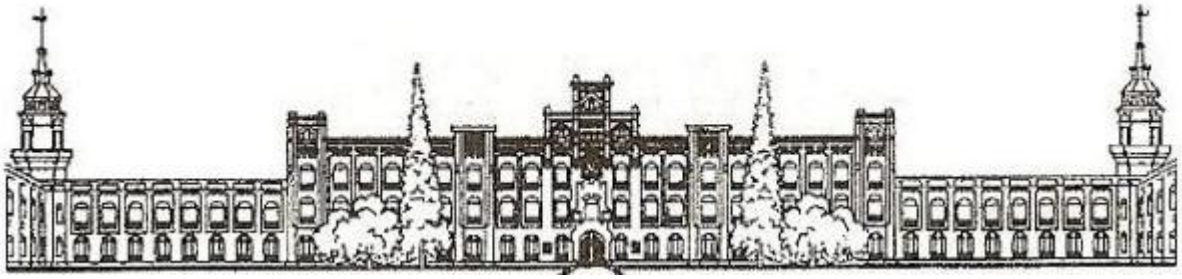


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Лабораторна робота № 3

З дисципліни: Комп’ютерні мережі

Протоколи DNS

Виконала:

Студентка III курсу

Групи КА-71

Кравченко А.А.

Перевірив: Кухарєв С. О.

