

**«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КПІ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

**Лабораторна робота №3
з курсу «Комп'ютерні мережі»**

Виконав: студент 3 курсу

групи КА-77

Котів С.В.

Прийняв: Кухарєв С.О.

Київ 2020 р.

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
+	50 19.755140	192.168.1.106	192.168.1.1	DNS	72	Standard query 0x4075 A www.ietf.org
-	51 19.762342	192.168.1.1	192.168.1.106	DNS	149	Standard query response 0x4075 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85
	1125 21.375027	192.168.1.106	192.168.1.1	DNS	78	Standard query 0x1590 A analytics.ietf.org
	1259 21.708491	192.168.1.1	192.168.1.106	DNS	108	Standard query response 0x1590 A analytics.ietf.org CNAME ietf.org A 4.31.198.44

```
> Frame 50: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0
> Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 1025, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00 45 00  ....).L...Q..E
0010  00 3a 04 b9 00 00 80 11 b2 3e c0 a8 01 6a c0 a8  :.....>...j..
0020  01 01 04 01 00 35 00 26 14 f6 40 75 01 00 00 01  .....5&...@u...
0030  00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03  ....WWWwww.ietf
0040  6f 72 67 00 00 01 00 01      org.....
```

// Термінал:

Wireshark packet capture window showing DNS traffic. The packet list pane displays several DNS queries and responses. The packet details pane shows the structure of a DNS query packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).

No.	Time	Source	Destination	Protocol	Length	Info
31	34.016571	192.168.1.106	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
32	34.048171	192.168.1.1	192.168.1.106	DNS	104	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT
33	34.051652	192.168.1.106	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
34	34.060514	192.168.1.1	192.168.1.106	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.96.143.80
35	34.073270	192.168.1.106	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
36	34.099881	192.168.1.1	192.168.1.106	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:d200:19...

> Frame 31: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0
> Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 11376, Dst Port: 53
> Domain Name System (query)

0000 00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00 45 00}..Q...E
0010 00 46 06 1d 00 00 11 b0 ce c0 a8 01 6a c0 a8 -F.....}..
0020 01 01 2c 70 00 35 09 32 c2 ac 00 01 01 00 00 01 -.,p 5.2
0030 00 00 00 00 00 00 01 31 01 31 03 31 36 38 03 311.1.168.1
0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92 in-ad dr arpa..

Wireshark packet capture window showing DNS traffic. The packet list pane displays several DNS queries and responses. The packet details pane shows the structure of a DNS query packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).

No.	Time	Source	Destination	Protocol	Length	Info
38	27.681071	192.168.1.106	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
39	27.683303	192.168.1.1	192.168.1.106	DNS	104	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT
40	27.688868	192.168.1.106	192.168.1.1	DNS	67	Standard query 0x0002 NS mit.edu
41	27.697085	192.168.1.1	192.168.1.106	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS use5.akam.net NS usw2.akam.net NS asia1.akam.net NS eur5.akam.net NS...

> Frame 38: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0
> Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 11380, Dst Port: 53
> Domain Name System (query)

0000 00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00 45 00}..Q...E
0010 00 46 06 20 00 00 11 b0 cb c0 a8 01 6a c0 a8 -F.....}..
0020 01 01 2c 74 00 35 09 32 c2 a8 00 01 01 00 00 01 -.,t 5.2
0030 00 00 00 00 00 00 01 31 01 31 03 31 36 38 03 311.1.168.1
0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92 in-ad dr arpa..
0050 00 0c 00 01

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
dns						
No.	Time	Source	Destination	Protocol	Length	Info
11	23.319707	192.168.1.106	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
12	25.336689	192.168.1.106	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
24	27.343916	192.168.1.106	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
26	29.350262	192.168.1.106	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
28	31.357371	192.168.1.106	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 11: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{105E81FF-1E88-49D2-B758-A6018706E6FA}, id 0

> Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)

> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 18.0.72.3

> User Datagram Protocol, Src Port: 1032, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0001

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ 3.72.0.18.in-addr.arpa: type PTR, class IN

Name: 3.72.0.18.in-addr.arpa

[Name Length: 22]

[Label Count: 61]

0000 00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00 45 00}...Q...E-
0010 00 44 4f 5a 00 00 80 11 cf 39 c0 a8 01 6a 12 00 .DOZ...9...j..
0020 48 03 04 08 00 35 00 30 34 48 00 01 01 00 00 01 H....5 0 4H.....
0030 00 00 00 00 00 00 01 33 02 37 32 01 30 02 31 383 72.0.18
0040 07 69 6e 2d 01 64 64 72 04 61 72 70 61 00 00 0e .in-addr.arpa..
0050 00 01

Теорія:

Типи DNS записів

Записи DNS, або Ресурсні записи (англ. Resource Records, RR) — одиниці зберігання і передачі інформації в DNS.

