

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Кафедра математичних методів системного аналізу

ЗВІТ

Про виконання лабораторних робіт

З дисципліни «Комп'ютерні мережі»

Виконав: ст. гр. ІС-ЗП91

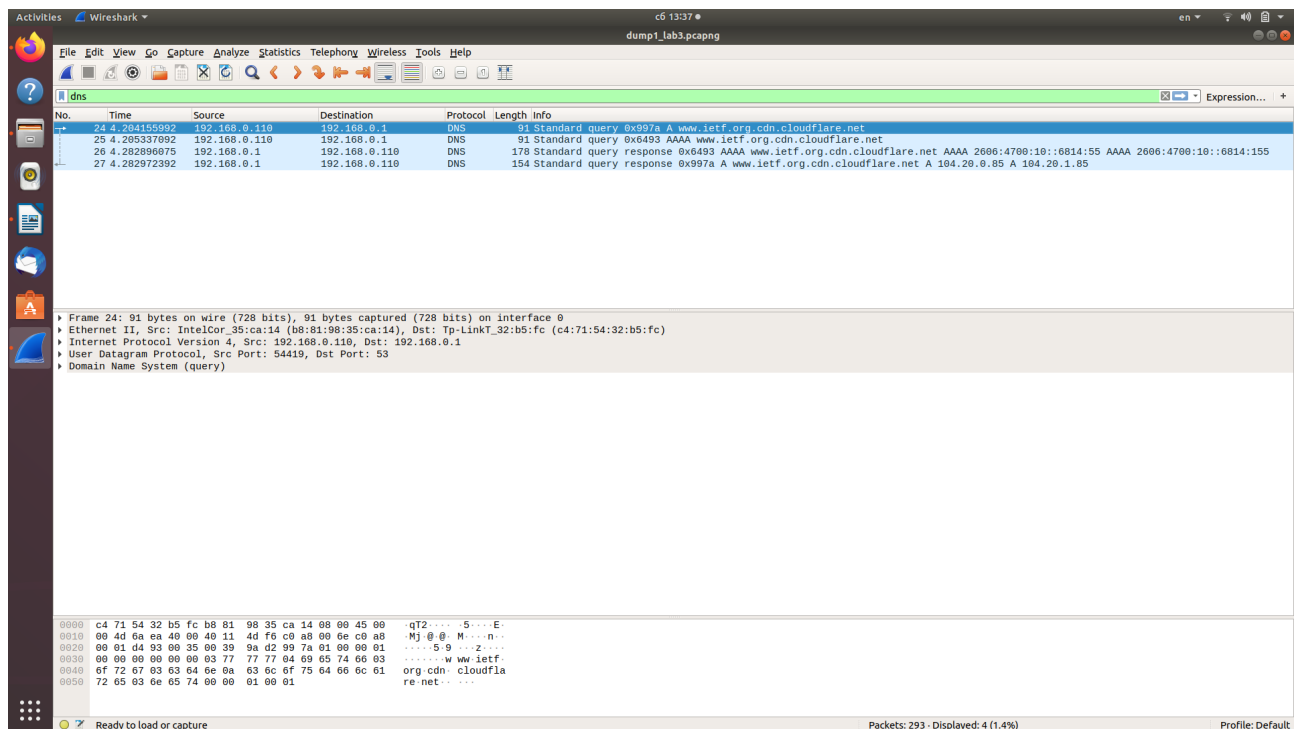
Резнік К.В.

Прийняв: Кухарєв С.О.

Лабораторна робота 3

Хід роботи

1. Очистіть кеш DNS-записів:
2. Запустіть веб-браузер, очистіть кеш браузера
3. Запустіть Wireshark, почніть захоплення пакетів.
4. Відкрийте за допомогою браузера одну із зазначених нижче адрес:
<http://www.ietf.org>
5. Зупиніть захоплення пакетів.
6. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/).
7. Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.