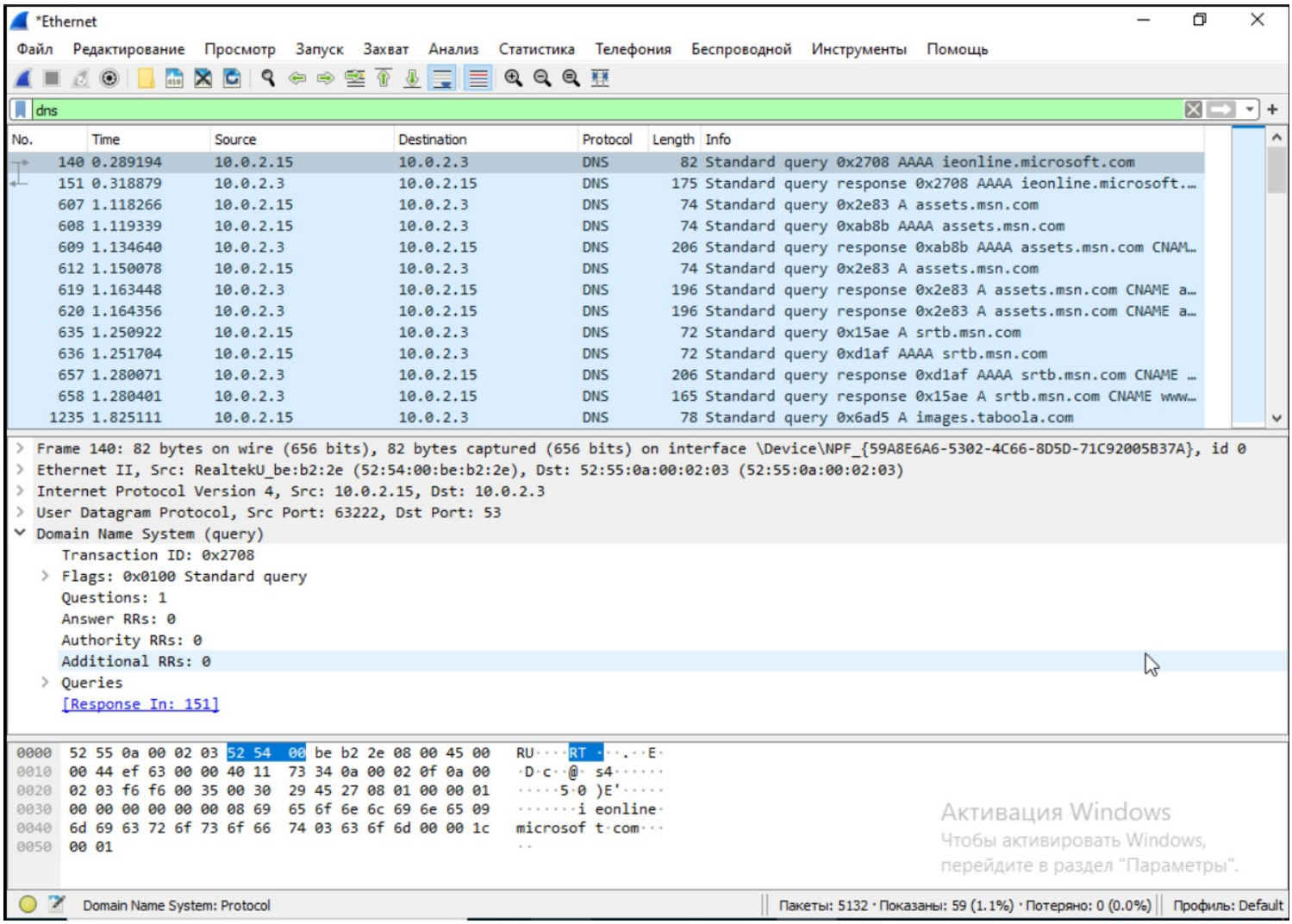
Київ 2020

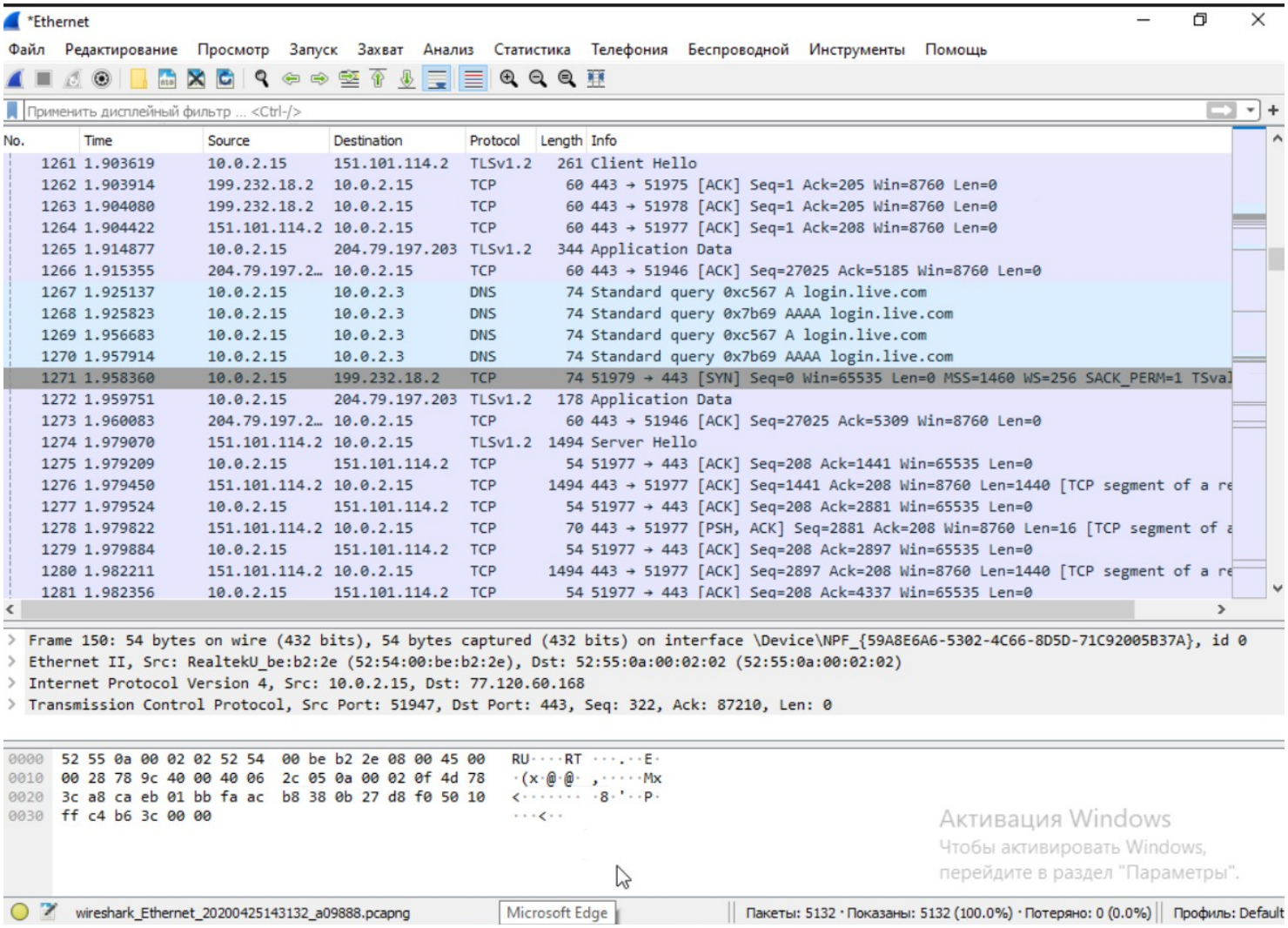
Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