Найбільш важливі типи DNS-записів:

- Запис A.
- Запис AAAA.
- Запис CNAME.
- Запис MX.
- Запис NS.
- TXT-запис.
- Запис PTR.
- Запис SOA.
- SRV-запис.

Запис A задає IP-адреса хоста. За допомогою записів A виконується запит на перетворення імені домену в IP-адресу.

Запис AAAA (IPv6 address record) зв'язує ім'я хоста з адресою протоколу IPv6. Наприклад, запит AAAA-запису на ім'я K.ROOT-SERVERS.NET поверне його IPv6 адреса — 2001:7fd::1

Запис типу CNAME (Canonical Name - Канонічне ім'я) дозволяють привласнювати хосту мнемонічні імена. Якщо DNS при зверненні до псевдоніму виявляє запис CNAME, що містить повне ім'я, DNS потім запитує повне ім'я домену.

Записи MX містять визначення хоста системи обміну поштою для поштових повідомлень, що відправляються в цей домен. За допомогою записів цього типу і значень параметрів

конфігурації хостів системи обміну поштою в SMTP (Простий протокол передачі пошти) визначаються адреси хостів, які опрацьовують і перенаправляють пошту для цього домену. Кожному хосту системи обміну поштою повинна відповідати запис адреси хоста (A) в існуючій області.

Запис NS вказує відповідальний сервер для даного хоста.

Запис типу TXT зазвичай використовується для текстового опису доменного імені.

Запис PTR (pointer) або запис покажчика зв'язує IP хоста з його канонічним ім'ям. Наприклад, (на момент написання), для IP адреси 192.0.34.164: запит запису PTR 164.34.0.192.in-addr.arpa поверне його канонічне ім'я referrals.icann.org. З метою зменшення обсягу небажаної кореспонденції (спаму) багато серверів-одержувачів електронної пошти можуть перевіряти наявність PTR запису для хоста, з якого відбувається відправлення. У цьому випадку PTR запис для IP адреси повинна відповідати імені відправляючого поштового сервера, яким він представляється в процесі SMTP сесії.

Запис SOA (Start Of Authority) містить ім'я первинного DNS-сервера (Primary Name Server), адреса, необхідний для встановлення технічних контактів (Hostmaster), серійний номер (Serial number) різні значення таймерів (Refresh, Retry, Expire, Minimum TTL)

SRV-запис (server selection) вказує на сервери для сервісів, використовується, зокрема, для Jabber і Active Directory.

Контрольні запитання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порту запиту DNS? Який номер вихідного порту відповіді DNS?

UDP, Цільовий порт запиту – 53, вихідний порт – 59917

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

8.8.8.8, no ;

