



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

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

***Основи захоплення та аналізу пакетів***

**Виконав:**  
**Студентка ІІІ курсу**  
**Групи КА-71**  
**Висоцька М. А.**  
**Перевірив: Кухарєв С. О.**

**Київ 2020**

**Мета роботи:** оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

## Хід виконання роботи

lab3.1.pcapng

Файл Правка Видгляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Tools Довідка

dns

No.	Time	Source	Destination	Protocol	Length	Info
45	7.101159	192.168.1.1	192.168.1.165	DNS	202	Standard query response 0x9cc6 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb...
46	7.110500	192.168.1.165	192.168.1.1	DNS	72	Standard query 0xe81d A www.ietf.org
47	7.135960	192.168.1.165	192.168.1.1	DNS	72	Standard query 0xe81d A www.ietf.org
59	7.773761	192.168.1.1	192.168.1.165	DNS	149	Standard query response 0xe81d A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 1...
61	7.775311	192.168.1.165	192.168.1.1	DNS	91	Standard query 0x5460 A www.ietf.org.cdn.cloudflare.net
62	7.776263	192.168.1.1	192.168.1.165	DNS	123	Standard query response 0x5460 A www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20...
63	7.777501	192.168.1.165	192.168.1.1	DNS	91	Standard query 0x1d89 AAAA www.ietf.org.cdn.cloudflare.net
66	7.803172	192.168.1.165	192.168.1.1	DNS	91	Standard query 0x1d89 AAAA www.ietf.org.cdn.cloudflare.net
70	7.817599	192.168.1.1	192.168.1.165	DNS	147	Standard query response 0x1d89 AAAA www.ietf.org.cdn.cloudflare.net AAAA 2606:4700:10:...
85	8.336083	192.168.1.165	192.168.1.1	DNS	77	Standard query response 0xf7fc A oosp.digicert.com
86	8.347144	192.168.1.1	192.168.1.165	DNS	125	Standard query response 0xf7fc A oosp.digicert.com CNAME cs9.wac.phicdn.net A 93.184.22...

> Frame 66: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF\_{9C329E68-482C-4E13-AE6B-2E92975BF30E}, id 0

> Ethernet II, Src: IntelCor\_a8:ee:e5 (28:16:ad:a8:ee:e5), Dst: ASUSTekC\_e5:4e:70 (18:31:bf:e5:4e:70)

> Internet Protocol Version 4, Src: 192.168.1.165, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 1025, Dst Port: 53

▼ Domain Name System (query)

> Transaction ID: 0x1d89

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

[Retransmitted request. Original request in: 63]

[Retransmission: True]

0000 18 31 bf e5 4e 70 28 16 ad a8 ee e5 08 00 45 00 -1-Np(.....E-

Frame (frame), 91 byte(s)

Packets: 2288 · Displayed: 35 (1.5%) · Dropped: 0 (0.0%) | Profile: Default

Type here to search

14:56 12.04.2020

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?

UDP

Source Port: 1025  
Destination Port: 53

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

192.168.1.1

Так

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

Тип Стандартний

[\[Response In: 41\]](#)

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

```
▼ Answers
> incoming.telemetry.mozilla.ORG: type CNAME, class IN, cname telemetry-incoming.r53-2.services.mozilla.com
> telemetry-incoming.r53-2.services.mozilla.com: type CNAME, class IN, cname pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 34.212.75.43
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 52.88.91.154
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 52.88.126.42
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 52.36.109.157
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 44.228.71.55
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 52.88.148.130
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 52.10.174.113
> pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com: type A, class IN, addr 34.212.193.45
[Request In: 39]
[Time: 0.014367000 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

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

Так

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

```
Source Port: 1031
Destination Port: 53
```

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

192.168.1.1

Так

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

Тип Стандартний

[\[Response In: 37\]](#)

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

```
Queries
  www.mit.edu: type AAAA, class IN
    Name: www.mit.edu
    [Name Length: 11]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)

Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:2d8:3:996::255e
  > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:2d8:3:9a2::255e
[Request In: 36]
[Time: 0.087325000 seconds]
```

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

192.168.1.1

Так

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

Стандартного типу. 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?

```
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
> Queries
Answers
  1.1.168.192.in-addr.arpa: type PTR, class IN, router.asus.com
    Name: 1.1.168.192.in-addr.arpa
    Type: PTR (domain name PointeR) (12)
    Class: IN (0x0001)
    Time to live: 0 (0 seconds)
    Data length: 17
    Domain Name: router.asus.com
[Request In: 50]
[Time: 0.002495000 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?

192.168.1.1

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

Стандартного типу

```
▼ Domain Name System (query)
  Transaction ID: 0x3fa4
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    > clients6.google.com: type A, class IN
    [Response In: 22]
```

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

```
> queries
▼ Answers
  > clients6.google.com: type CNAME, class IN, cname clients.1.google.com
  > clients.1.google.com: type A, class IN, addr 216.58.209.14
  [Request In: 21]
  [Time: 0.011973000 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 роботи даних протоколів.