«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИЕТУ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

**ЛАБОРАТОРНА РОБОТА № 1**

з дисципліни

Комп’ютерні мережі

Студент групи ІСзп-93

Шендрік А.О.

Київ – 2020

**Необхідно виконати наступні дії:**

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
   1. в випадку коли інтерфейс ще не ввімкнено можна вибрати any;
   2. в випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;
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)
7. Введіть текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу пакетів мають залишитися тільки пакети, які були створені протоколом HTTP.
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.
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).
11. Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.
12. Закрийте Wireshark.

**Контрольні запитання:**

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

**Відповідь:**

ARP, BROWSER, DNS, HTTP, IGMPv2, SSDP, STP, TCP, UDP

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

**Відповідь:**

Протоколи в збережених пакетах запиту: IPv4, HTP, TCP

Протоколи в збережених пакетах відповіді: IPv4, TCP, HTP, text/html

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

**Відповідь:**



1,273273-1,134747=0,138526с

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

**Відповідь:**

Вихідна та цільова адреси пакетів із запитом:

192.168.0.104 (джерело, вихід); 128.119.245.12 (цільова адреса)



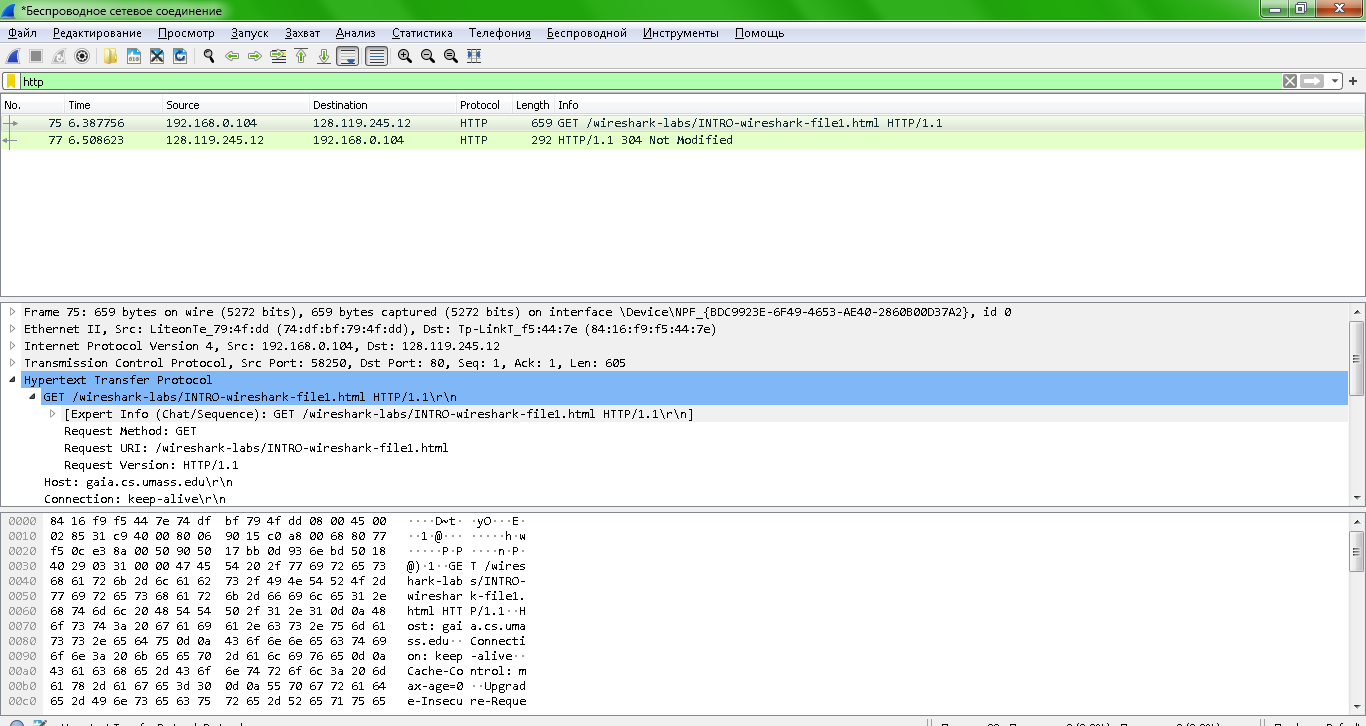
Вихідна та цільова адреси пакетів із відповіддю:

