

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 3
З дисципліни: Комп'ютерні мережі

Протоколи DNS

Виконав:
Студент III курсу
Групи КА-74
Джалаганія Б.І.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

The image shows a Windows command prompt window titled "Командная строка" (Command Prompt) and a Wireshark network traffic analysis window.

Command Prompt Output:

```
C:\Users\olena>ipconfig/flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.

C:\Users\olena>
```

Wireshark Network Traffic Analysis:

The Wireshark window displays a list of DNS queries and responses. The table below summarizes the captured traffic:

No.	Time	Source	Destination	Protocol	Length	Info
164	8.150742	77.47.197.26	77.47.128.130	DNS	84	Standard query 0xf5e6 A win10.ipv6.microsoft.com
165	8.155872	77.47.128.130	77.47.197.26	DNS	539	Standard query response 0xf5e6 A win10.ipv6.microsoft.com CNAME onprewindows.ipv6.microsoft.com.akadns.net CNAME trdovmsukwest.ipv6...
445	23.195238	77.47.197.26	77.47.128.130	DNS	72	Standard query 0xb0b01 A www.ietf.org
446	23.218902	77.47.128.130	77.47.197.26	DNS	239	Standard query response 0xb0b01 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85 NS ns3.cloudflare.ne...
455	23.479945	77.47.197.26	77.47.128.130	DNS	91	Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
456	23.505190	77.47.197.26	77.47.128.131	DNS	91	Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
463	23.640716	77.47.128.130	77.47.197.26	DNS	548	Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net A 161.69.169.73 A 161.69.169.70 A ...
464	23.640718	77.47.128.131	77.47.197.26	DNS	500	Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net A 161.69.169.73 A 161.69.169.70 A ...
509	24.222488	77.47.197.26	77.47.128.130	DNS	88	Standard query 0x013c A mip.api.mcafeewebadvisor.com
511	24.247527	77.47.197.26	77.47.128.131	DNS	88	Standard query 0x013c A mip.api.mcafeewebadvisor.com
525	24.276087	77.47.128.130	77.47.197.26	DNS	412	Standard query response 0x013c A mip.api.mcafeewebadvisor.com CNAME WACloudB-1801077940.us-east-1.elb.amazonaws.com A 52.55.223.53 ...
532	24.282583	77.47.128.131	77.47.197.26	DNS	412	Standard query response 0x013c A mip.api.mcafeewebadvisor.com CNAME WACloudB-1801077940.us-east-1.elb.amazonaws.com A 35.170.119.21...
767	25.254856	77.47.197.26	77.47.128.130	DNS	78	Standard query 0xba2e A analytics.ietf.org
791	25.279621	77.47.197.26	77.47.128.131	DNS	78	Standard query 0xba2e A analytics.ietf.org
953	25.625100	77.47.128.131	77.47.197.26	DNS	361	Standard query response 0xba2e A analytics.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.yyz1.afiliat-nst.info NS ns1.mial.afiliat-nst...
955	25.631900	77.47.128.130	77.47.197.26	DNS	361	Standard query response 0xba2e A analytics.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.mial.afiliat-nst.info NS ns1.ams1.afiliat-nst...
1685	32.540445	77.47.197.26	77.47.128.130	DNS	71	Standard query 0x8c6f A wpad.kpi.ua
1686	32.544087	77.47.128.130	77.47.197.26	DNS	123	Standard query response 0x8c6f No such name A wpad.kpi.ua SOA ns.kpi.ua
1737	35.362789	77.47.197.26	77.47.128.130	DNS	79	Standard query 0x3772 A clients4.google.com
1738	35.385936	77.47.128.130	77.47.197.26	DNS	255	Standard query response 0x3772 A clients4.google.com CNAME clients.l.google.com A 216.58.209.14 NS ns1.google.com NS ns3.google.com ...

