

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

**Практична робота № 3
З курсу: «Комп'ютерні мережі»**

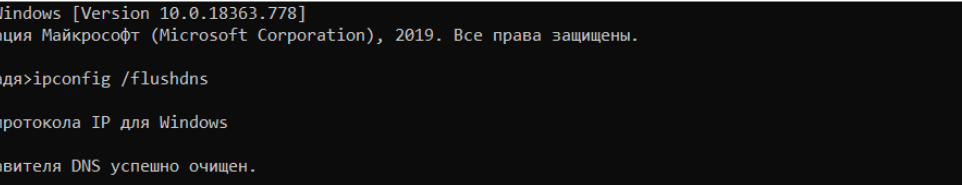
**Виконала:
Студентка III курсу
Групи КА-74
Торліна Н.М.
Прийняв: Кухарєв С.О.**

Київ 2020

Хід виконання роботи

No.	Time	Source	Destination	Protocol	Length	Info
80	4.195501	192.168.1.3	192.168.1.1	DNS	90	Standard query 0xc879 AAAA incoming.telemetry.mozilla.org
81	4.208609	192.168.1.1	192.168.1.3	DNS	90	Standard query response 0xc879 AAAA incoming.telemetry.mozilla.org [Malformed Packet]
482	5.090938	192.168.1.3	192.168.1.1	DNS	78	Standard query 0xf718 A analytics.ietf.org
512	5.116314	192.168.1.3	192.168.1.1	DNS	78	Standard query 0xf718 A analytics.ietf.org
1331	6.117356	192.168.1.3	192.168.1.1	DNS	78	Standard query 0xf718 A analytics.ietf.org
1332	6.458000	192.168.1.1	192.168.1.3	DNS	108	Standard query response 0xf718 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1333	6.462741	192.168.1.1	192.168.1.1	DNS	68	Standard query 0xf943 A ietf.org
1335	6.488159	192.168.1.3	192.168.1.1	DNS	68	Standard query 0xf943 A ietf.org
1336	6.585214	192.168.1.1	192.168.1.3	DNS	84	Standard query response 0xf943 A ietf.org A 4.31.198.44
1337	6.587238	192.168.1.3	192.168.1.1	DNS	68	Standard query 0xcd12 AAAA ietf.org
1338	6.592715	192.168.1.1	192.168.1.3	DNS	68	Standard query response 0xcd12 AAAA ietf.org [Malformed Packet]
1353	6.866527	192.168.1.3	192.168.1.1	DNS	82	Standard query 0x617 a csp.starfieldtech.com
1354	6.875645	192.168.1.1	192.168.1.3	DNS	203	Standard query response 0x617 a csp.starfieldtech.com CNAME ocsip.godaddy.com.akadns.net A 192.124.249.23 A 192.124.249.36 A 192.124.249.45
1355	6.877195	192.168.1.3	192.168.1.1	DNS	87	Standard query 0xf0e1 a csp.godaddy.com.akadns.net
1357	6.885734	192.168.1.1	192.168.1.3	DNS	167	Standard query response 0xf0e1 a csp.godaddy.com.akadns.net A 192.124.249.24 A 192.124.249.41 A 192.124.249.23 A 192.124.249.22 A
1358	6.887950	192.168.1.3	192.168.1.1	DNS	87	Standard query 0xd3ab AAAA csp.godaddy.com.akadns.net
1359	6.892743	192.168.1.1	192.168.1.3	DNS	87	Standard query response 0xd3ab AAAA csp.godaddy.com.akadns.net [Malformed Packet]

```
.....0 ..... = IG bit: Individual address (unicast)
    Source: IntelCor_b5:de:97 (30:24:32:b5:de:97)
      Address: IntelCor_b5:de:97 (30:24:32:b5:de:97)
        .....0 ..... = IG bit: Globally unique address (factory default)
          .....0 ..... = IG bit: Individual address (unicast)
            Type: IPv4 (d=6800e)
    Internet Protocol Version 4 Src: 102.168.1.3 Dest: 102.168.1.1
0000 00 1b fc d2 0d af 30 24 32 b5 de 97 00 00 45 00 .....0S 2 N ---E-
0010 00 4c d0 59 00 00 80 11 e6 f2 c0 a8 01 03 c0 a8 ...L Y-----
0020 01 01 04 01 00 35 00 38 30 44 c8 79 01 00 00 01 .....5 B 0 y---
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....P n incoming
0040 74 05 66 65 6d 65 74 72 79 07 6d 6f 7a 69 6c 6c telemetr y-mozill
0050 61 03 6f 72 67 00 00 1c 00 01 a.org <--
```



