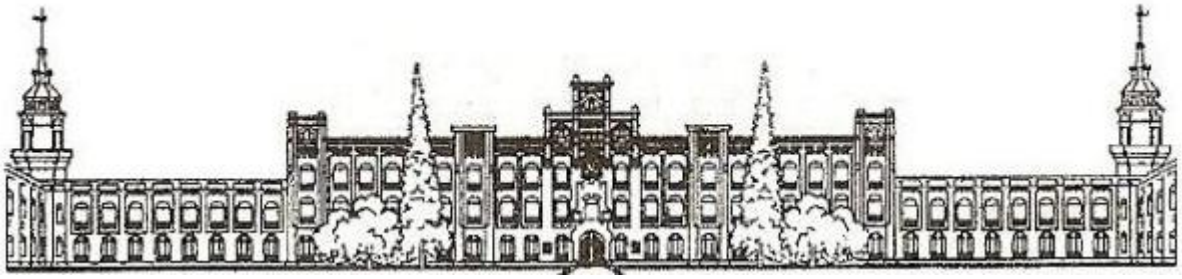


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

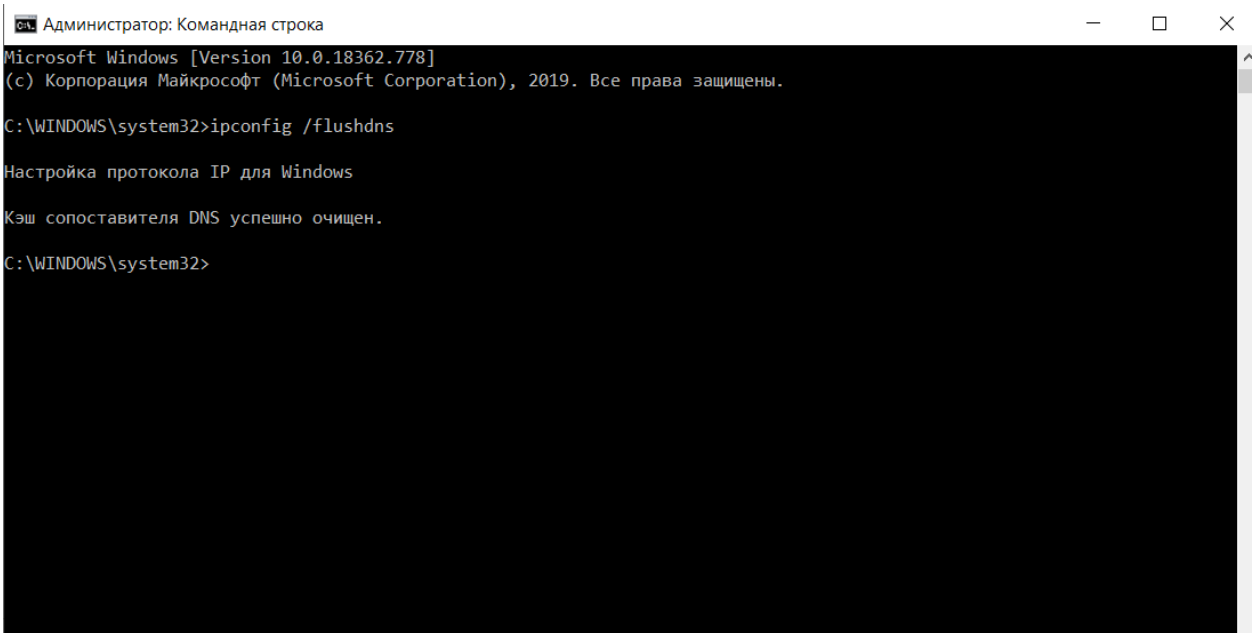
Поліщук А.Б.

