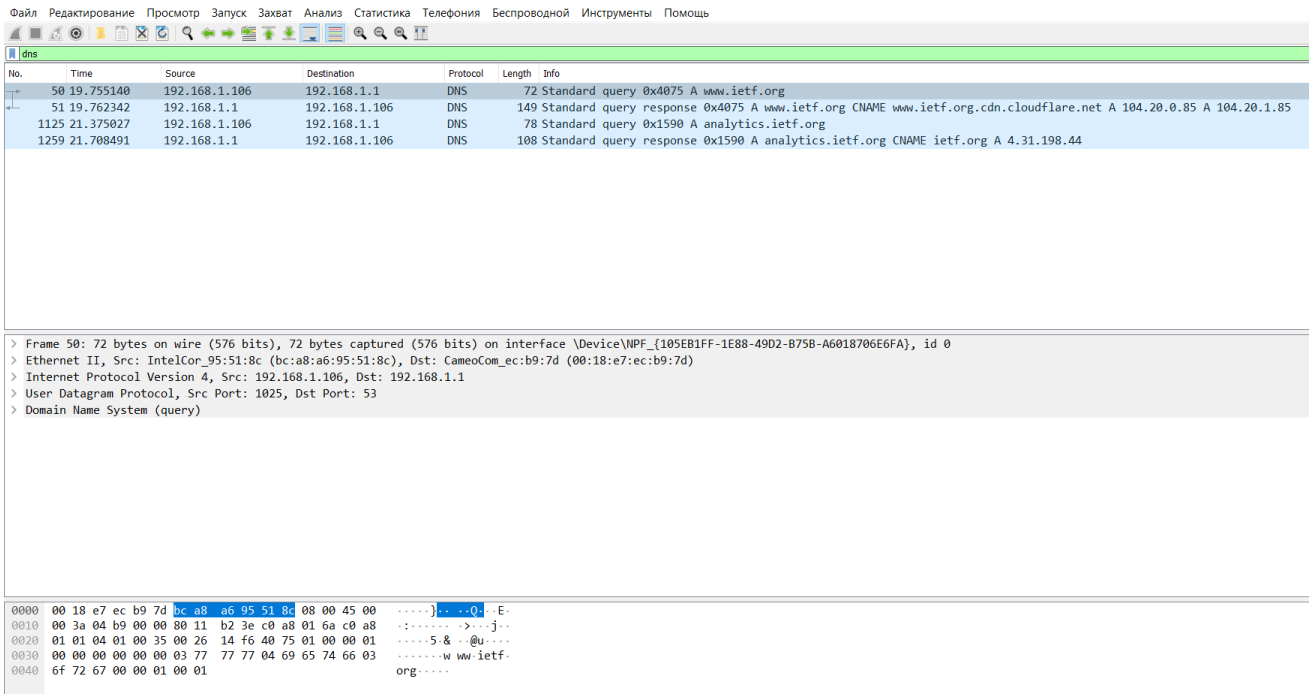
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КПІ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №3

з курсу «Комп'ютерні мережі»

Виконав: студент 3 курсу
групи КА-77
Котів С.В.
Прийняв: Кухарєв С.О.

Київ 2020 р.



Frame 50: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0

Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 1025, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x4075

