«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КПІ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №1

з курсу «Комп'ютерні мережі»

тема: «Основи захоплення та аналізу пакетів»

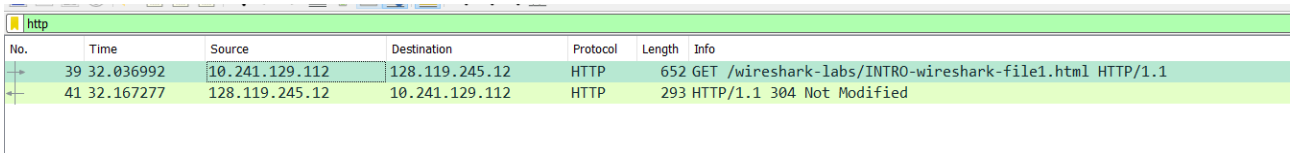
Виконала: студентка 3 курсу

групи КА-74

Лященко К. С.

Прийняв: Кухарєв С. О.

Київ – 2020



Запит

```
No.     Time           Source                Destination           Protocol Length Info
     39 32.036992      10.241.129.112        128.119.245.12        HTTP     652    GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 39: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \Device\NPF_{64D1ABB5-
F872-4E20-B500-6D1F7CF2C4C4}, id 0
Ethernet II, Src: IntelCor_b4:b8:38 (c0:b6:f9:b4:b8:38), Dst: JuniperN_7c:bb:c1 (5c:5e:ab:7c:bb:c1)
Internet Protocol Version 4, Src: 10.241.129.112, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59074, Dst Port: 80, Seq: 1, Ack: 1, Len: 598
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\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: "51-59f24ac6d8b1d"\r\n
    If-Modified-Since: Sat, 22 Feb 2020 06:59:04 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: 41]
```

Відповідь

```
No.     Time           Source                Destination           Protocol Length Info
     41 32.167277      128.119.245.12        10.241.129.112        HTTP     293    HTTP/1.1 304 Not Modified
Frame 41: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{64D1ABB5-
F872-4E20-B500-6D1F7CF2C4C4}, id 0
Ethernet II, Src: JuniperN_7c:bb:c1 (5c:5e:ab:7c:bb:c1), Dst: IntelCor_b4:b8:38 (c0:b6:f9:b4:b8:38)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.241.129.112
Transmission Control Protocol, Src Port: 80, Dst Port: 59074, Seq: 1, Ack: 599, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 22 Feb 2020 12:18:01 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: "51-59f24ac6d8b1d"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.130285000 seconds]
    [Request in frame: 39]
    [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?
   TCP, SSL, TLSv1.2, DNS, HTTP
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
   HTTP, TCP, IP
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
   Час відправлення пакету – 32.036992
   Час отримання відповіді – 32.167277
   Отже, час між відправленням запиту та отриманням відповіді:
   32.167277 – 32.036992 = 0.130285
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
   У запиті
   Вихідна: 10.241.129.112
   Цільова: 128.119.245.12
   У відповіді
   Вихідна: 128.119.245.12
   Цільова: 10.241.129.112
5. Яким був перший рядок запиту на рівні протоколу HTTP?
   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n,
   де GET – метод,
   /wireshark-labs/INTRO-wireshark-file1.html – адреса,
   HTTP/1.1 – код протоколу.
6. Яким був перший рядок відповіді на рівні протоколу HTTP?
   HTTP/1.1 304 Not Modified\r\n,
   де HTTP/1.1 – код протоколу,
   304 Not Modified – код відповіді.