Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут ім. І. Сікорського»
Інститут Прикладного Системного Аналізу

Лабораторна робота№3
з дисципліни Комп'ютерні мережі

Виконала
студентка групи КА-77
Кулина Анісія

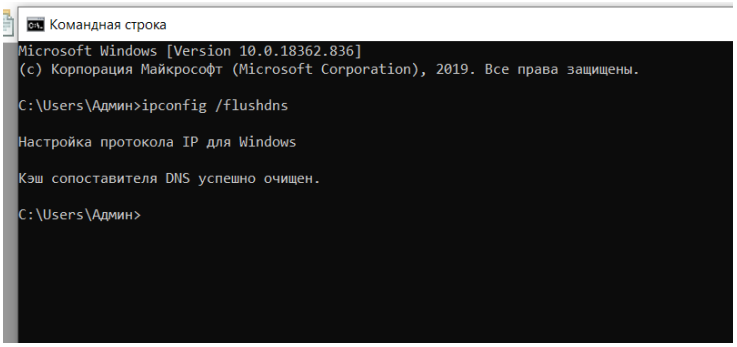
Прийняв Кухарєв С.О.

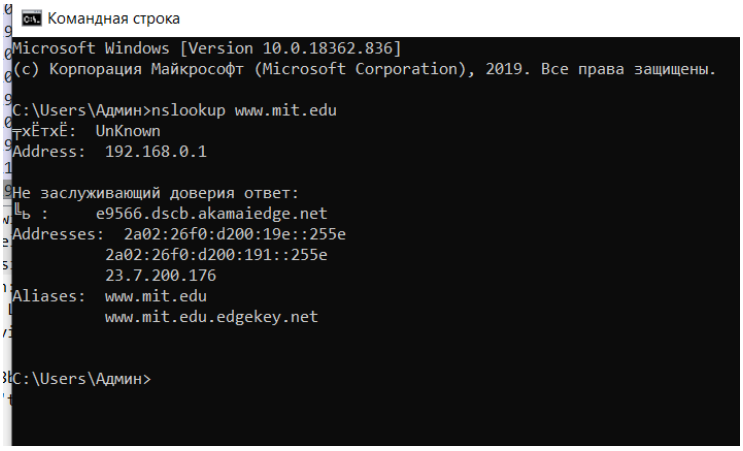
Київ 2020

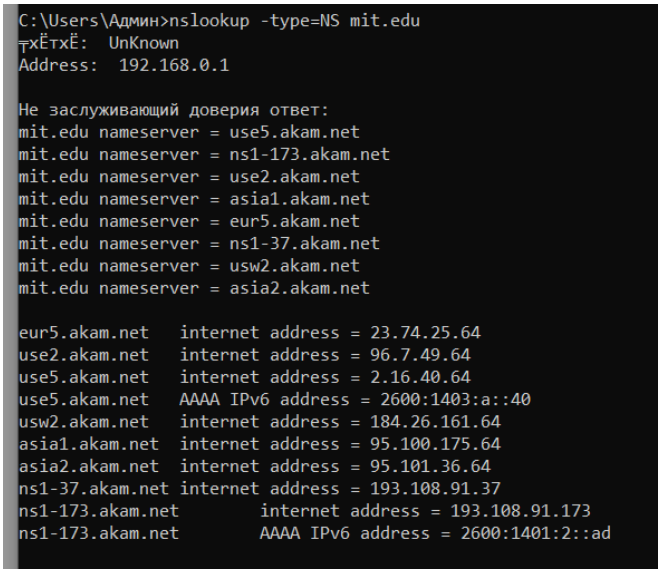
Тема. Протокол DNS

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід роботи:





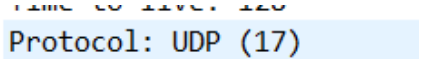


```
Microsoft Windows [Version 10.0.18362.836]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\Admin>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
ТхЁтхЁ:  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
```

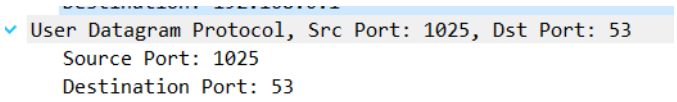
Контрольні запитання:

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?

