

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

### Лабораторна робота № 1

3 дисципліни: Комп'ютерні мережі

## Основи захоплення та аналізу пакетів

Виконала:

Студентка III курсу

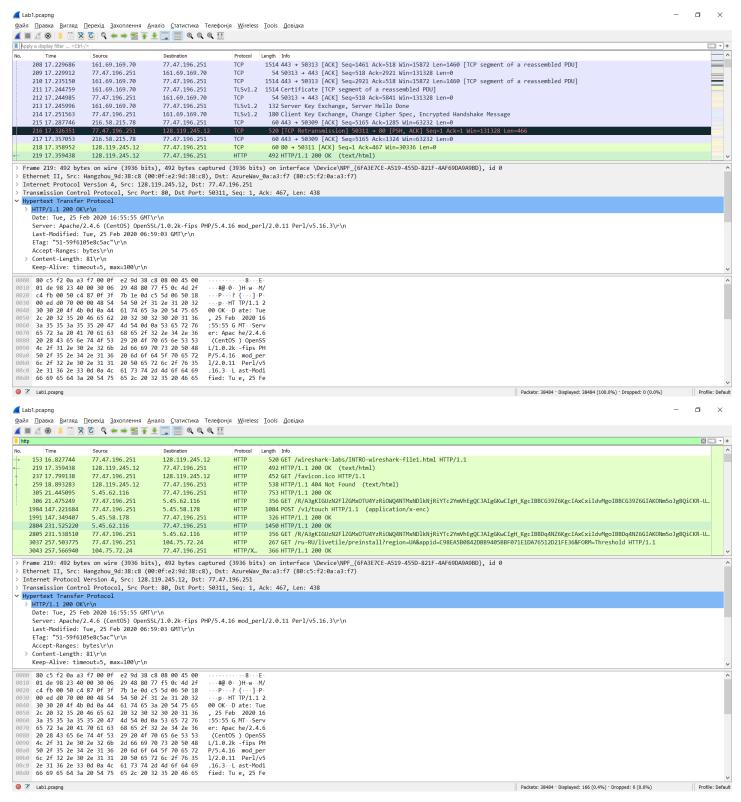
Групи КА-74

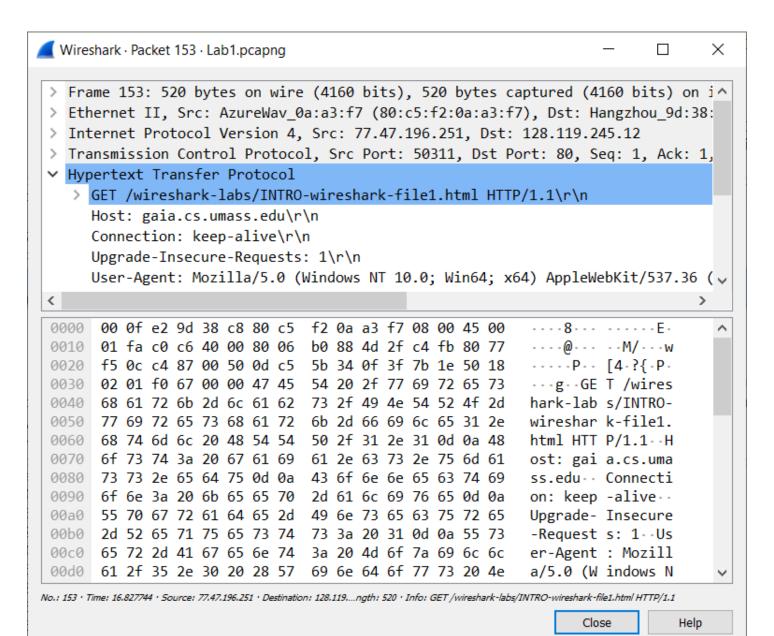
Соболь Н. О.

Перевірив: Кухарєв С. О.

**Мета роботи:** оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

#### Хід виконання роботи





✓ Wireshark · Роздрукувати		×
The state of the s	✓ Details:	column headings  upsed layed unded  cket on a new page
	Захоплені	Відображені
<u>В</u> сі пакети	38484	166
○ Тільки <u>в</u> ибрані пакети	1	1
○ Тільки <u>п</u> означені пакети	0	0
○ Від першого до останнього позначеного	0	0
○ Діапазон:	0	0
Видалити <u>п</u> роігноровані пакети	0	0
Page <u>S</u> etup <u>P</u> rint	Cancel	Help

```
No.
        Time
                         Source
                                                  Destination
                                                                          Protocol Length Info
                                                                                           GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
                         77.47.196.251
    153 16.827744
                                                  128.119.245.12
                                                                          HTTP
                                                                                    520
Frame 153: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{6FA3E7CE-A519-455D-821F-4AF69DA9A9BD}, id
Ethernet II, Src: AzureWav_0a:a3:f7 (80:c5:f2:0a:a3:f7), Dst: Hangzhou_9d:38:c8 (00:0f:e2:9d:38:c8)
Internet Protocol Version 4, Src: 77.47.196.251, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50311, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
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/79.0.3945.130 Safari/537.36\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/appg,*/*;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
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 219]
    [Next request in frame: 237]
```

#### Контрольні питання

- 1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації? ARP, HTTP, IGMPv2, NBNS, MDNS, LLMNR, LOOP, TCP, TLSv1.2, BROWSER, DNS, TLSv1.3
- 2. Які протоколи використовувалися в збережених пакетах запиту та відповіді? ARP, HTTP, IGMPv2, NBNS, MDNS, LLMNR, LOOP, TCP, TLSv1.2, BROWSER, DNS, TLSv1.3
- 3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Пройшло 0,531698 с.

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

Запит:

Вихідна:77.47.196.251

Цільова:128.119.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 77.47.196.251

5. Яким був перший рядок запиту на рівні протоколу НТТР?

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

6. Яким був перший рядок відповіді на рівні протоколу НТТР?

HTTP/1.1 200 OK (text/html)

#### Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.