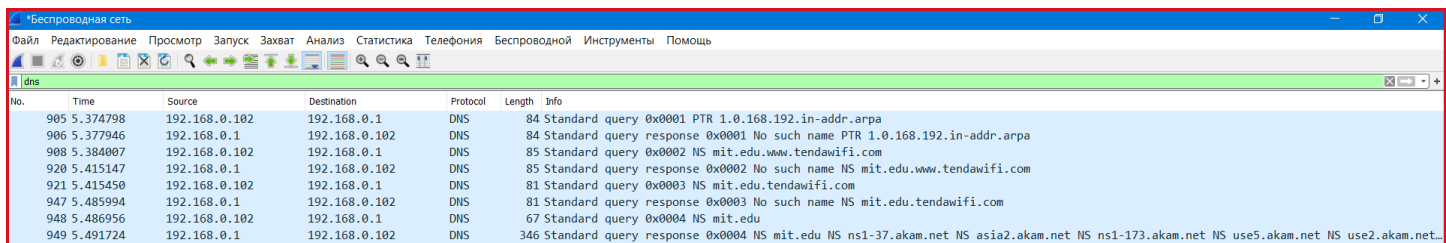
Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

Назви серверів видно на скріншоті. І те і інше, доменне ім'я у відповідях, а адреси IP у додаткових записах

```
C:\Users\Maks>nslookup -type=NS mit.edu
тхЁтхЁ: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia1.akam.net

mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-37.akam.net
```



No.	Time	Source	Destination	Protocol	Length	Info
905	5.374798	192.168.0.102	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
906	5.377946	192.168.0.1	192.168.0.102	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
908	5.384007	192.168.0.102	192.168.0.1	DNS	85	Standard query 0x0002 NS mit.edu.www.tendawifi.com
920	5.415147	192.168.0.1	192.168.0.102	DNS	85	Standard query response 0x0002 No such name NS mit.edu.www.tendawifi.com
921	5.415450	192.168.0.102	192.168.0.1	DNS	81	Standard query 0x0003 NS mit.edu.tendawifi.com
947	5.485994	192.168.0.1	192.168.0.102	DNS	81	Standard query response 0x0003 No such name NS mit.edu.tendawifi.com
948	5.486956	192.168.0.102	192.168.0.1	DNS	67	Standard query 0x0004 NS mit.edu
949	5.491724	192.168.0.1	192.168.0.102	DNS	346	Standard query response 0x0004 NS mit.edu NS ns1-37.akam.net NS asia2.akam.net NS ns1-173.akam.net NS use5.akam.net NS use2.akam.net

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?

18.0.72.3. Ні, вона відповідає bitsy.mit.edu

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

Типу «А». Всі компоненти блоку Queries.

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

Склад видно у скріншоті нижче.

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення та аналізу пакетів. Було розглянуто інформацію, що містить в собі протокол DNS.