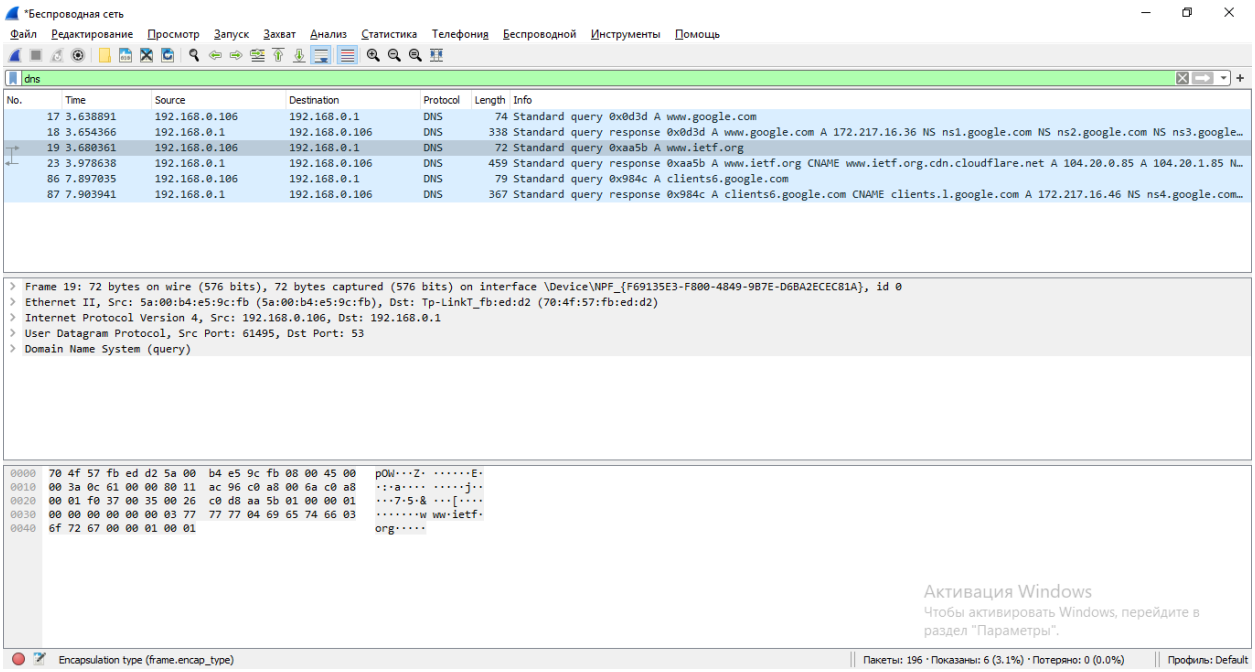
Перевірив: Кухарєв С. О.

