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: ст. гр. ІС-зп92

Щербак Р.В.

Прийняв: Кухарєв С.О.

Київ – 2020

**Лабораторна робота 1**

**Основи захоплення та аналізу пакетів**

**1. Хід роботи**

1. Запустіть веб-браузер

2. Запустіть Wireshark.

3. В Wireshark активуйте діалог вибору мережевого інтерфейсу для захоплення: Capture >> Interfaces (або ж Ctrl + I)

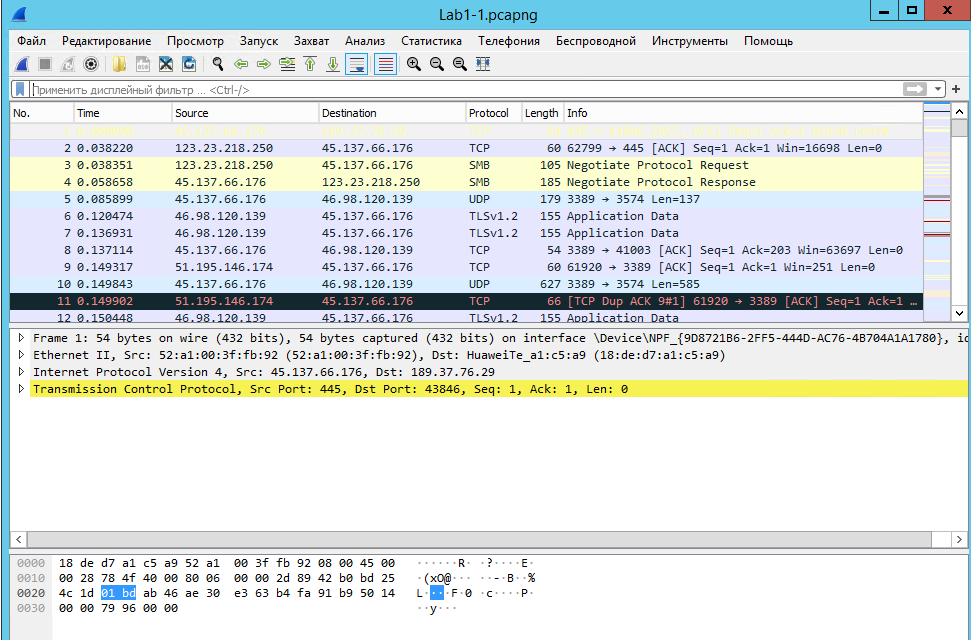
4. Далі виберіть той інтерфейс, для якого відображається найбільша кількість захоплених пакетів та натисніть кнопку Start навпроти нього

5. Поки Wireshark захоплює пакети, відкрийте 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

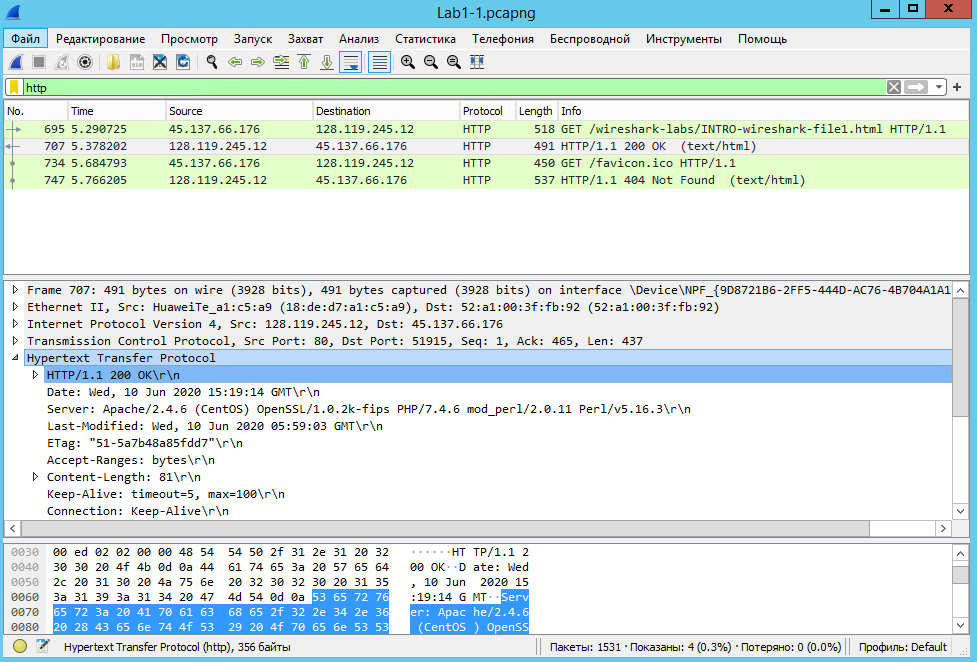
6. Зупиніть захоплення пакетів за допомогою команди Capture >> Stop (або Ctrl + E)