The screenshot shows a Windows Command Prompt window titled "Командная строка". The window has standard Windows window controls (minimize, maximize, close) in the top right corner. The command history is as follows:

```
Microsoft Windows [Version 10.0.18363.778]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\Надя>ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.

C:\Users\Надя>nslookup www.mit.edu
тхЕтхЕ: my.router
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Ь : e9566.dscb.akamaiedge.net
Address: 92.123.2.59
Aliases: www.mit.edu
         www.mit.edu.edgekey.net

C:\Users\Надя>
```

```
C:\Users\Надя>nslookup -type=NS mit.edu
mxËtxË: my.router
Address: 192.168.1.1

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

C:\Users\Надя>
```

```

C:\Users\Надя>nslookup www.aiit.or.kr bitsy.mit.edu
(root)
    primary name server = ns.lanet.ua
    responsible mail addr = hostmaster.lanet.kiev.ua
    serial   = 2013053101
    refresh  = 21600 (6 hours)
    retry    = 3600 (1 hour)
    expire   = 604800 (7 days)
    default TTL = 60 (1 min)
TxTxTxTx: UnKnown
Address: 18.0.72.3

Lь :      www.aiit.or.kr.WiFi
Address: 194.50.85.176

```

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?

```

> Frame 80: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{4097BEAC-29BC-4A0B-B36C-1A0B97A76A1B}, id 0
> Ethernet II, Src: IntelCor_b5:4e:97 (30:24:32:b5:4e:97), Dst: ASUSTekC_d2:0d:af (00:1b:fc:d2:0d:af)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 1025, Dst Port: 53

```

Протокол: UDP

Цільовий порт: 53

Вихідний порт: 1025

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

IP: 192.168.1.1, є адресом локального сервера.

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.

[\[Response In: 81\]](#)

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

```
Domain Name System (response)
  Transaction ID: 0xf718
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
```

2 відповіді.

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.

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

Так, виконує.

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

Цільовий порт: 53

Вихідний: 1059

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

192.168.1.1, 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.

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

3 відповіді

```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 92.123.2.59
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 4
    Address: 92.123.2.59
```

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

dns							
No.	Time	Source	Destination	Protocol	Length	Info	
4	3.171113	192.168.1.3	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa	
5	3.174766	192.168.1.1	192.168.1.3	DNS	107	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR my.router	
6	3.176924	192.168.1.3	192.168.1.1	DNS	72	Standard query 0x0002 NS mit.edu.WiFi	
7	3.198066	192.168.1.1	192.168.1.3	DNS	147	Standard query response 0x0002 No such name NS mit.edu.WiFi SOA a.root-servers.net	
8	3.198761	192.168.1.3	192.168.1.1	DNS	67	Standard query 0x0003 NS mit.edu	
9	3.203427	192.168.1.1	192.168.1.3	DNS	234	Standard query response 0x0003 NS mit.edu NS asia1.akam.net NS eur5.akam.net NS ns1	

> Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{4097BEAC-29BC-4A0B-B36C-1A0B97A76A1B}, id 0	
> Ethernet II, Src: IntelCor_b5:4e:97 (30:24:32:b5:4e:97), Dst: ASUSTekC_d2:0d:af (00:1b:fc:d2:0d:af)	
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.1	
User Datagram Protocol, Src Port: 8142, Dst Port: 53	
Source Port: 8142	
Destination Port: 53	
Length: 50	
Checksum: 0xcfb5 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 1]	

0000	00 1b fc d2 0d af 30 24	32 b5 4e 97 08 00 45 000\$ 2-N...E
0010	00 46 d1 15 00 00 80 11	e6 3c c0 a8 01 03 c0 a8	..F.....<.....
0020	01 01 1f ce 00 35 00 32	cf b5 00 01 01 00 00 015.....
0030	00 00 00 00 00 00 01 31	01 31 03 31 36 38 03 311..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	

IP: 192.168.1.1. Так є.