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

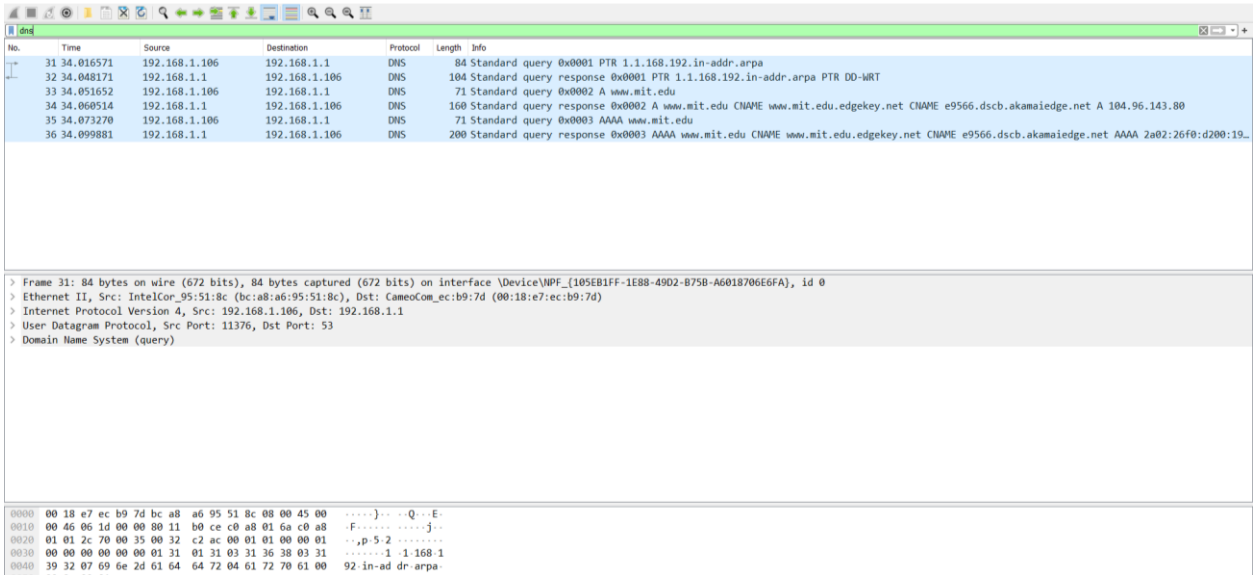
Queries

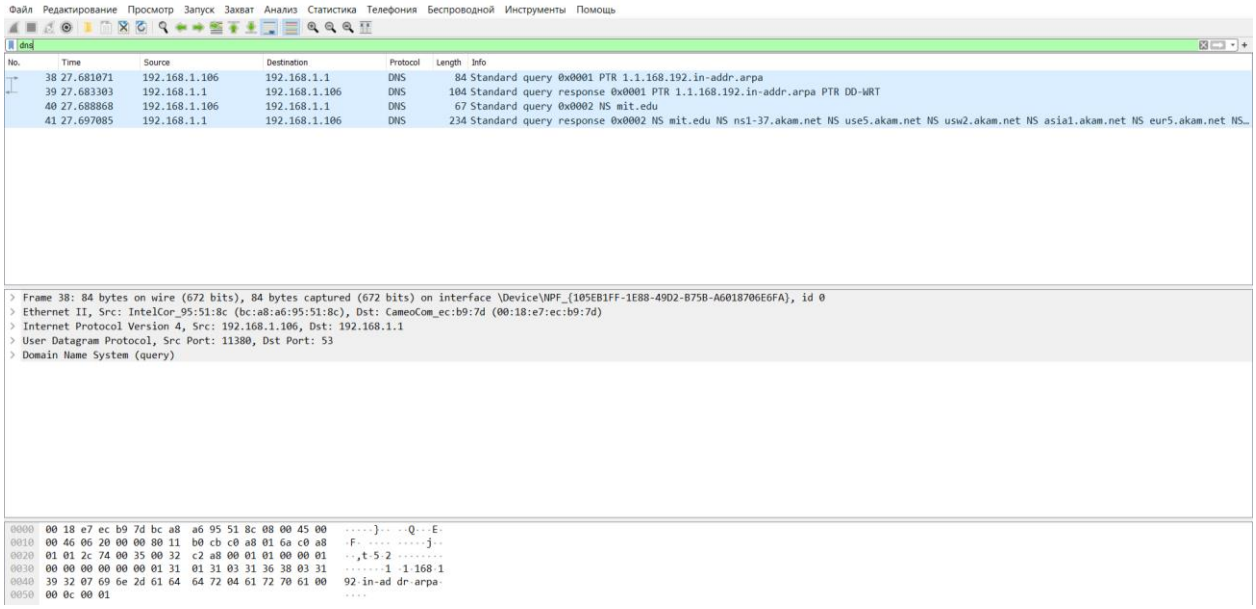
[Response In: 51]