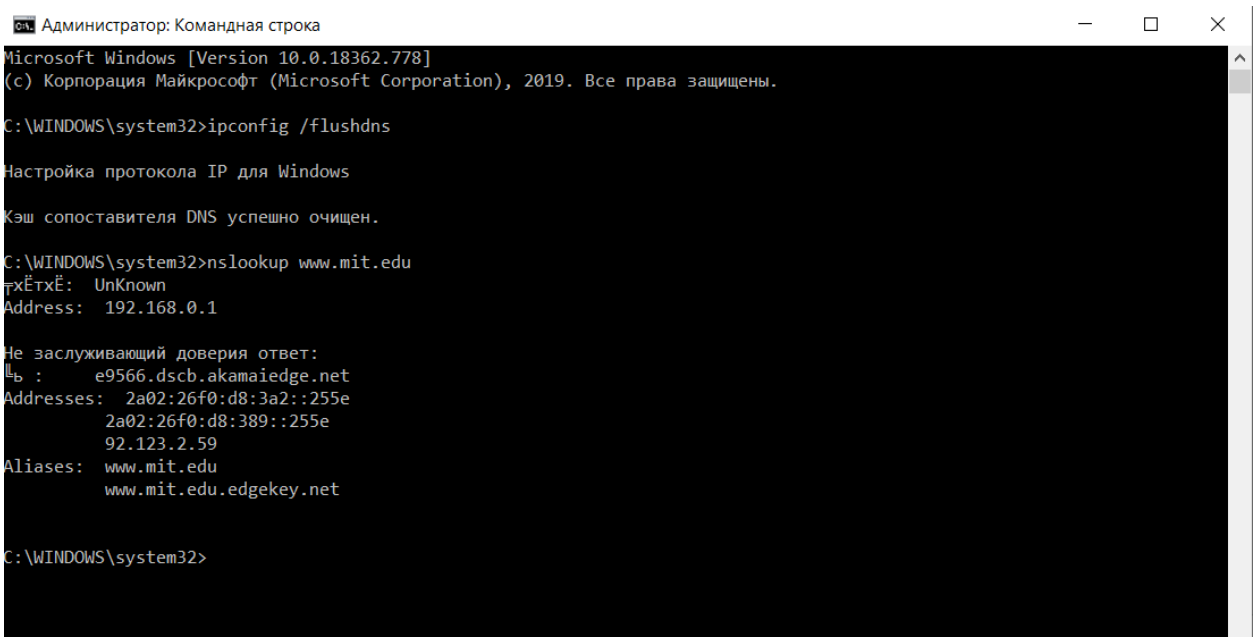
Київ 2020

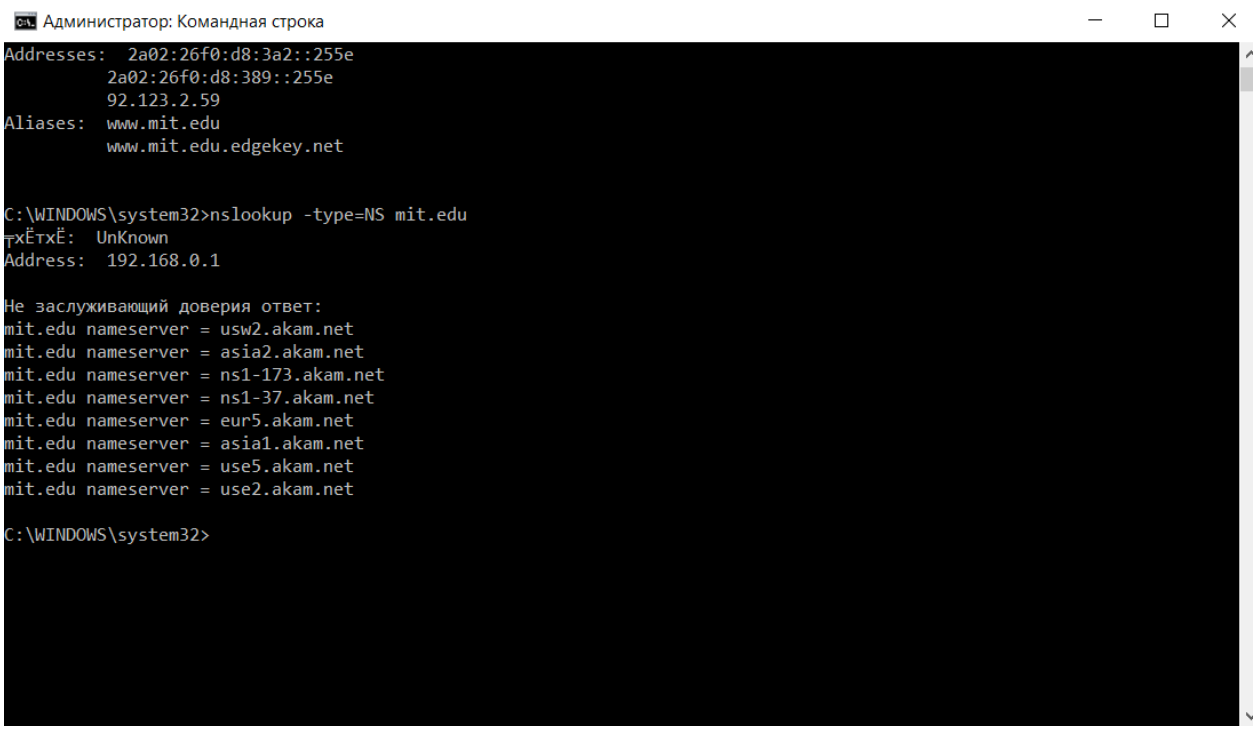
Мета роботи: аналіз деталей роботи протоколу DNS.

