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»

Виконав: студент групи ІС 91
Дуб М.М.

Київ – 2020

Лабораторна робота №3

3. Протокол DNS

Мета роботи: аналіз деталей роботи протоколу DNS NS.

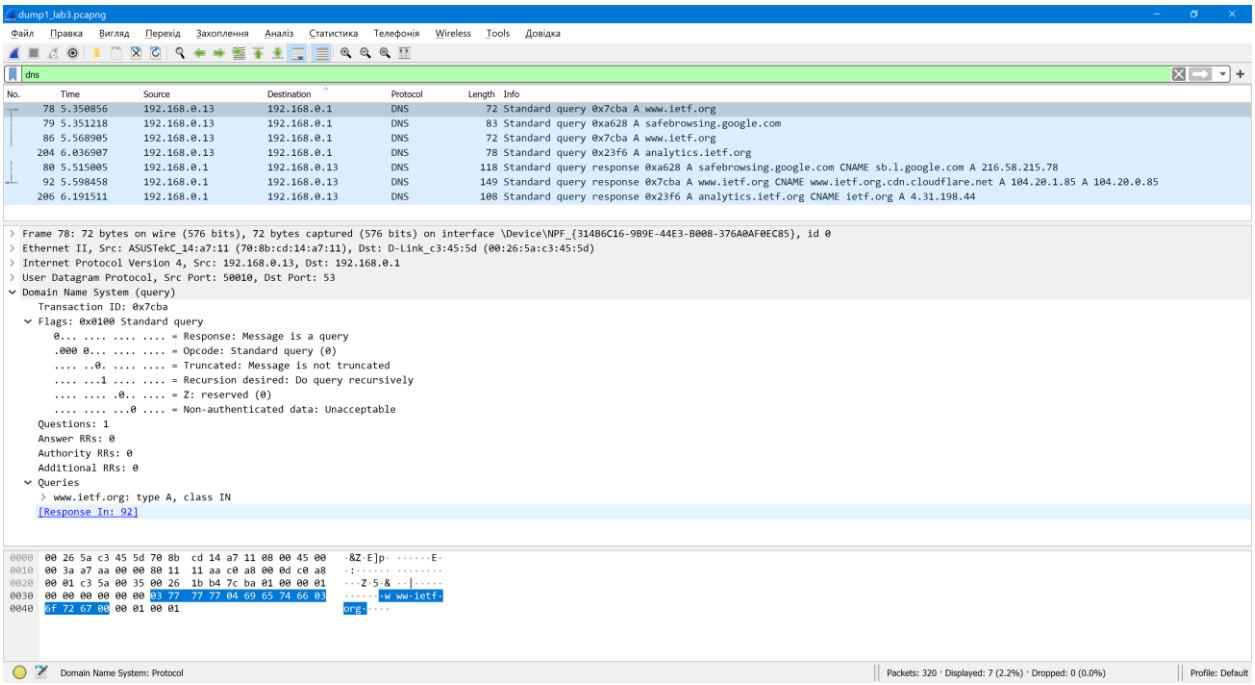
3.2. Хід роботи

Виконаємо наступні дії:

1. Очистимо кеш DNS-записів
2. Запустимо веб-браузер, очистимо кеш браузера:
3. Запустимо Wireshark, почнемо захоплення пакетів.
4. Відкриємо за допомогою браузера одну із зазначених нижче адрес:

http://www.ietf.org

5. Зупинемо захоплення пакетів.
6. Переглянемо деталі захоплених пакетів.



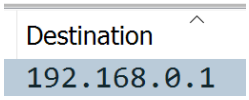
7. Приготуємо відповіді на контрольні запитання 1-6, роздрукуємо необхідні для цього пакети.

    7.1. Знайдемо запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер

вихідного порта відповіді DNS?

```
User Datagram Protocol, Src Port: 50010, Dst Port: 53
    Source Port: 50010
    Destination Port: 53
    Length: 38
    Checksum: 0x1bb4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
  > [Timestamps]
```

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



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

```
Queries
  www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

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

```
▾ 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: 349 (5 minutes, 49 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.20.1.85
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.20.0.85
  [Request In: 78]
  [Time: 0.247602000 seconds]
```

7.5. Проаналізуємо 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

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

