

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»

Виконала: студентка групи ІС-ЗП92
Макаренко Олена Сергіївна

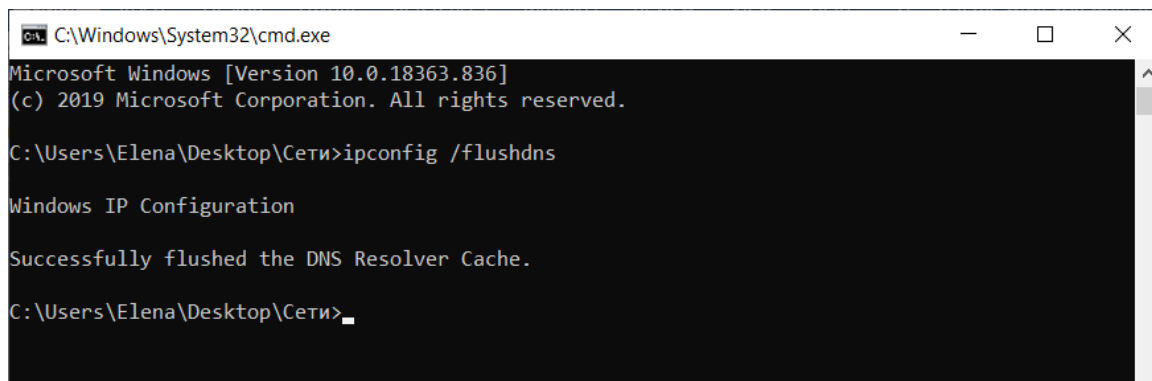
Прийняв: Кухарєв С.О.

Київ – 2020

Лабораторна робота 3

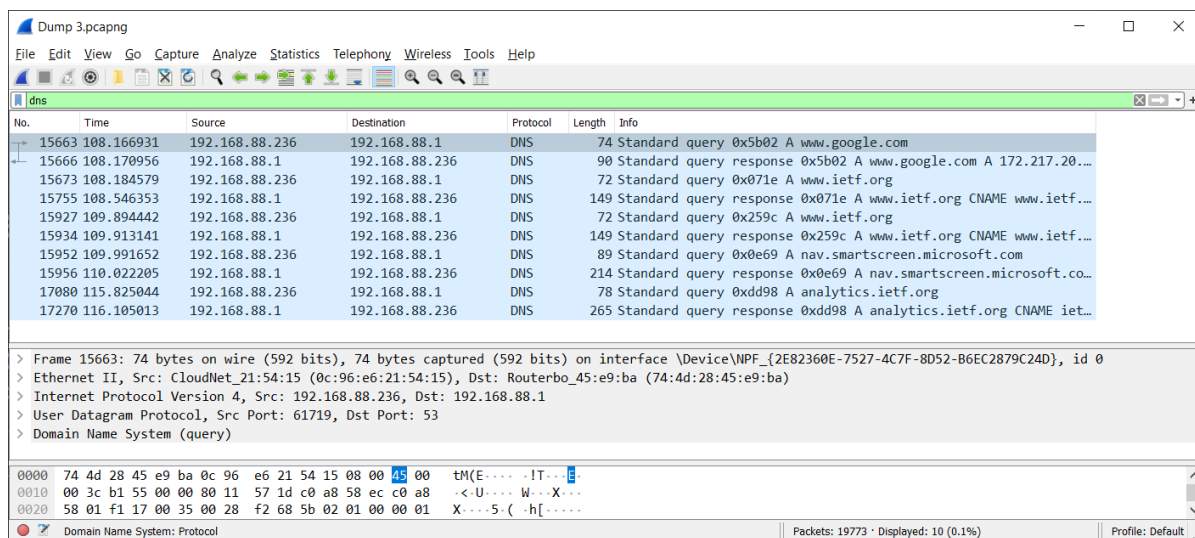
1. Хід роботи

1. Очистіть кеш DNS-записів:



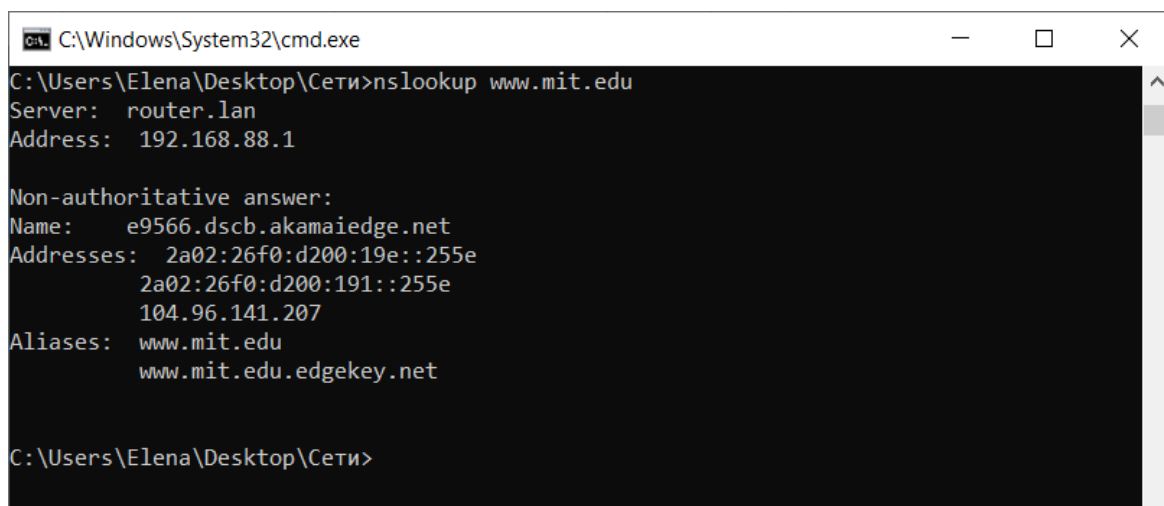
Мал. 1

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. 2

8. Почніть захоплення пакетів
9. Виконайте nslookup для домену `www.mit.edu` за допомогою команди `nslookup www.mit.edu`



```

C:\Windows\System32\cmd.exe
C:\Users\Elena\Desktop\Сети>nslookup www.mit.edu
Server: router.lan
Address: 192.168.88.1

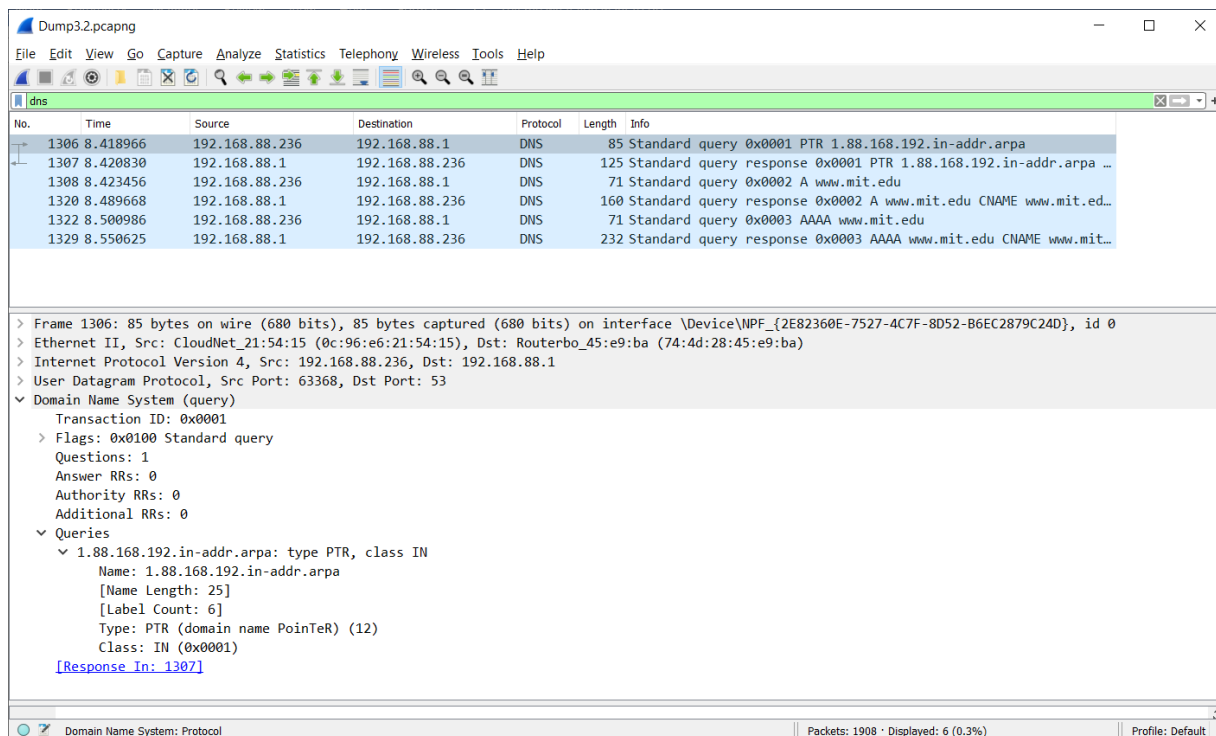
Non-authoritative answer:
Name: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d200:19e::255e
           2a02:26f0:d200:191::255e
           104.96.141.207
Aliases: www.mit.edu
          www.mit.edu.edgekey.net

C:\Users\Elena\Desktop\Сети>

```

Мал.3

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



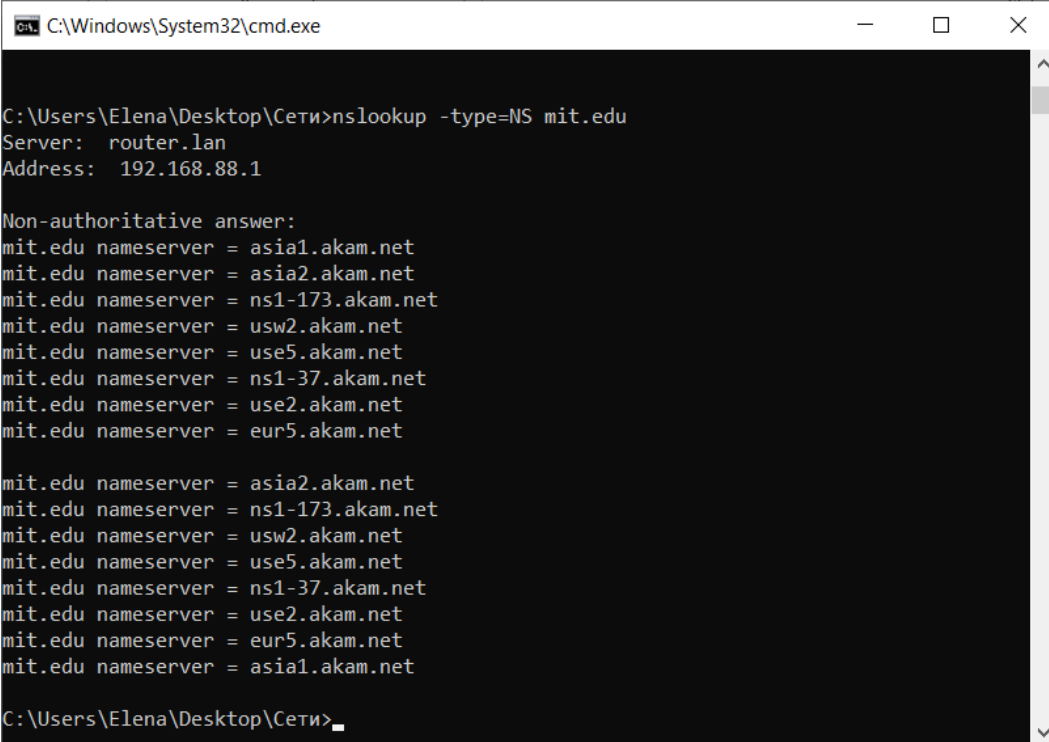
No.	Time	Source	Destination	Protocol	Length	Info
1306	8.418966	192.168.88.236	192.168.88.1	DNS	85	Standard query 0x0001 PTR 1.88.168.192.in-addr.arpa
1307	8.420830	192.168.88.1	192.168.88.236	DNS	125	Standard query response 0x0001 PTR 1.88.168.192.in-addr.arpa ...
1308	8.423456	192.168.88.236	192.168.88.1	DNS	71	Standard query 0x0002 A www.mit.edu
1320	8.489668	192.168.88.1	192.168.88.236	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.ed...
1322	8.500986	192.168.88.236	192.168.88.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
1329	8.550625	192.168.88.1	192.168.88.236	DNS	232	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit...