Малюнок 1.1 – Результати виклику

7. Введіть текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу

пакетів. Мають залишитися тільки пакети, які були створені протоколом HTTP



Малюнок 1.2 – Результати фільтрації

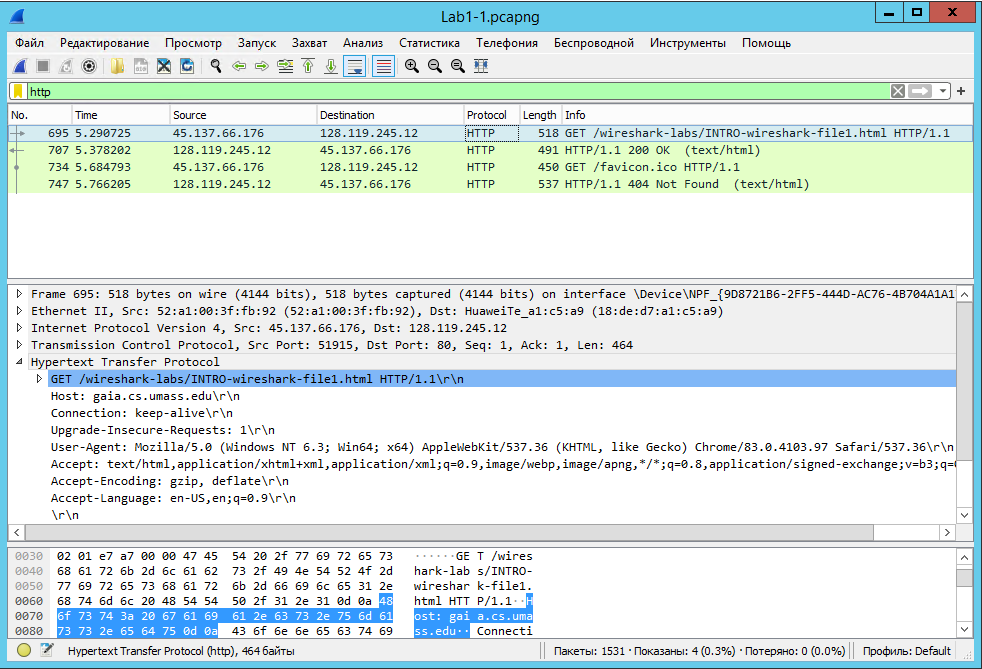
8. Виберіть перший пакет HTTP, який відображається в вікні лістингу, це має

Бути повідомлення GET протоколу HTTP. Також цей пакет має вміщувати

Інформації інших протоколів нижчих рівнів: TCP, IP, Ethernet.

9. У вікні деталей заголовків розкрийте деталі, пов’язані з протоколом HTTP та

скрийте детальну інформацію про інші протоколи.



Малюнок 1.3 – Деталі НТТР пакету

10. Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print, та налаштувати його так як показано на Малюнку 3 (ім’я файлу слід змінити на більш інформативне).

**2. Контрольні запитання:**

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

* TCP, UDP, DNS, HTTP, SMB, TLSv1.2, ARP, LLMNR, TLSv1.3, NBNS

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

* Request: IP, TCP, HTTP
* Response: IP, TCP, HTTP

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

* [Time since request: 0.087477000 seconds]

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

* Request: SRC: 45.137.66.176 DST: 128.119.245.12
* Response: SRC: 128.119.245.12 DST: 45.137.66.176

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