Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Кафедра математичних методів системного аналізу

ЗВІТ

про виконання лабораторних робіт
з дисципліни «Комп'ютерні мережі»

Виконав: студент групи ІС 91
Дуб М.М.

Київ – 2020

Лабораторна робота 1

1. Основи захоплення та аналізу пакетів

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

1.2. Хід роботи

Виконаємо наступні дії:

1. Запустимо веб-браузер.
2. Запустимо Wireshark.
3. В Wireshark активуємо діалог вибору мережевого інтерфейсу для захоплення: Capture >> Interfaces (або ж Ctrl + I)
4. Далі виберемо той інтерфейс, для якого відображається найбільша кількість захоплених пакетів та натиснемо кнопку Start навпроти нього
5. Поки Wireshark захоплює пакети, відкриємо в браузері сторінку за наступною адресою:
   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
   Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.
6. Зупинемо захоплення пакетів за допомогою команди Capture >> Stop (або Ctrl + E)
7. Введемо текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу пакетів залишилися тільки пакети, які були створені протоколом HTTP.
8. Виберемо перший пакет HTTP, який відображається в вікні лістингу, це повідомлення GET протоколу HTTP. Також цей пакет вміщує інформації інших протоколів нижчих рівнів: TCP, IP, Ethernet.
9. У вікні деталей заголовків розкриємо деталі, пов'язані з протоколом HTTP та звернемо детальну інформацію про інші протоколи.
10. Роздрукуємо перші пакети запиту та відповіді. Для цього слід виділимо пакет, який роздрукуємо в окремий файл.
11. Перевіримо, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.
12. Закриємо Wireshark.

1.3. Контрольні запитання

Форма звітності: роздруківки збережених в ході ЛР пакетів з фаміліями, ініціалами та групами виконавців (бажано на кожній сторінці).

Контрольні запитання:

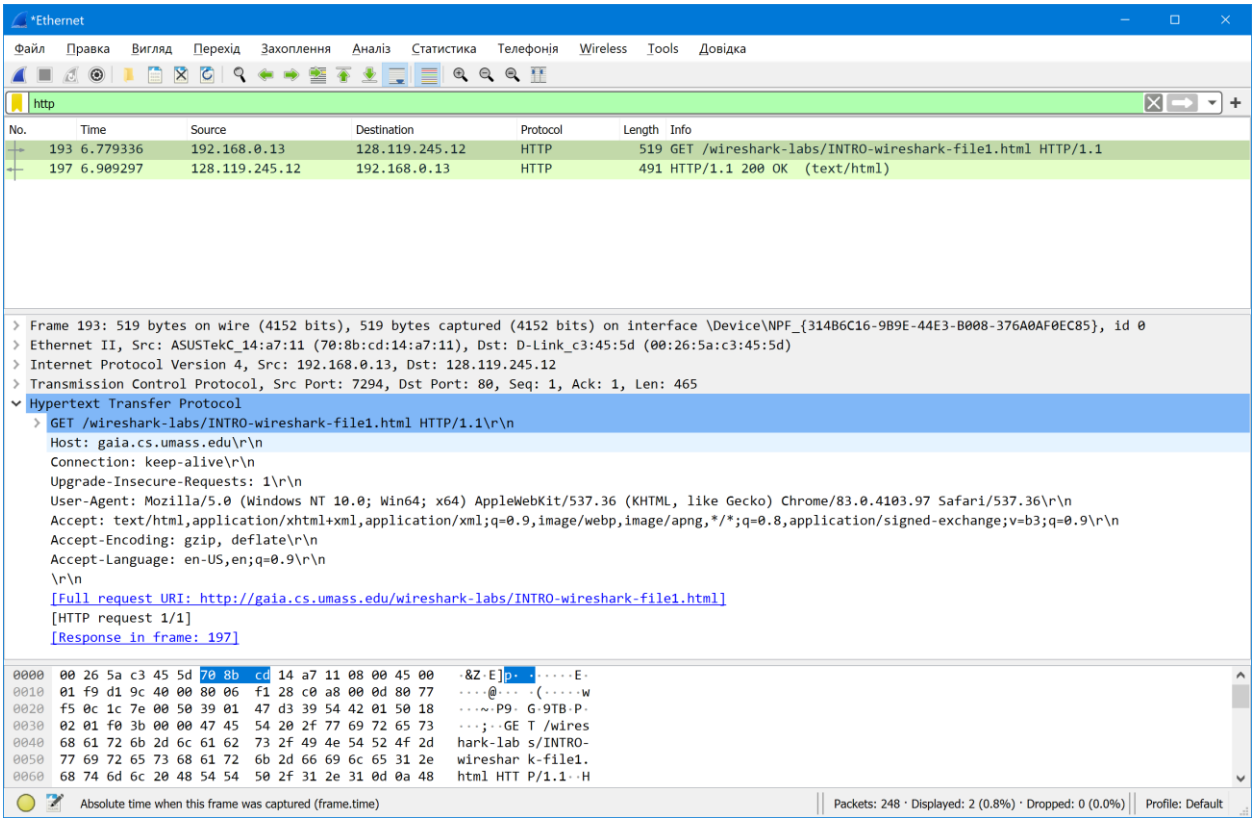
1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
   ARP, BROWSER, BitTorrent, CIP I/O, DNS, DHCPv6, HTTP, HTTPXML, ICMP, TCP, TLSv1.2, UDP, TLSv1.2, WireGuard, collectd