128.119.245.12 (джерело, вихід); 192.168.0.104 (цільова адреса)



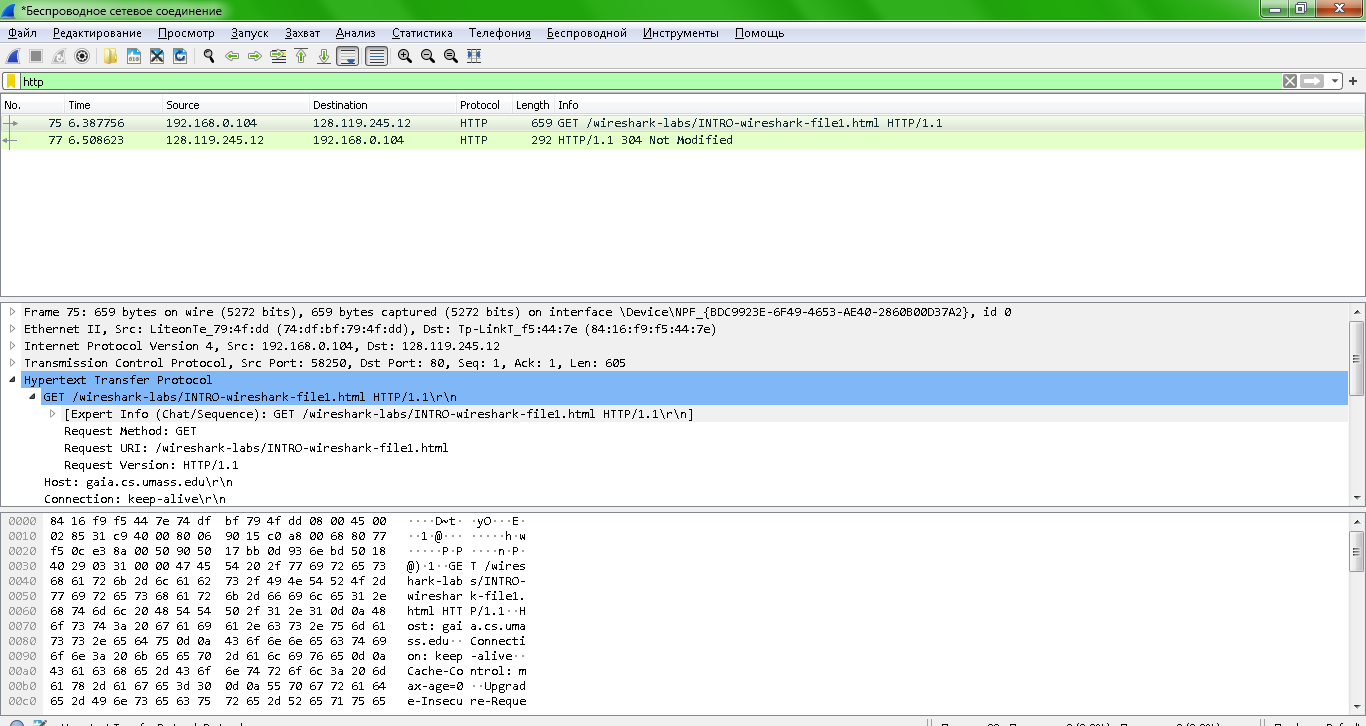
1. Яким був перший рядок запиту на рівні протоколу HTTP?

**Відповідь:** GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1



1. Яким був перший рядок відповіді на рівні протоколу HTTP?

**Відповідь:** HTTP/1.1



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