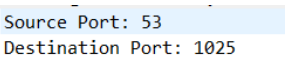
І запит і відповідь використувоють протокол UDP.



Номер цільового порта (destination) запиту DNS: 53

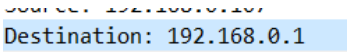


Номер вихідного порта (sourse) відповіді DNS: 53



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

Запит був направлений на наступну IP-адресу: 192.168.0.1. Так, ця адреса співпадає з адресою локального сервера DNS.



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

Запит містить запис типу A. Із можливих компонентів відповіді запит містить ім’я класу.

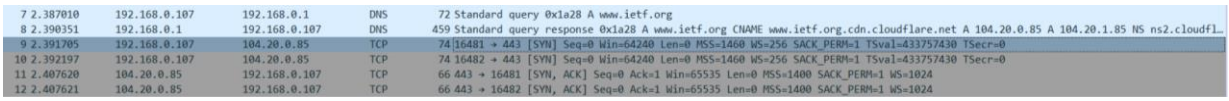
```
Queries
  www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 8]
```

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

Було запропоновано сервером 3 записи із відповідями. Кожна із цих відповідей складається із наступних пунктів: ім'я, тип, клас, час життя, довжина даних, канонічне ім'я або адресу.

```
  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 104.20.0.85
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

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: 1638 (27 minutes, 18 seconds)
      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: 138 (2 minutes, 18 seconds)
      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: 138 (2 minutes, 18 seconds)
      Data length: 4
      Address: 104.20.1.85
```

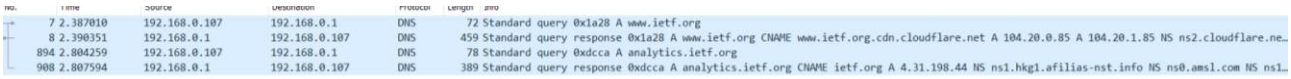
5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?



Ні. Не співпадає.

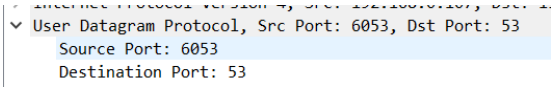
6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

Так, виконує.

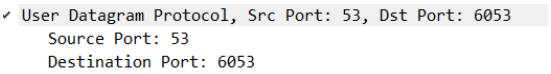


7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

цільовий порт повідомлення із запитом DNS: 53



вихідний порт повідомлення із відповіддю DNS: 53

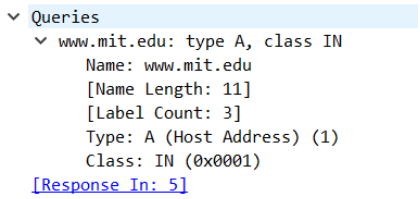


8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Запит був направлений на наступну IP-адресу: 192.168.0.1. Так, ця адреса є адресою локального сервера DNS.

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

Запит містить запис типу A. Із можливих компонентів відповіді запит містить ім’я класу.



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

Було запропоновано сервером 4 записи із відповідями. Кожна із цих відповідей складається із наступних пунктів: ім'я, тип, клас, час життя, довжина даних, канонічне ім'я або адресу.

```
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: 1308 (21 minutes, 48 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: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:19e::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 16
      AAAA Address: 2a02:26f0:d200:19e::255e
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:191::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 16
      AAAA Address: 2a02:26f0:d200:191::255e
```

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

Запит був направлений на наступну IP-адресу: 192.168.0.1. Так, ця адреса співпадає з адресою локального сервера DNS.

```
9 6.621839    192.168.0.107    192.168.0.1    DNS    67 Standard query 0x0002 NS mit.edu
```

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

Запит містить запис типу IN. Із можливих компонентів відповіді запит містить ім’я класу.

```
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: 10]
```