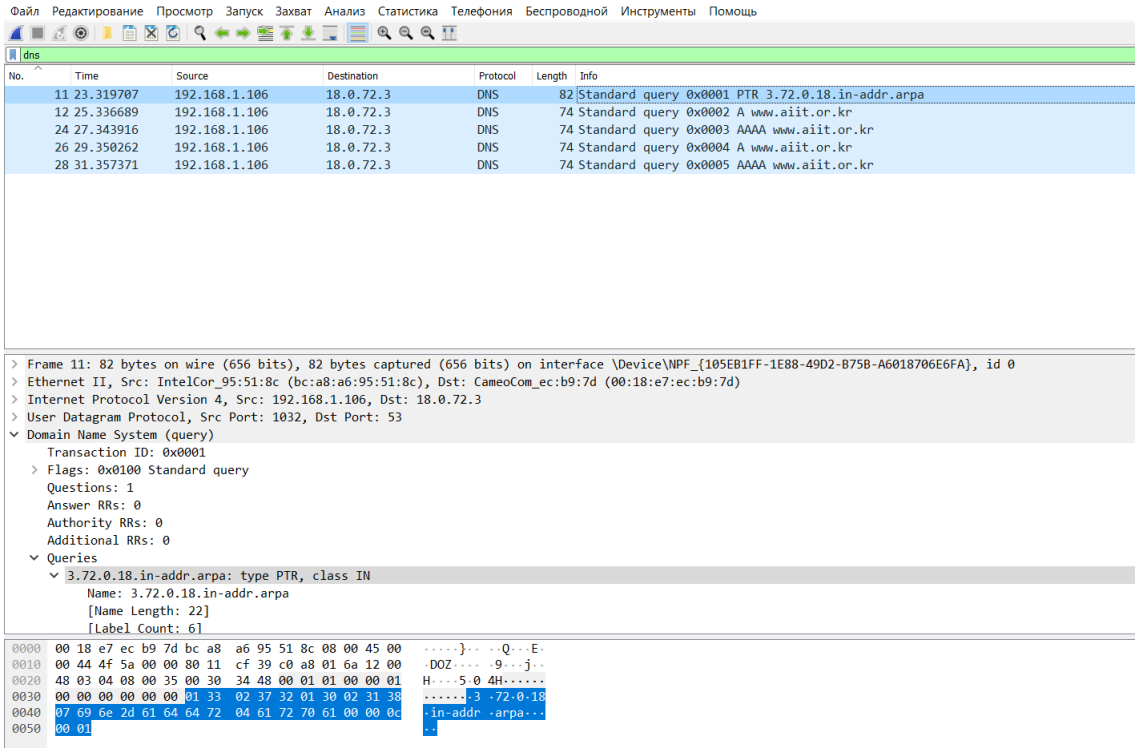
// Термінал:

Значок Windows + R

Cmd


dns
No. Time Source Destination Protocol Length Info
31 34.016571 192.168.1.106 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
32 34.048171 192.168.1.1 192.168.1.106 DNS 104 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT
33 34.051652 192.168.1.106 192.168.1.1 DNS 71 Standard query 0x0002 A www.mit.edu
34 34.060514 192.168.1.1 192.168.1.106 DNS 160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.96.143.80
35 34.073270 192.168.1.106 192.168.1.1 DNS 71 Standard query 0x0003 AAAA www.mit.edu
36 34.099881 192.168.1.1 192.168.1.106 DNS 200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:d200:19…
> Frame 31: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0
> Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 11376, Dst Port: 53
> Domain Name System (query)
0000 00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00 45 00 .....}.. ..Q...E.
0010 00 46 06 1d 00 00 80 11 b0 ce c0 a8 01 6a c0 a8 .F...... .....j..
0020 01 01 2c 70 00 35 00 32 c2 ac 00 01 01 00 00 01 ..,p.5.2 ....
0030 00 00 00 00 00 00 01 31 01 31 03 31 36 38 03 31 ....1 .1.168.1
0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92.in-ad dr.arpa.


Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
dns
No. Time Source Destination Protocol Length Info
38 27.681071 192.168.1.106 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
39 27.683303 192.168.1.1 192.168.1.106 DNS 104 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT
40 27.688868 192.168.1.106 192.168.1.1 DNS 67 Standard query 0x0002 NS mit.edu
41 27.697085 192.168.1.1 192.168.1.106 DNS 234 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS use5.akam.net NS usw2.akam.net NS asia1.akam.net NS eur5.akam.net NS…
> Frame 38: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0
> Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 11380, Dst Port: 53
> Domain Name System (query)
0000 00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00 45 00 .....}.. ..Q...E.
0010 00 46 06 20 00 00 80 11 b0 cb c0 a8 01 6a c0 a8 .F. ....j..
0020 01 01 2c 74 00 35 00 32 c2 a8 00 01 01 00 00 01 ..,t.5.2 ....
0030 00 00 00 00 00 00 01 31 01 31 03 31 36 38 03 31 ....1 .1.168.1
0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92.in-ad dr.arpa.
0050 00 0c 00 01 ....



Теорія:

Типи DNS записів

Записи DNS, або Ресурсні записи (англ. Resource Records, RR) — одиниці зберігання і передачі інформації в DNS.

Найбільш важливі типи DNS-записів:

- Запис A.
- Запис AAAA.
- Запис CNAME.
- Запис MX.
- Запис NS.
- TXT-запис.
- Запис PTR.
- Запис SOA.
- SRV-запис.

Запис A задає IP-адреса хоста. За допомогою записів A виконується запит на перетворення імені домену в IP-адресу.

Запис AAAA (IPv6 address record) зв'язує ім'я хоста з адресою протоколу IPv6. Наприклад, запит AAAA-запису на ім'я K.ROOT-SERVERS.NET поверне його IPv6 адреса — 2001:7fd::1

Запис типу CNAME (Canonical Name - Канонічне ім'я) дозволяють привласнювати хосту мнемонічні імена. Якщо DNS при зверненні до псевдоніму виявляє запис CNAME, що містить повне ім'я, DNS потім запитує повне ім'я домену.

Записи MX містять визначення хоста системи обміну поштою для поштових повідомлень, що відправляються в цей домен. За допомогою записів цього типу і значень параметрів

конфігурації хостів системи обміну поштою в SMTP (Простий протокол передачі пошти) визначаються адреси хостів, які опрацьовують і перенаправляє пошту для цього домену. Кожному хосту системи обміну поштою повинна відповідати запис адреси хоста (A) в існуючій області.

Запис NS вказує відповідальний сервер для даного хоста.

Запис типу TXT зазвичай використовується для текстового опису доменного імені.

Запис PTR (pointer) або запис покажчика зв'язує IP хоста з його канонічним ім'ям. Наприклад, (на момент написання), для IP адреси 192.0.34.164: запит запису PTR 164.34.0.192.in-addr.arpa поверне його канонічне ім'я referrals.icann.org. З метою зменшення обсягу небажаної кореспонденції (спаму) багато серверів-одержувачі електронної пошти можуть перевіряти наявність PTR запису для хоста, з якого відбувається відправлення. У цьому випадку PTR запис для IP адреси повинна відповідати імені відправляючого поштового сервера, яким він представляється в процесі SMTP сесії.

Запис SOA (Start Of Authority) містить ім'я первинного DNS-сервера (Primary Name Server), адреса, необхідний для встановлення технічних контактів (Hostmaster), серійний номер (Serial number) різні значення таймерів (Refresh, Retry, Expire, Minimum TTL)

SRV-запис (server selection) вказує на сервери для сервісів, використовується, зокрема, для Jabber і Active Directory.

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?