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

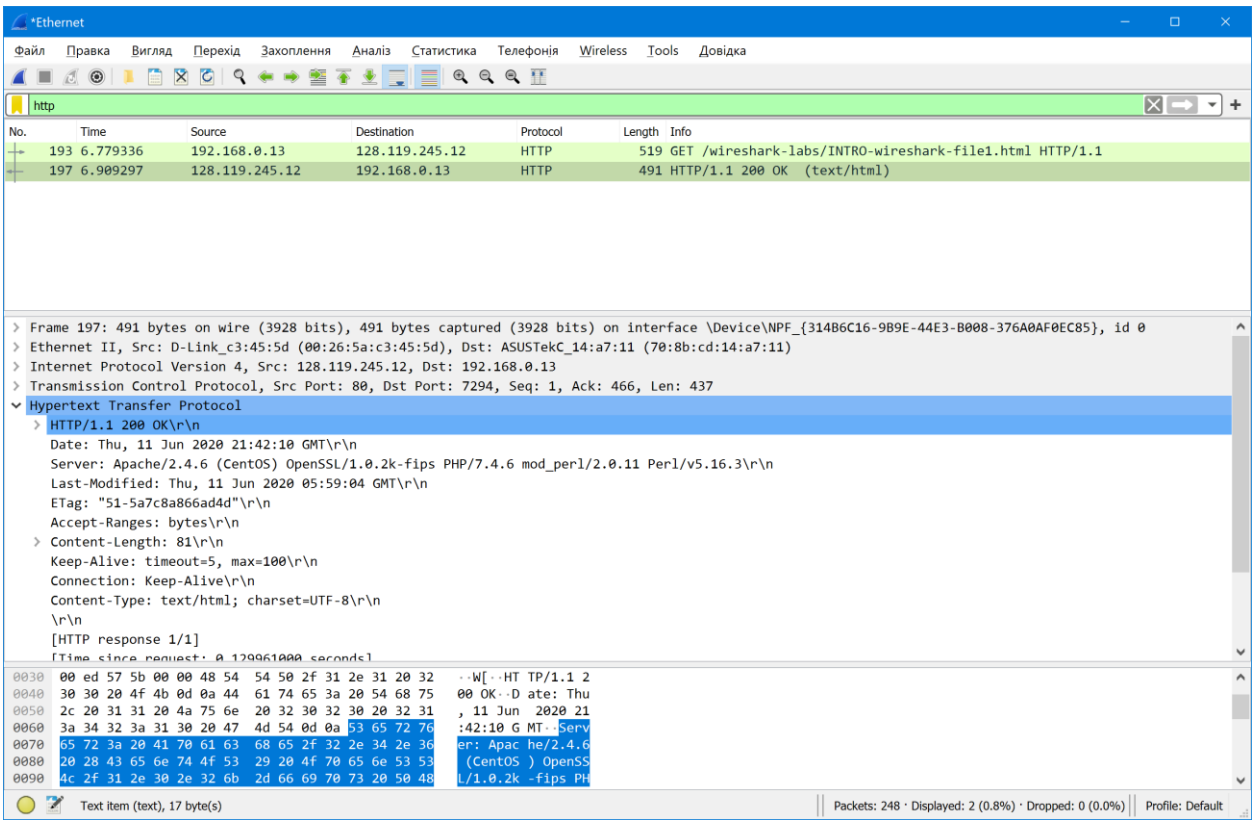
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
   Jun 12, 2020 00:42:08.568406000 Фінляндія (літо)
   Jun 12, 2020 00:42:08.698367000 Фінляндія (літо)
   Прошло 0,13 с

