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

Лабораторна робота №1

З дисципліни: **«Комп'ютерні мережі»**

На тему: **«Основи захоплення та аналізу пакетів»**

Виконала:

Студентка III курсу

Групи КА-74

Горюшкіна К.Г.

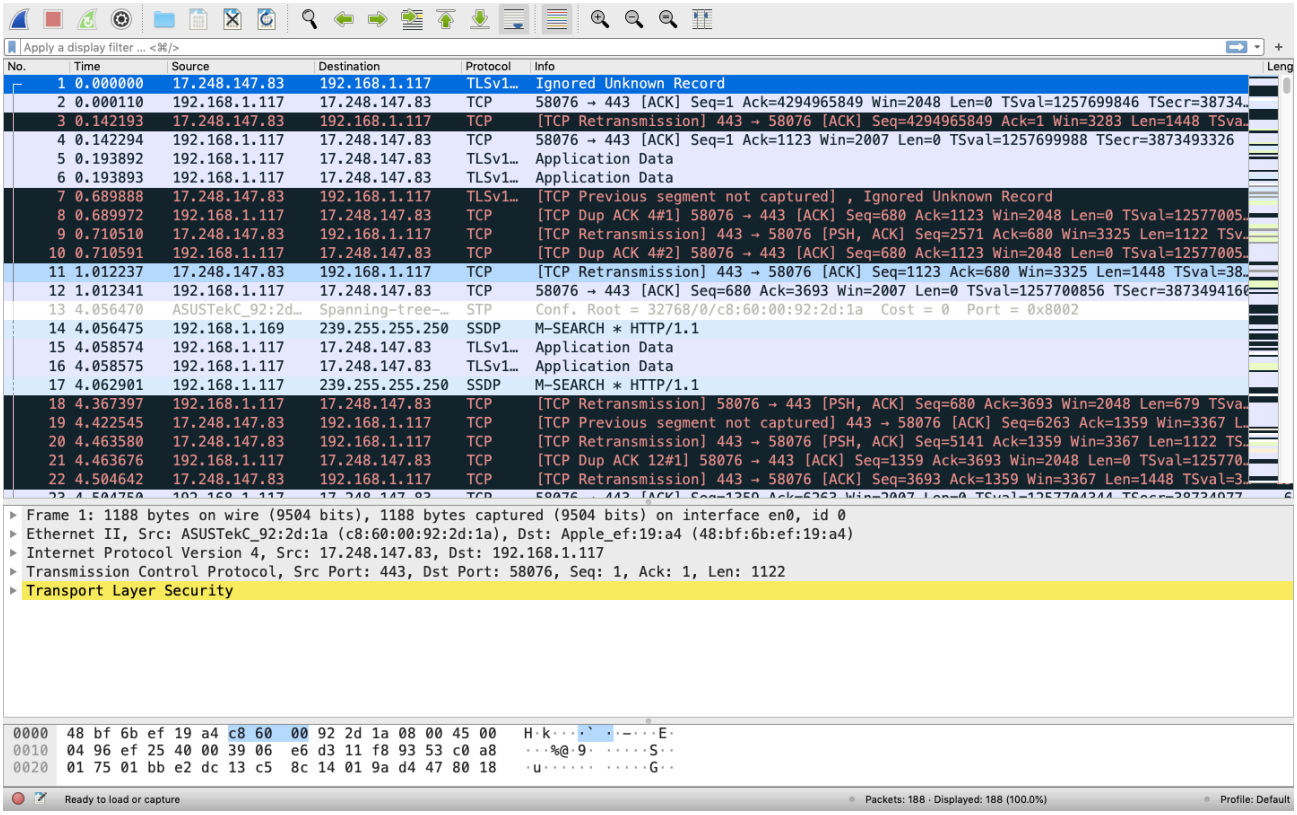
Перевірив:

Кухарєв С.О.

