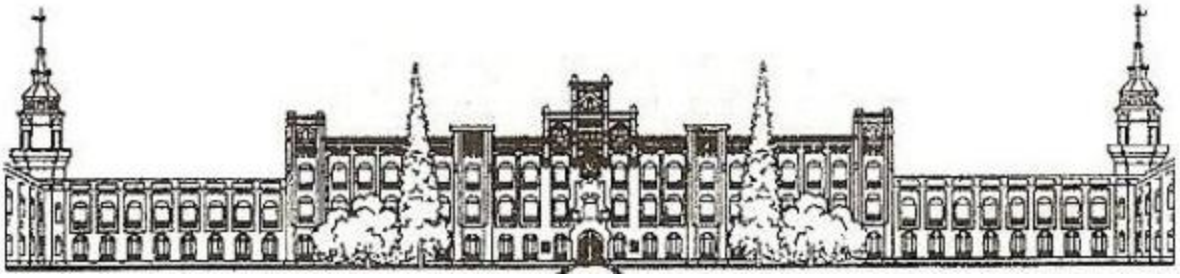

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Лабораторна робота № 1

З дисципліни: Комп'ютерні мережі

Основи захоплення та аналізу пакетів

Виконала:

Студентка III курсу

Групи КА-72

Третьяков М.Ю.

Перевірив: Кухарєв С. О.

Київ 2020

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

Хід виконання роботи

Відсилка пакету:

```
No.     Time           Source                Destination           Protocol Length Info
    104 24.978757      192.168.1.110         128.119.245.12        HTTP     550    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 104: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id
0
Ethernet II, Src: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd), Dst: Tp-LinkT_71:2a:bb (e8:94:f6:71:2a:bb)
Internet Protocol Version 4, Src: 192.168.1.110, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52380, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 106]
    [Next request in frame: 115]
```

Відповідь:

```
No.     Time           Source                Destination           Protocol Length Info
    106 25.113321      128.119.245.12        192.168.1.110         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 106: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id
0
Ethernet II, Src: Tp-LinkT_71:2a:bb (e8:94:f6:71:2a:bb), Dst: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.110
Transmission Control Protocol, Src Port: 80, Dst Port: 52380, Seq: 1, Ack: 497, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 16 Feb 2020 20:58:02 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 16 Feb 2020 06:59:03 GMT\r\n
    ETag: "51-59eabf95317c3"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.134564000 seconds]
    [Request in frame: 104]
    [Next request in frame: 115]
    [Next response in frame: 125]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?

   TCP, HTTP, DNS, SSL, TLSv1.3, ICMPv6, UDP

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?

ICP, Ethernet II, HTTP, TCP.

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Пройшло 0,135 с.

4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

Запит:

Вихідна:192.168.1.110

Цільова:128.119.45.12

Відповідь:

Вихідний: 128.119.45.12

Цільовий: 192.168.1.110

5. Яким був перший рядок запиту на рівні протоколу HTTP?

GET /wireshark-labs/...

6. Яким був перший рядок відповіді на рівні протоколу HTTP?

HTTP/1.1 OK\r\n

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.