Стандартний тип запиту. Так вміщує.

```
Microsoft  Windows [Version 10.0.18363.778]                    (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>
```





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?

```
> Ethernet II, Src: RealtekU_be:b2:2e (52:54:00:be:b2:2e), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
> User Datagram Protocol, Src Port: 63222, Dst Port: 53
```

Цільовий порт: 53

Вихідний порт: 57547

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?
   IP: 10.0.2.15 Так є.
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Цей запит – є запитом стандартного типу. Вміщує.

[Response In: 151]

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

```
Transaction ID: 0x2708
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
> Queries
v Answers
  > ieonline.microsoft.com: type CNAME, class IN, cname any.edge.bing.com
> Authoritative nameservers
[Request In: 140]
[Time: 0.029685000 seconds]
```

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.

No.	Time	Source	Destination	Protocol	Length	Info
47	0.188693	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=105 Ack=28035 Win=64095 Len=0
48	0.189192	77.120.60.168	10.0.2.15	TLSv1.2	886	Application Data, Application Data
49	0.189390	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=105 Ack=28867 Win=65535 Len=0
50	0.245433	10.0.2.15	77.120.60.168	TLSv1.2	157	Application Data
51	0.245733	77.120.60.168	10.0.2.15	TCP	60	443 → 51947 [ACK] Seq=28867 Ack=208 Win=8760 Len=0
52	0.257323	10.0.2.15	77.120.60.160	TCP	74	51963 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256…
53	0.257345	10.0.2.15	77.120.60.160	TCP	74	51964 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256…
54	0.261160	77.120.60.168	10.0.2.15	TLSv1.2	1107	Application Data
55	0.261288	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=208 Ack=29920 Win=64482 Len=0
56	0.266477	77.120.60.168	10.0.2.15	TLSv1.2	1107	Application Data
57	0.266587	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=208 Ack=30973 Win=65535 Len=0
58	0.266926	77.120.60.168	10.0.2.15	TLSv1.2	1494	Application Data
59	0.267082	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=208 Ack=32413 Win=64095 Len=0

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

Так виконує.

```
 82 Standard query 0x2708 AAAA ieonline.microsoft.com
175 Standard query response 0x2708 AAAA ieonline.microsoft.…
 74 Standard query 0x2e83 A assets.msn.com
 74 Standard query 0xab8b AAAA assets.msn.com
206 Standard query response 0xab8b AAAA assets.msn.com CNAM…
 74 Standard query 0x2e83 A assets.msn.com
196 Standard query response 0x2e83 A assets.msn.com CNAME a…
196 Standard query response 0x2e83 A assets.msn.com CNAME a…
 72 Standard query 0x15ae A srtb.msn.com
 72 Standard query 0xd1af AAAA srtb.msn.com
206 Standard query response 0xd1af AAAA srtb.msn.com CNAME …
165 Standard query response 0x15ae A srtb.msn.com CNAME www…
 78 Standard query 0x6ad5 A images.taboola.com
```

