НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС

«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИЕТУ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

**ЛАБОРАТОРНА РОБОТА № 3**

з дисципліни

Комп’ютерні мережі

Студента 3 курсу групи ІСЗП-93

Спеціальність 122 Комп’ютерні науки

Чех Олексій Васильович

Київ – 2020 рік

**Необхідно виконати наступні дії:**

1. Очистіть кеш DNS-записів

a. для windows-систем виконайте в терміналі ipconfig /flushdns

b. для linux-систем (можливо) спрацює перезапуск операційної системи;

2. Запустіть веб-браузер, очистіть кеш браузера:

a. для Firefox виконайте Tools >> Clear Private Data (або Ctrl + Shift + Del)

b. для MS IE виконайте Tools >> Internet Options >> Delete File

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.

8. Почніть захоплення пакетів.

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

a. nslookup [www.mit.edu](http://www.mit.edu)

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

a. 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.aiit.or.kr bitsy.mit.edu

18. Зупиніть захоплення пакетів.

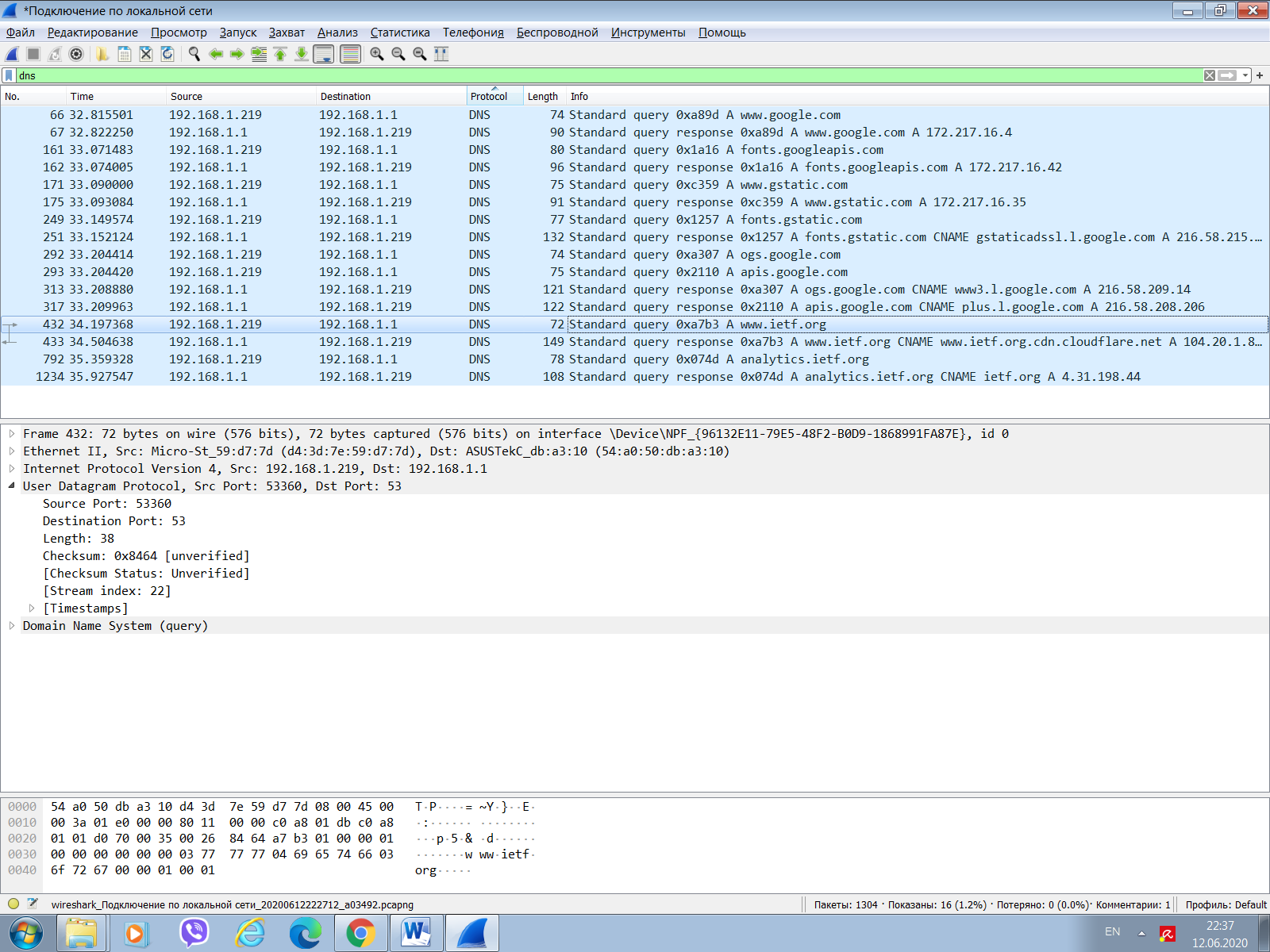
19. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.

20. Закрийте Wireshark.

**Контрольні запитання:**

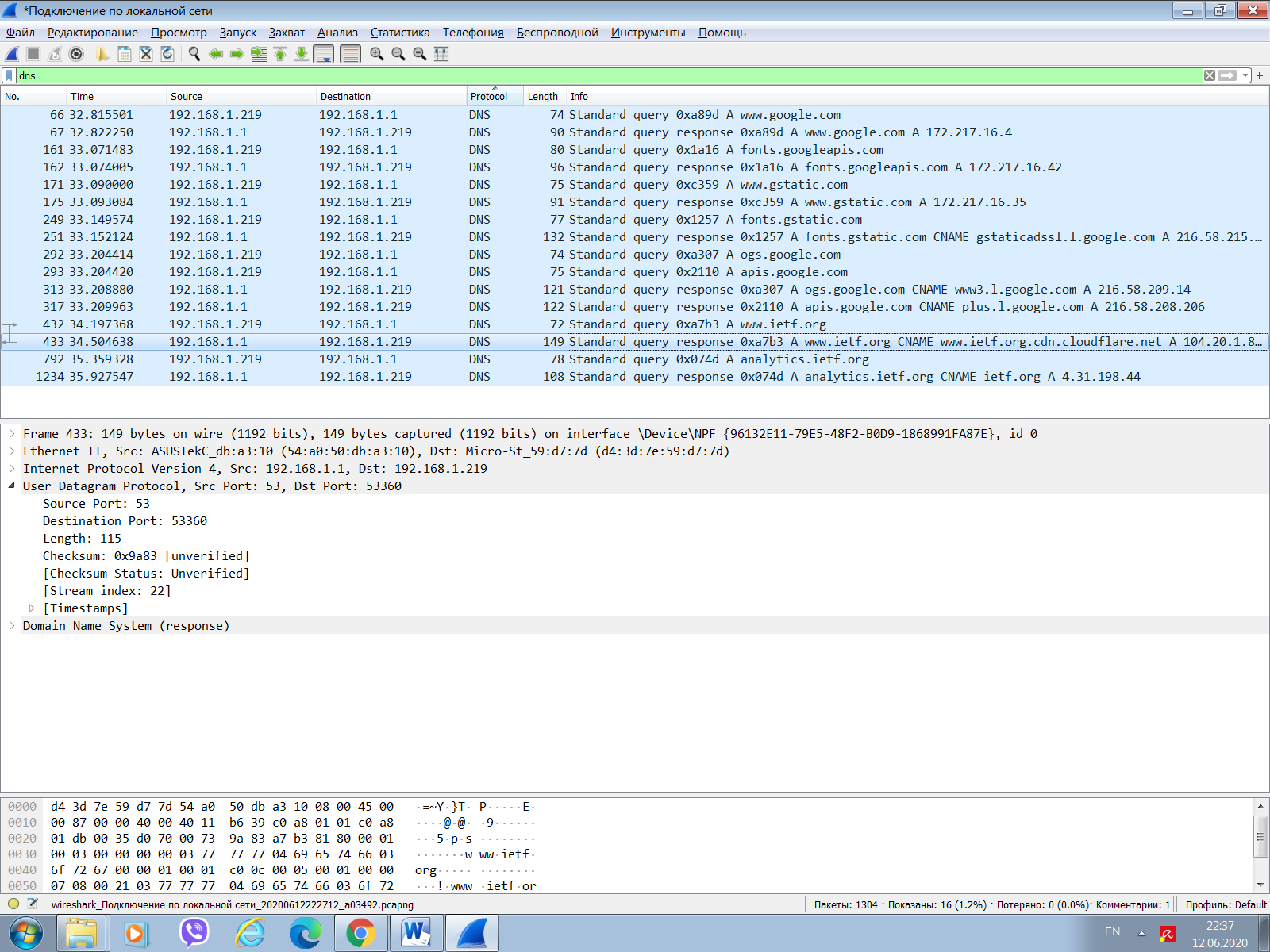
1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

**Відповідь:** використовується протокол UDP (і запит, і відповідь)



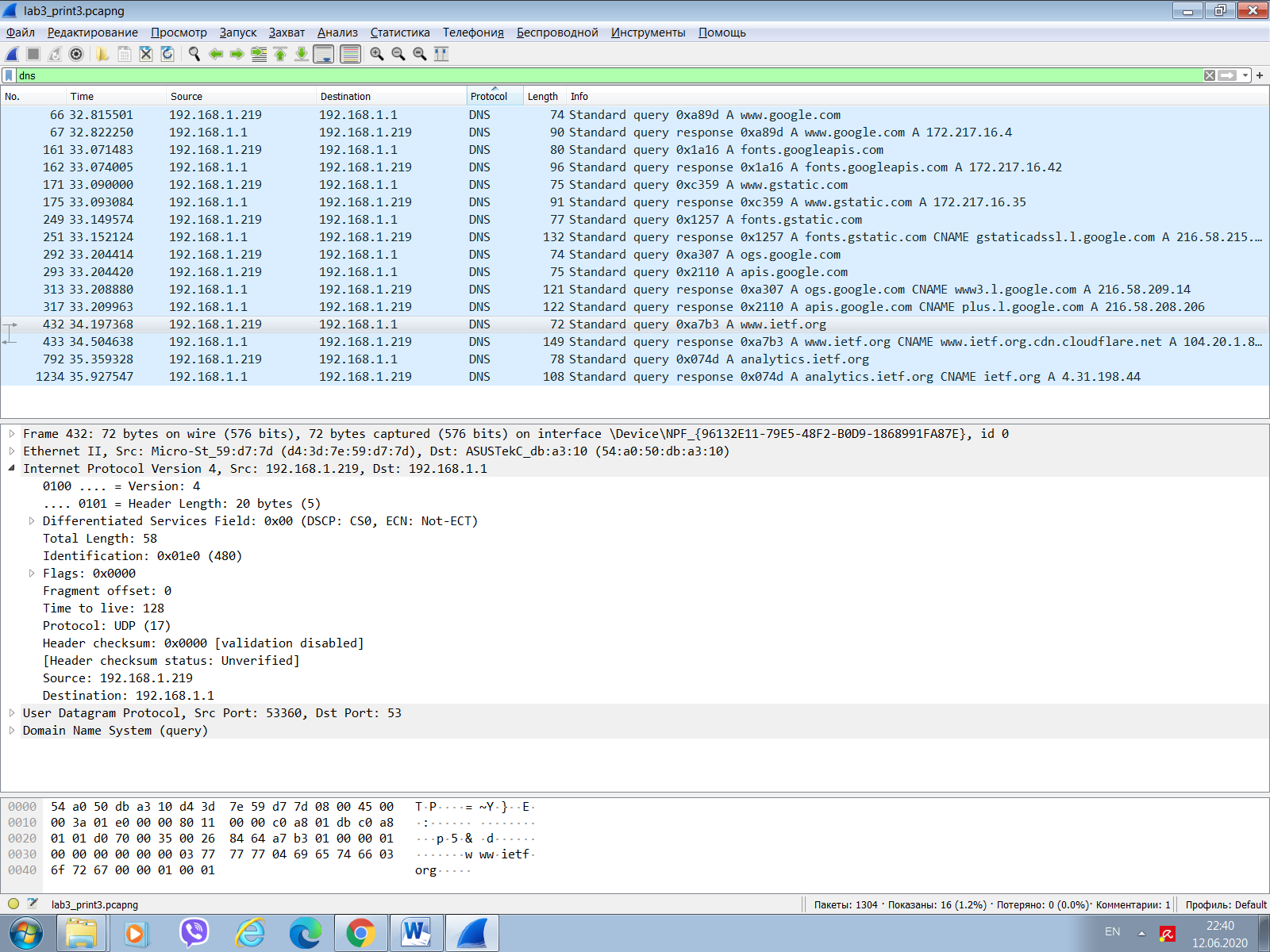
При цьому (у випадку запиту сторінки http://www.ietf.org ) використовується порт: 53360

