МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №1

з курсу «Комп’ютерні мережі»

тема: «Основи захоплення та аналізу пакетів»

Виконала: студентка 3 курсу
групи КА-77
Нерубенко А.А
Прийняв: Кухарєв С.О.

Київ – 2020р.

Вихідний пакет:

```
No.     Time           Source                Destination           Protocol Length Info
     35 4.657366       192.168.31.207        128.119.245.12        HTTP     670    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 35: 670 bytes on wire (5360 bits), 670 bytes captured (5360 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEl_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50337, Dst Port: 80, Seq: 1, Ack: 1, Len: 616
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
    Cache-Control: max-age=0\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 OPR/66.0.3515.115\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\r\n
    If-None-Match: "51-5a16b37287b8d"\r\n
    If-Modified-Since: Sun, 22 Mar 2020 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 37]
```

Вхідні пакет:

```
No.     Time           Source                Destination           Protocol Length Info
     37 4.787665       128.119.245.12        192.168.31.207        HTTP     293    HTTP/1.1 304 Not Modified
Frame 37: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: XIAOMIEl_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.31.207
Transmission Control Protocol, Src Port: 80, Dst Port: 50337, Seq: 1, Ack: 617, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 22 Mar 2020 12:05:05 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-5a16b37287b8d"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.130299000 seconds]
    [Request in frame: 35]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

Контрольні запитання:

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

   ARP, SSDP, TCP, NBNS, MDSN, LLMNR, HTTP

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

   Ethernet II, Internet Protocol Version 4, Transmission Control Protocol.

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до

отримання першого пакету з відповіддю сервера?

   4.787665-4.657366=0.130299

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

   Вихідна - 192.168.31.207

   Цільова - 128.119.245.12

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

```
GET  /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
```

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

```
HTTP/1.1 304 Not Modified
```

Висновки:

Оволоділи методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих проколів.