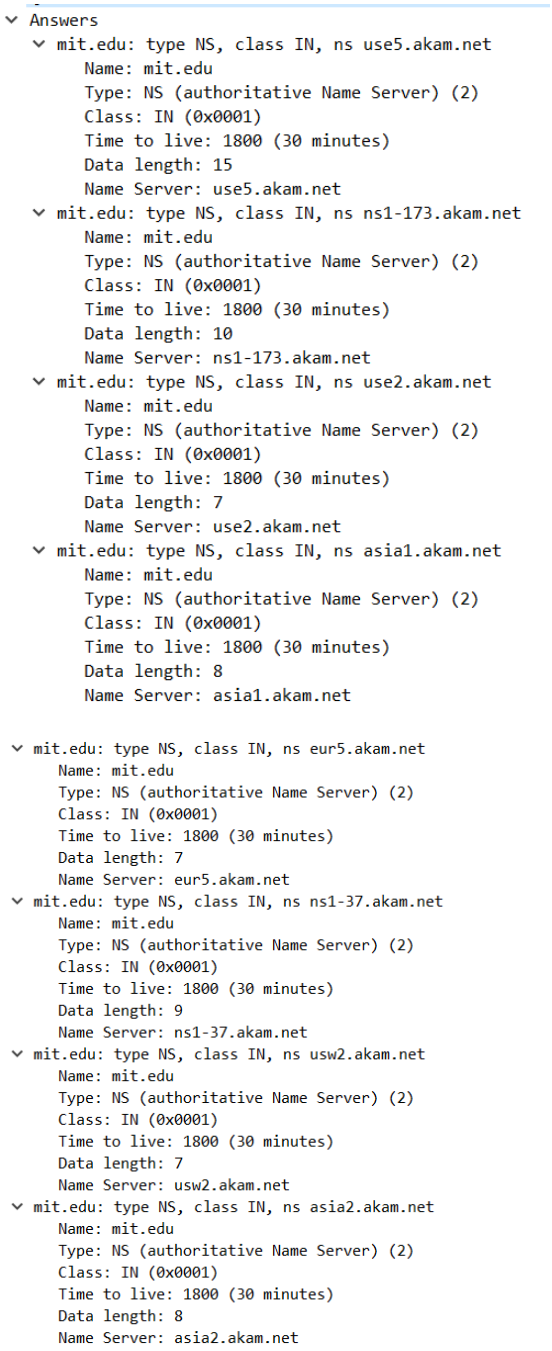
13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді?

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

Було запропоновано сервером 8 записів із відповідями.

У відповіді були запропоновані сервери з наступними іменами: use5.akam.net, ns1-173.akam.net, use2.akam.net, asia1.akam.net, eur5.akam.net, ns1-37.akam.net, usw2.akam.net, asia2.akam.net.

Сервери були запропоновані за допомогою доменного імені.



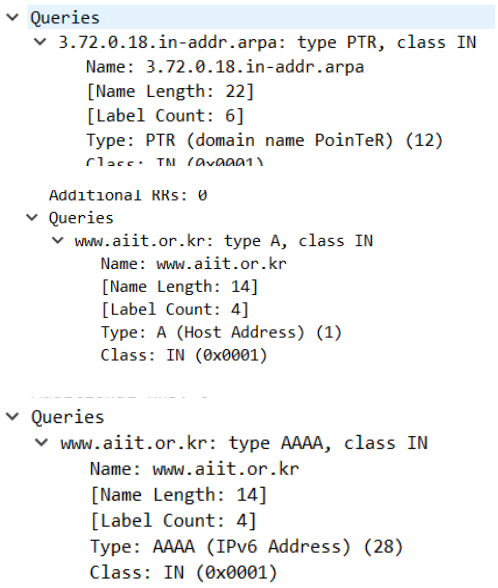
14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

Запит був направлений на наступну IP-адресу: 18.0.72.3

Ні, ця адреса не є адресою локального сервера DNS за замовчанням. Це IP-адреса доменного імені bitsy.mit.edu

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

Запити містять записи типу A, AAAA та PTR. Із можливих компонентів відповіді запит містить ім’я класу IN.



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

Відповідь не надішла.

Висновок: у ході виконання третьої лабораторної роботи було виконано аналіз деталей роботи протоколу DNS та покращено навички роботи з Wireshark.