



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

**Лабораторна робота № 1**

**З дисципліни: Комп'ютерні мережі**

***Основи захоплення та аналізу пакетів***

**Виконала:**

**Студентка III курсу**

**Групи КА-72**

**Фалілеєва Дар'я**

**Перевірив: Кухарєв С. О.**

**Київ 2020**

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

## Хід виконання роботи

### Відсилка пакету:

No.	Time	Source	Destination	Protocol	Length	Info
172	4.759248	192.168.1.101	128.119.245.12	HTTP	463	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Wireshark · Packet 172 · Wi-Fi: en0

▶ Frame 172: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0

▶ Ethernet II, Src: Apple\_e6:c4:ee (64:c7:53:e6:c4:ee), Dst: Tp-LinkT\_71:6f:20 (e8:94:f6:71:6f:20)

▶ Internet Protocol Version 4, Src: 192.168.1.101, Dst: 128.119.245.12

▶ Transmission Control Protocol, Src Port: 49683, Dst Port: 80, Seq: 1, Ack: 1, Len: 397

▼ **Hypertext Transfer Protocol**

▶ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Upgrade-Insecure-Requests: 1\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.5 Safari/605.1.15\r\n

Accept-Language: ru\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

\r\n

[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html\]](#)

[HTTP request 1/1]

[\[Response in frame: 225\]](#)

### Відповідь:

225	4.894645	128.119.245.12	192.168.1.101	HTTP	504	HTTP/1.1 200 OK (text/html)
-----	----------	----------------	---------------	------	-----	-----------------------------

Wireshark · Packet 225 · Wi-Fi: en0

▶ Frame 225: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0

▶ Ethernet II, Src: Tp-LinkT\_71:6f:20 (e8:94:f6:71:6f:20), Dst: Apple\_e6:c4:ee (64:c7:53:e6:c4:ee)

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.101

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49683, Seq: 1, Ack: 398, Len: 438

▼ **Hypertext Transfer Protocol**

▶ HTTP/1.1 200 OK\r\n

Date: Sun, 12 Apr 2020 11:21:19 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sun, 12 Apr 2020 05:59:03 GMT\r\n

ETag: "51-5a311a9e7b607"\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: 0.135397000 seconds]

[\[Request in frame: 172\]](#)

[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)

### Контрольні питання

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

TCP, HTTP, DNS, TLSv1.2, , TLSv1.3, ICMP, IGMPv2, SSDP

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді? ІСР, Ethernet II, HTTP, TCP.
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Прошло 0,135 с.

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

Запит:

Вихідна: 192.168.1.101

Цільова: 128.119.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 192.168.1.101

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

GET /wireshark-labs/...

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

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.