

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

**Лабораторна робота № 3**  
**З дисципліни: Комп'ютерні мережі**

***Протокол DNS***

**Виконав:**  
**Студент III курсу**  
**Групи КА-74**  
**Микитенко О.В.**  
**Перевірів: Кухарєв С. О.**

**Київ 2020**

**Мета роботи:** аналіз деталей роботи протоколу DNS.

## Хід роботи

Необхідно виконати наступні дії:

- ✓ Очистіть кеш DNS-записів
  - для windows-систем виконайте в терміналі `ipconfig /flushdns`
  - для linux-систем (можливо) спрацює перезапуск операційної системи;

```
Командная строка

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::fdb3:d963:ecfe:7ebf%17
IPv4-адрес. . . . . : 192.168.95.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :

Адаптер Ethernet VMware Network Adapter VMnet8:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::910c:aeb:833c:d2c%22
IPv4-адрес. . . . . : 192.168.233.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :

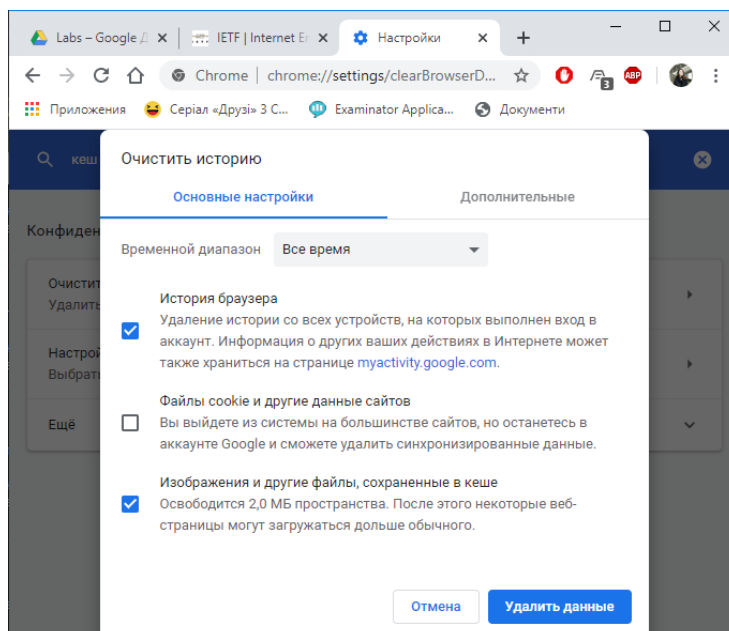
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::145a:abb6:d207:b47d%23
IPv4-адрес. . . . . : 192.168.1.3
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : fe80::1%23
                        192.168.1.1

Адаптер Ethernet Сетевое подключение Bluetooth 2:

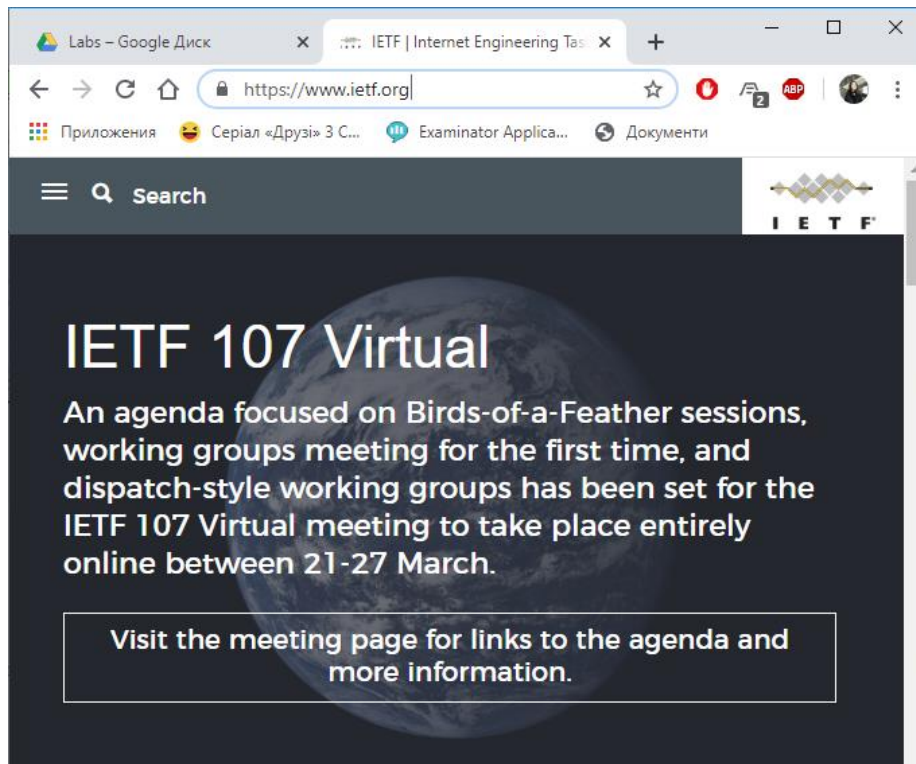
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
```