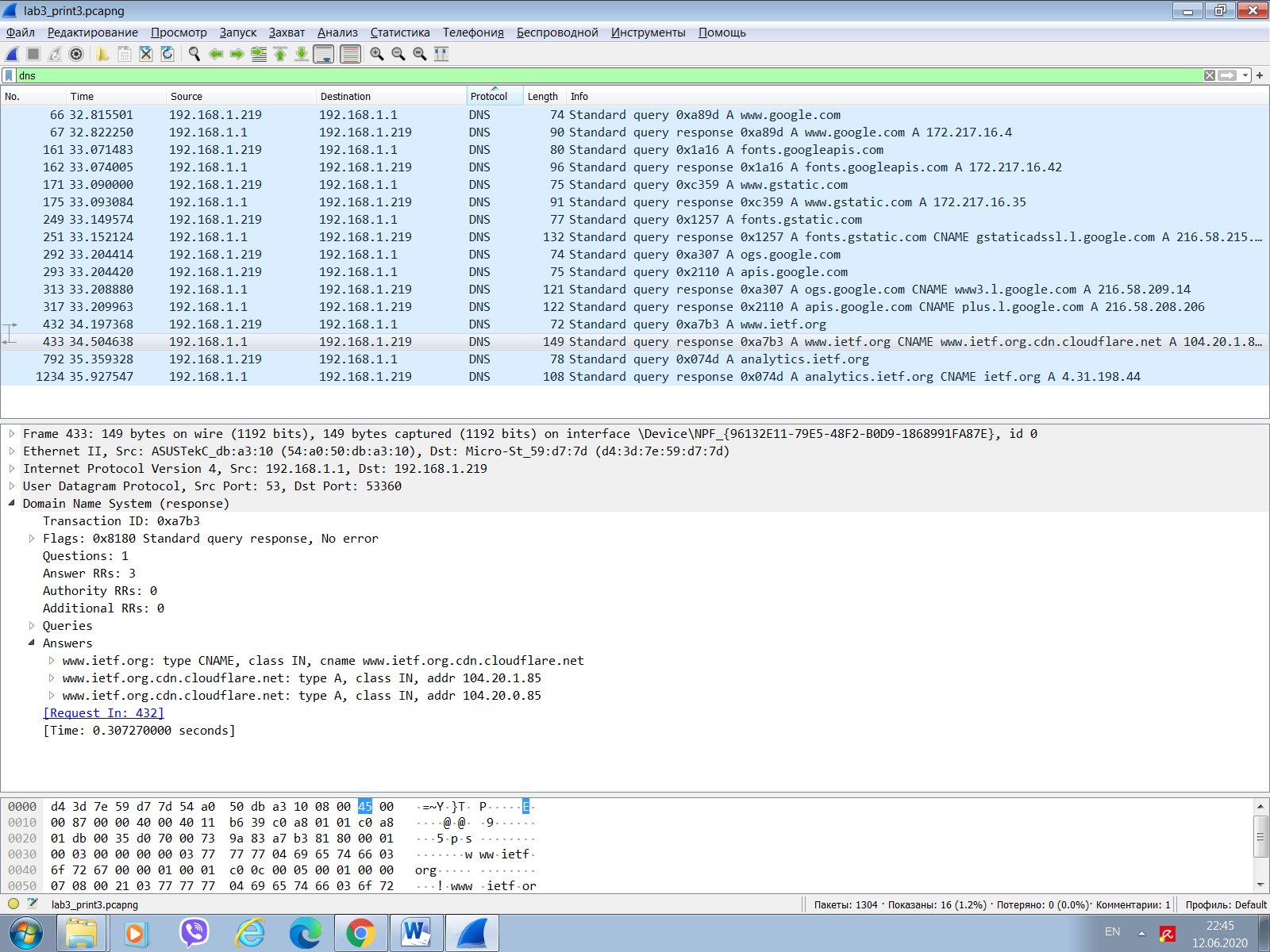
Номер вихідного порта відповіді: 53



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

**Відповідь:** IP-адреса: 192.168.1.1.

 Однак ця адреса не є адресою локального сервера DNS



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

**Відповідь:** З попереднього скріну видно, що тип CNAME (канонічне ім’я). Запит вміщує як «Тип», так і «клас», посилання на реальну IP-адресу (104.20.1/0.85)

