

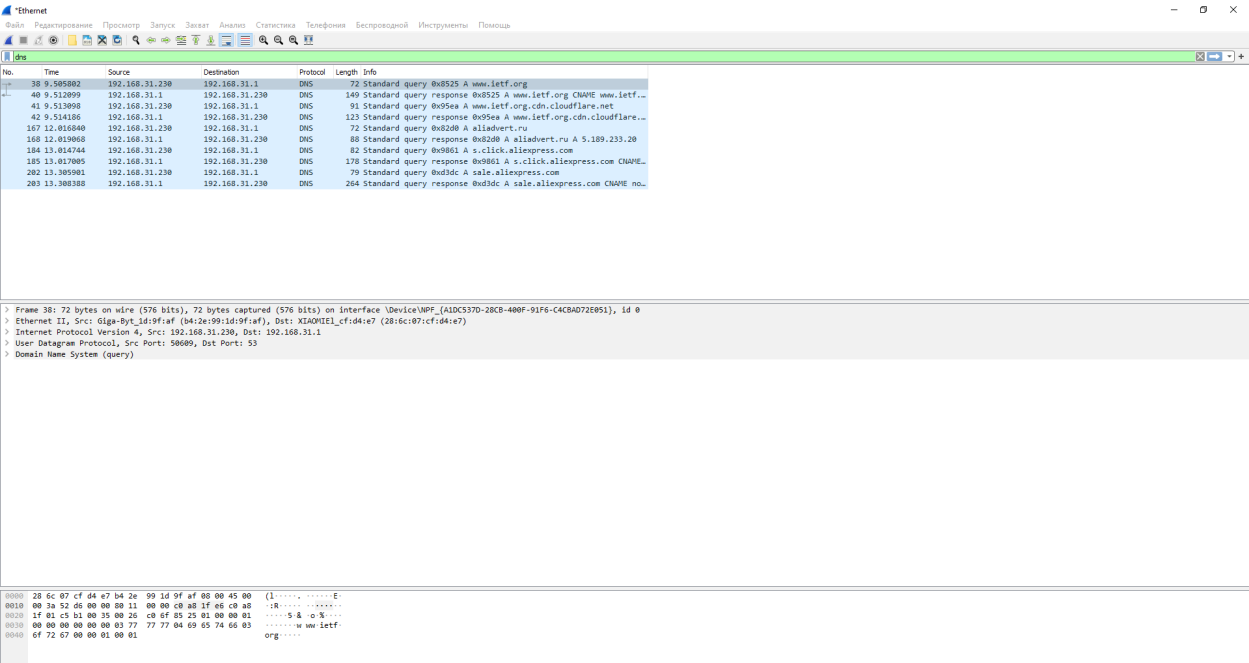
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
“ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ”
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №3
з дисципліни “Комп'ютерні мережі”