Packet Details:

Frame 456: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF{E7910771-2CFD-4CF3-A912-85B68977EB6D}, id 0

Ethernet II, Src: AzureWav_87:73:0d (74:c6:3b:87:73:0d), Dst: Hangzhou_9d:38:c8 (08:0f:e2:9d:38:c8)

Internet Protocol Version 4, Src: 77.47.197.26, Dst: 77.47.128.131

User Datagram Protocol, Src Port: 61854, Dst Port: 53

Domain Name System (query)

Packet Bytes:

0000 00 0f e2 9d 38 c8 74 c6 3b 87 73 0d 08 00 45 008 t : ; s...E
0010 00 4d 32 7a 00 00 80 11 28 2a 4d 2f c5 1a 4d 2f -M2z... (*/-H/
0020 80 83 f1 9e 00 35 00 39 fd 9a a9 32 01 00 00 015 9 --2...
0030 00 00 00 00 00 00 77 65 62 61 64 76 69 73 6fw ebadviso
0040 72 63 04 72 65 73 74 03 67 74 69 06 6d 63 61 66 rc rest- gti mcaf

Беспроводная сеть

Файл Редактирование Просмотр Запуск Завхват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисковый фильтр ... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
450	23.358186	Hangzhou_9d:38:c8	Broadcast	ARP	60	Who has 77.47.196.164? Tell 77.47.196.1
451	23.358566	Hangzhou_9d:38:c8	Broadcast	ARP	60	Who has 77.47.196.194? Tell 77.47.196.1
452	23.359240	Hangzhou_9d:38:c8	Broadcast	ARP	60	Who has 77.47.196.41? Tell 77.47.196.1
453	23.476313	77.47.197.26	104.20.1.85	TCP	66	53977 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
454	23.476855	77.47.197.26	104.20.1.85	TCP	66	53978 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
455	23.479945	77.47.197.26	77.47.128.130	DNS	91	Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
456	23.505190	77.47.197.26	77.47.128.131	DNS	91	Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
457	23.556467	Hangzhou_9d:38:c8	Broadcast	ARP	60	Who has 77.47.196.65? Tell 77.47.196.1
458	23.585142	104.20.1.85	77.47.197.26	TCP	66	80 → 53977 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
459	23.585545	77.47.197.26	104.20.1.85	TCP	54	53977 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
460	23.618040	104.20.1.85	77.47.197.26	TCP	66	80 → 53978 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
461	23.618592	77.47.197.26	104.20.1.85	TCP	54	53978 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
462	23.626213	77.47.197.26	104.20.1.85	HTTP	504	GET / HTTP/1.1
463	23.640716	77.47.128.130	77.47.197.26	DNS	548	Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net A 161.69.169.73 A 161.69.169.73
464	23.640718	77.47.128.131	77.47.197.26	DNS	500	Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net A 161.69.169.73 A 161.69.169.73
465	23.644651	77.47.197.26	161.69.169.73	TCP	66	53979 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
466	23.648587	104.20.1.85	77.47.197.26	TCP	60	80 → 53977 [ACK] Seq=1 Ack=451 Win=67584 Len=0
467	23.738502	77.47.197.26	161.69.169.73	TCP	66	53980 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
468	23.764642	Hangzhou_9d:38:c8	Broadcast	ARP	60	Who has 77.47.197.69? Tell 77.47.196.1
469	23.765636	Hangzhou_9d:38:c8	Broadcast	ARP	60	Who has 77.47.196.252? Tell 77.47.196.1
470	23.790684	161.69.169.73	77.47.197.26	TCP	66	443 → 53979 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=512
471	23.790968	77.47.197.26	161.69.169.73	TCP	54	53979 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
472	23.792785	77.47.197.26	161.69.169.73	TLSv1.2	500	Client Hello

> Frame 471: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF{E7910711-2CFD-4CF3-A912-85868977E86D}, id 0