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

**Відповідь:** з попереднього скріну видно, що відповідь DNS складається з 3-х відповідей:

**Тип CNAME** з найбільшим часом TTL (1800 проти 300 у двох наступних відповідях)

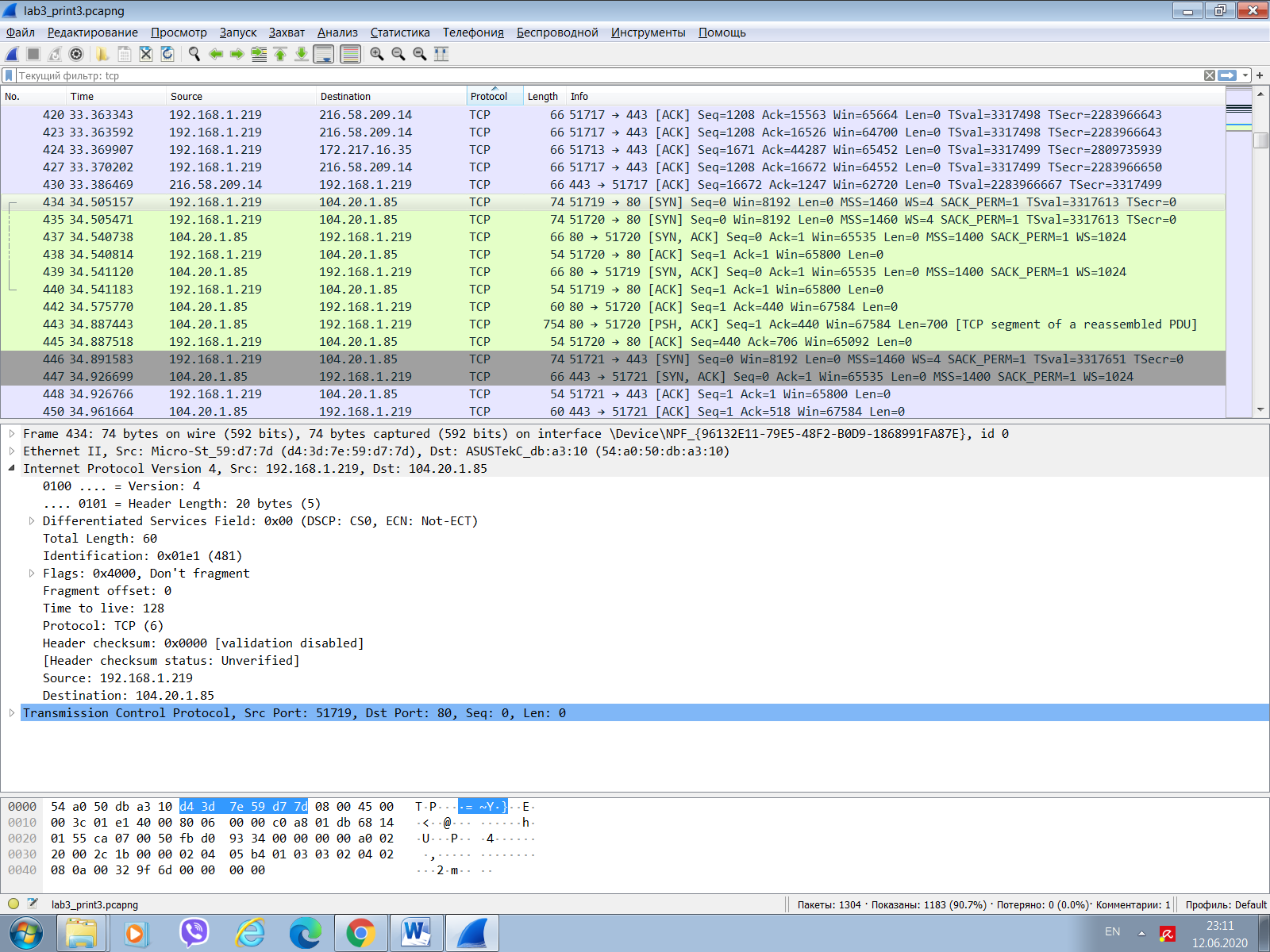
**Тип А з адресою 104.20.1.85**

**Тип А з адресою 104.20.0.85**

В обох випадках, хоча IP-адреса перенаправляє нас до Сан-Франциско, США, хоча

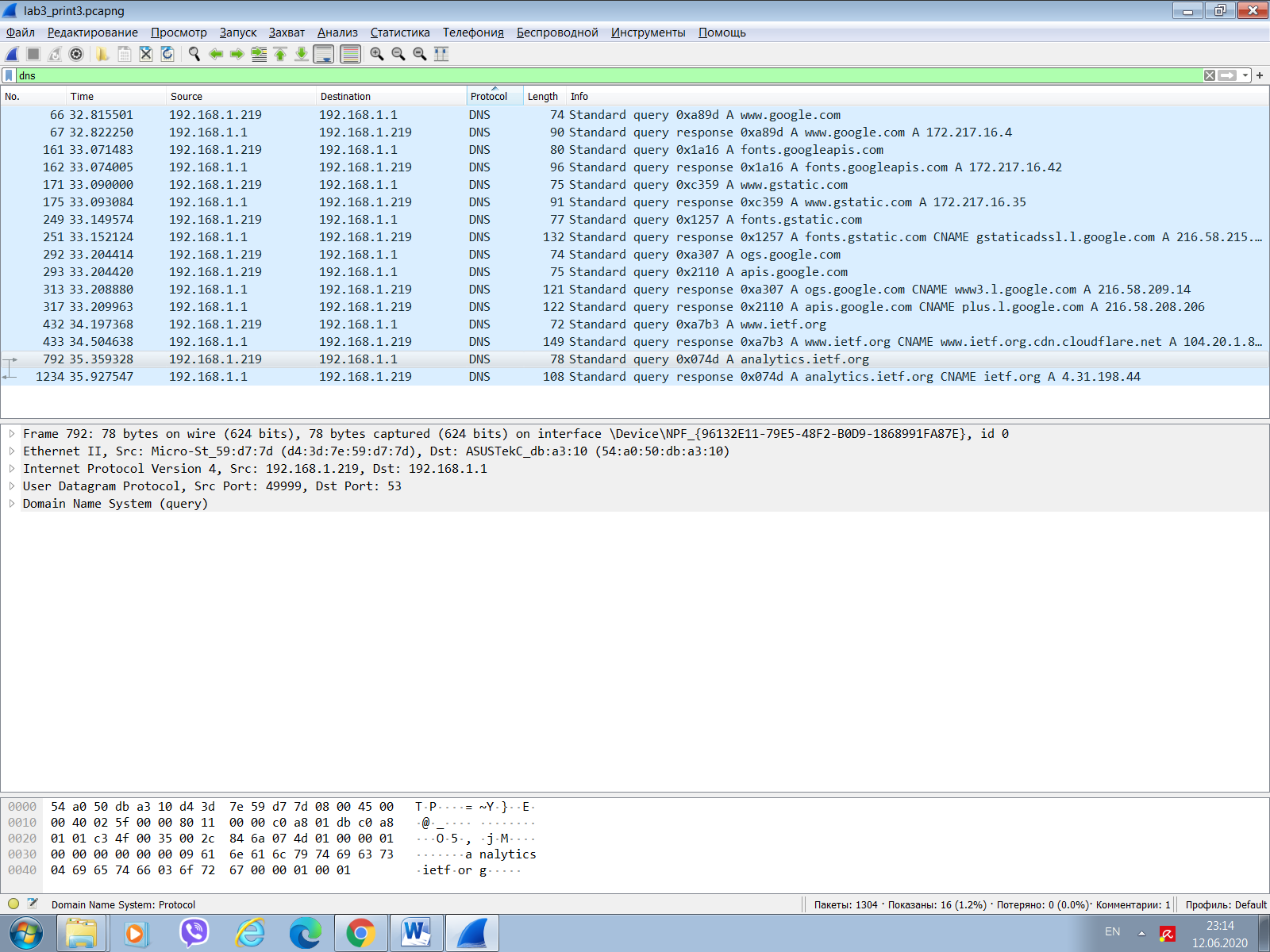
1. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

**Відповідь:**  так, співпадає з одною із запропонованих IP-адрес (104.20.1.85)



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

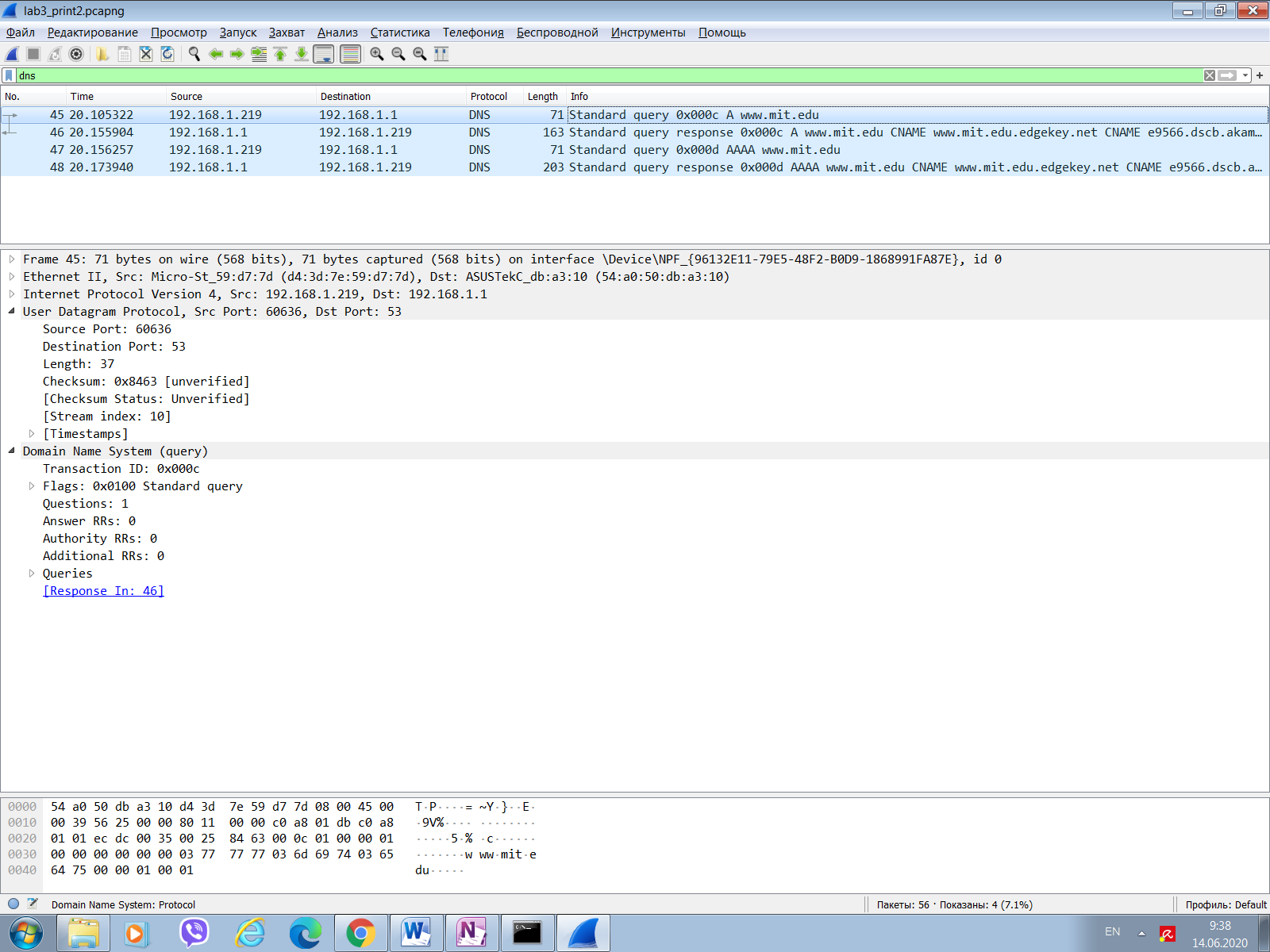
**Відповідь:** так, був направлений запит щодо аналітики сайту ietf.org (analytics.ietf.org)



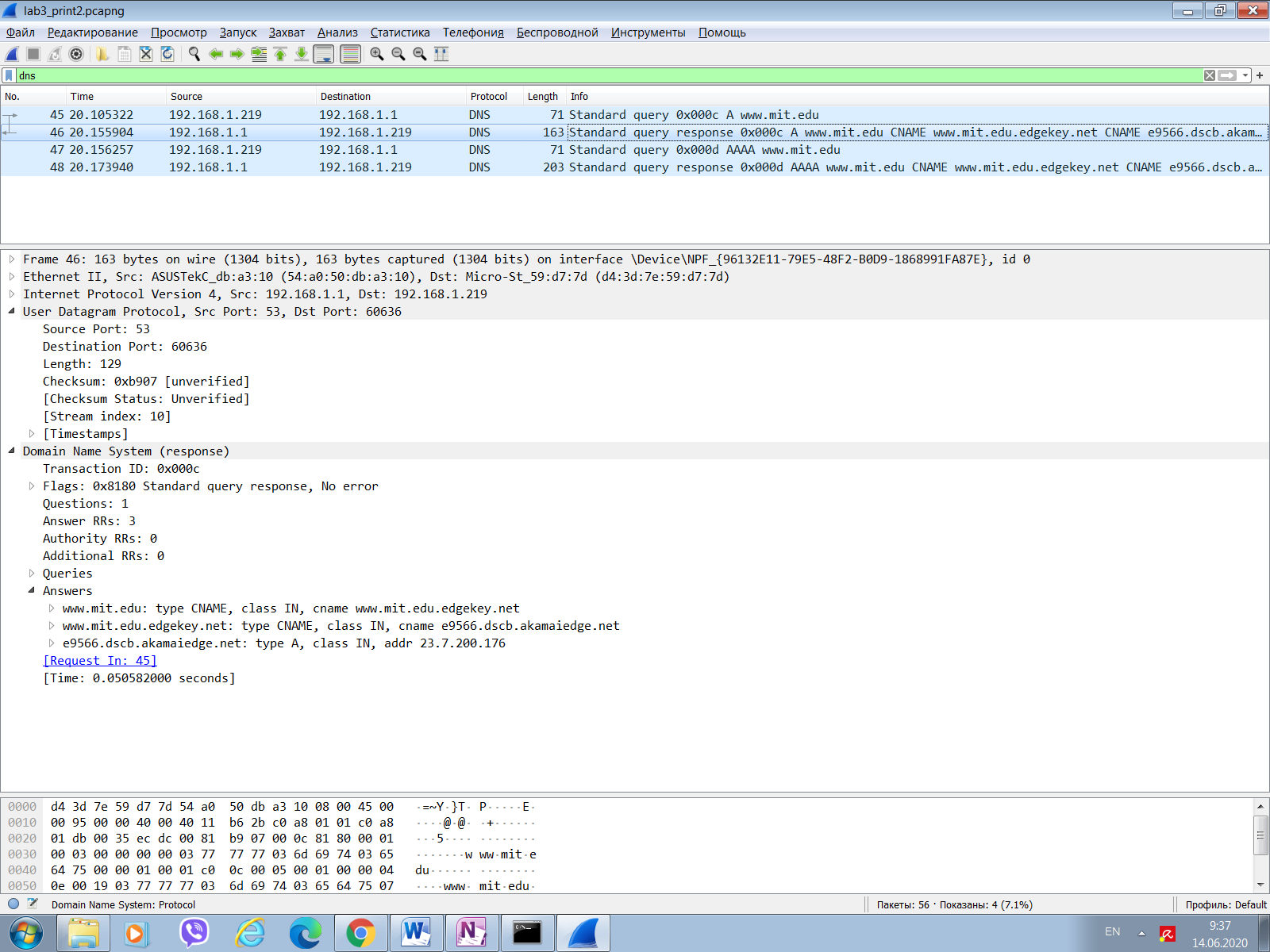
1. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