4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
   Пакет із запитом - Source: 192.168.0.13 Destination: 128.119.245.12
   Пакет із відповіддю - Source: 128.119.245.12 Destination: 192.168.0.13

5. Яким був перший рядок запиту на рівні протоколу HTTP?
   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n



6. Яким був перший рядок відповіді на рівні протоколу HTTP?
   HTTP/1.1 200 OK\r\n


*Ethernet
Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Tools Довідка
http
No. Time Source Destination Protocol Length Info
193 6.779336 192.168.0.13 128.119.245.12 HTTP 519 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
197 6.909297 128.119.245.12 192.168.0.13 HTTP 491 HTTP/1.1 200 OK (text/html)
Frame 197: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{314B6C16-9B9E-44E3-B008-376A0AF0EC85}, id 0
Ethernet II, Src: D-Link_c3:45:5d (00:26:5a:c3:45:5d), Dst: ASUSTekC_14:a7:11 (70:8b:cd:14:a7:11)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.13
Transmission Control Protocol, Src Port: 80, Dst Port: 7294, Seq: 1, Ack: 466, Len: 437
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 11 Jun 2020 21:42:10 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.6 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Thu, 11 Jun 2020 05:59:04 GMT\r\n
ETag: "51-5a7c8a866ad4d"\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 1/1]
0030 00 ed 57 5b 00 00 48 54 54 50 2f 31 2e 31 20 32 ··W[··HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 00 OK··D ate: Thu
0050 2c 20 31 31 20 4a 75 6e 20 32 30 32 30 20 32 31 , 11 Jun 2020 21
0060 3a 34 32 3a 31 30 20 47 4d 54 0d 0a 53 65 72 76 :42:10 G MT··Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
Text item (text), 17 byte(s)
Packets: 248 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%)
Profile: Default

C:\Users\ASUS\AppData\Local\Temp\wireshark_Ethernet_20200612004201_a25916.pcapng 248 total packets, 2 shown

```
No.     Time           Source                Destination           Protocol Length Info
    193 6.779336       192.168.0.13          128.119.245.12        HTTP     519    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 193: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits) on interface \Device\NPF_{314B6C16-9B9E-44E3-
B008-376A0AF0EC85}, id 0
Ethernet II, Src: ASUSTekC_14:a7:11 (70:8b:cd:14:a7:11), Dst: D-Link_c3:45:5d (00:26:5a:c3:45:5d)
Internet Protocol Version 4, Src: 192.168.0.13, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 7294, Dst Port: 80, Seq: 1, Ack: 1, Len: 465
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/83.0.4103.97 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: en-US,en;q=0.9\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: 197]
No.     Time           Source                Destination           Protocol Length Info
    197 6.909297       128.119.245.12        192.168.0.13          HTTP     491    HTTP/1.1 200 OK  (text/html)
Frame 197: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{314B6C16-9B9E-44E3-
B008-376A0AF0EC85}, id 0
Ethernet II, Src: D-Link_c3:45:5d (00:26:5a:c3:45:5d), Dst: ASUSTekC_14:a7:11 (70:8b:cd:14:a7:11)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.13
Transmission Control Protocol, Src Port: 80, Dst Port: 7294, Seq: 1, Ack: 466, Len: 437
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 11 Jun 2020 21:42:10 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.6 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 11 Jun 2020 05:59:04 GMT\r\n
    ETag: "51-5a7c8a866ad4d"\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 1/1]
    [Time since request: 0.129961000 seconds]
    [Request in frame: 193]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```