> Ethernet II, Src: AzureNav_87:73:0d (74:c6:3b:87:73:0d), Dst: Hangzhou_9d:38:c8 (00:0f:e2:9d:38:c8)

> Internet Protocol Version 4, Src: 77.47.197.26, Dst: 161.69.169.73

> Transmission Control Protocol, Src Port: 53979, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000 00 0f e2 9d 38 c8 74 c6 3b 87 73 0d 08 00 45 00 ... 8 t : ; s ... E

0010 00 28 41 14 40 00 80 06 5c e3 4d 2f c5 1a a1 45 ... (A @ ... \ N / ... E

0020 a9 49 d2 db 01 bb 86 0d e5 46 03 fa 91 c5 50 10 ... I - ... F ... P

0030 01 00 7c 51 00 00 ... [Q ...

wireshark_Беспроводная сеть_20200306145545_810028.pcapng

Пакеты: 1819 · Показаны: 1819 (100.0%) · Потеряно: 0 (0.0%)

Профили: Default

15:38 06.03.2020

Беспроводная сеть

Файл Редактирование Просмотр Запуск Завхват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

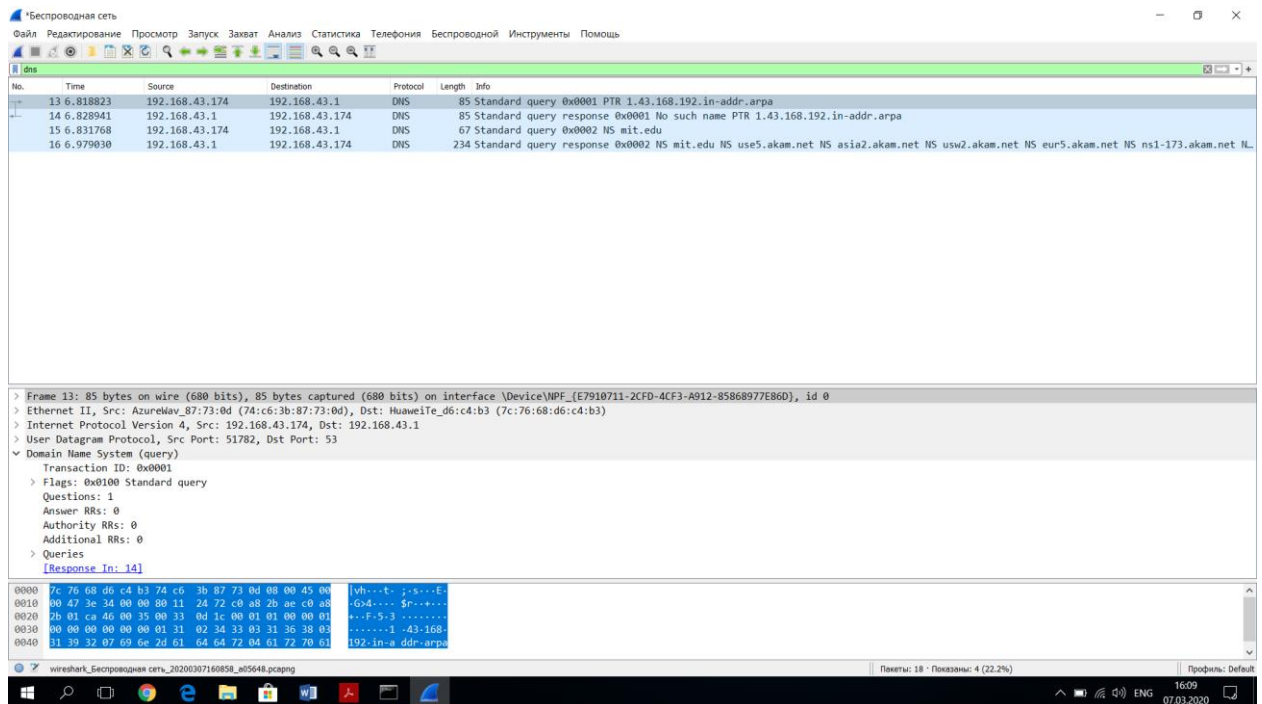
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.174	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
2	0.053013	192.168.43.1	192.168.43.174	DNS	134	Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa SOA localhost
3	0.075658	192.168.43.174	192.168.43.1	DNS	71	Standard query 0x0002 A www.mit.edu
4	0.208225	192.168.43.1	192.168.43.174	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
5	0.219517	192.168.43.174	192.168.43.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
6	0.414062	192.168.43.1	192.168.43.174	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:10e:197...
9	4.389456	192.168.43.174	192.168.43.1	DNS	76	Standard query 0xdc07 A beacons.gvt2.com
10	4.429671	192.168.43.1	192.168.43.174	DNS	92	Standard query response 0xdc07 A beacons.gvt2.com A 172.217.16.3