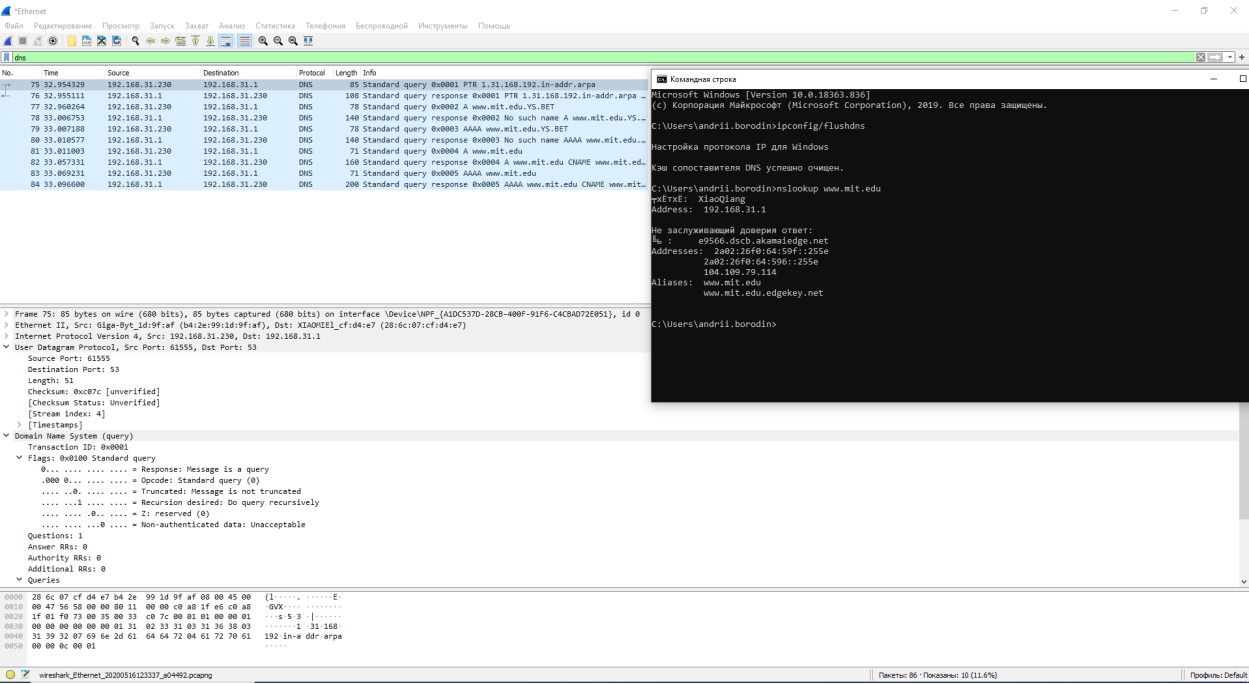
Виконав:
Студент групи ІС-зп92
Бородін А.А.
Перевірив:
Кухарєв С.О.

Київ – 2020

Перше захоплення пакетів



Друге захоплення пакетів



Трете захоплення пакетів

Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
75	32.954329	192.168.31.230	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
76	32.955111	192.168.31.1	192.168.31.230	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa
77	32.960264	192.168.31.230	192.168.31.1	DNS	78	Standard query 0x0002 A www.mit.edu.YS.BET
78	33.006753	192.168.31.1	192.168.31.230	DNS	140	Standard query response 0x0002 No such name A www.mit.edu.YS...
79	33.007168	192.168.31.230	192.168.31.1	DNS	78	Standard query 0x0003 AAAA www.mit.edu.YS.BET
80	33.010577	192.168.31.1	192.168.31.230	DNS	140	Standard query response 0x0003 No such name AAAA www.mit.edu...
81	33.011003	192.168.31.230	192.168.31.1	DNS	71	Standard query 0x0004 A www.mit.edu
82	33.057331	192.168.31.1	192.168.31.230	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.ed...
83	33.069231	192.168.31.230	192.168.31.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
84	33.096600	192.168.31.1	192.168.31.230	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit...

.....0.. = Z: reserved (0)
..... ..0. = Answer authenticated: Answer/authority portion was not authenticated by the server
..... ...0 = Non-authenticated data: Unacceptable
.....0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
 ▼ 1.31.168.192.in-addr.arpa: type PTR, class IN
 Name: 1.31.168.192.in-addr.arpa
 [Name Length: 25]
 [Label Count: 6]
 Type: PTR (domain name PointTeR) (12)
 Class: IN (0x0001)
 ▼ Answers
 ▼ 1.31.168.192.in-addr.arpa: type PTR, class IN, XiaoQiang
 Name: 1.31.168.192.in-addr.arpa
 Type: PTR (domain name PointTeR) (12)
 Class: IN (0x0001)
 Time to live: 0 (0 seconds)
 Data length: 11
 Domain Name: XiaoQiang
 [Request In: 75]
 [Time: 0.000782000 seconds]