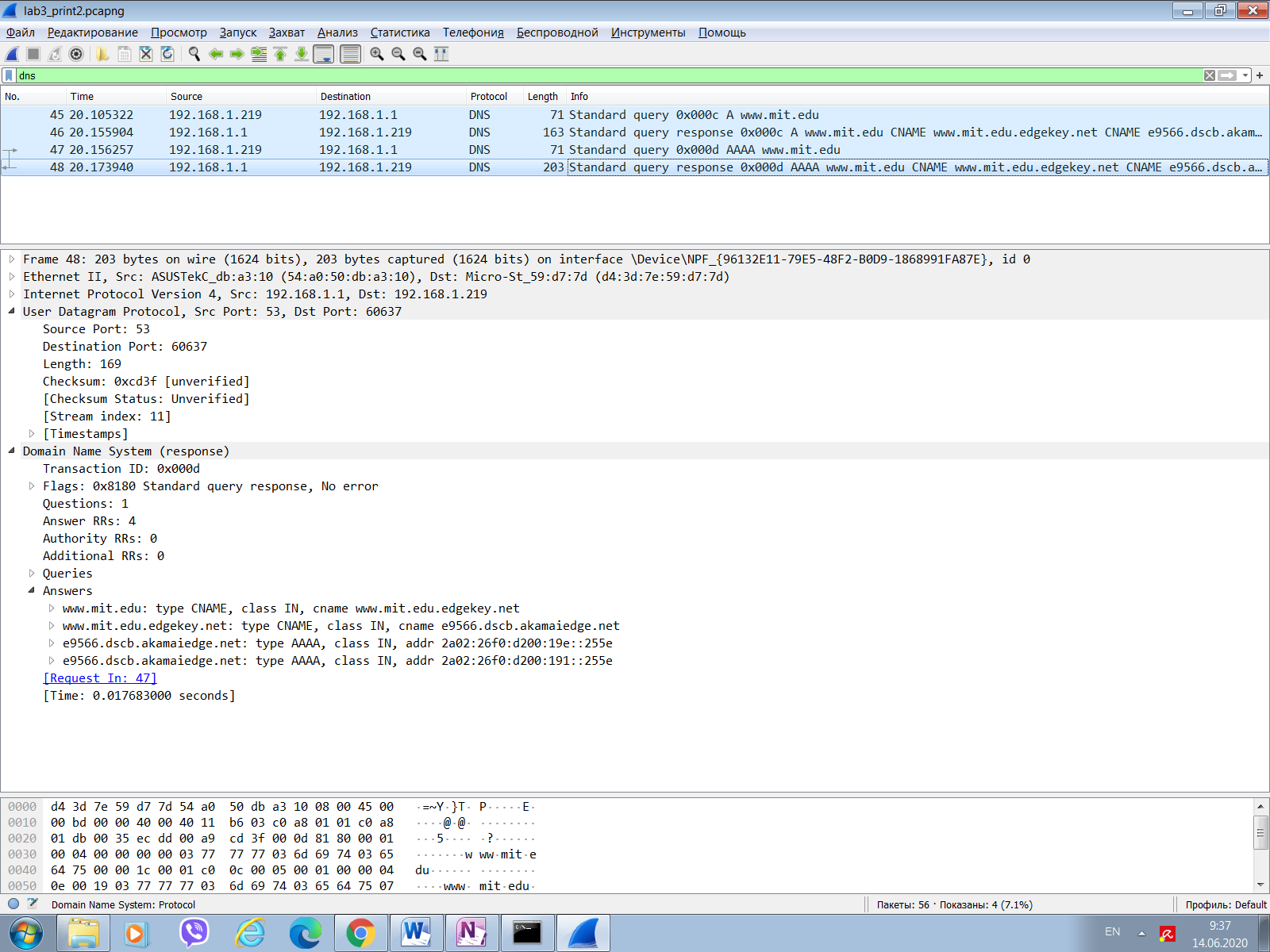
**Відповідь:**

Цільовий порт повідомлення із запитом: 53



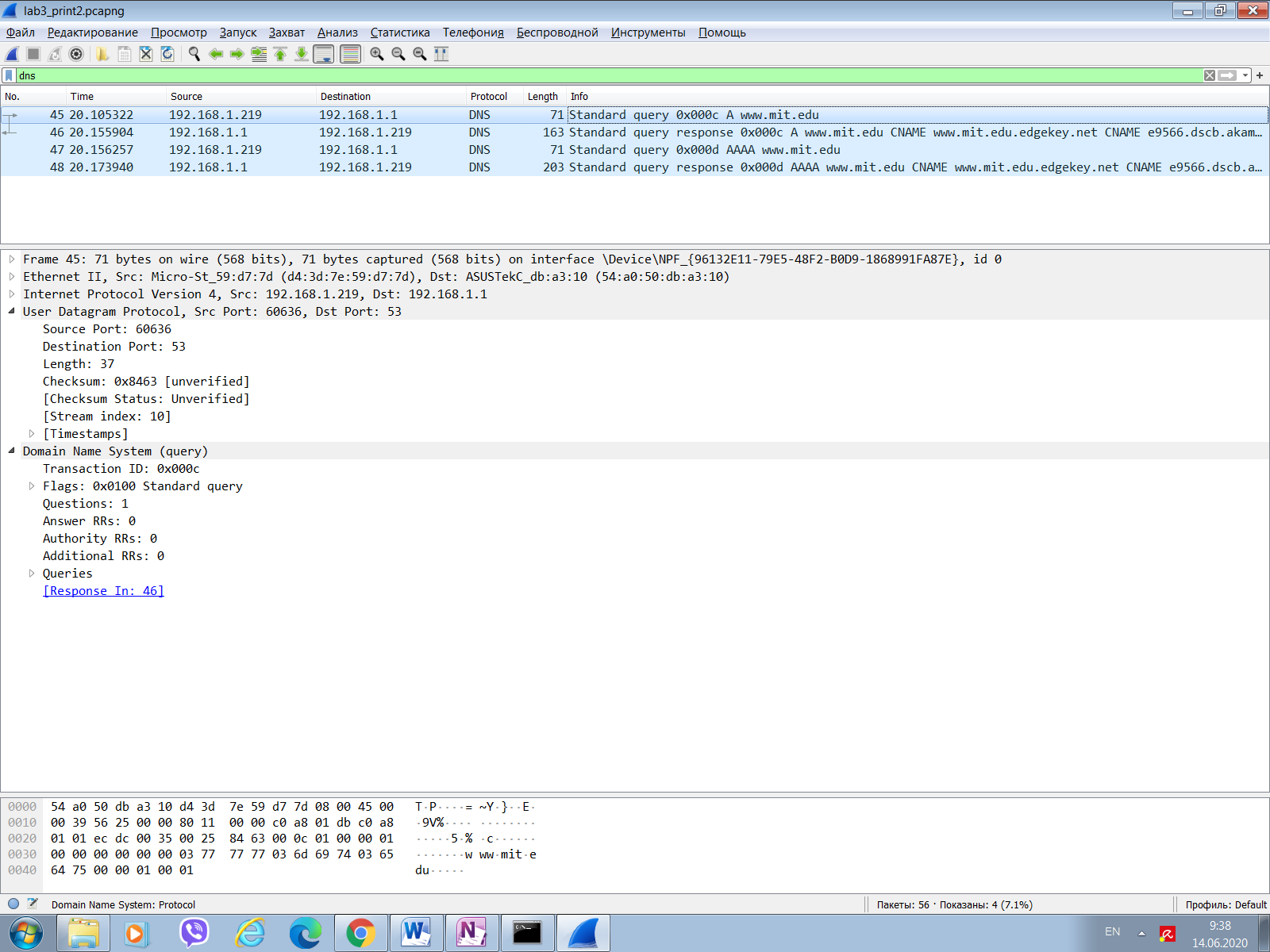
Вихідний порт повідомлення із відповіддю: 60636/60637