wireshark_Беспроводная сеть_20200307160338_805196.pcapng

Пакеты: 44 · Показаны: 8 (18.2%) · Потеряно: 0 (0.0%)

Профили: Default

16:03 07.03.2020



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: AzureWav_87:73:0d (74:c6:3b:87:73:0d), D:
> Internet Protocol Version 4, Src: 77.47.197.26, Dst: 77.47
> User Datagram Protocol, Src Port: 59826, Dst Port: 53
> Domain Name System (query)
```

Цільовий порт: 53

Вихідний порт: 59826

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

IP: 77.47.128.130. 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.

[\[Response In: 446\]](#)

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

```
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 5
Additional RRs: 0
> Queries
> Answers
  > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
> Authoritative nameservers
\[Request In: 445\]
[Time: 0.015664000 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.

452	23.359240	Hangzhou_9d:38:c8	Broadcast	ARP	60 Who has 77.47.196.41? Tell 77.47.196.1
453	23.476313	77.47.197.26	104.20.1.85	TCP	66 53977 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
454	23.476855	77.47.197.26	104.20.1.85	TCP	66 53978 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
455	23.479945	77.47.197.26	77.47.128.130	DNS	91 Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
456	23.505190	77.47.197.26	77.47.128.131	DNS	91 Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
457	23.556467	Hangzhou_9d:38:c8	Broadcast	ARP	60 Who has 77.47.196.65? Tell 77.47.196.1
458	23.585142	104.20.1.85	77.47.197.26	TCP	66 80 → 53977 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
459	23.585545	77.47.197.26	104.20.1.85	TCP	54 53977 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
460	23.618040	104.20.1.85	77.47.197.26	TCP	66 80 → 53978 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
461	23.618592	77.47.197.26	104.20.1.85	TCP	54 53978 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
462	23.626213	77.47.197.26	104.20.1.85	HTTP	504 GET / HTTP/1.1
463	23.640716	77.47.128.130	77.47.197.26	DNS	548 Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.com
464	23.640718	77.47.128.131	77.47.197.26	DNS	500 Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.com
465	23.644651	77.47.197.26	161.69.169.73	TCP	66 53979 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
466	23.648587	104.20.1.85	77.47.197.26	TCP	60 80 → 53977 [ACK] Seq=1 Ack=451 Win=67584 Len=0