- ✓ Запустіть веб-браузер, очистіть кеш браузера:
  - для Firefox виконайте Tools >> Clear Private Data (або Ctrl + Shift + Del)
  - для MS IE виконайте Tools >> Internet Options >> Delete File
- ✓ Запустіть Wireshark, почніть захоплення пакетів.

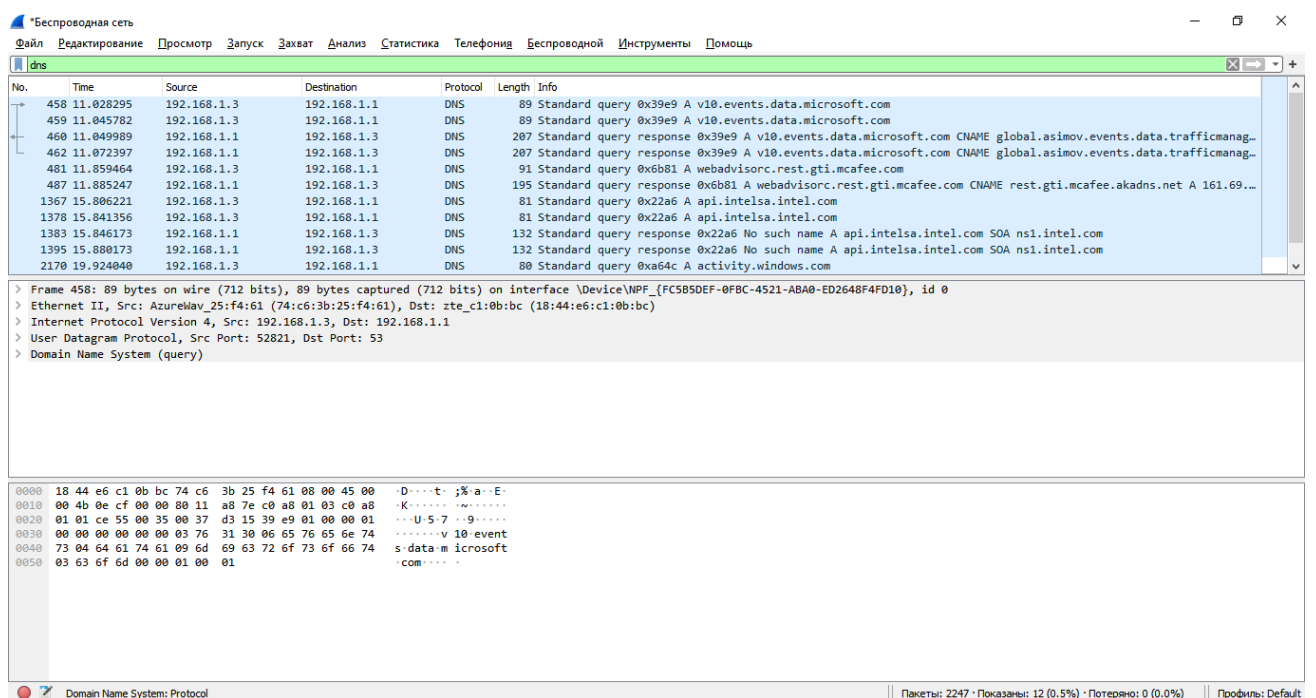


- ✓ Відкрийте за допомогою браузера одну із зазначених нижче адрес:

<http://www.ietf.org>



- ✓ Зупиніть захоплення пакетів.
- ✓ Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).