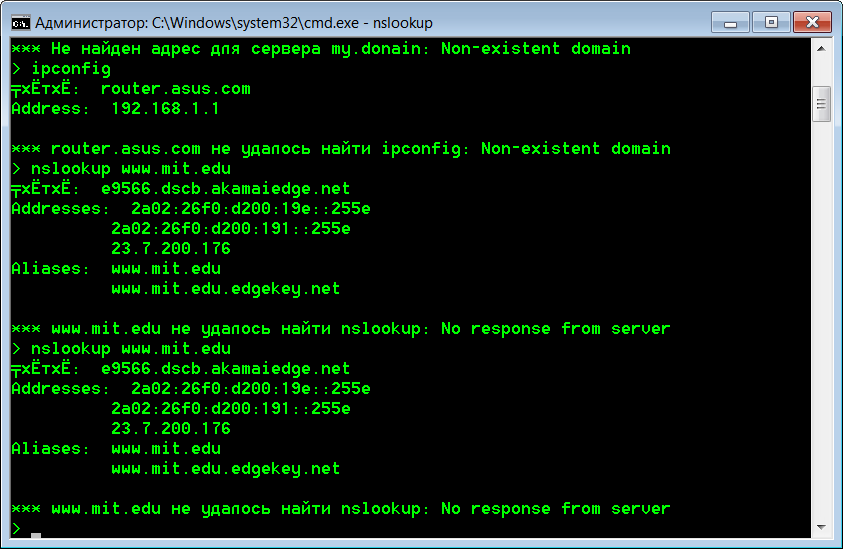


1. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

**Відповідь:** на наступну IP-адресу: 192.168.1.1

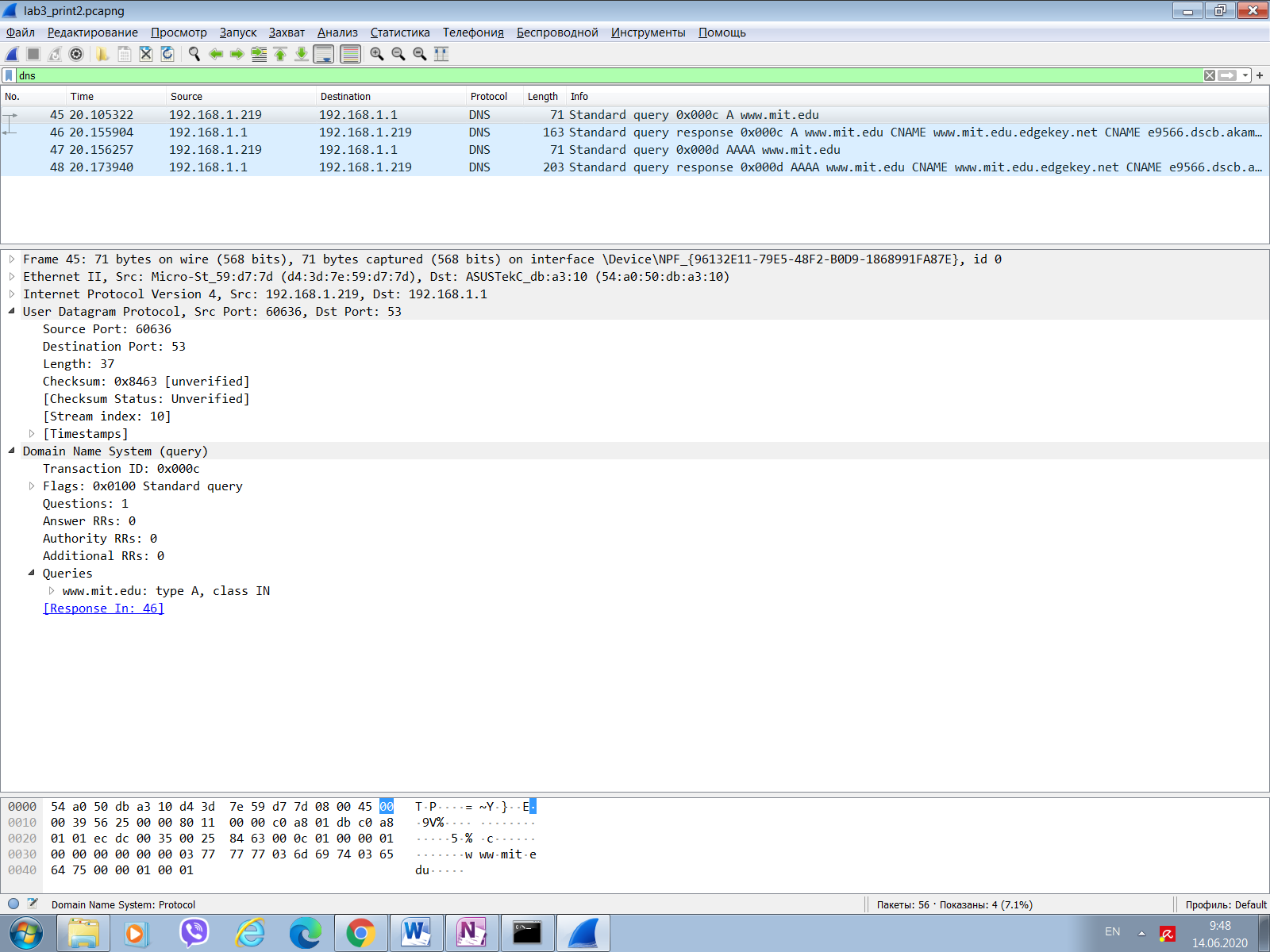


Що відповідає адресі мого локального сервера

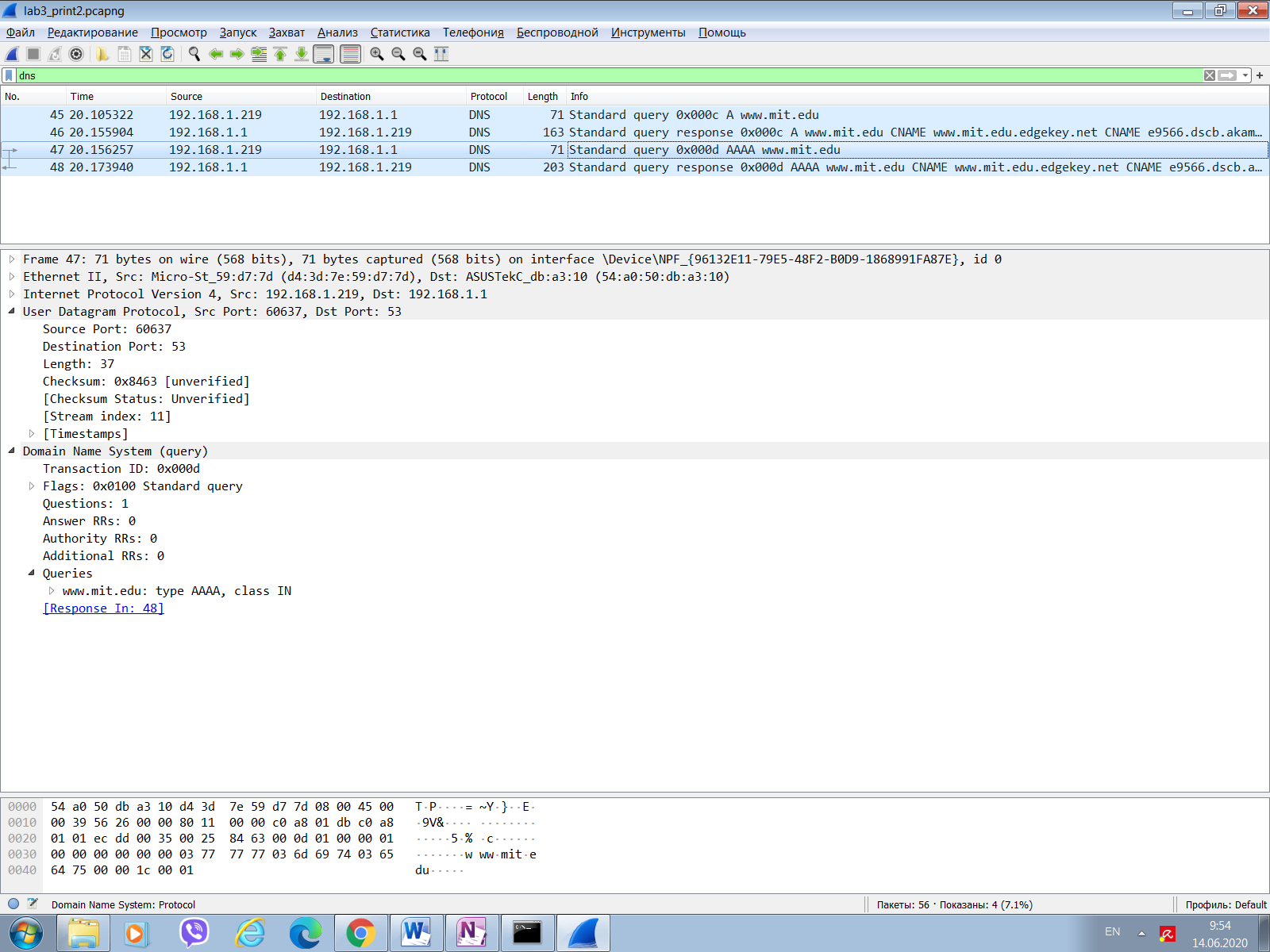


1. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

**Відповідь:** Типу «А» (псевдонім хосту), Класу «IN» (Інтернет). Тобто запит вказує де шукати і в якому форматі шукається ім’я.



Другий запит мав вже тип «АААА», посилаючись вже не на IPv4-адресу, а на IPv6

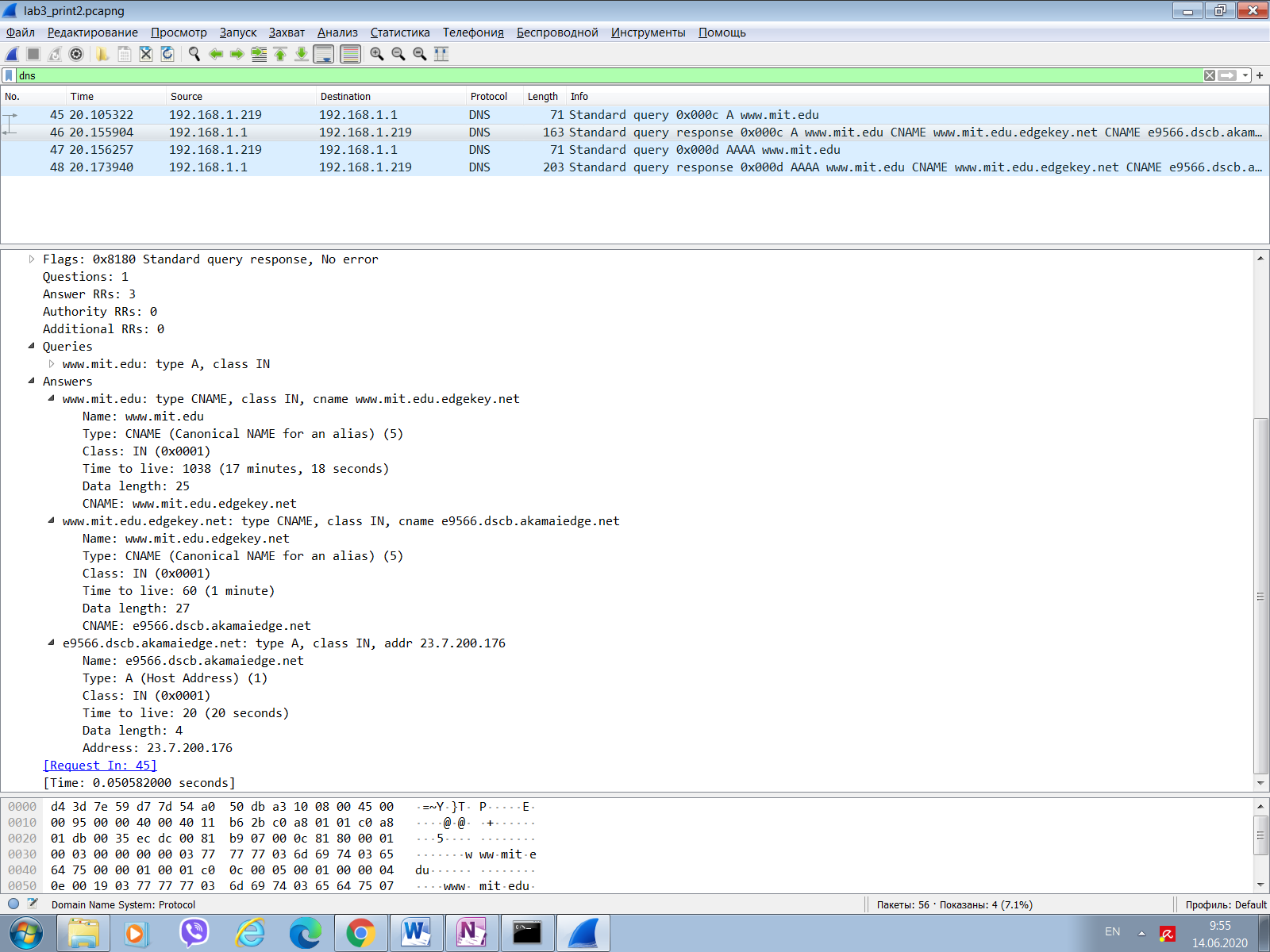


1. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?

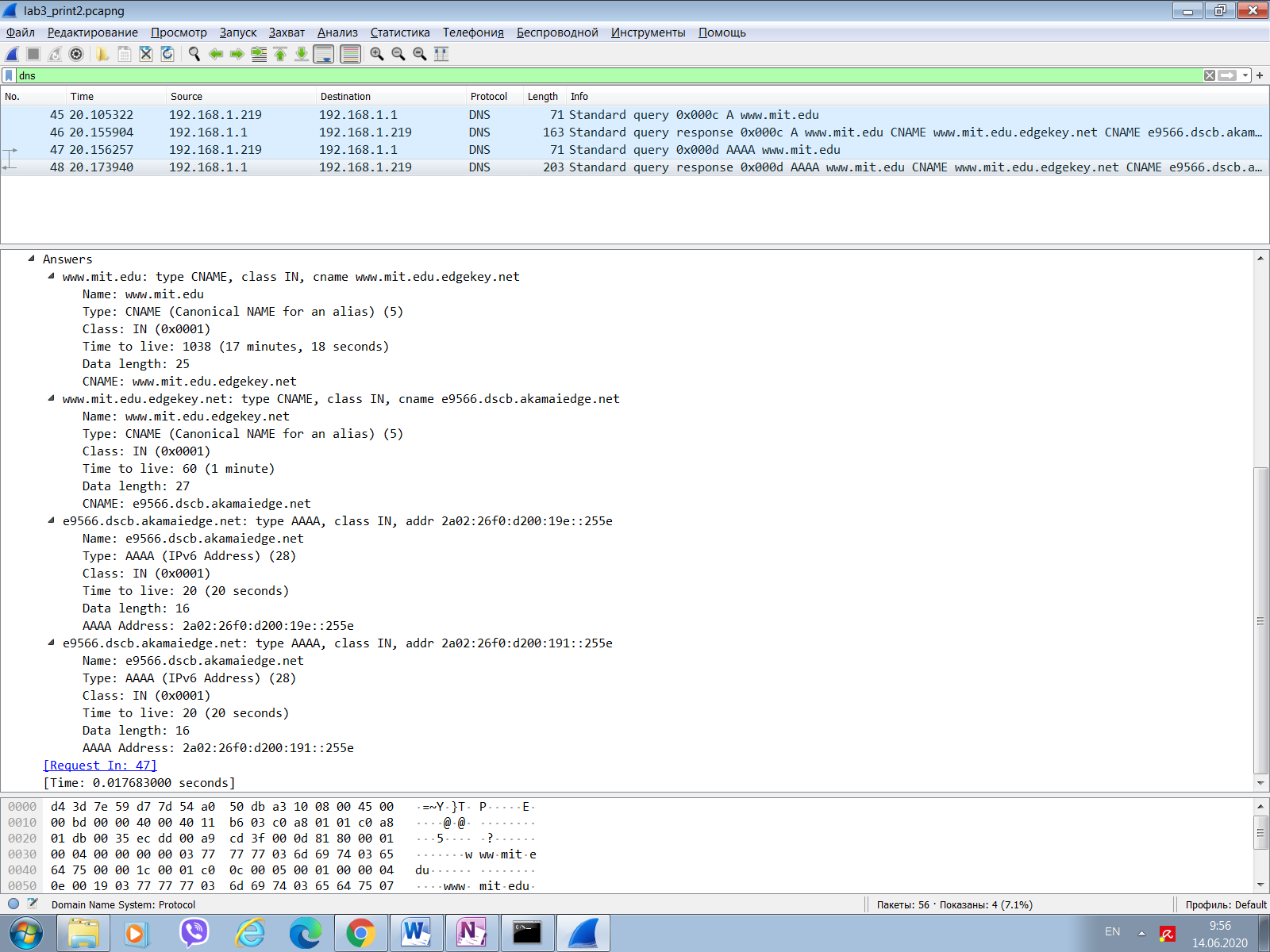
**Відповідь:** було запропоновано два записи із відповідями DNS, в першому випадку тип «А» (як відповідно ми і запитали), в другому – тип «АААА».