> Frame 1306: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{2E82360E-7527-4C7F-8D52-B6EC2879C24D}, id 0
 > Ethernet II, Src: CloudNet_21:54:15 (0c:96:e6:21:54:15), Dst: Routerbo_45:e9:ba (74:4d:28:45:e9:ba)
 > Internet Protocol Version 4, Src: 192.168.88.236, Dst: 192.168.88.1
 > User Datagram Protocol, Src Port: 63368, Dst Port: 53
 > Domain Name System (query)
 Transaction ID: 0x0001
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > 1.88.168.192.in-addr.arpa: type PTR, class IN
 Name: 1.88.168.192.in-addr.arpa
 [Name Length: 25]
 [Label Count: 6]
 Type: PTR (domain name PoinTeR) (12)
 Class: IN (0x0001)
 [Response In: 1307]

Мал. 4

12. Почніть захоплення пакетів

13. Виконайте nslookup для домену `www.mit.edu` за допомогою команди
`nslookup -type=NS mit.edu`



```

C:\Windows\System32\cmd.exe

C:\Users\Elena\Desktop\Сети>nslookup -type=NS mit.edu
Server:  router.lan
Address:  192.168.88.1

Non-authoritative answer:
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net

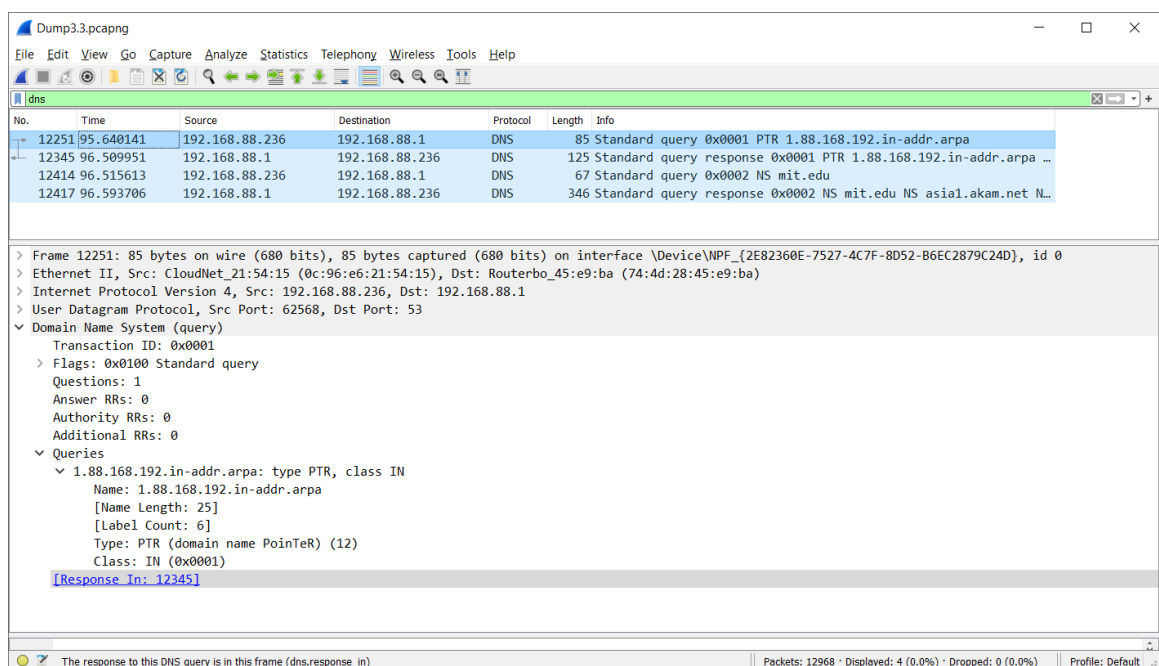
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net

C:\Users\Elena\Desktop\Сети>
  
```

Мал. 5

14. Зупиніть захоплення пакетів

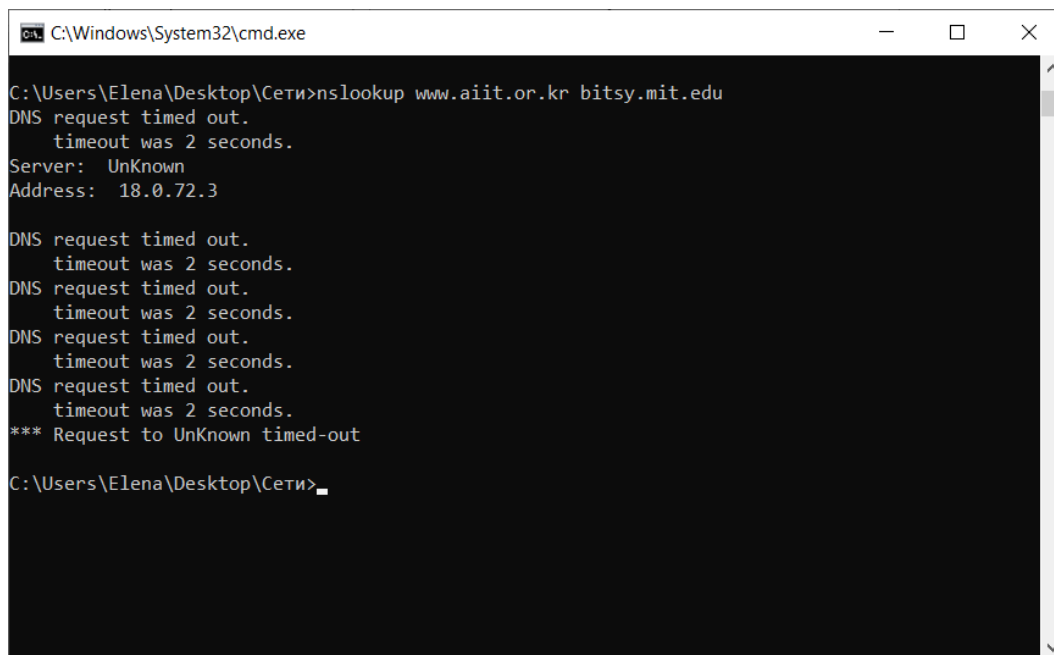
15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети



Мал. 6

16. Почніть захоплення пакетів

17. Виконайте nslookup для домену `www.mit.edu` за допомогою команди `nslookup www.aiit.or.kr bitsy.mit.edu`



```

C:\Windows\System32\cmd.exe
C:\Users\Elena\Desktop\Сети>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  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.
*** Request to UnKnown timed-out

C:\Users\Elena\Desktop\Сети>

```

Мал. 7

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

2. 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?