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

Так виконує.

```
84 Standard query 0xf5e6 A win10.ipv6.microsoft.com
539 Standard query response 0xf5e6 A win10.ipv6.microsoft.com CNAME onpremiwindows.ipv6.microsoft.com.akadns.net CNAME trdovmssukwest
72 Standard query 0x6b01 A www.ietf.org
239 Standard query response 0x6b01 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85 NS ns3.cloudflare
91 Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
91 Standard query 0xa932 A webadvisorc.rest.gti.mcafee.com
548 Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net A 161.69.169.73 A 161.69.169.7
500 Standard query response 0xa932 A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net A 161.69.169.73 A 161.69.169.7
88 Standard query 0x013c A mip.api.mcafeewebadvisor.com
88 Standard query 0x013c A mip.api.mcafeewebadvisor.com
412 Standard query response 0x013c A mip.api.mcafeewebadvisor.com CNAME WACloudLB-1801077940.us-east-1.elb.amazonaws.com A 52.55.223
412 Standard query response 0x013c A mip.api.mcafeewebadvisor.com CNAME WACloudLB-1801077940.us-east-1.elb.amazonaws.com A 35.170.11
78 Standard query 0xba2e A analytics.ietf.org
78 Standard query 0xba2e A analytics.ietf.org
361 Standard query response 0xba2e A analytics.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.yy21.afiliat-nst.info NS ns1.mia1.afilia
361 Standard query response 0xba2e A analytics.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.mia1.afiliat-nst.info NS ns1.ams1.afilia
71 Standard query 0x8c6f A wpad.kpi.ua
123 Standard query response 0x8c6f No such name A wpad.kpi.ua SOA ns.kpi.ua
79 Standard query 0x3772 A clients4.google.com
255 Standard query response 0x3772 A clients4.google.com CNAME clients.l.google.com A 216.58.209.14 NS ns1.google.com NS ns3.google.com
```

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

Цільовий: 192.168.43.1

Вихідний: 192.168.43.1

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

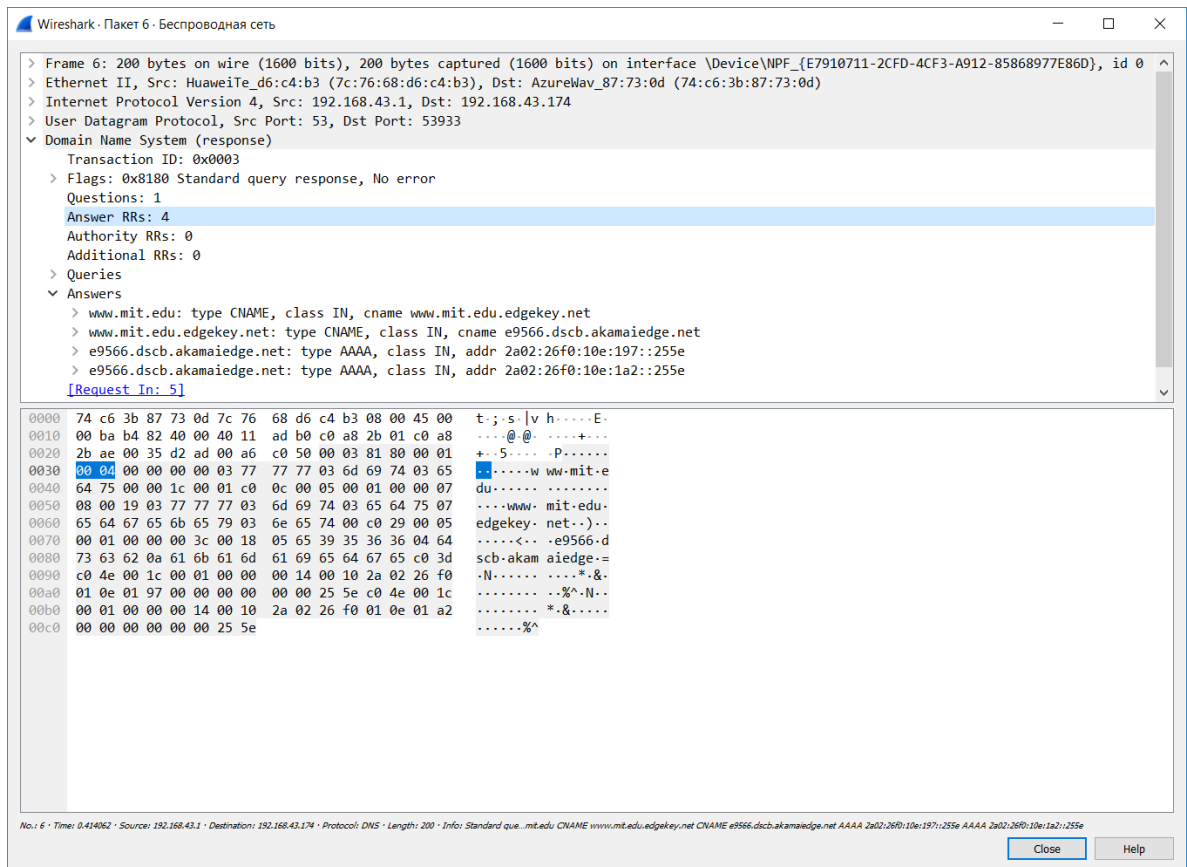
192.168.43.1. Так є адресою локального сервера.