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

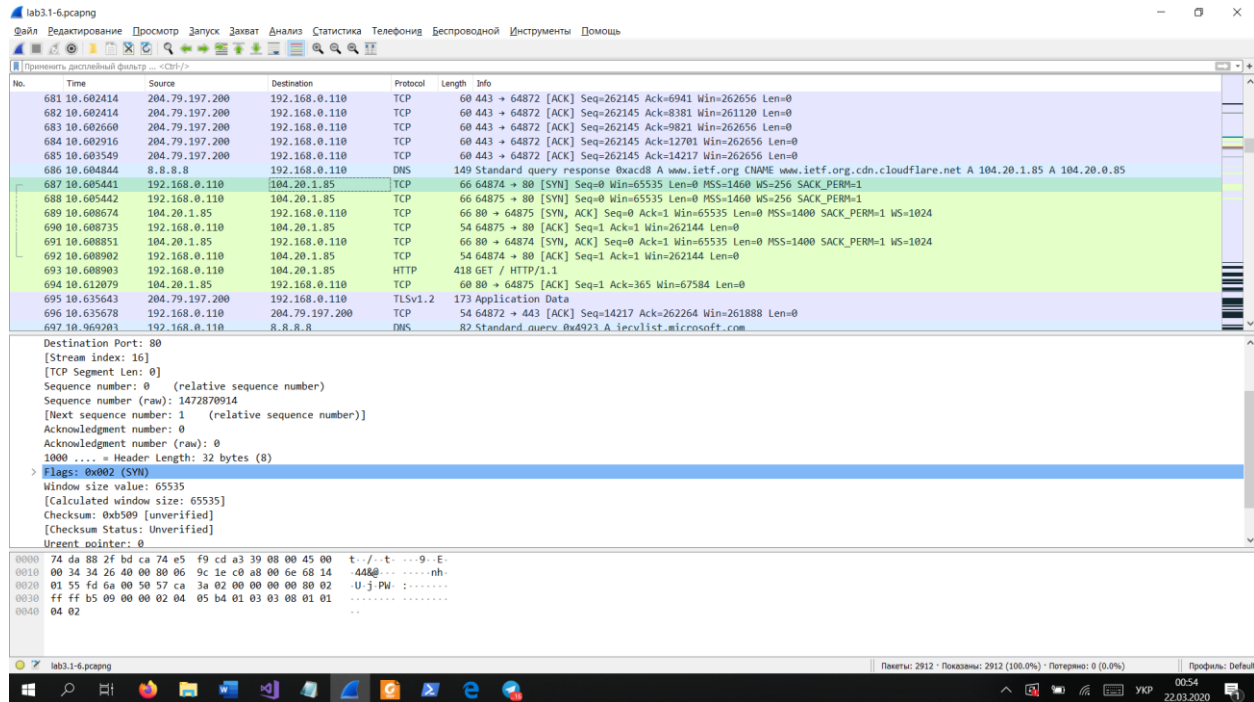
Типу A (Host address). Da (name, type)

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

```
▼ 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
    > 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
```

Lds, Name, Type, Class, Time to live, Data length, 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?



да

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

Но, сразу после syn был отправлен http-запрос

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

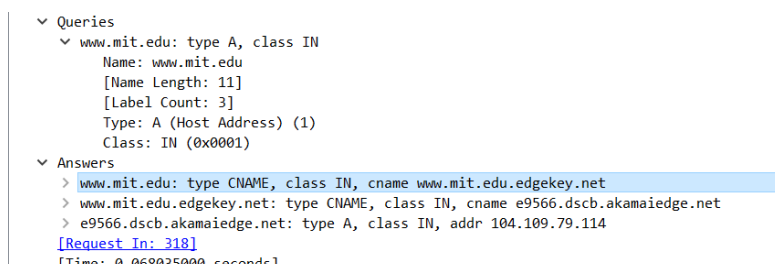
Цільовий порт запиту – 53, вихідний порт – 61228 ;

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

8.8.8.8, по

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

Типу A (Host address). Yes (name, class) ;



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

3 відповіді. Name, Type, Class, Time to live, Data length, CNAME/Adress

```
КГ $ 6«г|Ёу ойЁ0 пёуГаЁп 0вугв:
Имя: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d200:19e::255e
           2a02:26f0:d200:191::255e
           104.109.79.114
Aliases: www.mit.edu
          www.mit.edu.edgekey.net
PS C:\Users\Dragon>
```

```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

PS C:\Users\Dragon> nslookup -type=NS mit.edu
*** Серверы по умолчанию недоступны
тхЁтхЁ: UnKnown
Address: 127.0.0.1

*** UnKnown не удалось найти mit.edu: No response from server
PS C:\Users\Dragon> nslookup -type=NS mit.edu
тхЁтхЁ: dns.google
Address: 8.8.8.8

Не заслуживающий доверия ответ:
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = ns1-173.akam.net
PS C:\Users\Dragon>
```

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

8.8.8.8 , по.

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

Типу NS, type, name? ;

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?

8 штук

(asia1.akam.net, eur5.akam.net, usw2.akam.net, ns1-37.akam.net, asia2.akam.net, ns1-

173.akam.net, use2.akam.net, use5.akam.net).

Лише 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?

На 8.8.8.8, no (google.com)

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

Типу A (Host address), типу AAAA (IPv6 Address). Ні ;

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

1 відповідь;

Name, Type, Class, Time to live, Data length, Address

Висновок:

В лабораторній роботі ознайомився з концепціями локальних серверів DNS; кешування DNS-записів і повідомлень, а також з типами полів у записі DNS.