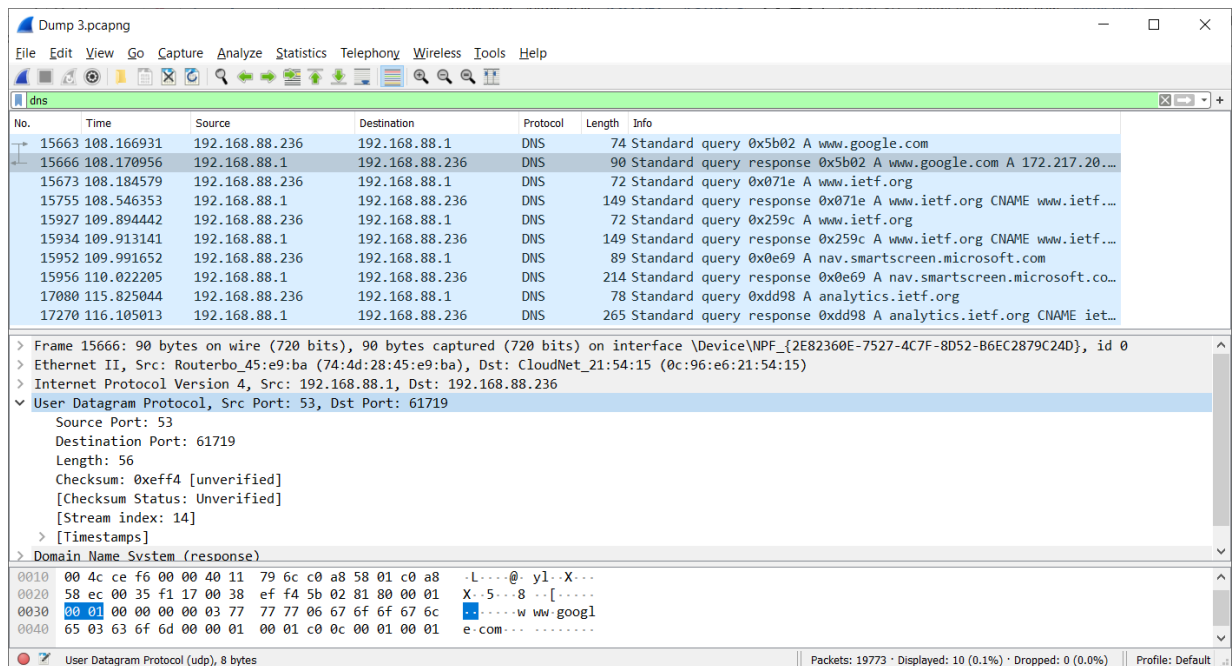
Відповідь: DNS використовує прототокол UDP

Номер цільового порта запиту DNS та номер вихідного порта відповіді DNS -

53

User Datagram Protocol, Src Port: 61719, Dst Port: 53

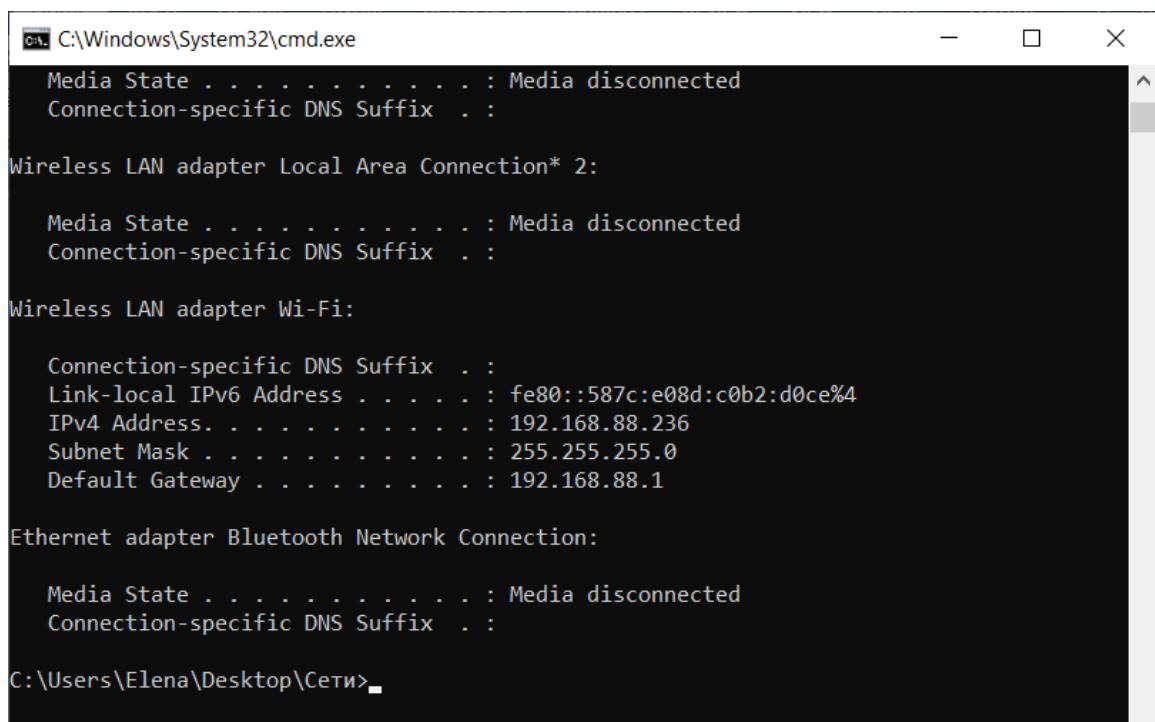
User Datagram Protocol, Src Port: 53, Dst Port: 61719



Мал. 8

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

Відповідь: Destination: 192.168.88.1 – є адресою локального DNS сервера



Мал. 9

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

Відповідь: Запит типу A; Має посилання на відповідь. [Response In: 15755]

Dump 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
15663	108.166931	192.168.88.236	192.168.88.1	DNS	74	Standard query 0x5b02 A www.google.com
15666	108.170956	192.168.88.1	192.168.88.236	DNS	90	Standard query response 0x5b02 A www.google.com A 172.217.20...
15673	108.184579	192.168.88.236	192.168.88.1	DNS	72	Standard query 0x071e A www.ietf.org
15755	108.546353	192.168.88.1	192.168.88.236	DNS	149	Standard query response 0x071e A www.ietf.org CNAME www.ietf...
15927	109.894442	192.168.88.236	192.168.88.1	DNS	72	Standard query 0x259c A www.ietf.org
15934	109.913141	192.168.88.1	192.168.88.236	DNS	149	Standard query response 0x259c A www.ietf.org CNAME www.ietf...
15952	109.991652	192.168.88.236	192.168.88.1	DNS	89	Standard query 0x0e69 A nav.smartscreen.microsoft.com
15956	110.022205	192.168.88.1	192.168.88.236	DNS	214	Standard query response 0x0e69 A nav.smartscreen.microsoft.co...
17080	115.825044	192.168.88.236	192.168.88.1	DNS	78	Standard query 0xdd98 A analytics.ietf.org
17270	116.105013	192.168.88.1	192.168.88.236	DNS	265	Standard query response 0xdd98 A analytics.ietf.org CNAME iet...