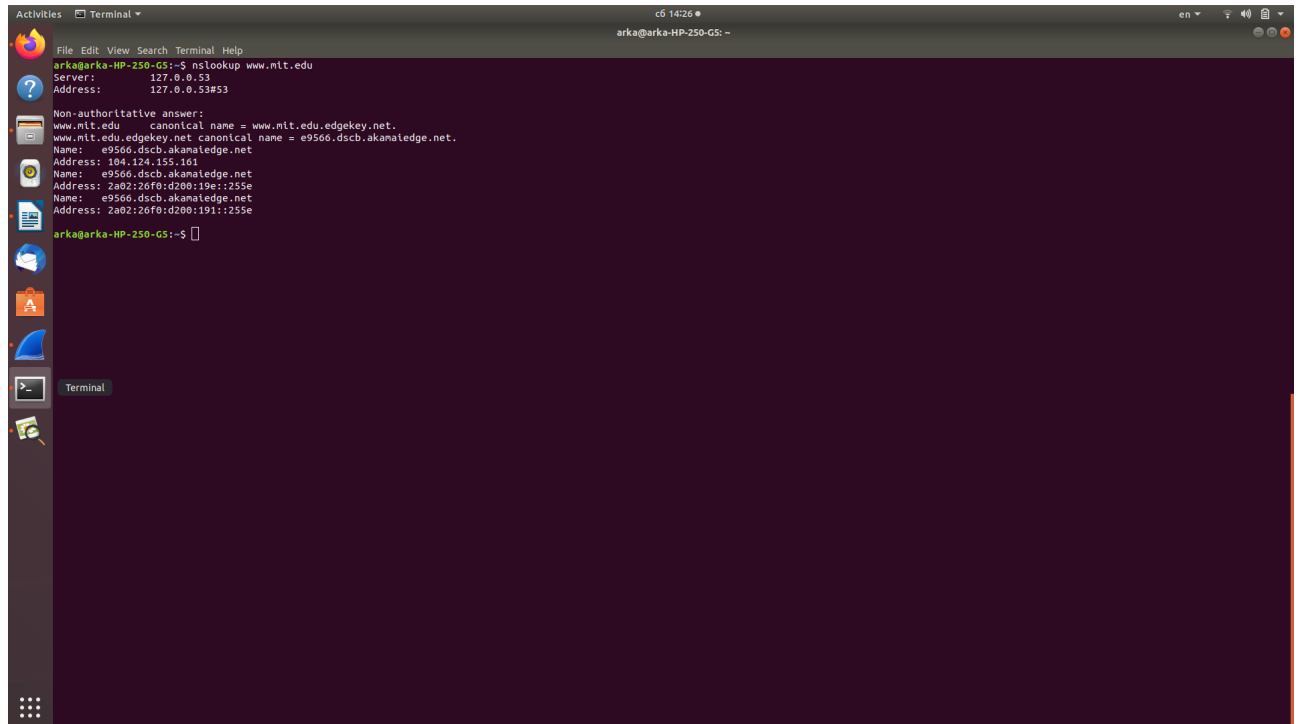


Мал. 1 –Результати запиту

8. Почніть захоплення пакетів

9. Виконайте nslookup для домену www.mit.edu за допомогою команди

nslookup www.mit.edu



```
ark@arka-HP-250-G5:~$ nslookup www.mit.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.mit.edu canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.124.155.101
Name:   e9566.dscb.akamaiedge.net
Address: 2a02:26f0:d200:19e::255e
Name:   e9566.dscb.akamaiedge.net
Address: 2a02:26f0:d200:191::255e

ark@arka-HP-250-G5:~$
```

10. Зупиніть захоплення пакетів.

11. Приготуйте відповіді на контрольні запитання 7-10, роздрукуйте необхідні для цього пакети. Утиліта nslookup відправляє три запити та отримує три відповіді, така поведінка є специфічною, тому слід ігнорувати перші два запити та перші дві відповіді

12. Почніть захоплення пакетів

13. Виконайте nslookup для домену www.mit.edu за допомогою команди

nslookup -type=NS mit.edu

14. Зупиніть захоплення пакетів

15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі

захоплені пакети

16. Почніть захоплення пакетів

17. Виконайте nslookup для домену `www.mit.edu` за допомогою команди

a. `nslookup www.mit.edu`

18. Зупиніть захоплення пакетів.

19. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі

захоплені пакети

20. Приготуйте відповіді на запитання 16, 17. Роздрукуйте необхідні для цього пакети.