UDP, Цільовий порт запиту – 53, вихідний порт – 59917

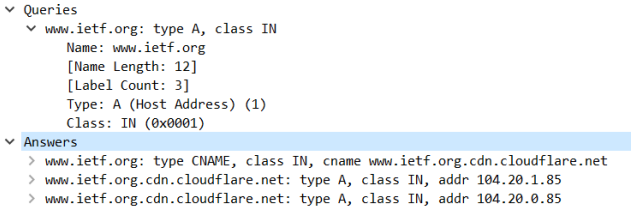
2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

8.8.8.8 , no ;

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

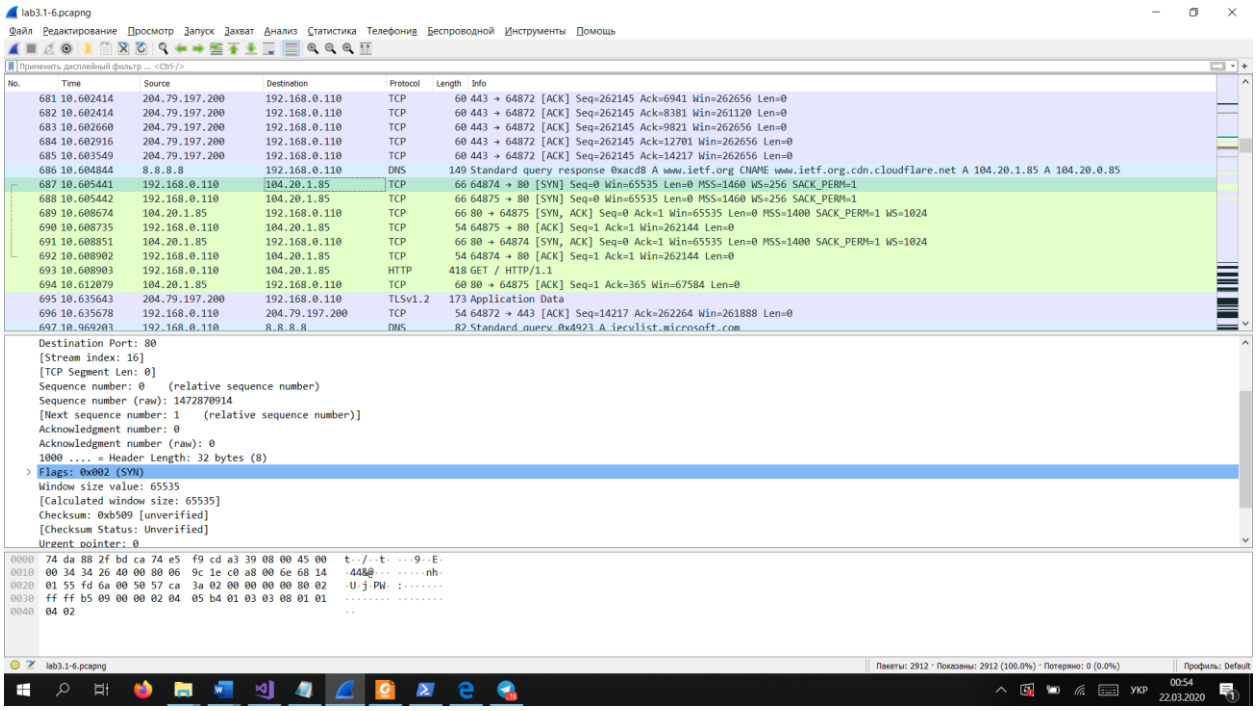
Типу A (Host address). Da (name, type)

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



Lds, Name, Type, Class, Time to live, Data length, Adress ,

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?