> Frame 15673: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2E82360E-7527-4C7F-8D52-B6EC2879C24D}, id 0

> Ethernet II, Src: CloudNet_21:54:15 (0c:96:e6:21:54:15), Dst: Routerbo_45:e9:ba (74:4d:28:45:e9:ba)

> Internet Protocol Version 4, Src: 192.168.88.236, Dst: 192.168.88.1

> User Datagram Protocol, Src Port: 64702, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x071e

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> www.ietf.org: type A, class IN

[Response In: 15755]

Мал. 10

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

Відповідь: Запропоновано 3 відповіді, Кожна з відповідей містить наступні поля: Name, Type, Class, TTL, Data length, CNAME;

Приклад відповіді:

```

v www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  Name: www.ietf.org
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 1800 (30 minutes)
  Data length: 33
  CNAME: www.ietf.org.cdn.cloudflare.net

```

Мал. 11

Dump 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
15663	108.166931	192.168.88.236	192.168.88.1	DNS	74	Standard query 0x5b02 A www.google.com
15666	108.170956	192.168.88.1	192.168.88.236	DNS	90	Standard query response 0x5b02 A www.google.com A 172.217.20...
15673	108.184579	192.168.88.236	192.168.88.1	DNS	72	Standard query 0x071e A www.ietf.org
15755	108.546353	192.168.88.1	192.168.88.236	DNS	149	Standard query response 0x071e A www.ietf.org CNAME www.ietf...
15927	109.894442	192.168.88.236	192.168.88.1	DNS	72	Standard query 0x259c A www.ietf.org
15934	109.913141	192.168.88.1	192.168.88.236	DNS	149	Standard query response 0x259c A www.ietf.org CNAME www.ietf...
15952	109.991652	192.168.88.236	192.168.88.1	DNS	89	Standard query 0x0e69 A nav.smartscreen.microsoft.com
15956	110.022205	192.168.88.1	192.168.88.236	DNS	214	Standard query response 0x0e69 A nav.smartscreen.microsoft.co...
17080	115.825044	192.168.88.236	192.168.88.1	DNS	78	Standard query 0xdd98 A analytics.ietf.org
17270	116.105013	192.168.88.1	192.168.88.236	DNS	265	Standard query response 0xdd98 A analytics.ietf.org CNAME iet...

> User Datagram Protocol, Src Port: 53, Dst Port: 64702

Domain Name System (response)

Transaction ID: 0x071e

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

Queries

> www.ietf.org: type A, class IN

Answers

> www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net

Name: www.ietf.org

Type: CNAME (Canonical Name for an alias) (5)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 33

CNAME: www.ietf.org.cdn.cloudflare.net

> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

[Request In: 15673]

[Time: 0.361774000 seconds]

Text item (text), 45 bytes

Packets: 19773 · Displayed: 10 (0.1%) · Dropped: 0 (0.0%)

Мал. 12

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?

Відповідь: в TCP SYN Destination: 172.217.20.196 співпадає з однією з запропонованих віповідей сервера DNS.

Dump 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
15657	108.130446	192.168.88.236	18.218.240.132	UDP	57	52025 → 8801 Len=15
15658	108.130632	192.168.88.236	18.218.240.132	UDP	271	52024 → 8801 Len=229
15659	108.140538	192.168.88.236	18.218.240.132	UDP	275	52024 → 8801 Len=233
15660	108.151910	192.168.88.236	18.218.240.132	UDP	100	52025 → 8801 Len=58
15661	108.156522	18.218.240.132	192.168.88.236	UDP	60	8801 → 52025 Len=15
15662	108.156756	18.218.240.132	192.168.88.236	TLSv1.2	123	Application Data
15663	108.166931	192.168.88.236	192.168.88.1	DNS	74	Standard query 0x5b02 A www.google.com
15664	108.167653	192.168.88.236	18.218.240.132	TLSv1.2	92	Application Data
15665	108.167793	192.168.88.236	18.218.240.132	UDP	292	52024 → 8801 Len=250
15666	108.170956	192.168.88.1	192.168.88.236	DNS	90	Standard query response 0x5b02 A www.google.com A 172.217.20...
15667	108.177308	192.168.88.236	192.168.88.255	NBNS	92	Name query NB WPAD<00>
15668	108.178901	192.168.88.236	172.217.20.196	TCP	66	55132 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK...
15669	108.179721	192.168.88.236	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
15670	108.180250	fe80::587c:e08d:c0b...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
15671	108.181075	fe80::587c:e08d:c0b...	ff02::1:2	MDNS	84	Standard query 0x0000 A wpad...

Domain Name System (response)

Transaction ID: 0x5b02

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

> www.google.com: type A, class IN

Name: www.google.com

[Name Length: 14]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

> www.google.com: type A, class IN, addr 172.217.20.196

[Request In: 15663]

Dump 3.pcapng

Packets: 19773 · Displayed: 19773 (100.0%) · Dropped: 0 (0.0%)

Мал. 13

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

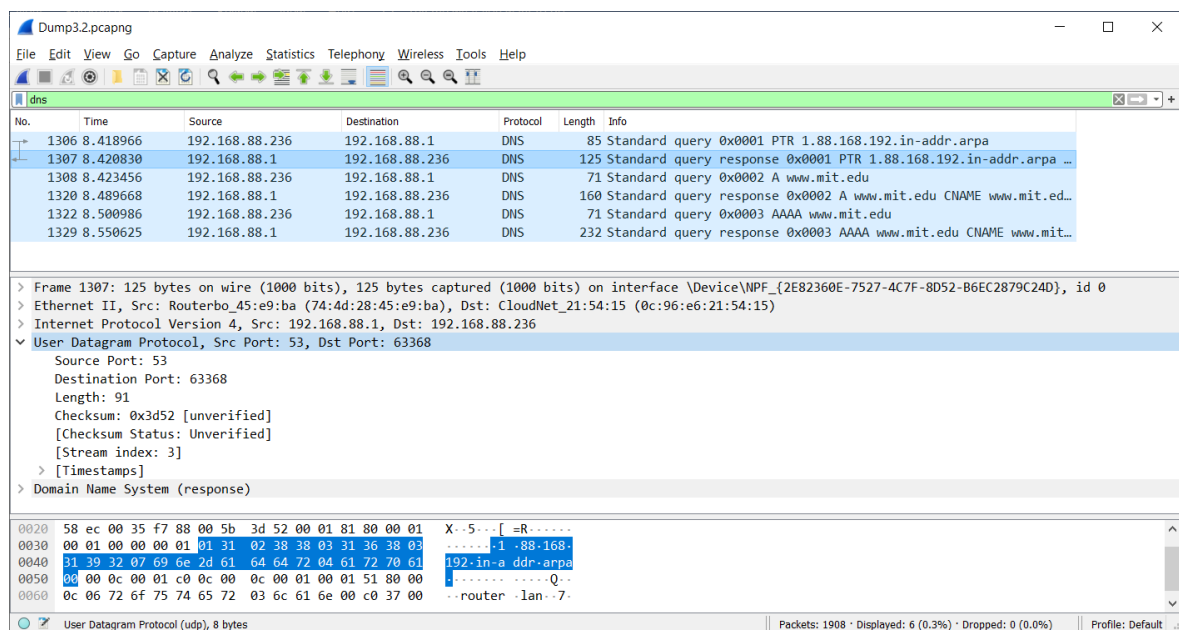
Відповідь: так. Було виконано ще 4 нових DNS запити. Взагалі було 5 DNS запитів разом із першим.