Четверте захоплення пакетів

Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
67	33.701300	192.168.31.230	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
68	33.702032	192.168.31.1	192.168.31.230	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa
69	33.705026	192.168.31.230	192.168.31.1	DNS	81	Standard query 0x0002 A www.sit.or.kr.YS.BET
70	33.710807	192.168.31.1	192.168.31.230	DNS	143	Standard query response 0x0002 No such name A www.sit.or.kr...
71	33.718327	192.168.31.230	192.168.31.1	DNS	81	Standard query 0x0003 AAAA www.sit.or.kr.YS.BET
72	33.721432	192.168.31.1	192.168.31.230	DNS	143	Standard query response 0x0003 No such name AAAA www.sit.or...
73	33.721710	192.168.31.230	192.168.31.1	DNS	74	Standard query 0x0004 A www.sit.or.kr
86	34.354051	192.168.31.1	192.168.31.230	DNS	90	Standard query response 0x0004 A www.sit.or.kr A 58.229.6.225
87	34.365648	192.168.31.230	192.168.31.1	DNS	74	Standard query 0x0005 AAAA www.sit.or.kr
101	35.818474	192.168.31.1	192.168.31.230	DNS	128	Standard query response 0x0005 AAAA www.sit.or.kr SOA ns9.dn...
112	37.674660	192.168.31.230	192.168.31.1	DNS	72	Standard query 0x1e05 A aliadvert.ru
113	37.676337	192.168.31.1	192.168.31.230	DNS	88	Standard query response 0x1e05 A aliadvert.ru A 5.189.233.20
136	38.679354	192.168.31.230	192.168.31.1	DNS	82	Standard query 0xc09d A s.click.aliexpress.com
137	38.681224	192.168.31.1	192.168.31.230	DNS	178	Standard query response 0xc09d A s.click.aliexpress.com CNAME...
154	38.935640	192.168.31.230	192.168.31.1	DNS	79	Standard query 0xfc0a A sale.aliexpress.com
155	38.938522	192.168.31.1	192.168.31.230	DNS	264	Standard query response 0xfc0a A sale.aliexpress.com CNAME no...

> Frame 67: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{A1DC3370-28CB-400F-91F6-C4CBAD72E951}, Id 0
> Ethernet II, Src: Giga-Byt_i619f:af (04:1a:99:16:9f:af), Dst: XiaoQiang_cf:d4:e7 (28:6c:07:cf:d4:e7)
> Internet Protocol Version 4, Src: 192.168.31.230, Dst: 192.168.31.1
> User Datagram Protocol, Src Port: 49597, Dst Port: 53
 Source Port: 49597
 Destination Port: 53
 Length: 51
 Checksum: 0xc07c [unverified]
 [Checksum Status: Unverified]
 [Stream Index: 4]
 [Timestamps]
 ▼ Domain Name System (query)
 Transaction ID: 0x0001
 ▼ Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 = Truncated: Message is not truncated
 = Recursion desired: Do query recursively
 0.. = Z: reserved (0)
 0. = Non-authenticated data: Unacceptable
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 ▼ Queries
 ▼ 1.31.168.192.in-addr.arpa: type PTR, class IN
 Name: 1.31.168.192.in-addr.arpa
 [Name Length: 25]

0000 28 6c 07 cf d4 e7 b4 2e 99 1d 9f af 00 00 45 00 (1.....E
0010 00 47 56 9e 00 00 00 11 00 00 c0 a8 1f 65 c0 a8 0v.....
0020 1f 01 c1 bd 00 35 00 33 c0 7c 00 01 01 00 00 015 3 |.....
0030 00 00 00 00 00 00 01 31 02 33 31 03 31 36 38 031 31 168
0040 31 39 32 07 09 6e 2d 61 64 64 72 04 61 72 70 61 192 in-a-addr-arpa
0050 00 00 0c 00 01
wireshark_Ethernet_20200516124757_815448.pcapng

Пакеты: 183 | Показаны: 16 (8.7%)

Профиль: Default

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?