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

Тип запиту PTR. Так, вміщує.

```
▼ Domain Name System (query)
  Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    [Response In: 5]
```

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?

1 запис із відповіддю.

dns						
No.	Time	Source	Destination	Protocol	Length	Info
4	3.171113	192.168.1.3	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
5	3.174766	192.168.1.1	192.168.1.3	DNS	107	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR my.router
6	3.176924	192.168.1.3	192.168.1.1	DNS	72	Standard query 0x0002 NS mit.edu.WiFi
7	3.198066	192.168.1.1	192.168.1.3	DNS	147	Standard query response 0x0002 No such name NS mit.edu.WiFi SOA a.root-servers.n
8	3.198761	192.168.1.3	192.168.1.1	DNS	67	Standard query 0x0003 NS mit.edu
9	3.203427	192.168.1.1	192.168.1.3	DNS	234	Standard query response 0x0003 NS mit.edu NS asia1.akam.net NS eur5.akam.net NS

> Frame 5: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface \Device\NPF_{4097BEAC-29BC-4A0B-B36C-1A0B97A76A1B}, id 0
> Ethernet II, Src: ASUSTekC_d2:0d:af (00:1b:fc:d2:0d:af), Dst: IntelCor_b5:4e:97 (30:24:32:b5:4e:97)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
> User Datagram Protocol, Src Port: 53, Dst Port: 8142
▼ Domain Name System (response)
 Transaction ID: 0x0001
 > Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 ▼ Answers
 > 1.1.168.192.in-addr.arpa: type PTR, class IN, my.router
 Name: 1.1.168.192.in-addr.arpa
 Type: PTR (domain name PointeR) (12)
 Class: IN (0x0001)
 Time to live: 10000 (2 hours, 46 minutes, 40 seconds)
 Data length: 11
 Domain Name: my.router
 [Request In: 4]
 [Time: 0.003653000 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?

dns						
No.	Time	Source	Destination	Protocol	Length	Info
8	2.841183	192.168.1.3	192.168.1.1	DNS	73	Standard query 0xae9 A bitsy.mit.edu
9	2.867153	192.168.1.1	192.168.1.1	DNS	73	Standard query 0xae9 A bitsy.mit.edu
10	2.878549	192.168.1.1	192.168.1.3	DNS	89	Standard query response 0xae9 A bitsy.mit.edu A 18.0.72.3
11	2.887282	192.168.1.3	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
12	2.889997	18.0.72.3	192.168.1.3	DNS	150	Standard query response 0x0001 PTR 3.72.0.18.in-addr.arpa SOA ns.lanet.ua
13	2.898332	192.168.1.3	18.0.72.3	DNS	79	Standard query 0x0002 A www.aiit.or.kr.WiFi
14	2.901329	18.0.72.3	192.168.1.3	DNS	135	Standard query response 0x0002 A www.aiit.or.kr.WiFi A 194.50.85.176 NS ns.lanet.ua A 194.50.85.1
15	2.902870	192.168.1.3	18.0.72.3	DNS	79	Standard query 0x0003 AAAA www.aiit.or.kr.WiFi
16	2.905025	18.0.72.3	192.168.1.3	DNS	147	Standard query response 0x0003 AAAA www.aiit.or.kr.WiFi SOA ns.lanet.ua

IP: 192.168.1.1. Є адресою локального сервера.

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

Стандартний тип запиту. Вміщує.

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

1 відповідь.

```
▼ Domain Name System (response)
  Transaction ID: 0xae9
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  ▼ Answers
    ▼ 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: 300 (5 minutes)
      Data length: 4
      Address: 18.0.72.3
    [Request In: 8]
    [Time: 0.037366000 seconds]
```

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.