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

Відповідь: Порт 53

Порти у запиті: Src Port: 63368, Dst Port: 53

Порти у відповіді: Src Port: 53, Dst Port: 63368



Мал. 14

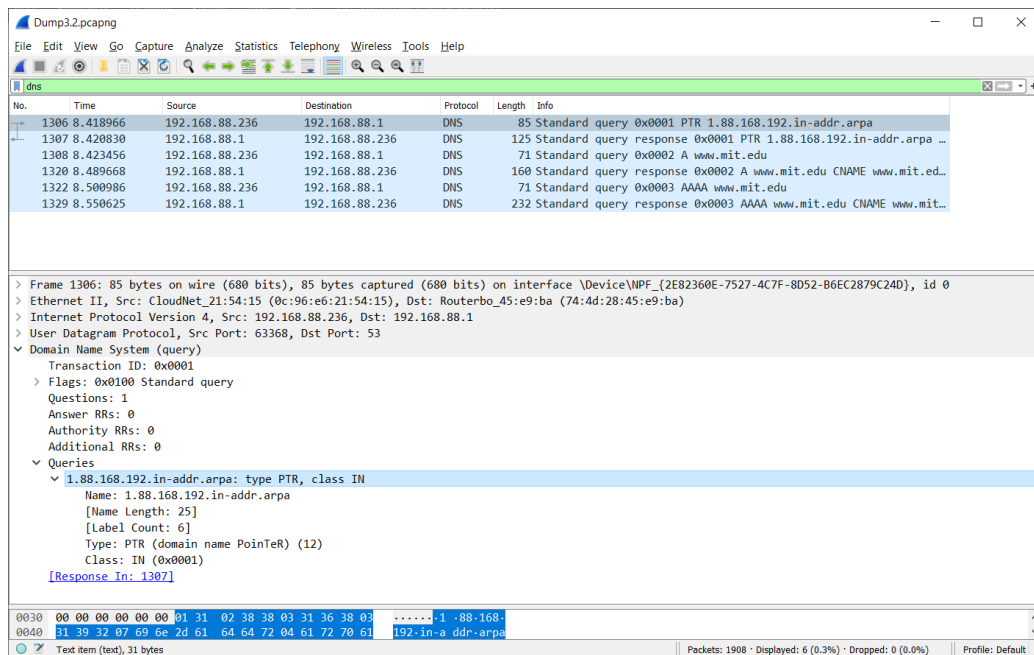
8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Відповідь: Dst: 192.168.88.1— це є адреса локального сервера DNS за замовчанням.

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

Відповідь: Було 3 запити — тип PTR, тип A та AAAA.

Має посилання на відповідь. [Response In: 1307]



Мал. 15

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

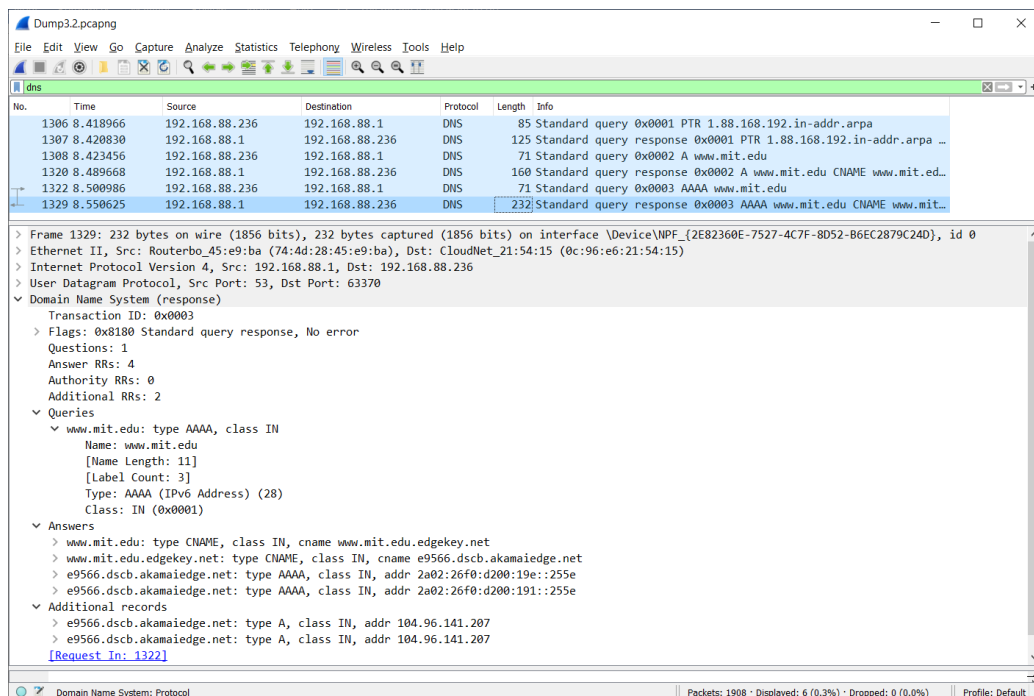
Відповідь: 3 запити і 3 відповіді.