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.

```
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[Response In: 6]
```


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?

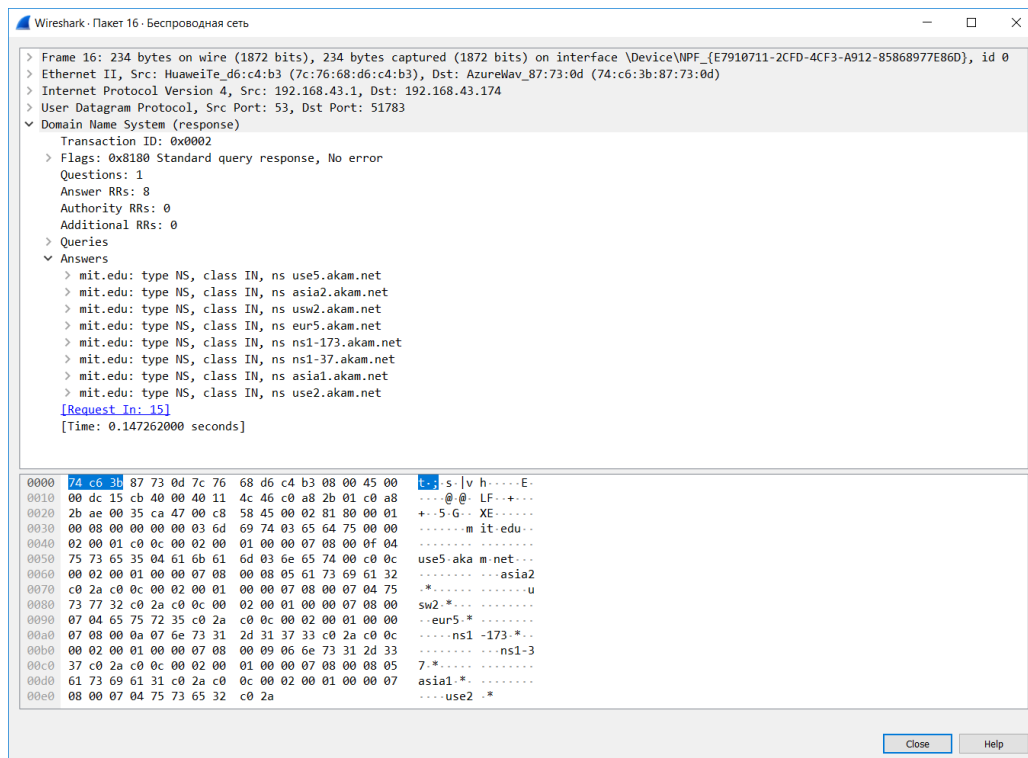
IP: 192.168.43.1. Так є.

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

Стандартний тип запиту. Так вміщує.

```
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[Response In: 14]
```

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: 18.0.72.3. Не є адресою локального сервера.

> Domain Name System (query)

Transaction ID: 0x0001

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

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

Стандартний тип запиту. Ні не вміщує.

> Domain Name System (query)

Transaction ID: 0x0001

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

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

Відповідь не була отримана.

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.