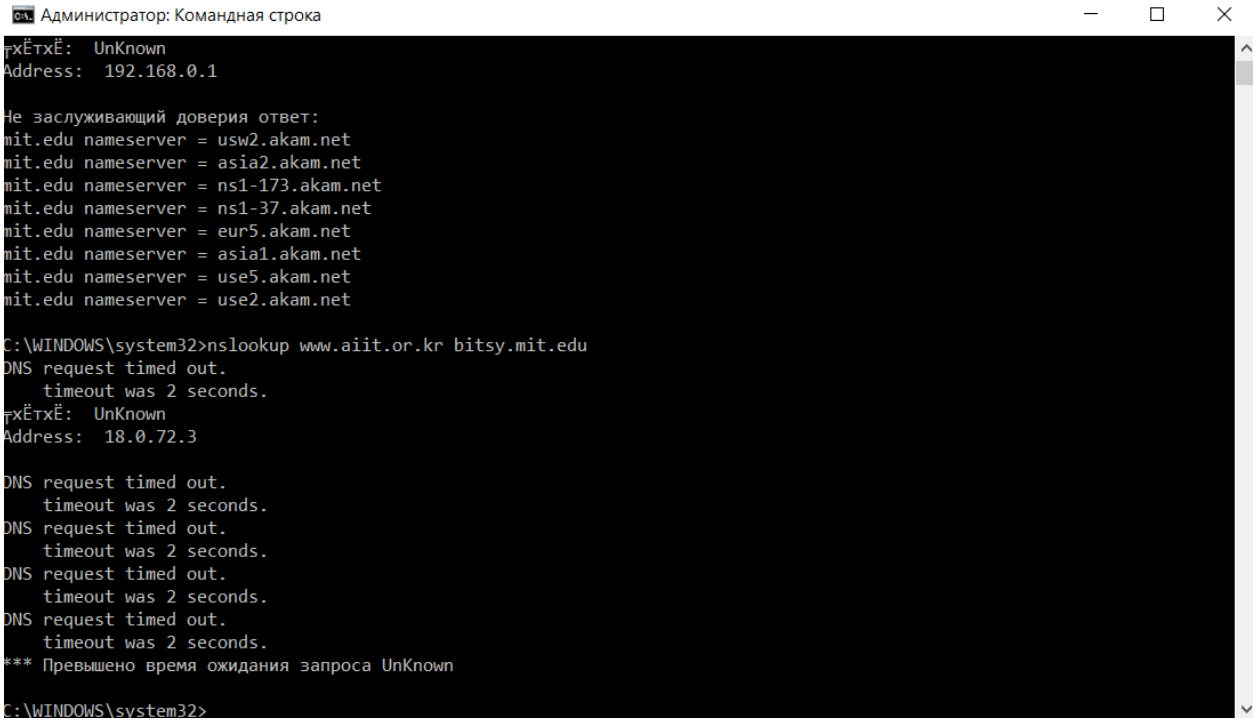
Хід виконання роботи






Администратор: Командная строка
Microsoft Windows [Version 10.0.18362.778]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.
C:\WINDOWS\system32>ipconfig /flushdns
Настройка протокола IP для Windows
Кэш сопоставителя DNS успешно очищен.
C:\WINDOWS\system32>nslookup www.mit.edu
UnKnown
192.168.0.1
Не заслуживающий доверия ответ:
e9566.dscb.akamaiedge.net
2a02:26f0:d8:3a2::255e
2a02:26f0:d8:389::255e
92.123.2.59
www.mit.edu
www.mit.edu.edgekey.net
C:\WINDOWS\system32>