Кожна з відповідей складається з:

для PTR – була 1 відповідь;

для типу A – 3 відповіді;

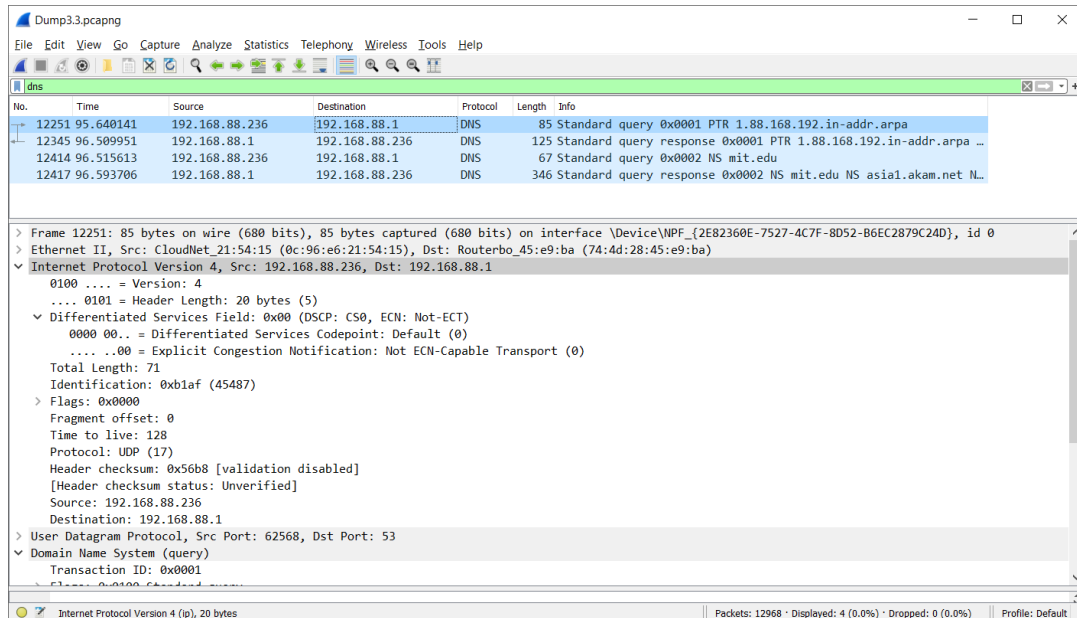
для типу AAAA – 4 відповіді.



Мал. 16

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

Відповідь: Destination: 192.168.88.1 – це є адреса локального сервера DNS за замовчанням

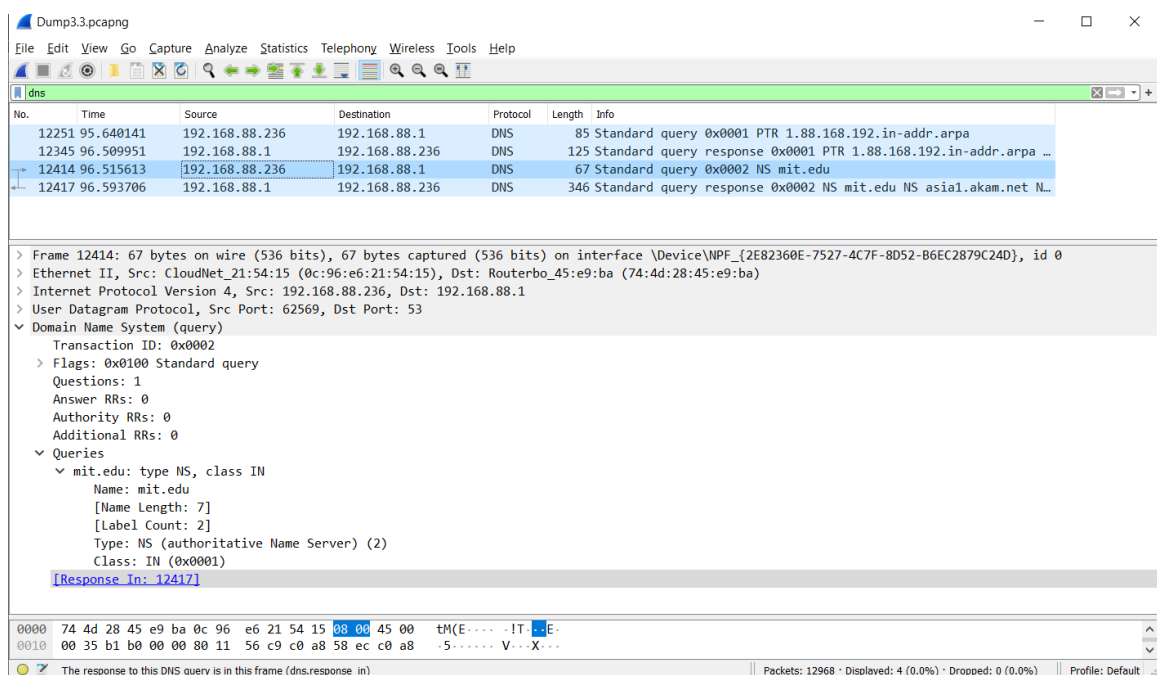


Мал. 17

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

Відповідь: було 2 запити - типу PTR та типу NS.

Так, цей запит вміщує посилку на відповіді: [Response In: 12417]



Мал. 18

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?

Відповідь: було 2 відповіді. У першій запропоновано 1 запис, у другій запропоновано 16 записів. Кожна з відповідей складається з таких полів: Name, Type, Class, TTL, Data length, Name Server.

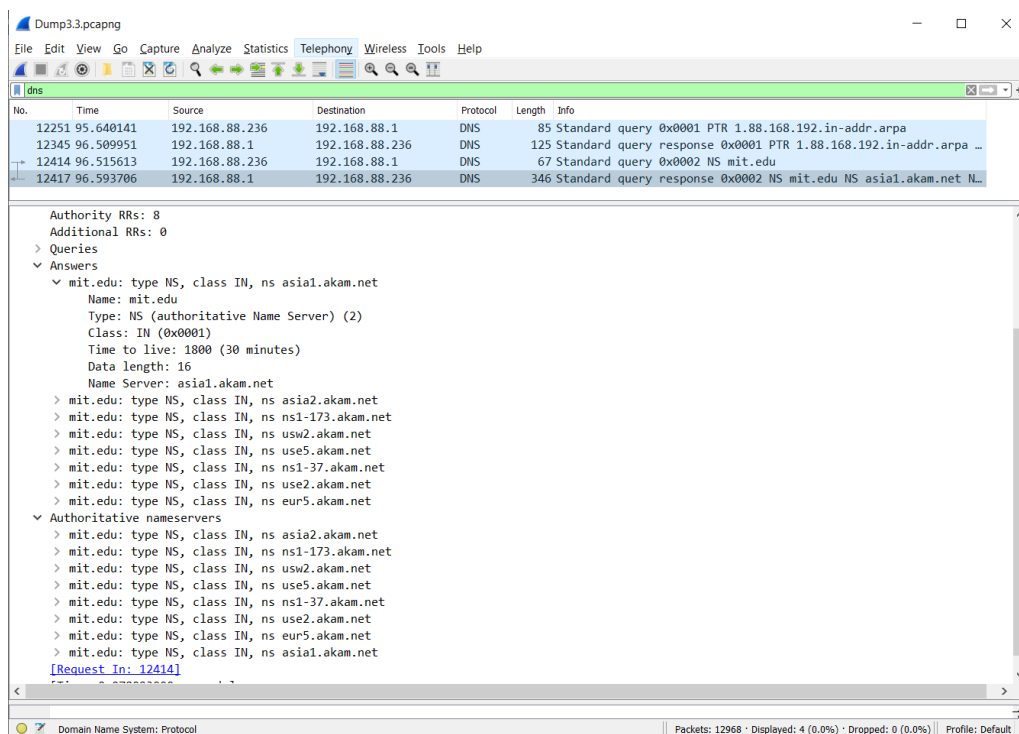
Приклад відповіді:

```

▼ mit.edu: type NS, class IN, ns asia1.akam.net
  Name: mit.edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 1800 (30 minutes)
  Data length: 16
  Name Server: asia1.akam.net

```

Мал. 19



Мал. 20 Запропоновані сервери

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?