У першому випадку це такий ланцюжок запитів: www.mit.edu -> www.mit.edu.edgekey.net -> e9566.dscb.akamaiedge.net -> 23.7.200.176

У другому випадку це такий ланцюжок запитів: www.mit.edu -> www.mit.edu.edgekey.net -> e9566.dscb.akamaiedge.net -> 2a02:26f0:d200:**19e**:255e -> 2a02:26f0:d200:**191**:255e

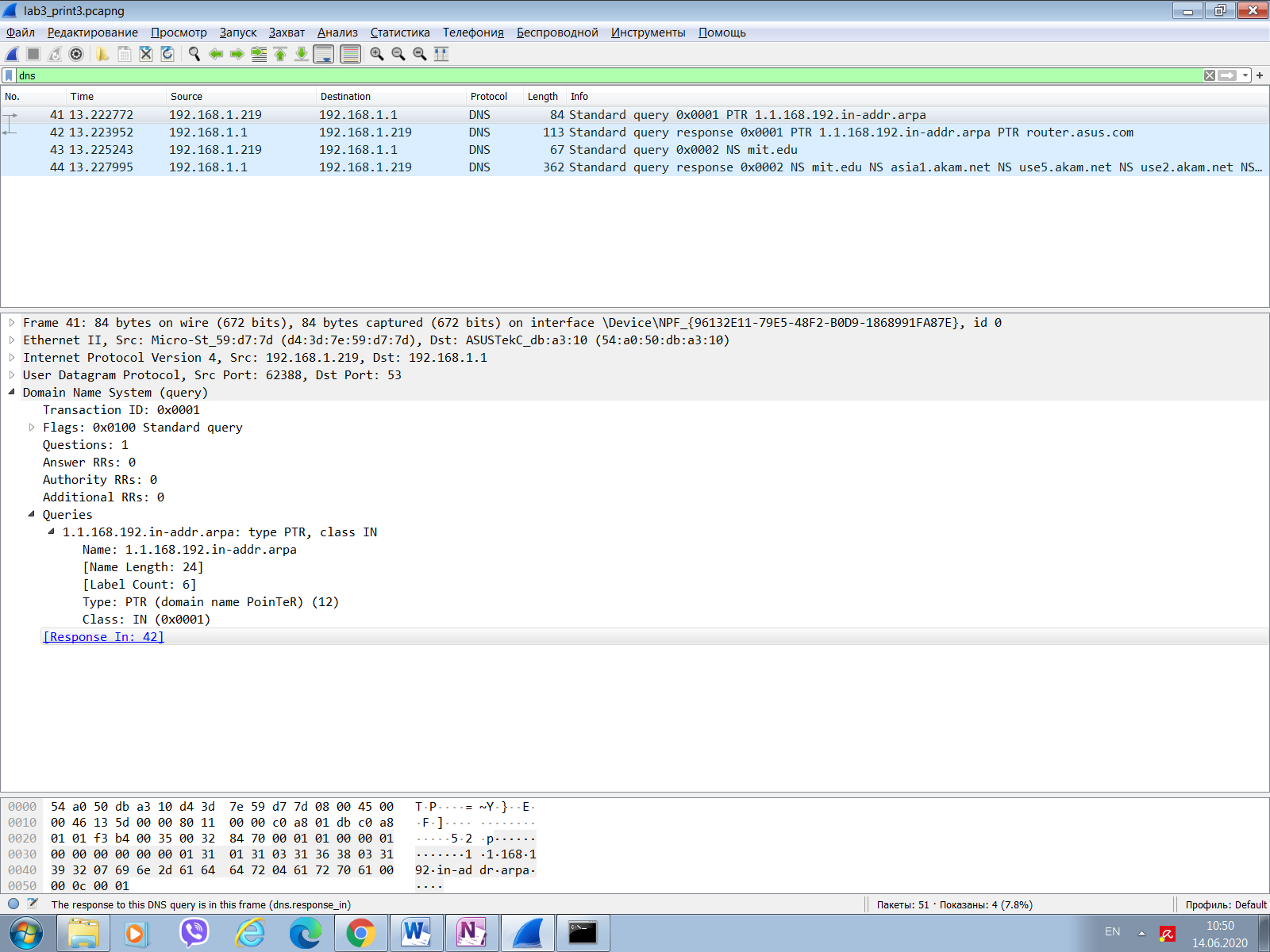


Сwww.mit.edu -> www.mit.edu.edgekey.net -> e9566.dscb.akamaiedge.net ->www.mit.edu -> www.mit.edu.edgekey.net -> e9566.dscb.akamaiedge.net ->



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

**Відповідь:** запит був відправлений на мою IP-адресу: 192.168.1.1

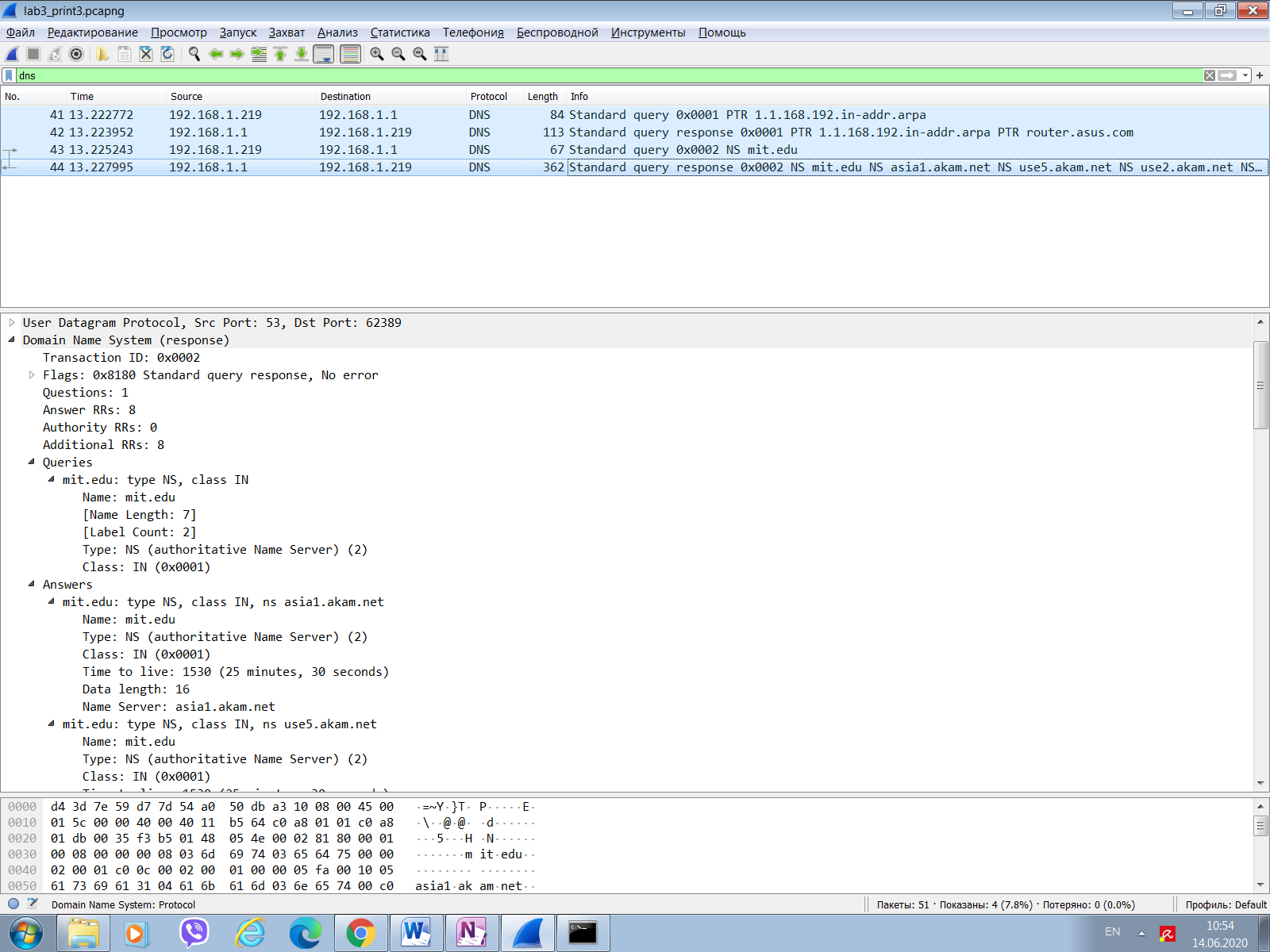


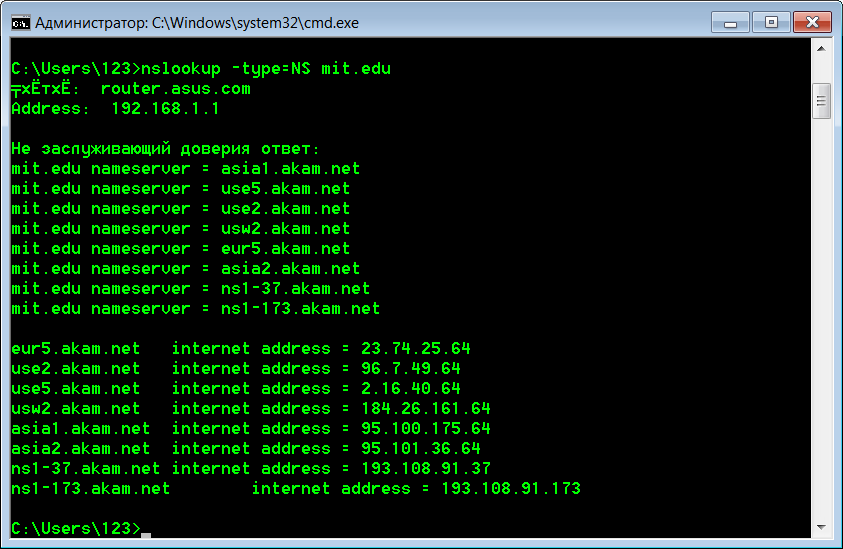
1. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

**Відповідь:** тип першого запиту DNS - «PTR» (вказівник), клас «IN», другого запиту – «NS».

1. 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?