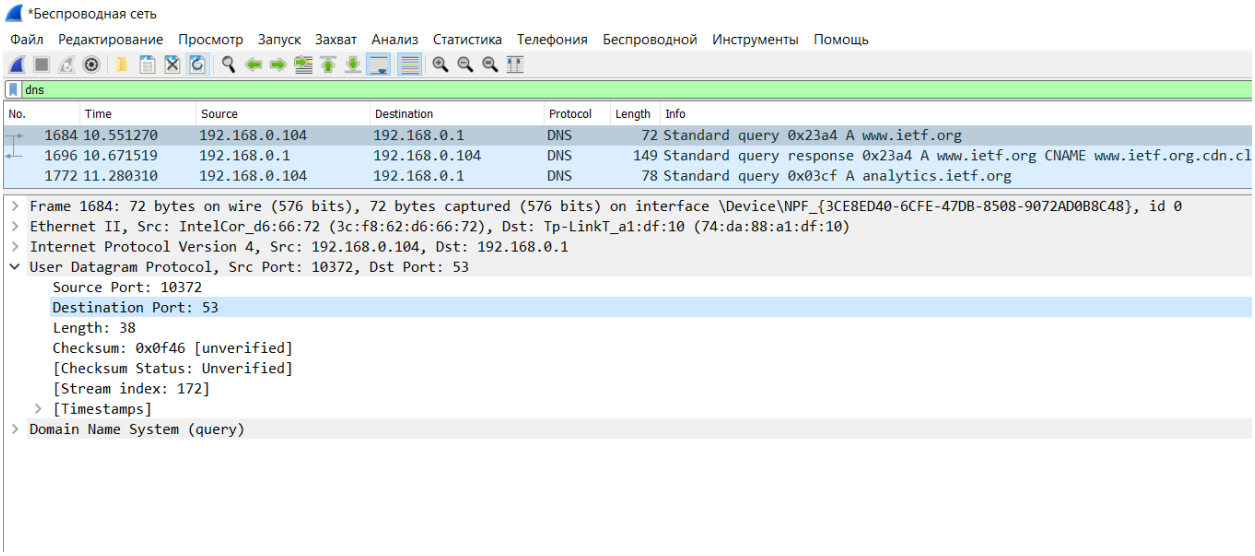

Администратор: Командная строка
2a02:26f0:d8:3a2::255e
2a02:26f0:d8:389::255e
92.123.2.59
www.mit.edu
www.mit.edu.edgekey.net
C:\WINDOWS\system32>nslookup -type=NS mit.edu
UnKnown
192.168.0.1
Не заслуживающий доверия ответ:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
C:\WINDOWS\system32>


Администратор: Командная строка
╥xËтxË: UnKnown
Address: 192.168.0.1
Не заслуживающий доверия ответ:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
C:\WINDOWS\system32>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
timeout was 2 seconds.
╥xËтxË: 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
C:\WINDOWS\system32>

Контрольні запитання:

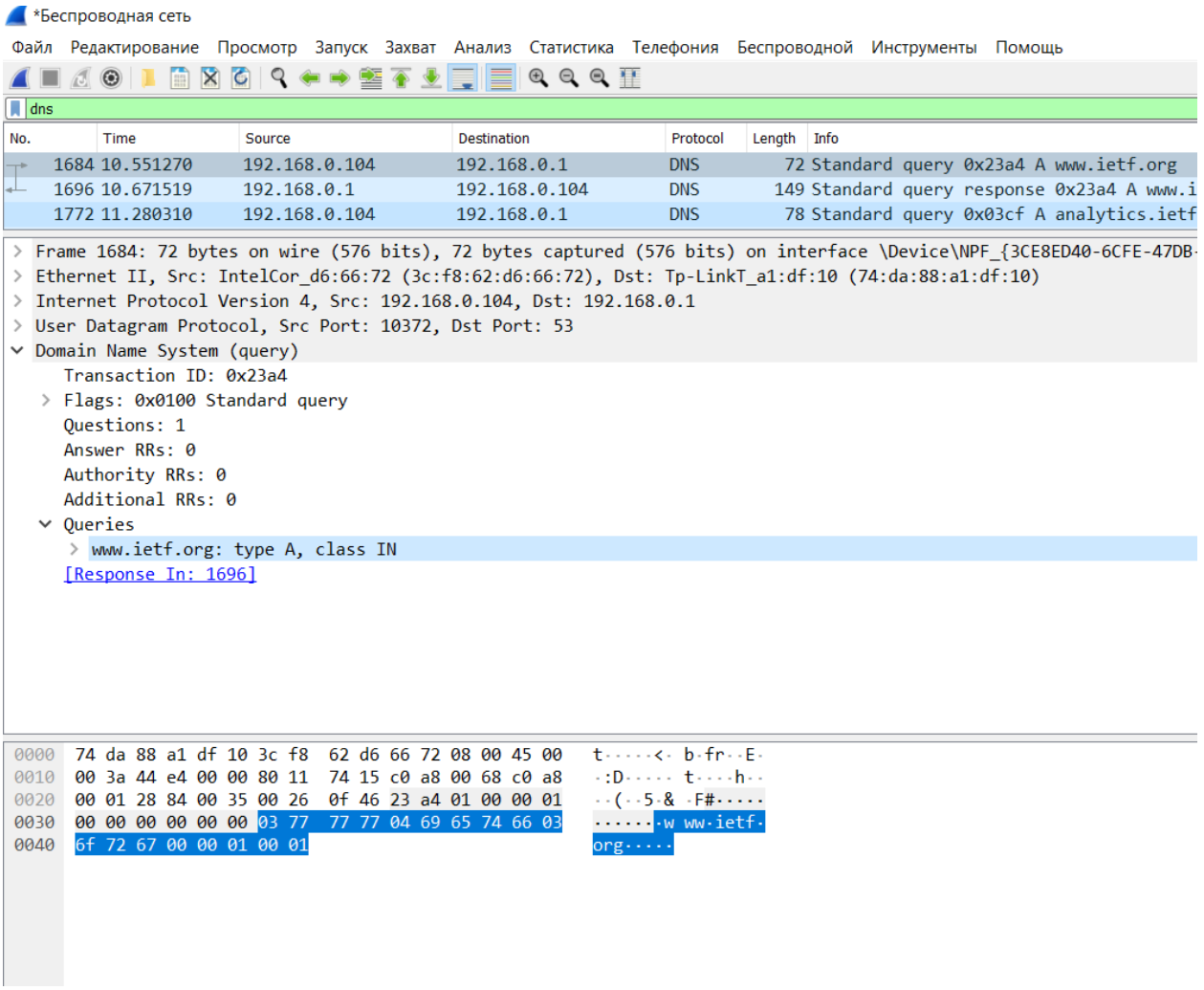
1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

DNS використовує UDP.