21. Закрийте Wireshark

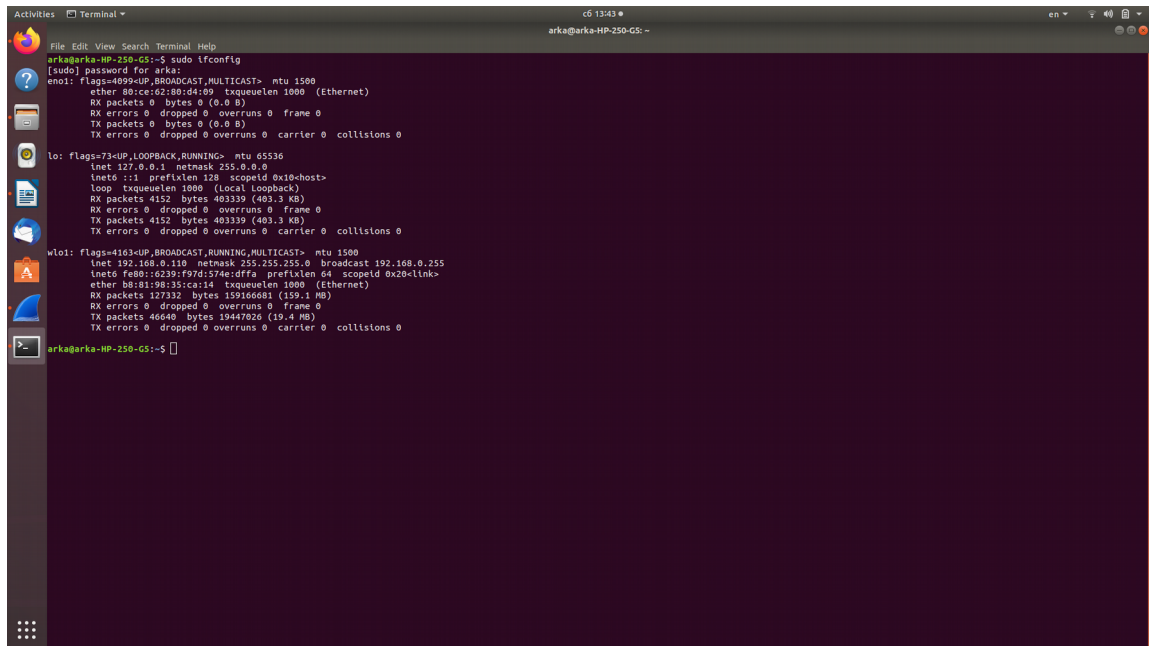
Контрольні запитання

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?