Запит UDP, відповідь UDP, номер вихідного порта відповіді DNS: 53

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

192.168.31.1 Так, це адреса локального сервера DNS

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

Так вміщує

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Packets, Analysis, Statistics, Telephone, Wireless, Instruments, and Help. The packet list pane shows a list of captured packets, with the selected packet being a DNS query from 192.168.31.1 to 192.168.31.230. The packet details pane shows the structure of the DNS message, including the query for www.ietf.org and the answer section with CNAME and A records.

No.	Time	Source	Destination	Protocol	Length	Info
40	9.512099	192.168.31.1	192.168.31.230	DNS	149	Standard query response 0x8525 A www.ietf.org CNAME www.ietf...
42	9.514186	192.168.31.1	192.168.31.230	DNS	123	Standard query response 0x95ea A www.ietf.org.cdn.cloudflare...
168	12.019068	192.168.31.1	192.168.31.230	DNS	88	Standard query response 0x82d0 A aliadvert.ru A 5.189.233.20
185	13.017005	192.168.31.1	192.168.31.230	DNS	178	Standard query response 0x9861 A s.click.aliexpress.com CNAME...
203	13.308388	192.168.31.1	192.168.31.230	DNS	264	Standard query response 0xd3dc A sale.aliexpress.com CNAME no...
38	9.505802	192.168.31.230	192.168.31.1	DNS	72	Standard query 0x8525 A www.ietf.org
41	9.513098	192.168.31.230	192.168.31.1	DNS	91	Standard query 0x95ea A www.ietf.org.cdn.cloudflare.net
167	12.016840	192.168.31.230	192.168.31.1	DNS	72	Standard query 0x82d0 A aliadvert.ru
184	13.014744	192.168.31.230	192.168.31.1	DNS	82	Standard query 0x9861 A s.click.aliexpress.com
202	13.305901	192.168.31.230	192.168.31.1	DNS	79	Standard query 0xd3dc A sale.aliexpress.com

Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
Name: www.ietf.org
[Name Length: 12]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
Name: www.ietf.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 33
CNAME: www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.20.0.85
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.20.1.85
[Request In: 38]
[Time: 0.006297000 seconds]

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

Кількість відповідей — 3, відповіді вміщують: Name, Type, Class, Time to live, Data Length, CNAME, 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 виконує

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

цільовий порт повідомлення — 53

вихідний порт повідомлення — 61555

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

192.168.31.1

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

Так вміщує

Ethernet						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
dns						
No.	Time	Source	Destination	Protocol	Length	Info
75	32.954329	192.168.31.230	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
76	32.955111	192.168.31.1	192.168.31.230	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa
77	32.960264	192.168.31.230	192.168.31.1	DNS	78	Standard query 0x0002 A www.mit.edu.YS.BET
78	33.006753	192.168.31.1	192.168.31.230	DNS	140	Standard query response 0x0002 No such name A www.mit.edu.YS...
79	33.007188	192.168.31.230	192.168.31.1	DNS	78	Standard query 0x0003 AAAA www.mit.edu.YS.BET
80	33.010577	192.168.31.1	192.168.31.230	DNS	140	Standard query response 0x0003 No such name AAAA www.mit.edu...
81	33.011003	192.168.31.230	192.168.31.1	DNS	71	Standard query 0x0004 A www.mit.edu
82	33.057331	192.168.31.1	192.168.31.230	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.ed...
83	33.069231	192.168.31.230	192.168.31.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
84	33.096600	192.168.31.1	192.168.31.230	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit...


```

.....0.. = Z: reserved (0)
.....0.. = Answer authenticated: Answer/authority portion was not authenticated by the server
.....0.. = Non-authenticated data: Unacceptable
.....0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ 1.31.168.192.in-addr.arpa: type PTR, class IN
    Name: 1.31.168.192.in-addr.arpa
    [Name Length: 25]
    [Label Count: 6]
    Type: PTR (domain name PointeR) (12)
    Class: IN (0x0001)
  ▼ Answers
    ▼ 1.31.168.192.in-addr.arpa: type PTR, class IN, XiaoQiang
      Name: 1.31.168.192.in-addr.arpa
      Type: PTR (domain name PointeR) (12)
      Class: IN (0x0001)
      Time to live: 0 (0 seconds)
      Data length: 11
      Domain Name: XiaoQiang
      [Request In: 75]
      [Time: 0.000782000 seconds]