да

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

No, сразу после syn был отправлен http-запрос

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

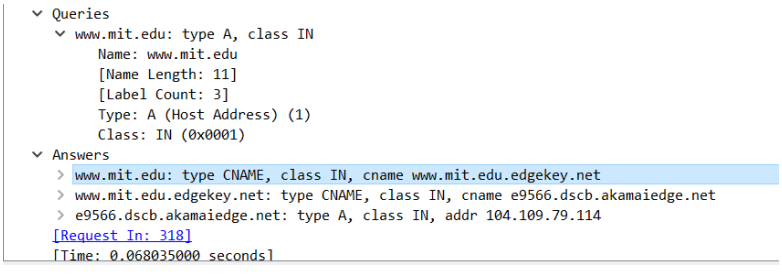
Цільовий порт запиту – 53, вихідний порт – 61228 ;

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

8.8.8.8, no

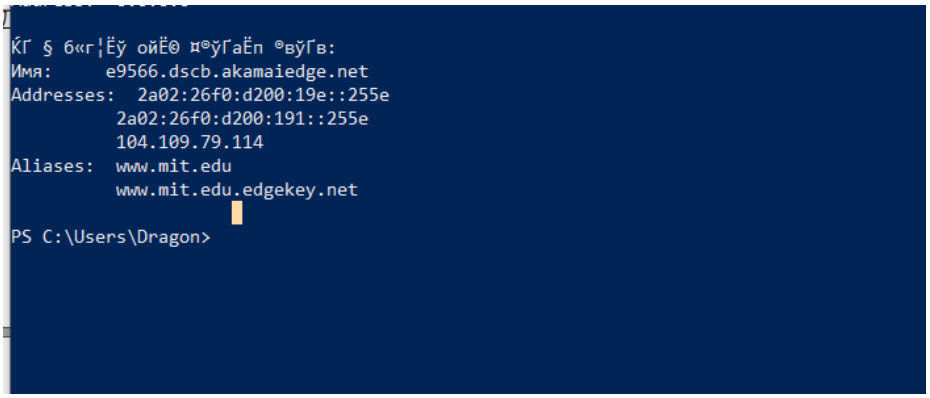
9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

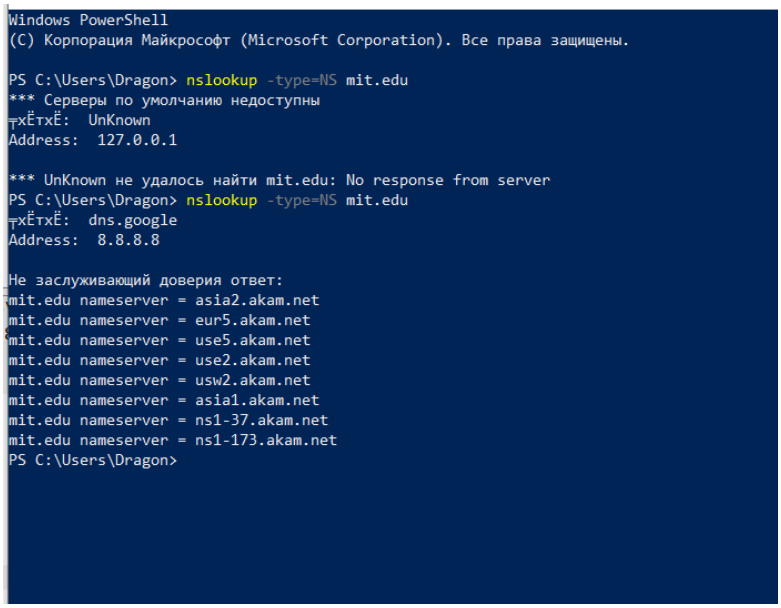
Типу A (Host address). Yes (name, class) ;



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

3 відповіді. Name, Type, Class, Time to live, Data length, CNAME/Adress





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

8.8.8.8 , no.

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

Типу NS, type, name? ;

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?

8 штук

(asia1.akam.net, eur5.akam.net, usw2.akam.net, ns1-37.akam.net, asia2.akam.net, ns1-

173.akam.net, use2.akam.net, use5.akam.net).

Лише 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?

На 8.8.8.8, no (google.com)

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

Типу A (Host address), типу AAAA (IPv6 Address). Ні ;

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

1 відповідь;

Name, Type, Class, Time to live, Data length, Adress

Висновок:

В лабораторній роботі ознайомився з концепціями локальних сервер DNS; кешування DNS-записів і повідомлень, а також з типами поля в записі DNS.