- User Datagram Protocol, Src Port: 54419, Dst Port: 53

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

- Source: 192.168.0.110, Destination: 192.168.0.1(Спершу запит був відправлений за цією адресою)
- Локальна адреса IP на скріншоті знизу



```
arkagarka-HP-250-GS:~$ sudo ifconfig
[sudo] password for arka:
vni1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:ce:62:80:d4:09 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4152 bytes 403339 (403.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4152 bytes 403339 (403.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.110 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::5239:f97d:574e:dffa prefixlen 64 scopeid 0x20<link>
    ether b8:81:98:35:ca:14 txqueuelen 1000 (Ethernet)
    RX packets 127332 bytes 159166681 (159.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46640 bytes 19447026 (19.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

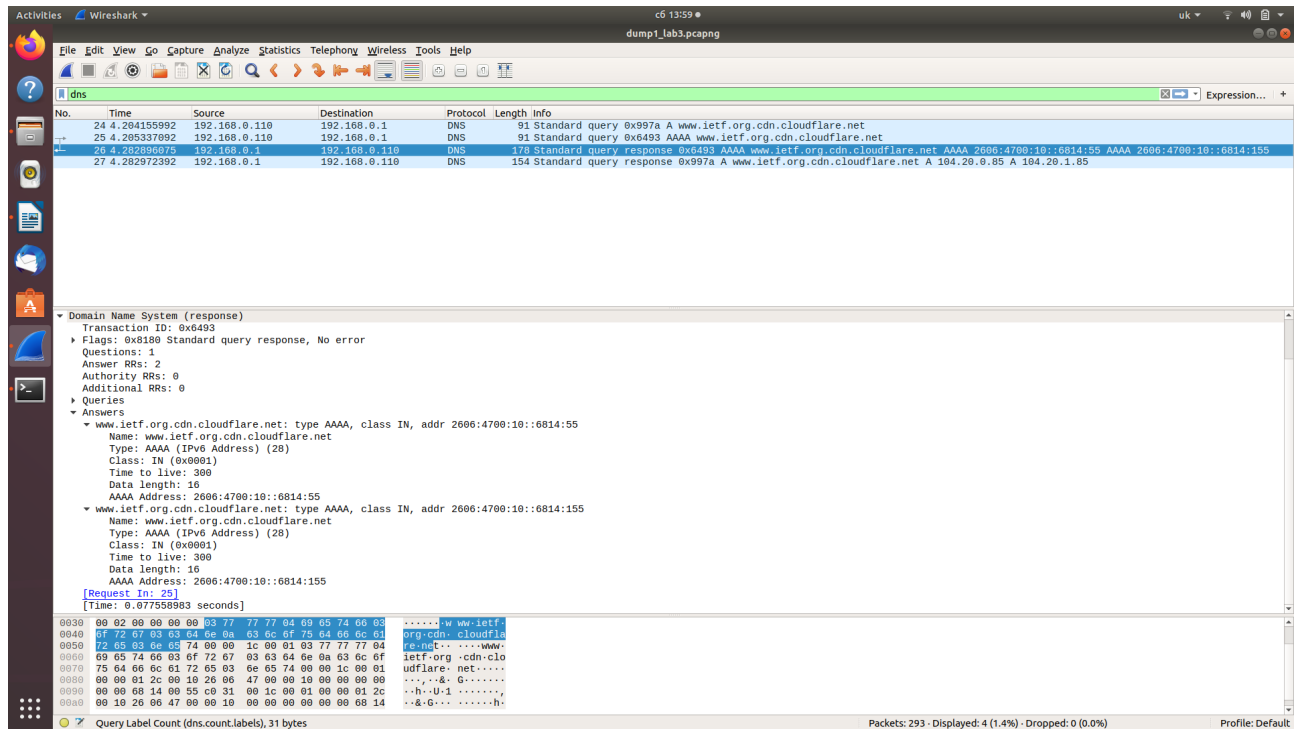
arkagarka-HP-250-GS:~$
```

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

- Було отримано дві відповідь типу: Type: A (Host Address) (1)
- Також він вміщує компонент “відповіді”:[Response In: 27]

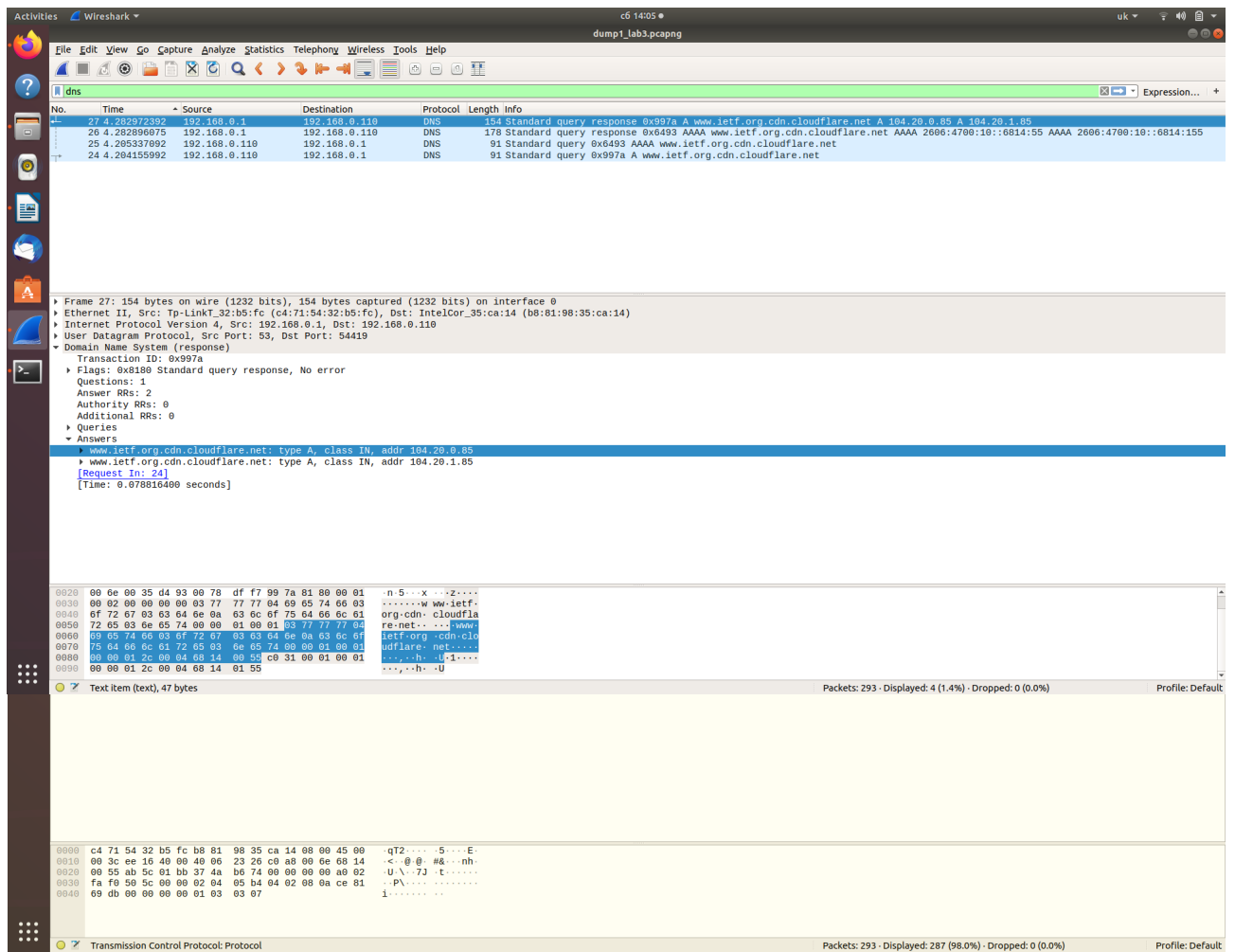
4. Дослідить повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