Київ 2020

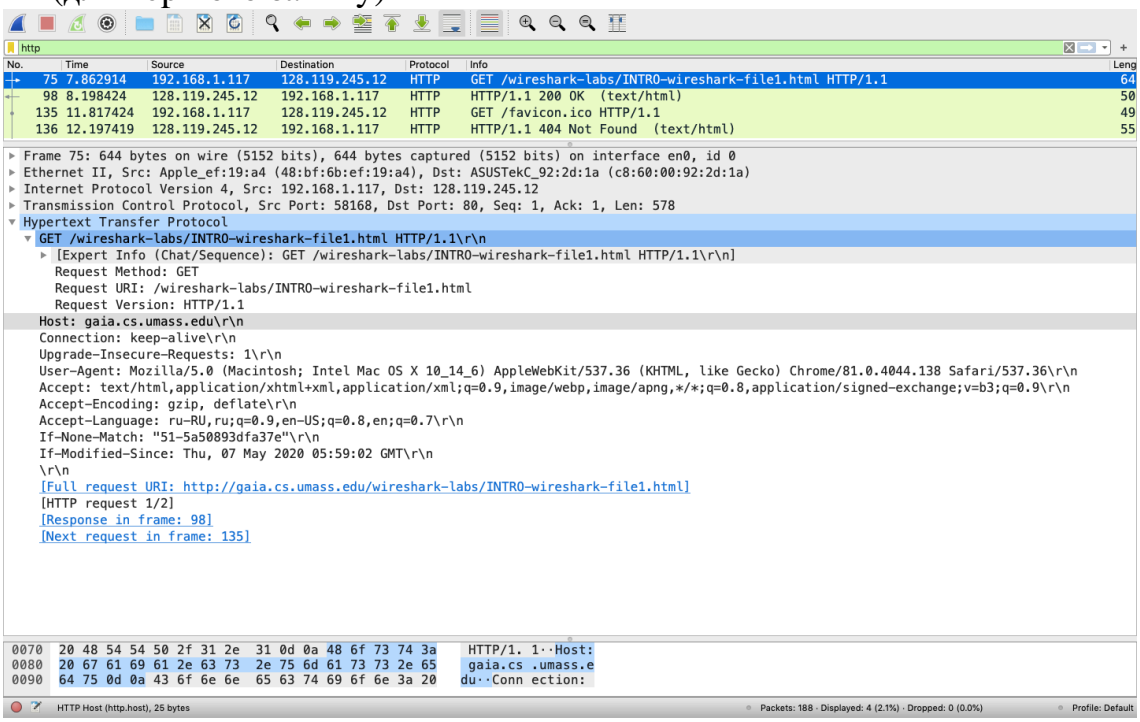
Хід виконання роботи

1. Після запуску Wireshark та введення відповідного запиту у браузері отримали захоплені пакети:

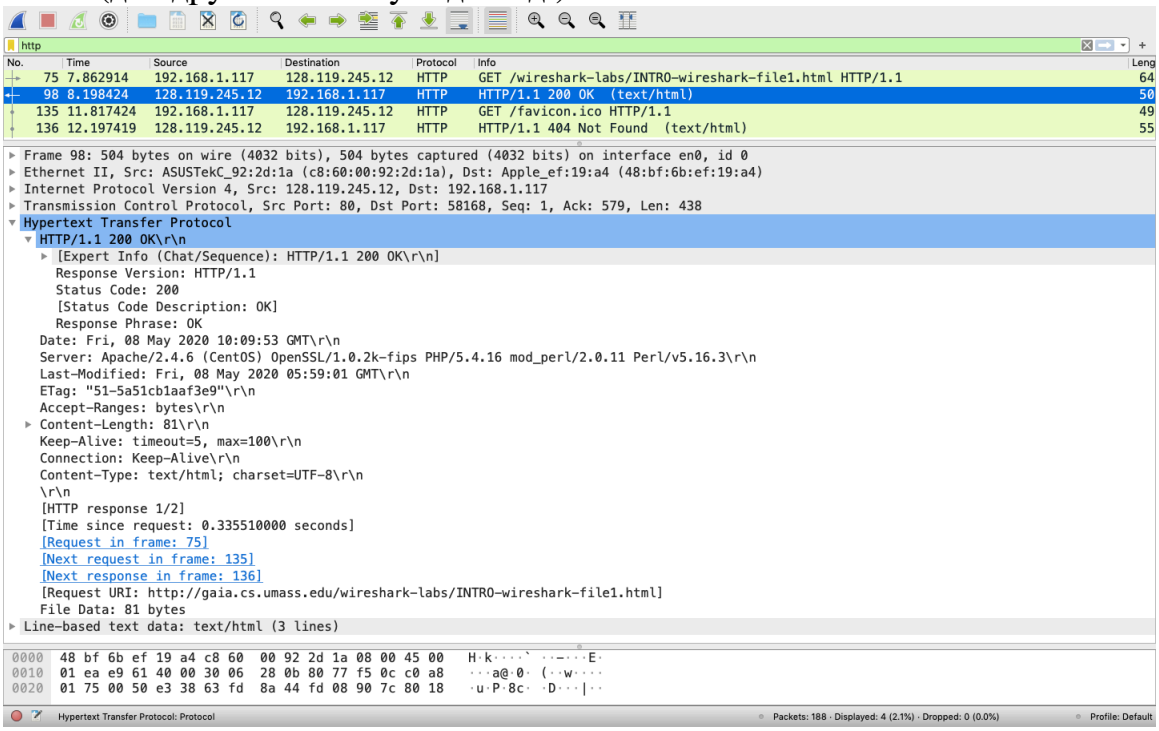


2. Серед них обираємо лише ті пакети, які створені протоколом HTTP і розкриваємо деталі, пов’язані з цим протоколом:

(для першого запиту)



(для другого запиту-відповіді)



3. Друкуємо пакети:
   (Пакет запиту):

```
No.     Time           Source                Destination           Protocol Info
Length
     75 7.862914       192.168.1.117         128.119.245.12        HTTP     GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1         644
Frame 75: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface en0, id 0
Ethernet II, Src: Apple_ef:19:a4 (48:bf:6b:ef:19:a4), Dst: ASUSTekC_92:2d:1a (c8:60:00:92:2d:
1a)
Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58168, Dst Port: 80, Seq: 1, Ack: 1, Len: 578
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/81.0.4044.138 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: "51-5a50893dfa37e"\r\n
    If-Modified-Since: Thu, 07 May 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 1/2]
    [Response in frame: 98]
    [Next request in frame: 135]
```

(Пакет відповіді):

```
No.     Time           Source                Destination           Protocol Info
Length
     98 8.198424       128.119.245.12        192.168.1.117         HTTP     HTTP/1.1 200 OK
(text/html)                                    504
Frame 98: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0
Ethernet II, Src: ASUSTekC_92:2d:1a (c8:60:00:92:2d:1a), Dst: Apple_ef:19:a4 (48:bf:6b:ef:
19:a4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117
Transmission Control Protocol, Src Port: 80, Dst Port: 58168, Seq: 1, Ack: 579, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Fri, 08 May 2020 10:09:53 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: Fri, 08 May 2020 05:59:01 GMT\r\n
    ETag: "51-5a51cb1aaf3e9"\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: 0.335510000 seconds]
    [Request in frame: 75]
    [Next request in frame: 135]
    [Next response in frame: 136]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
```

Контрольні запитання:

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

   TLS (Transport Layer Security)

   Захист на транспортному рівні(4); надає можливості безпечної передачі даних в Інтернет для навігації/пошти/спілкування/обміну файлами

   TCP (Transmission Control Protocol)

   Працює на транспортному рівні моделі OSI(4), управляє передачею даних в комп'ютерній мережі

   STP (Spanning Tree Protocol)

   Протокол канального рівня(2), усуває зайві з'єдання (петлі) в топології довільної мережі Ethernet

   UDP (User Datagram Protocol)

   Працює на транспортному рівні(4) моделі OSI як і TCP, але виконує обмін повідомленнями (датаграмами) без підтвердження та гарантії їх доставки

   ARP (Address Resolution Protocol)

   Канальний рівень(2), визначає MAC-адресу по IP-адресі іншого комп'ютера

   Наприклад: комп'ютери, з'єднані через Ithernet, не можуть працювати за допомогою IP, тоді один робить запит іншому повідомити номер його MAC-адреси

   DNS (Domain Name System)

   Прикладний рівень(7) (доступ до мережевих служб), перетворє ім'я хоста (комп'ютера/мережевого пристрою) в IP-адресу

   SSDP (Simple Service Discovery Protocol)

   Сеансовий рівень OSI(5), описує механізм, за допомогою якого мережеві клієнти виявляють різні мережеві сервіси

   HTTP (Hypertext Transfer Protocol)

Прикладний рівень(7), передає веб-сторінки (текстові файли з рзміткою HTML), а також зображення і застосунки

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
   Ethernet II, Internet Protocol version 4, TCP (Transmission Control Protocol), HTTP
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
   t = 8.198424 – 7.862914 = 0.33551
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
   Пакет із запитом:
   Вихідна адреса: 192.168.1.117
   Цільова адреса: 128.119.245.12
   Пакет із відповіддю:
   Вихідна адреса: 128.119.245.12
   Цільова адреса: 192.168.1.117

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/1.1 200 OK (text/html)

Висновки: у ході роботи я ознайомилась з методами роботи в середовищі захоплення та аналізу пакетів Wireshark