```

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

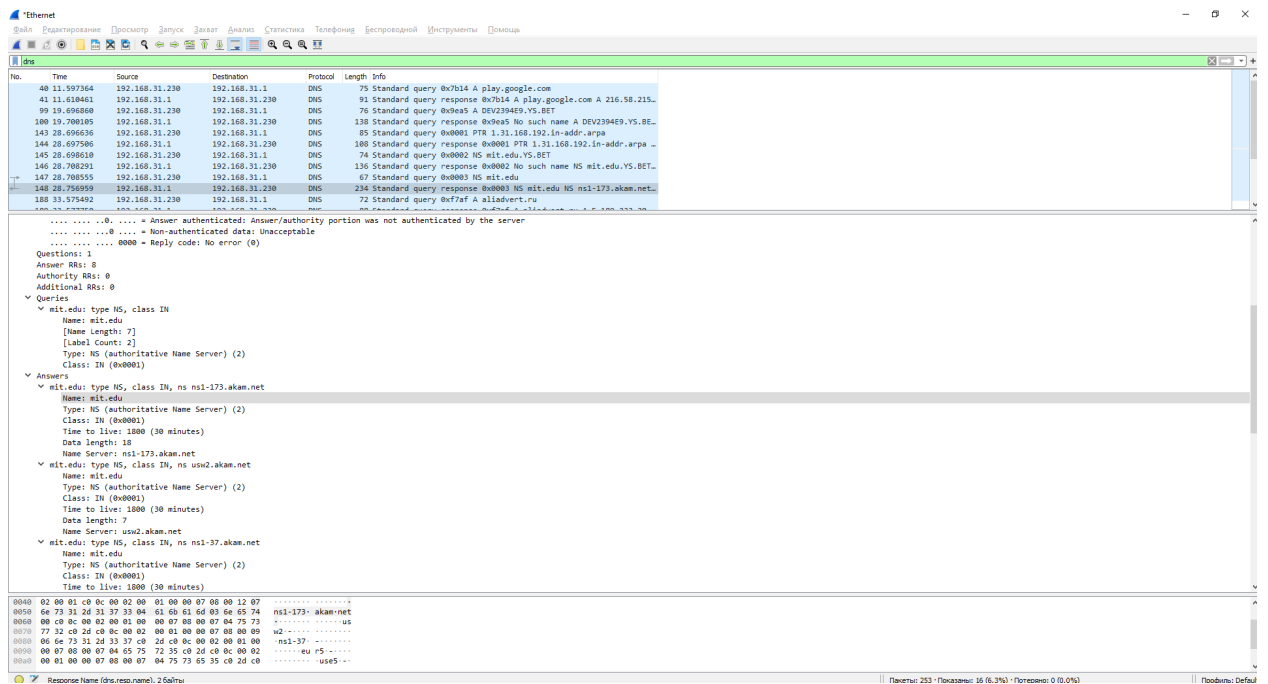
Один запис з відповіддю, складається з: Name, Type, Class, Time to live, Data length, Domain name

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

192.168.31.1 Так ця адреса є адресою локального сервера DNS за замовчанням

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

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?

Вісім записів з відповідями, сервери були запропоновані за допомогою доменного імені

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?

192.168.31.230, Ні, це одна з адрес локального середовища

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

Так вміщує, Name, Type, Class

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

8 відповідей складається з Name, Type, Class, Time to live, Data length, Domain name