**«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»**

**НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КПІ»**

**КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

**Лабораторна робота №1**

**з курсу «Комп»ютерні мережі»**

**Виконала: студентка 3 курсу**

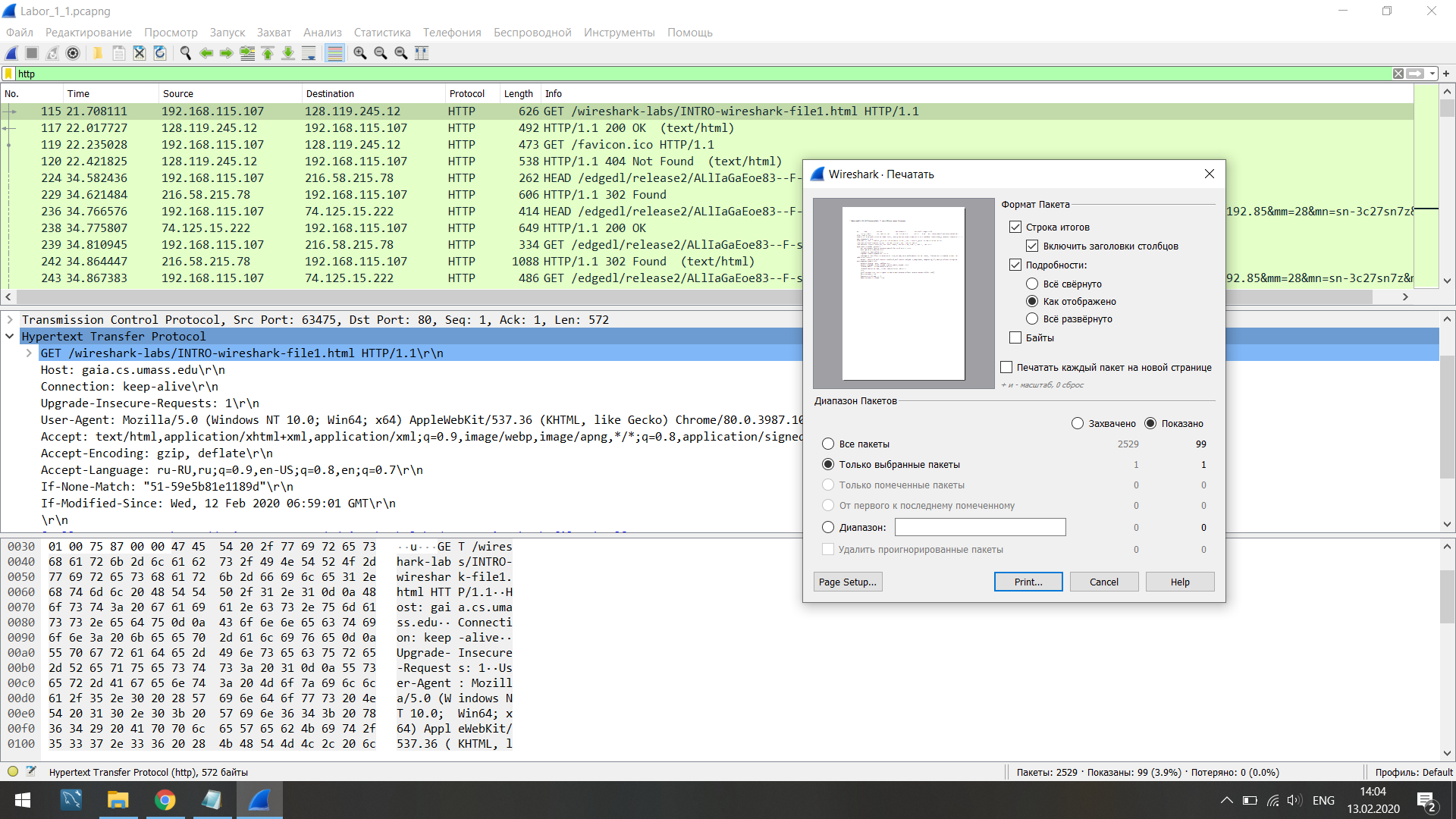
**групи КА 73**

**Собкович В.С.**

**Прийняв: Кухарєв С.О.**

**Київ 2020 р.**

**Лабораторна робота:**



Frame 115: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF\_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0

Ethernet II, Src: IntelCor\_95:51:8c (bc:a8:a6:95:51:8c), Dst: Cisco-Li\_43:47:22 (00:25:9c:43:47:22)

Internet Protocol Version 4, Src: 192.168.115.107, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 63475, Dst Port: 80, Seq: 1, Ack: 1, Len: 572

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/80.0.3987.100 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: "51-59e5b81e1189d"\r\n

If-Modified-Since: Wed, 12 Feb 2020 06:59:01 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: 117]

[Next request in frame: 119]

**Контрольні запитання:**

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

ARP, TLSv1.2, UDP, TCP, DNC, NBNS, MDNS, LLMNR, HTTP, TLSv1.3,

*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?*

22.017727 – 21.708111 = 0.3096160

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

192.168.115.107 128.119.245.12

128.119.245.12 192.168.115.107

*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)

**Висновок:**

В даній лабораторній роботі я оволоділа методами роботи в середовищі захоплення та аналізу пакетів Wireshark.

Основні теоретичні дані

Основним інструментом для спостереження за обміном повідомленнями між

робочими станціями, що підтримують деякий протокол комунікації є снифер пакетів. Як

випливає з назви, сніфер захоплює ( "нюхає") повідомлення, відправлені/отримані з/в

робочої станції. Також сніфер, як правило, зберігає та/або відображає вміст значень

заголовків протоколів у цих захоплених повідомленнях.

Сніфер пакетів являє собою пасивну компоненту. Це означає, що відбувається

спостереження повідомлень, відправлених та отриманих прикладними процесами

декількох робочих станцій, але сніфер ніколи не відправляє нові чи модифікує виявлені

пакети. Аналогічним чином, неможливо адресувати пакети напряму процесу

перехоплювача пакетів. Замість цього, пакет сніфер отримує копії пакетів, які

відправляються/отримуються додатками та протоколами його робочої станції.

Малюнок 1. Архітектура сніферу пакетів.

Малюнок 1 показує структуру сніферу пакетів. Справа показані протоколи (в

даному випадку, інтернет-протоколи) і додатки наприклад, веб-браузер або FTP-клієнт),

які зазвичай запускаються на комп'ютері. Перехоплювач пакетів, як показано в

пунктирному прямокутнику на малюнку 1 є доповненням до звичайних програмних

додатків на комп'ютері, і складається з двох частин. Бібліотеки Packet Capture отримують

копію кожного фрейма канального рівня, який передається/отримується комп'ютером.

Захоплення всіх кадрів канального рівня, забезпечує можливість аналізу усіх повідомлень,

що надіслані/отримані від/для всіх протоколів і програм, виконуваних робочою станцією.

Другим компонентом сніферу є аналізатор пакетів, що відображає зміст усіх заголовків

пакету для кожного з протоколів. Для того щоб зробити це, то пакет Аналізатор повинен

"розуміти" структуру заголовків для більшості протоколів.

Для виконання лабораторних робіт рекомендується використовувати сніфер

Wireshark, за допомогою якого ми зможемо відобразити вміст повідомлень та заголовків

для різних рівнів стеку мережевих протоколів. В аудиторіях використовується віртуальна

машина з заздалегідь встановленим Wireshark.