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

   Цільовий: 10.0.2.3

   Вихідний: 10.0.2.15

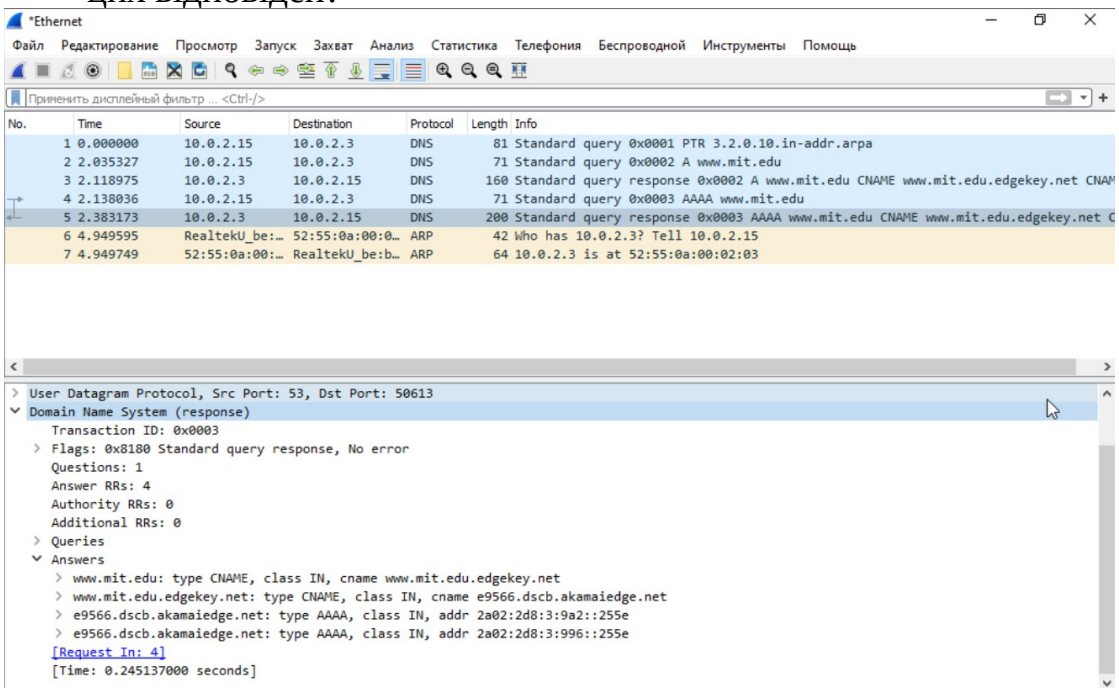
8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?
   10.0.2.15 Так є адресою локального сервера.

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

Цей запит – є запитом стандартного типу. Вміщує.

```
Transaction ID: 0x0003
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[Response In: 5]
```

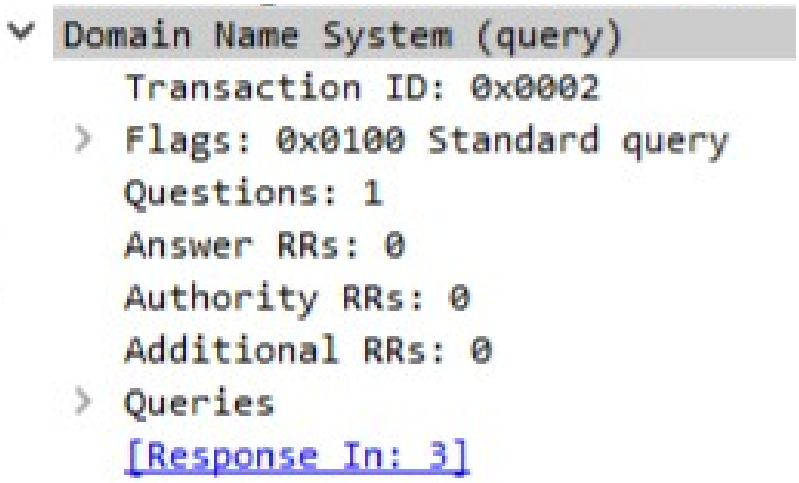
10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?