**Відповідь:** 2 записів з відповідями було запропоновано сервером (з попереднього скану). При цьому змінюються цільові порти (з 62388-по 62389). При цьому пропонується ланцюжок відповідей на 8 дочірніх (NS) сервери:

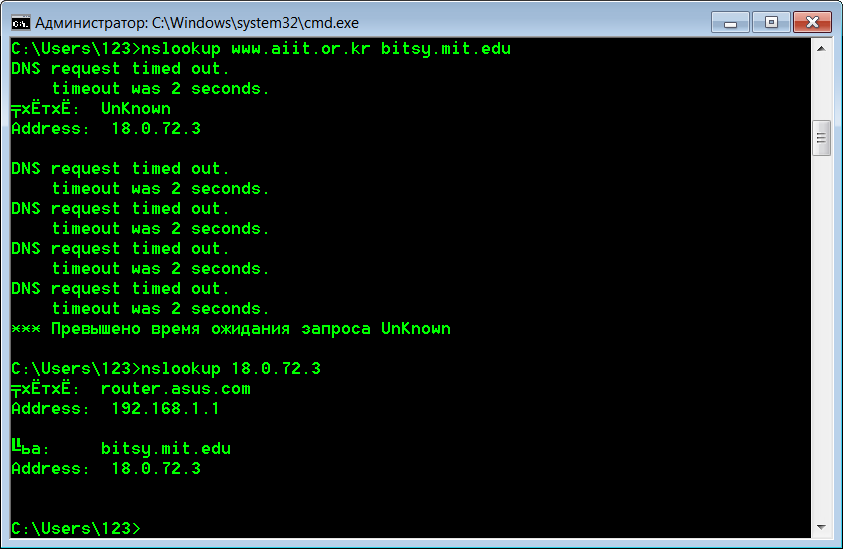


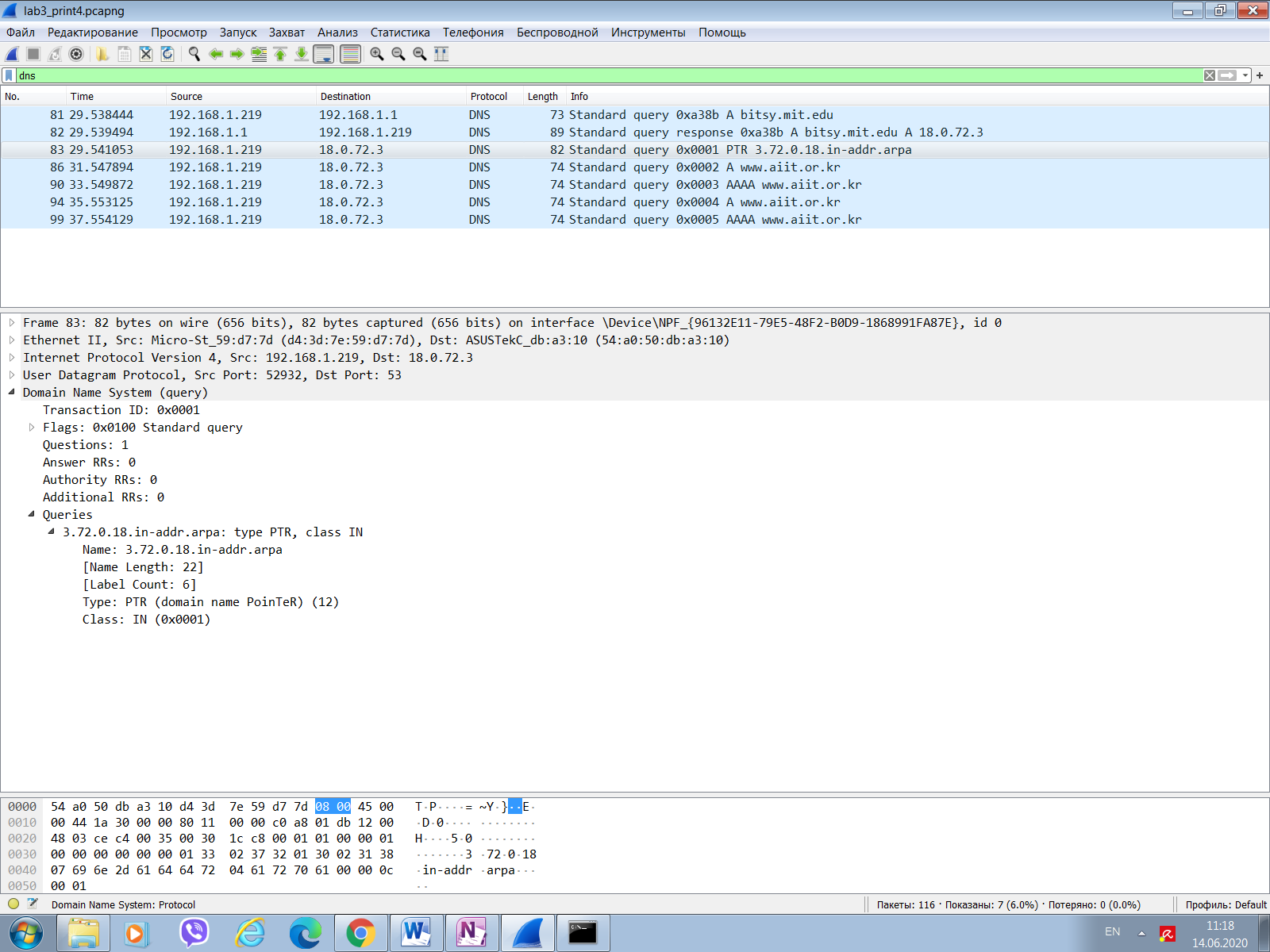


1. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

**Відповідь:** запит щодо bitsy.mit.edu був відправлений на мою IP-адресу: 192.168.1.1

Запит щодо aiit.or.kr був відправлений на IP-адресу: 18.0.72.3, що відповідає доменному імені bitsy.mit.edu





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

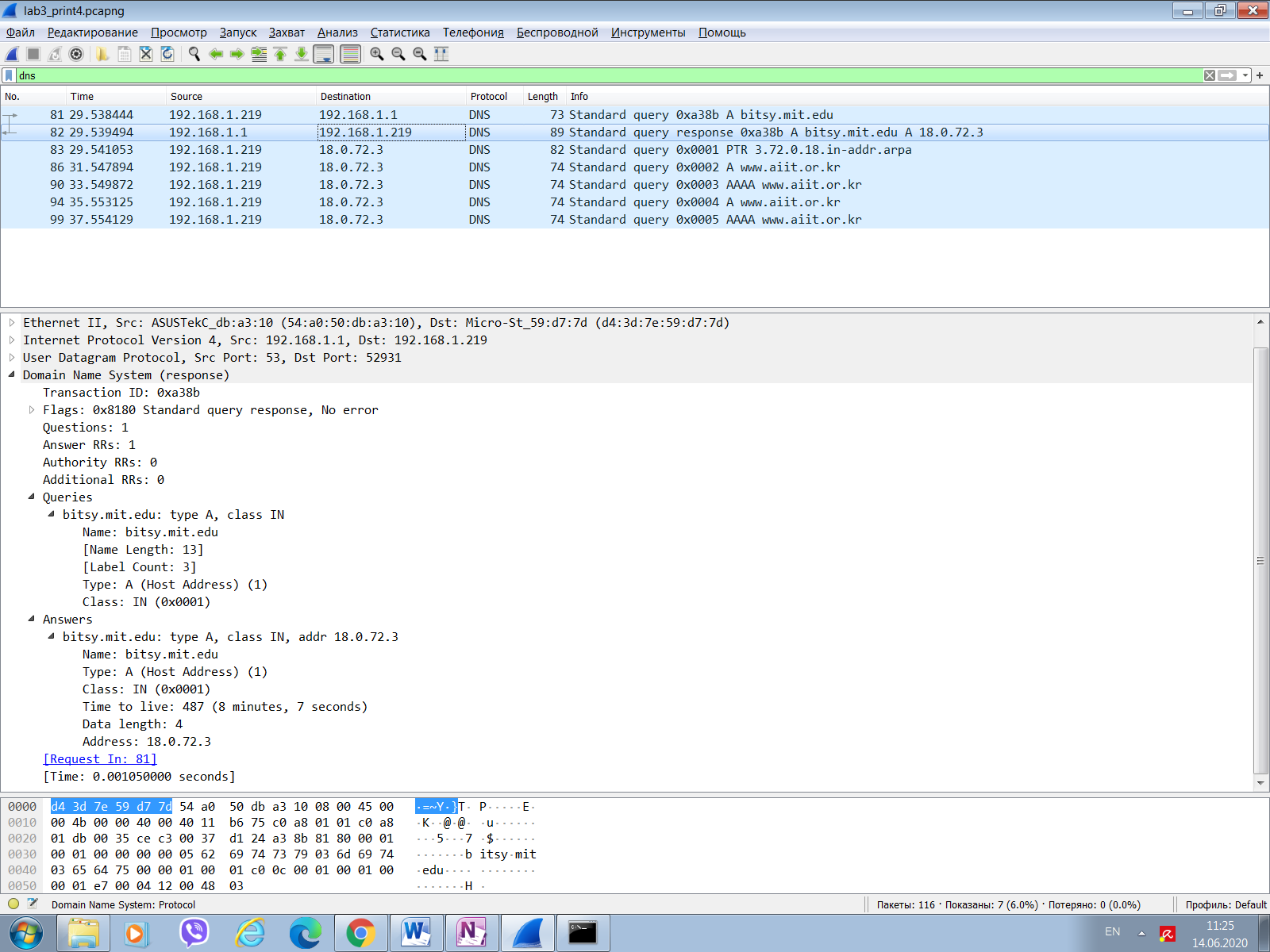
**Відповідь:**

Запити були типу «А» (на що була отримана відповідь), потім «PTR», «A», «AAAA», «A», «AAAA». Враховуючи те, що було відображено в cmd-вікні, схоже на те, що браузер направляв запити по кільком різним типам, проте на одну і ту саму IP-адресу.