- 2 відповіді, кожна має такі поля: 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?

- Так, співпадає



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

- Так, був виконан ще один запит, Type AAAA.(для перетворення імені хоста). Інших запитів немає, можливо, через швидку зупинку Wireshark.

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

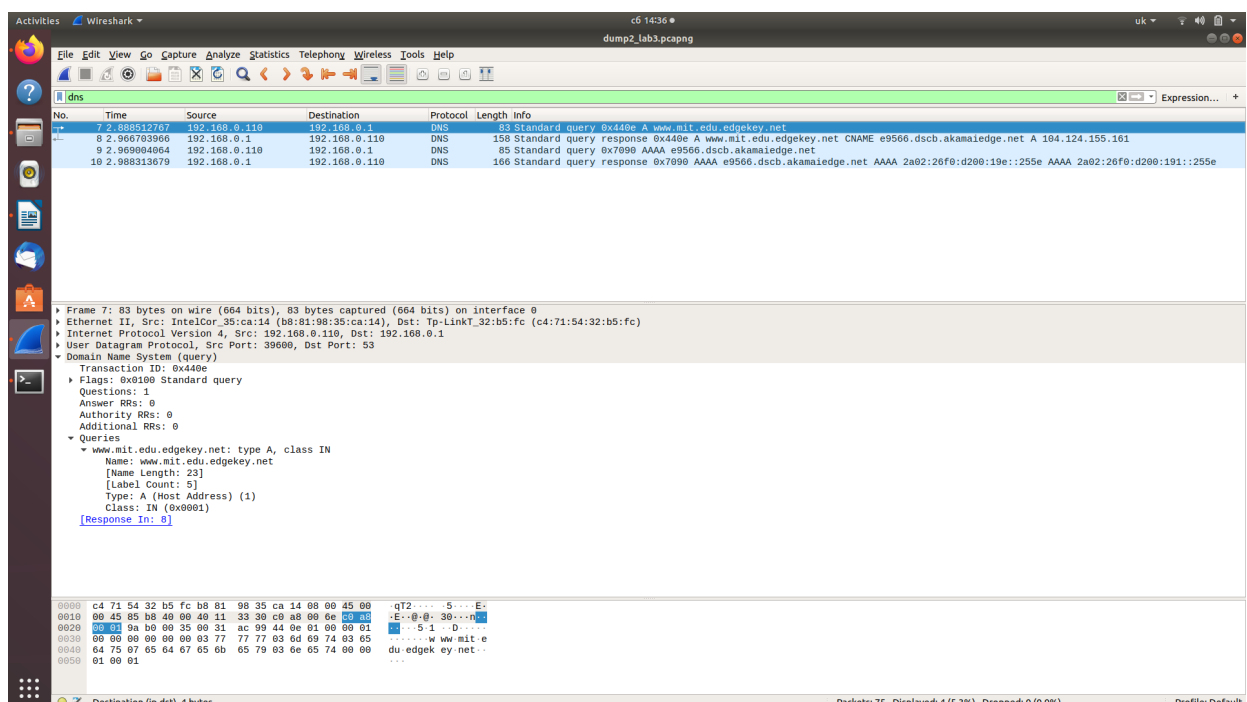
- Запит: Source Port: 39600, Destination Port: 53
- Відповідь: Source Port: 53, Destination Port: 39600