- ✓ Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.
- ✓ Почніть захоплення пакетів.
- ✓ Виконайте nslookup для домену [www.mit.edu](http://www.mit.edu) за допомогою команди
  - nslookup [www.mit.edu](http://www.mit.edu)

```
C:\Users\Admin>nslookup www.mit.edu
ѠxĖtxĖ: UnKnown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Ѡь : e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d200:19e::255e
           2a02:26f0:d200:191::255e
           104.87.213.214
Aliases: www.mit.edu
          www.mit.edu.edgekey.net

C:\Users\Admin>
```

- ✓ Зупиніть захоплення пакетів.
- ✓ 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.
- ✓ Почніть захоплення пакетів.
- ✓ Виконайте nslookup для домену [www.mit.edu](http://www.mit.edu) за допомогою команди
  - nslookup -type=NS mit.edu

```
C:\Users\Admin>nslookup -type=NS mit.edu
ѠxĖtxĖ: UnKnown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia1.akam.net

C:\Users\Admin>
```

- ✓ Зупиніть захоплення пакетів.
- ✓ Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.
- ✓ Почніть захоплення пакетів.
- ✓ Виконайте nslookup для домену [www.mit.edu](http://www.mit.edu) за допомогою команди

- nslookup www.aiit.or.kr bitsy.mit.edu

```
C:\Users\Admin>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
*~x~x~x~: 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.
*** Превышено время ожидания запроса UnKnown
C:\Users\Admin>
```

- ✓ Зупиніть захоплення пакетів.
- ✓ Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
- ✓ Закрийте Wireshark.

### Контрольні питання

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?

```
> Frame 458: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{FC5B...}
> Ethernet II, Src: AzureWav_25:f4:61 (74:c6:3b:25:f4:61), Dst: zte_c1:0b:bc (18:44:e6:c1:0b:bc)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 52821, Dst Port: 53
> Domain Name System (query)
```

Цільовий: 53

Вихідний: 52821

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

192.168.1.1. Так, є.

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

```
> v10.events.data.microsoft.com: type A, class IN
[Response In: 460]
```

Вміщує.

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

```
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
▼ Queries
  > v10.events.data.microsoft.com: type A, class IN
▼ Answers
  > v10.events.data.microsoft.com: type CNAME, class IN, cname global.asimov.events.data.trafficmanager.net
  > global.asimov.events.data.trafficmanager.net: type CNAME, class IN, cname skypedataprddcoleus04.cloudapp.net
  > skypedataprddcoleus04.cloudapp.net: type A, class IN, addr 52.114.132.73
[Request In: 458]
[Time: 0.021694000 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?

Ні, не співпадає.

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

Так, виконує.

```
89 Standard query 0x39e9 A v10...
89 Standard query 0x39e9 A v10...
91 Standard query 0x6b81 A web...
81 Standard query 0x22a6 A api...
81 Standard query 0x22a6 A api...
80 Standard query 0xa64c A act...
207 Standard query response 0x3...
207 Standard query response 0x3...
195 Standard query response 0x6...
132 Standard query response 0x2...
132 Standard query response 0x2...
189 Standard query response 0xa...
```

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

Цільовий: 192.168.1.3

Вихідний: 192.168.1.3

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

192.168.1.3 . Так, є.

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

```
Transaction ID: 0xe164
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  > lh3.googleusercontent.com: type A, class IN
  [Response In: 869]
```

Так, вміщує.

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