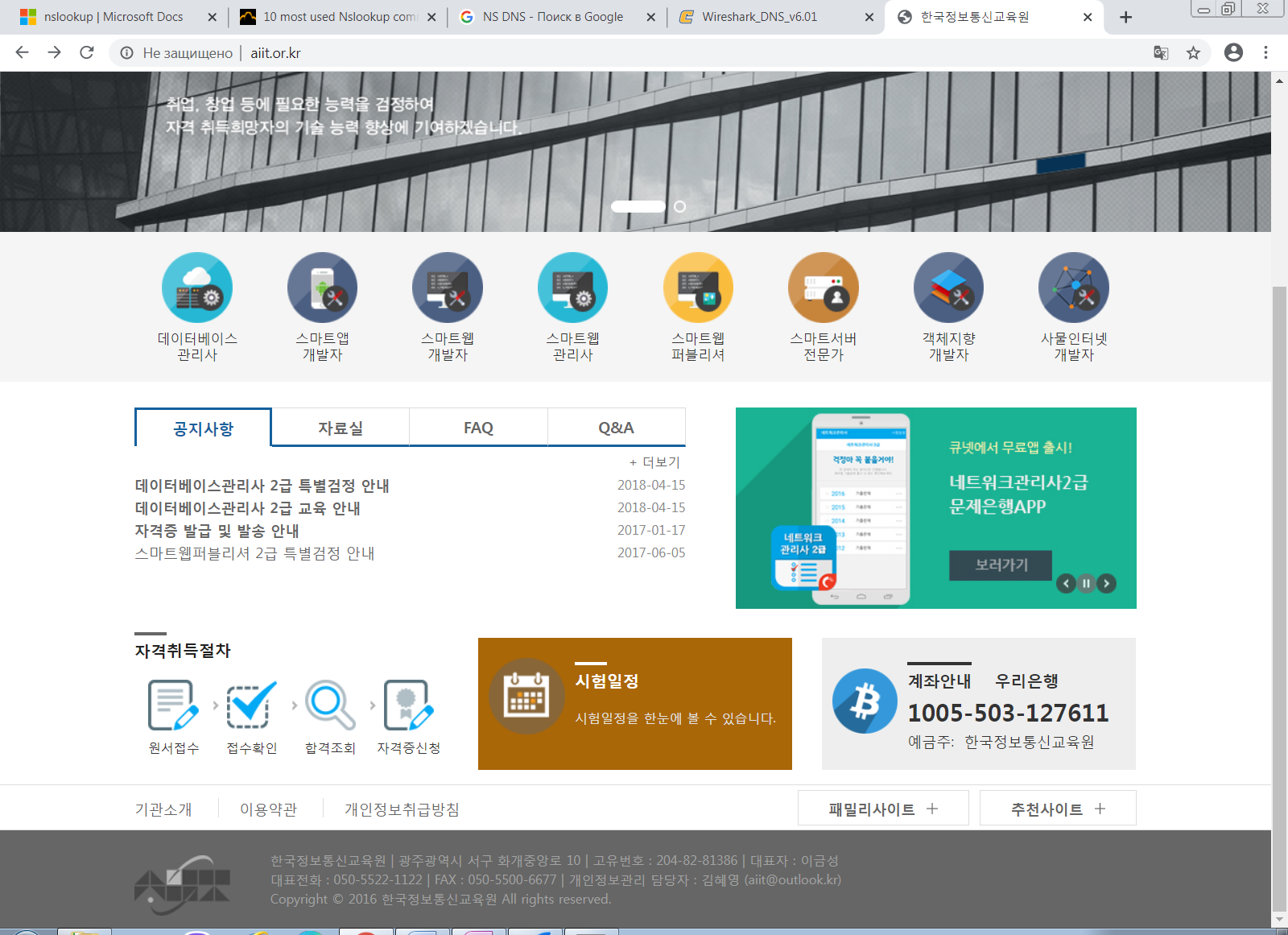
1. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

**Відповідь:**

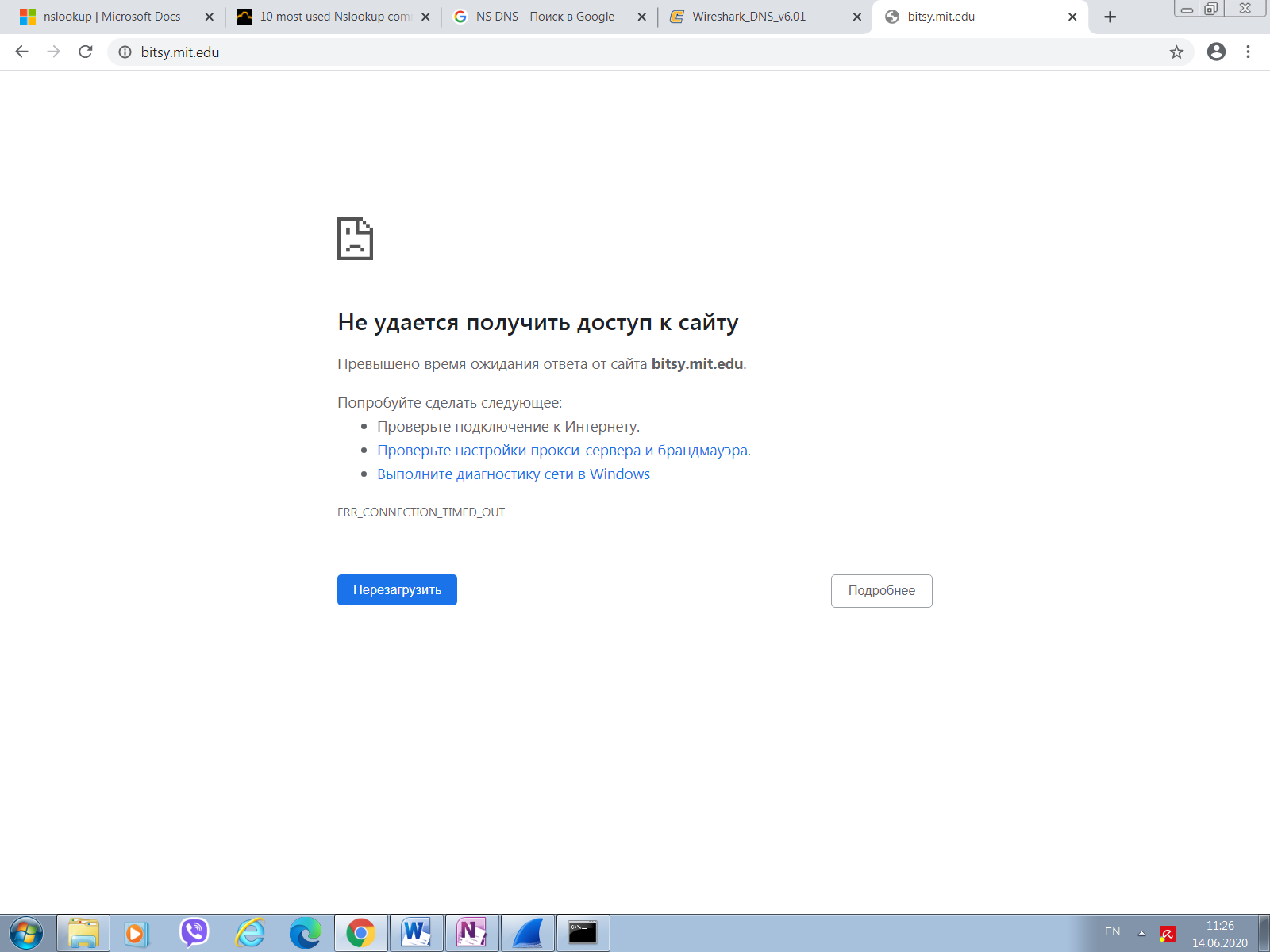
Відповідь була надіслана лише одна, в якій і був вказаний шукана IP-адреса (18.0.72.3), по якій потім пішли наступні 5 запитів без відповіді.



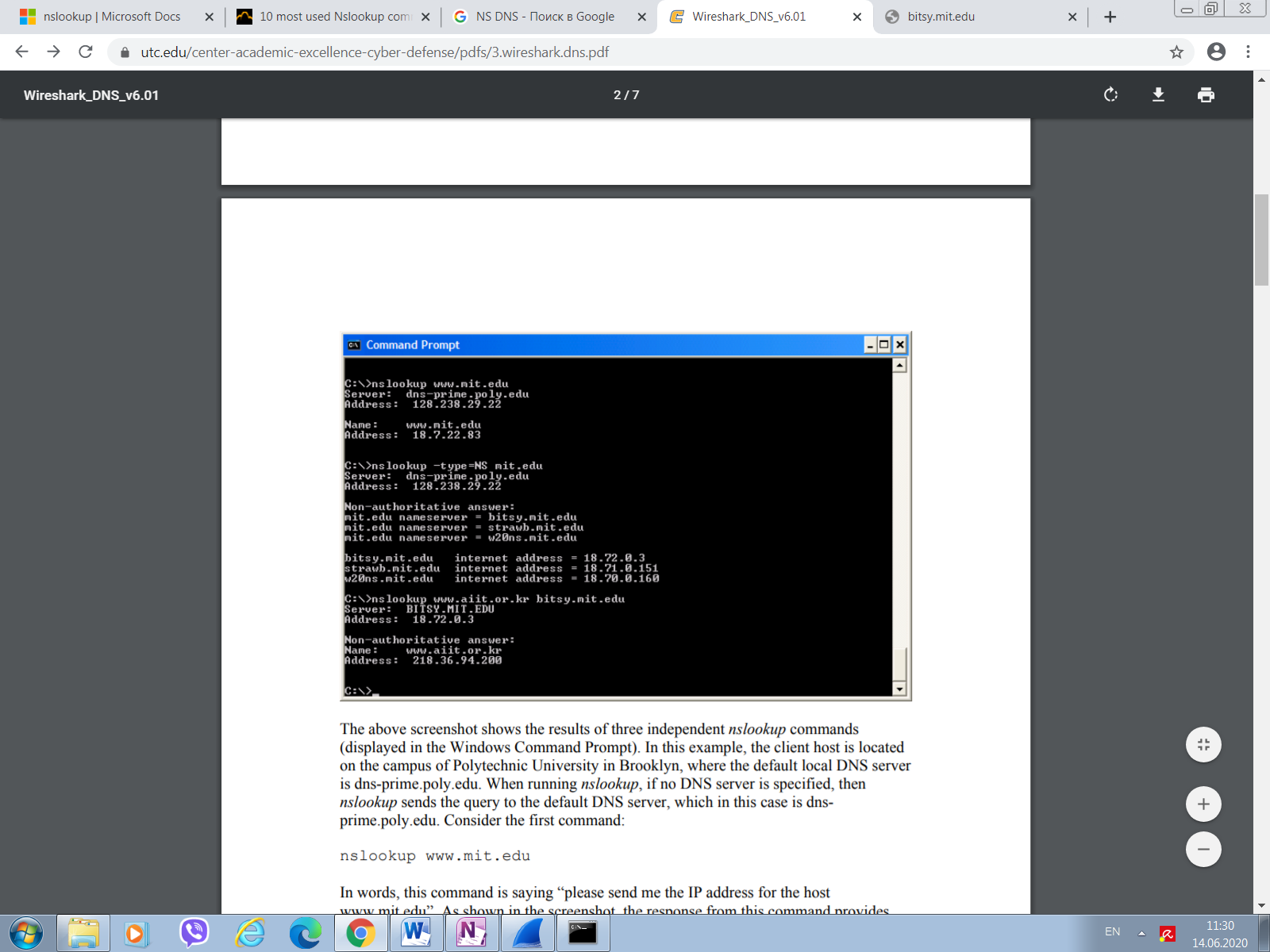
Такі самі результати були отримані при наочній перевірці: доступ до південнокорейського сайту інституту aiit.or.kr



Доступ до bitsy.mit.edu



З іншої сторони, я знайшов через Google-пошук сторінку із підручника [Wireshark Lab: DNS v6.01](https://www.utc.edu/center-academic-excellence-cyber-defense/pdfs/3.wireshark.dns.pdf) (2005), звідки можна дійти висновку, що відповідь мала б бути трохи іншою (щонайменше щодо bitsy.mit.edu, де не заслуговуючи на довіру відповіді мали також включати дочірні імена strawb.mit.edu, v20ns.mit.edu – IP-адреси схожі; а aiit.or.kr мала знаходитися за іншою IP-адресою):



**Форма звітності:** роздруківки збережених в ході ЛР пакетів з фаміліями, ініціалами та групами виконавців (бажано на кожній сторінці)