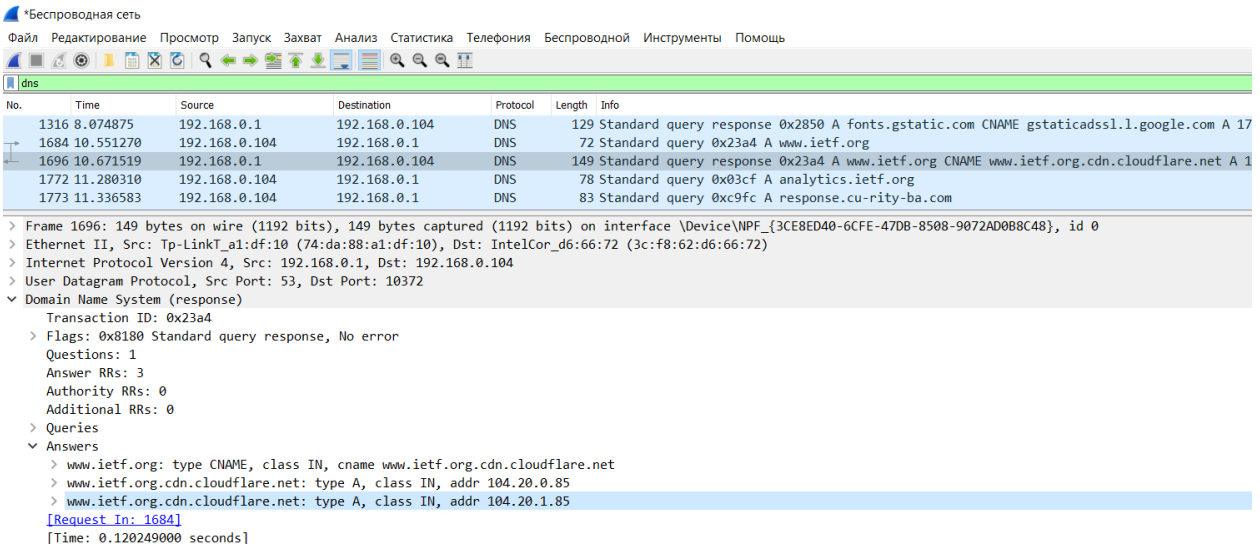
Цільовий порт: 53
Вихідний порт: 10372

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?
   IP: 192.168.0.1 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?



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 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: 53
   Вихідний: 1036

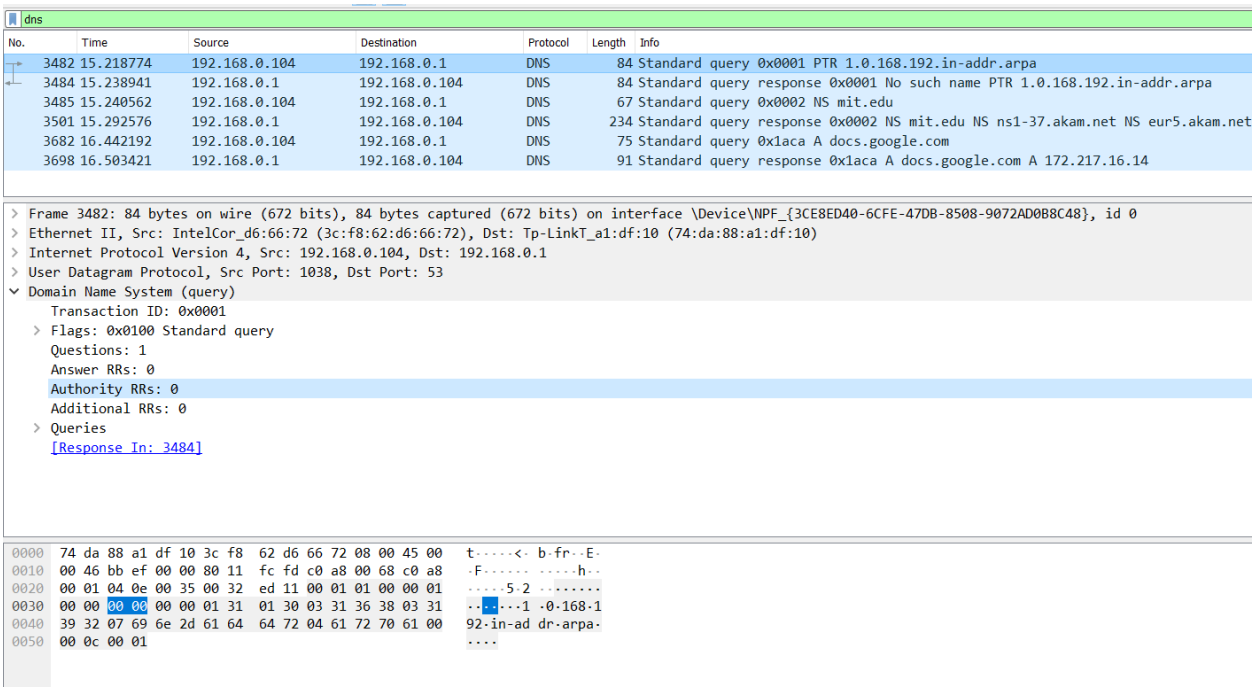
8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?
   192.168.0.1. Так, є адресою локального сервера.