```
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
▼ Queries
  > lh3.googleusercontent.com: type A, class IN
▼ Answers
  > lh3.googleusercontent.com: type CNAME, class IN, cname googlehosted.l.googleusercontent.com
  > googlehosted.l.googleusercontent.com: type A, class IN, addr 172.217.20.193
  [Request In: 811]
[Time: 0.106796000 seconds]
```

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

192.168.1.3 , Так, є.

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

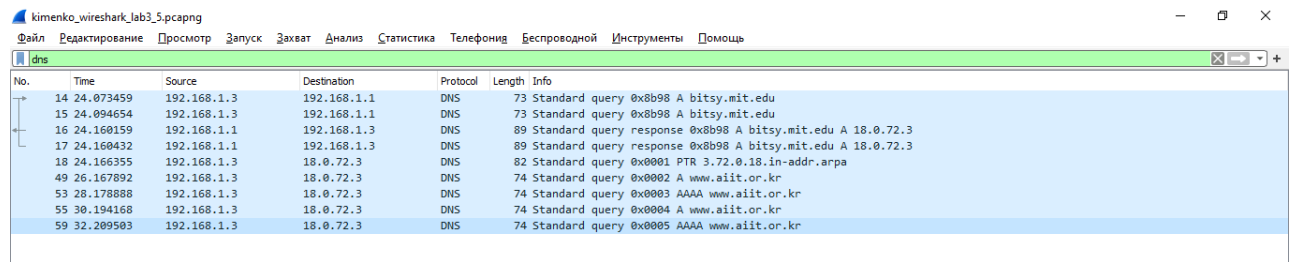
```
> User Datagram Protocol, Src Port: 56368, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x7878
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    > roaming.officeapps.live.com: type A, class IN
    [Response In: 6]
```

Так, вміщує.

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?

```
Wireshark - Пакет 6 - Беспроводная сеть
> User Datagram Protocol, Src Port: 53, Dst Port: 56368
▼ Domain Name System (response)
  Transaction ID: 0x7878
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    > roaming.officeapps.live.com: type A, class IN
  ▼ Answers
    > roaming.officeapps.live.com: type CNAME, class IN, cname prod.roaming1.live.com.akadns.net
    > prod.roaming1.live.com.akadns.net: type A, class IN, addr 52.109.88.10
    [Request In: 5]
    [Time: 0.021765000 seconds]
```

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

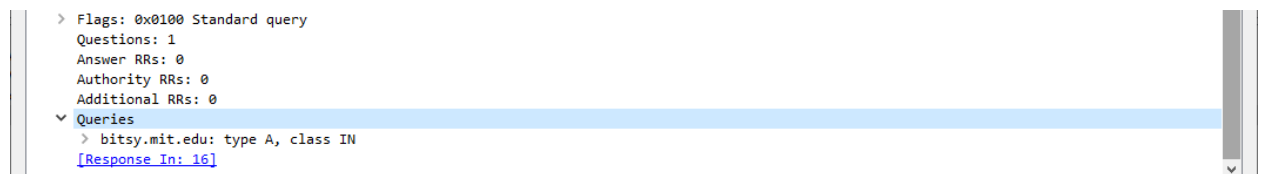


The image shows a Wireshark packet capture of DNS traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
14	24.073459	192.168.1.3	192.168.1.1	DNS	73	Standard query 0x8b98 A bitsy.mit.edu
15	24.094654	192.168.1.3	192.168.1.1	DNS	73	Standard query 0x8b98 A bitsy.mit.edu
16	24.160159	192.168.1.1	192.168.1.3	DNS	89	Standard query response 0x8b98 A bitsy.mit.edu A 18.0.72.3
17	24.160432	192.168.1.1	192.168.1.3	DNS	89	Standard query response 0x8b98 A bitsy.mit.edu A 18.0.72.3
18	24.166355	192.168.1.3	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
49	26.167892	192.168.1.3	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
53	28.178888	192.168.1.3	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
55	30.194168	192.168.1.3	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
59	32.209503	192.168.1.3	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

192.168.1.3 , Так, є

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



Так, 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.