```
User Datagram Protocol, Src Port: 64447, Dst Port: 53
    Source Port: 64447
    Destination Port: 53
    Length: 44
    Checksum: 0xfadc [unverified]
    [Checksum Status: Unverified]
    [Stream index: 13]
  > [Timestamps]
Domain Name System (query)
    Transaction ID: 0x23f6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v analytics.ietf.org: type A, class IN
        Name: analytics.ietf.org
        [Name Length: 18]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 206]
```

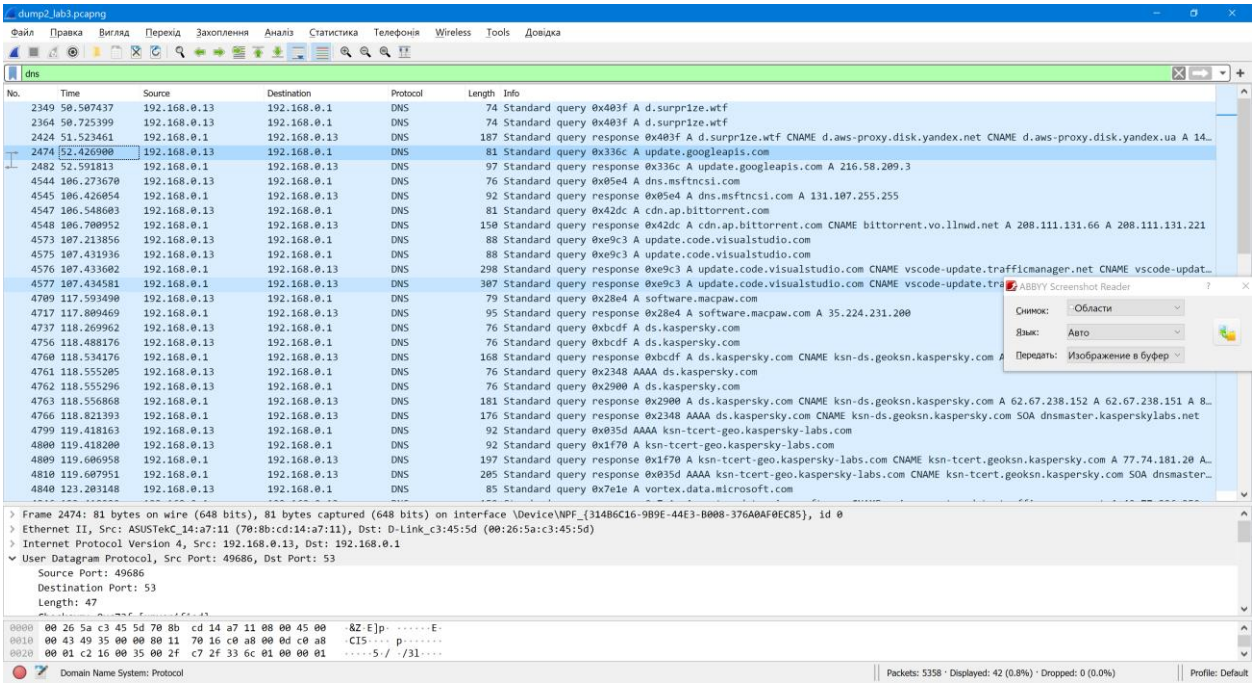
8. Почнимо захоплення пакетів.
9. Виконаємо nslookup для домену www.mit.edu за допомогою команди
   a. nslookup www.mit.edu

```
C:\Users\ASUS>nslookup www.mit.edu
╤xËTxË:  UnKnown
Address:  192.168.0.1

Не заслуживающий доверия ответ:
╚ь :     e9566.dscb.akamaiedge.net
Addresses:  2001:2030:b:18e::255e
          2001:2030:b:196::255e
          104.120.255.198
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net


C:\Users\ASUS>
```

10. Зупинимо захоплення пакетів.



11. Приготуємо відповіді на контрольні запитання 7-10, роздрукуємо 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.

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

```
User Datagram Protocol, Src Port: 49686, Dst Port: 53
    Source Port: 49686
    Destination Port: 53
    Length: 47
    Checksum: 0xc72f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 93]
  > [Timestamps]
```

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

192.168.0.13	192.168.0.1
192.168.0.1	192.168.0.13

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

```
Queries
  update.googleapis.com: type A, class IN
      Name: update.googleapis.com
      [Name Length: 21]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

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

```
Answers
  update.googleapis.com: type A, class IN, addr 216.58.209.3
      Name: update.googleapis.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 216.58.209.3
  [Request In: 2474]
  [Time: 0.164913000 seconds]
```

12. Почнимо захоплення пакетів.
13. Виконаємо nslookup для домену www.mit.edu за допомогою команди
    a. nslookup –type=NS mit.edu

```
C:\Users\ASUS>nslookup -type=NS mit.edu
╤xËTxË:  UnKnown
Address:  192.168.0.1

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

14. Зупинимо захоплення пакетів.

15. Приготуємо відповіді на запитання 11-13. При необхідності роздрукуємо деякі захоплені пакети.

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

Source	Destination
192.168.0.1	192.168.0.13
192.168.0.13	192.168.0.1

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

```
Queries
  mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
  [Response In: 2923]
```

15.13. Дослідимо 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?

```
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
  Queries
    mit.edu: type NS, class IN
  Answers
    mit.edu: type NS, class IN, ns eur5.akam.net
    mit.edu: type NS, class IN, ns use2.akam.net
    mit.edu: type NS, class IN, ns use5.akam.net
    mit.edu: type NS, class IN, ns usw2.akam.net
    mit.edu: type NS, class IN, ns asia1.akam.net
    mit.edu: type NS, class IN, ns asia2.akam.net
    mit.edu: type NS, class IN, ns ns1-37.akam.net
    mit.edu: type NS, class IN, ns ns1-173.akam.net
  [Request In: 2918]
  [Time: 0.290000000 seconds]
```

16. Почнемо захоплення пакетів.
17. Виконаємо nslookup для домену www.mit.edu за допомогою команди
    a. nslookup www.aiit.or.kr bitsy.mit.edu

```
C:\Users\ASUS>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
╤xËTxË:  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\ASUS>
```

18. Зупинимо захоплення пакетів.

19. Приготуємо відповіді на запитання 14-16

19.14. 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?

Source	Destination
192.168.0.13	192.168.0.1
192.168.0.1	192.168.0.13

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

```
▾ 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: 147]
```

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

```
▾ 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: 1127 (18 minutes, 47 seconds)
      Data length: 4
      Address: 18.0.72.3
  [Request In: 146]
  [Time: 0.151612000 seconds]
```