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

10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей? – 3 відповіді.

```
▾ 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: 1294 (21 minutes, 34 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: 11 (11 seconds)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▾ e9566.dscb.akamaiedge.net: type A, class IN, addr 92.123.2.59
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 19 (19 seconds)
      Data length: 4
      Address: 92.123.2.59
  [Request In: 1166]
```

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

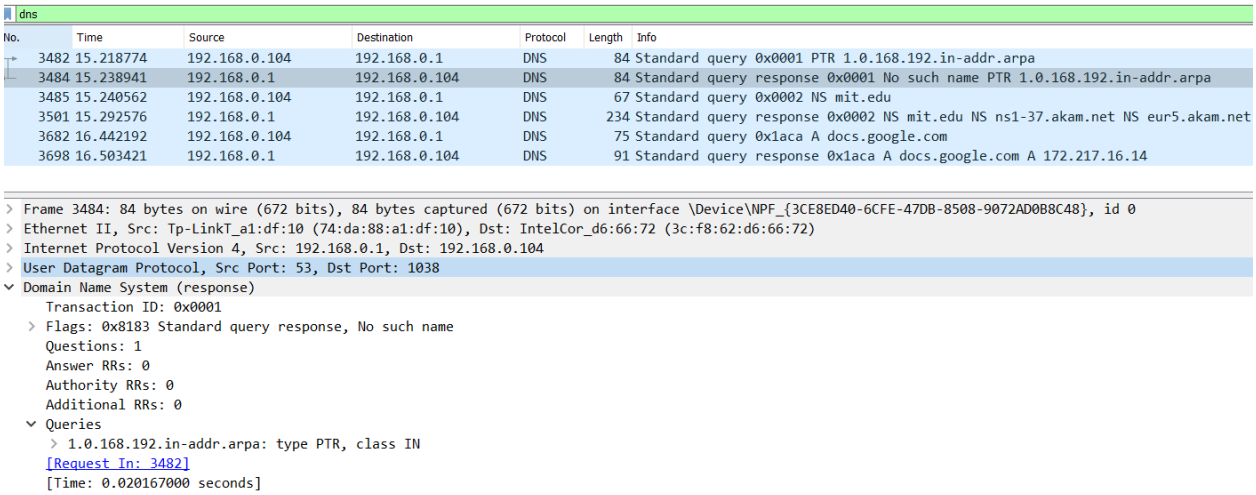


IP: 192.168.0.1. Так є.

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

Тип запиту - PTR. Так вміщує.

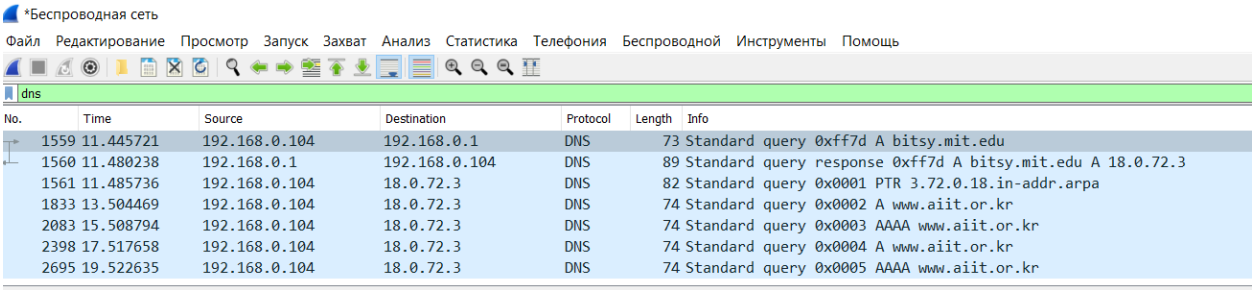
13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?



0 записів із відповіддю. У відповідь було запропоновано сервер: *__*

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?

IP: 192.168.0.1. Є адресою локального сервера.



15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?/
Тип запиту - A. Вміщує.

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

Була отримана одна відповідь.

```
Transaction ID: 0xff7d
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
> Queries
v Answers
  v 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: 1677 (27 minutes, 57 seconds)
      Data length: 4
      Address: 18.0.72.3
  [Request In: 1559]
  [Time: 0.034517000 seconds]
```

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.