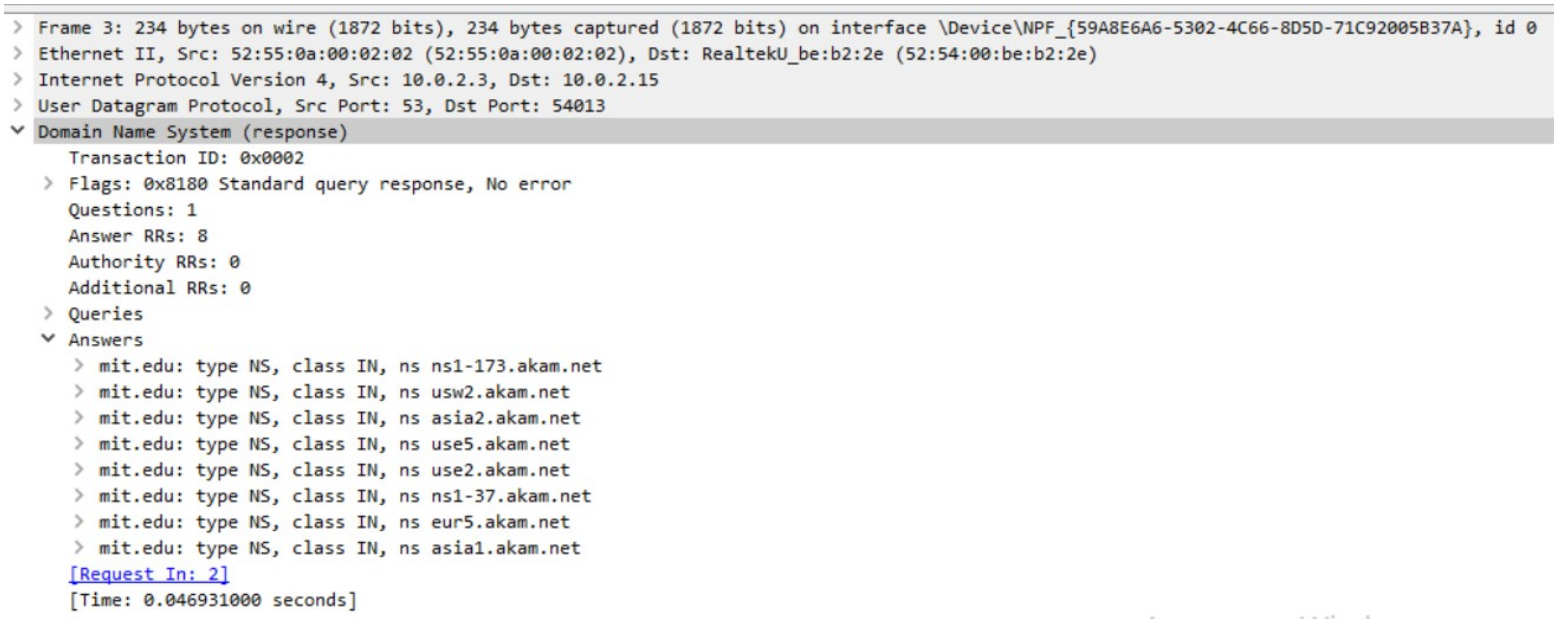
11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

IP: 10.0.2.15 Так є.

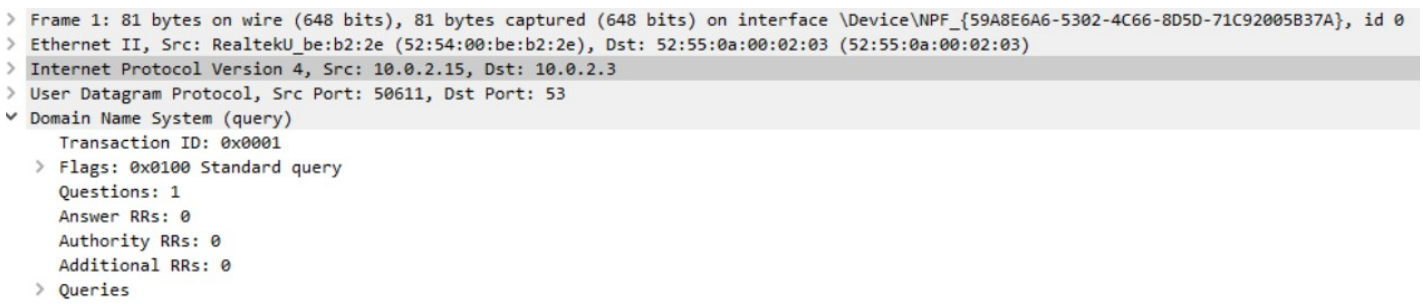
12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?



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?

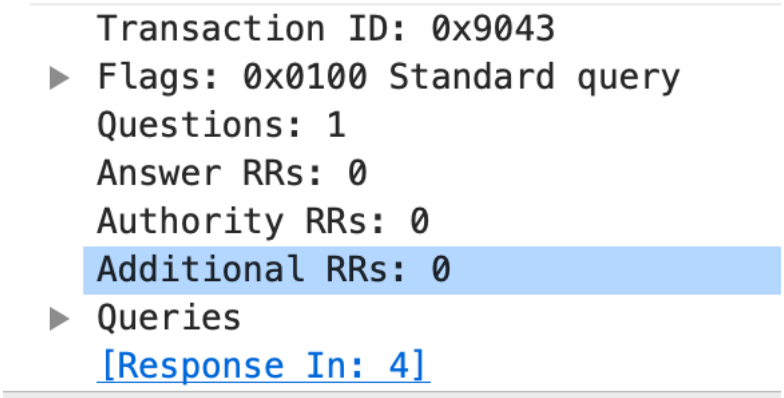


14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?
IP: 10.0.2.15 є адресою локального сервера.



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

Стандартний тип запиту. вміщує.



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

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.