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

- Destination: 192.168.0.110
- Так, це адреса мого локального сервера за замовчанням
- **inet 192.168.0.110** netmask 255.255.255.0 broadcast 192.168.0.255

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

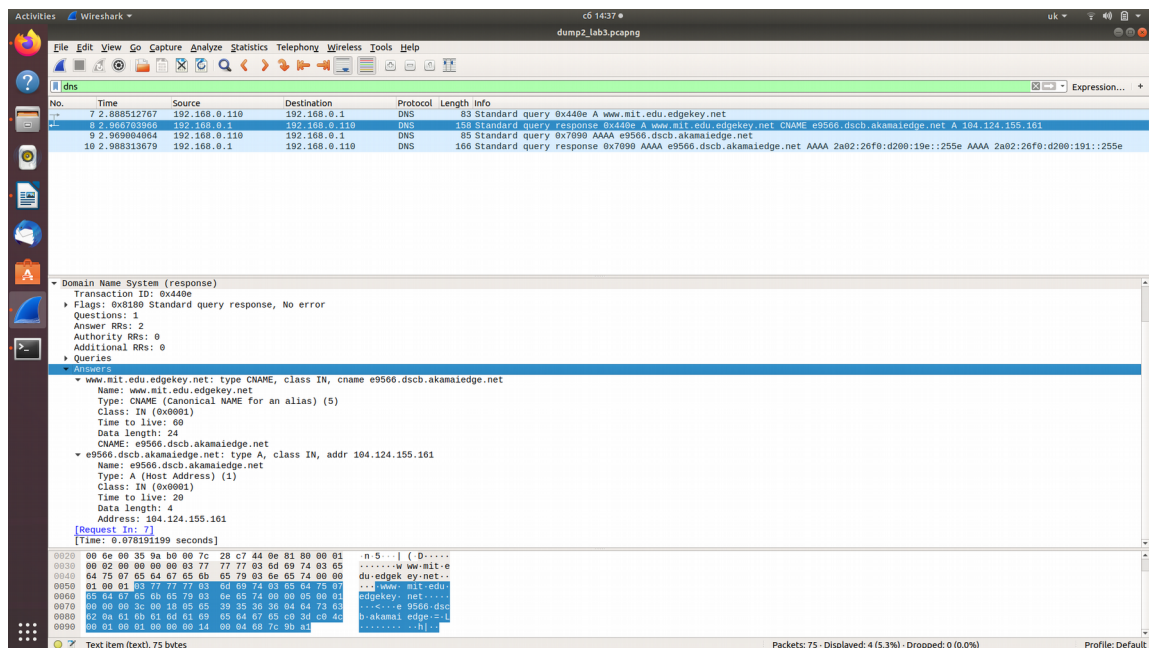
- Запит по UDP протоколу з посиланням на відповідь



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

- 2 записи із 2ма відповідями на вибір, кожна складається з таких значень:

11.
На
яку
IP-



адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

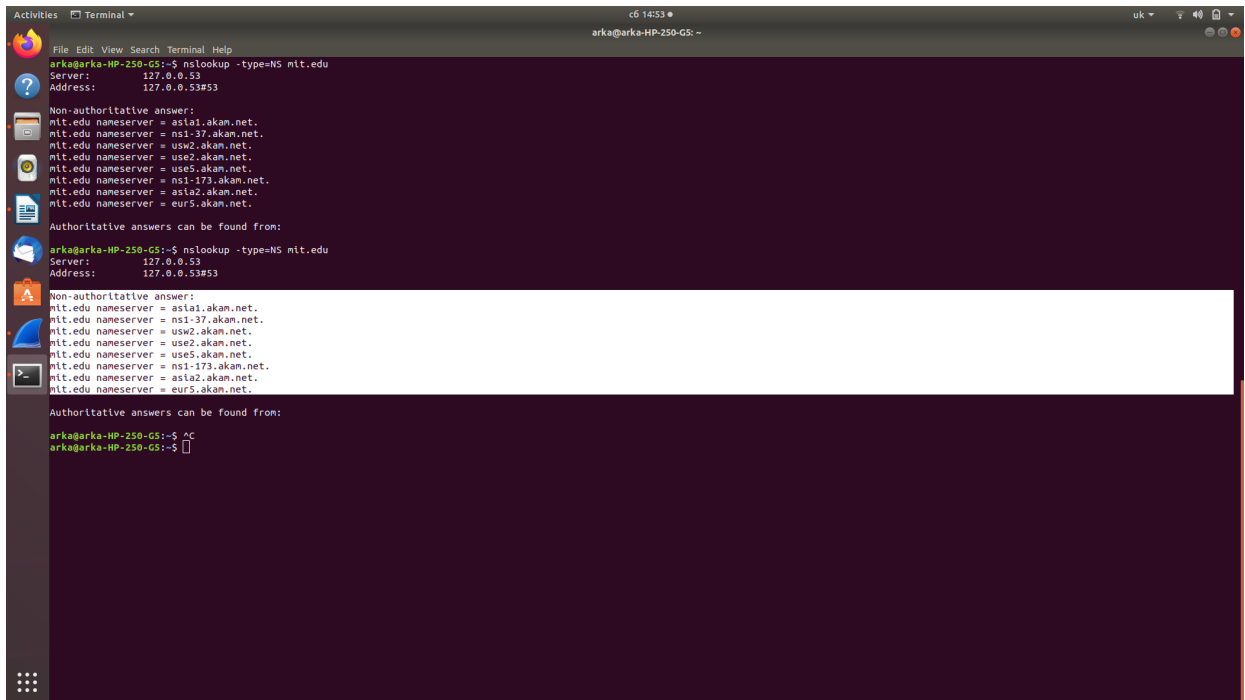
- Destination: 192.168.0.1– це є адреса локального сервера DNS за замовчанням

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

- Відповідь: Це був запит по UDP протоколу. Так, цей запит вміщує ссилку на відповідь: [Response In: 75]

13. Дослідите 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 одну відповідь типу A у Wireshark:
 - ssl.gstatic.com: type A, class IN, addr 216.58.208.195
- В терміналі також були запропоновані наступні відповіді:



```
ark@arka-HP-250-G5:~$ nslookup -type=NS mtt.edu
Server:
127.0.0.53
Address:
127.0.0.53#53

Non-authoritative answer:
mtt.edu nameserver = as1a1.akan.net.
mtt.edu nameserver = ns1-37.akan.net.
mtt.edu nameserver = usw2.akan.net.
mtt.edu nameserver = use2.akan.net.
mtt.edu nameserver = use5.akan.net.
mtt.edu nameserver = ns1-173.akan.net.
mtt.edu nameserver = as1a2.akan.net.
mtt.edu nameserver = eur5.akan.net.

Authoritative answers can be found from:

ark@arka-HP-250-G5:~$ nslookup -type=NS mtt.edu
Server:
127.0.0.53
Address:
127.0.0.53#53

Non-authoritative answer:
mtt.edu nameserver = as1a1.akan.net.
mtt.edu nameserver = ns1-37.akan.net.
mtt.edu nameserver = usw2.akan.net.
mtt.edu nameserver = use2.akan.net.
mtt.edu nameserver = use5.akan.net.
mtt.edu nameserver = ns1-173.akan.net.
mtt.edu nameserver = as1a2.akan.net.
mtt.edu nameserver = eur5.akan.net.

Authoritative answers can be found from:
```

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?

- Ні, під час здійснення сесії було зроблено 2 запити(Типу A та AAAA), але обидва були направлені на локальну адресу:
- Source: 192.168.0.110, Destination: 192.168.0.1

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

Тип запиту A, вміщує посилання на відповідь

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

- 1 відповідь що вміщує такі дані
 - Name: ssl.gstatic.com
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 210
 - Data length: 4
 - Address: 216.58.208.195

- [Request In: 94]