Відповідь: Destination: 192.168.88.1 – це є адреса локального сервера DNS за

замовчанням, також був запит на Destination: 91.193.32.50, а також 5 запитів на Destination: 18.0.72.3

The screenshot shows the Wireshark interface with a packet list and a packet details pane. The packet list shows several DNS queries and responses. The packet details pane shows the structure of an Internet Protocol Version 4 packet, including the header and flags.

No.	Time	Source	Destination	Protocol	Length	Info
3579	23.912381	192.168.88.236	192.168.88.1	DNS	73	Standard query 0x1dab A bitsy.mit.edu
3585	23.943920	192.168.88.236	91.193.32.50	DNS	73	Standard query 0x1dab A bitsy.mit.edu
3589	23.979053	192.168.88.1	192.168.88.236	DNS	256	Standard query response 0x1dab A bitsy.mit.edu A 18.0.72.3 NS...
3590	23.983166	192.168.88.236	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
3595	24.004914	91.193.32.50	192.168.88.236	DNS	89	Standard query response 0x1dab A bitsy.mit.edu A 18.0.72.3
3846	25.987146	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
4124	27.988892	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
4365	29.990746	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
4683	31.991742	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Frame 3579: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{2E82360E-7527-4C7F-8D52-B6EC2879C24D}, id 0
 Ethernet II, Src: CloudNet_21:54:15 (0c:96:e6:21:54:15), Dst: Routerbo_45:e9:ba (74:4d:28:45:e9:ba)
 Internet Protocol Version 4, Src: 192.168.88.236, Dst: 192.168.88.1
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 59
 Identification: 0xb1c0 (45504)
 Flags: 0x0000
 Fragment offset: 0
 Time to live: 128

Мал. 21

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

Відповідь: виконано 7 запитів DNS. Були запити типу A, PTR, AAAA.

Так, цей запит вміщує посилку на відповіді: [Response In: 3589]

The screenshot shows the Wireshark interface with a packet list and a packet details pane. The packet list shows several DNS queries and responses. The packet details pane shows the structure of a Domain Name System (query) packet, including the transaction ID, flags, and queries.

No.	Time	Source	Destination	Protocol	Length	Info
3579	23.912381	192.168.88.236	192.168.88.1	DNS	73	Standard query 0x1dab A bitsy.mit.edu
3585	23.943920	192.168.88.236	91.193.32.50	DNS	73	Standard query 0x1dab A bitsy.mit.edu
3589	23.979053	192.168.88.1	192.168.88.236	DNS	256	Standard query response 0x1dab A bitsy.mit.edu A 18.0.72.3 NS...
3590	23.983166	192.168.88.236	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
3595	24.004914	91.193.32.50	192.168.88.236	DNS	89	Standard query response 0x1dab A bitsy.mit.edu A 18.0.72.3
3846	25.987146	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
4124	27.988892	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
4365	29.990746	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
4683	31.991742	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Frame 3579: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{2E82360E-7527-4C7F-8D52-B6EC2879C24D}, id 0
 Ethernet II, Src: CloudNet_21:54:15 (0c:96:e6:21:54:15), Dst: Routerbo_45:e9:ba (74:4d:28:45:e9:ba)
 Internet Protocol Version 4, Src: 192.168.88.236, Dst: 192.168.88.1
 User Datagram Protocol, Src Port: 51900, Dst Port: 53
 Domain Name System (query)
 Transaction ID: 0x1dab
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 bitsy.mit.edu: type A, class IN
 Name: bitsy.mit.edu
 [Name Length: 13]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 3589]

Мал. 22

16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями

було запропоновано сервером? З чого складається кожна з цих відповідей?
Відповідь: отримано 2 відповіді DNS. У відповіді для bitsy.mit.edu було 9 відповідей, які складаються з таких полів:

Name, Type, Class, TTL, Data length, Address;

Приклад відповіді:

```

▼ 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: 1800 (30 minutes)
  Data length: 4
  Address: 18.0.72.3

```

Мал. 23

No.	Time	Source	Destination	Protocol	Length	Info
3579	23.912381	192.168.88.236	192.168.88.1	DNS	73	Standard query 0x1dab A bitsy.mit.edu
3585	23.943920	192.168.88.236	91.193.32.50	DNS	73	Standard query 0x1dab A bitsy.mit.edu
3589	23.979053	192.168.88.1	192.168.88.236	DNS	256	Standard query response 0x1dab A bitsy.mit.edu A 18.0.72.3 NS ns1-173.akam.net NS usw2.akam...
3590	23.983166	192.168.88.236	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
3595	24.004914	91.193.32.50	192.168.88.236	DNS	89	Standard query response 0x1dab A bitsy.mit.edu A 18.0.72.3
3846	25.987146	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
4124	27.988892	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
4365	29.990746	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
4683	31.991742	192.168.88.236	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Questions: 1
Answer RRs: 1
Authority RRs: 8
Additional RRs: 0

▼ Queries

- bitsy.mit.edu: type A, class IN
 - Name: bitsy.mit.edu
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

▼ Answers

- bitsy.mit.edu: type A, class IN, addr 18.0.72.3

▼ Authoritative nameservers

- mit.edu: type NS, class IN, ns ns1-173.akam.net
- mit.edu: type NS, class IN, ns usw2.akam.net
- mit.edu: type NS, class IN, ns use5.akam.net
- mit.edu: type NS, class IN, ns ns1-37.akam.net
- mit.edu: type NS, class IN, ns use2.akam.net
- mit.edu: type NS, class IN, ns eur5.akam.net
- mit.edu: type NS, class IN, ns asia1.akam.net
- mit.edu: type NS, class IN, ns asia2.akam.net

[Request In: 3579]
[Time: 0.066672000 seconds]

0000 0c 96 e6 21 54 15 74 d0 28 45 e9 ba 08 00 45 00 ...!T.tM (E...E

Domain Name System: Protocol

Packets: 20240 · Displayed: 9 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

Мал. 24