



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

**Лабораторна робота № 1**  
**З дисципліни: Комп'ютерні мережі**

***Основи захоплення та аналізу пакетів***

**Виконав:**  
**Студент III курсу**  
**Групи КА-72**  
**Братцев Антін**  
**Перевірив: Кухарєв С. О.**

**Київ 2020**

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

No.	Time	Source	Destination	Protocol	Length	Info
28	1.236948	192.168.1.2	128.119.245.12	HTTP	537	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 28: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface \Device\NPF\_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: Chongqin\_d9:c0:f7 (ac:d5:64:d9:c0:f7), Dst: ASUSTekC\_dc:ce:a0 (e0:cb:4e:dc:ce:a0)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 51035, Dst Port: 80, Seq: 1, Ack: 1, Len: 483

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/83.0.4103.61 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: en-US,en;q=0.9,ru;q=0.8,uk;q=0.7\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: 30]

No.	Time	Source	Destination	Protocol	Length	Info
30	1.363813	128.119.245.12	192.168.1.2	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 30: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: ASUSTekC\_dc:ce:a0 (e0:cb:4e:dc:ce:a0), Dst: Chongqin\_d9:c0:f7 (ac:d5:64:d9:c0:f7)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

Transmission Control Protocol, Src Port: 80, Dst Port: 51035, Seq: 1, Ack: 484, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Mon, 25 May 2020 16:01:21 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: Mon, 25 May 2020 05:59:03 GMT\r\n

ETag: "51-5a672ad13a986"\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: 0.126865000 seconds]  
[Request in frame: 28]  
[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?  
ARP, TCP, HTTP, SSL, TLSv1.2, UDP
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?  
IPv4, Ethernet II, HTTP, TCP.
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?  
Пройшло 0.126865 с.
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?  
Запит:  
Вихідна: 192.168.1.2  
Цільова: 128.119.245.12  
Відповідь:  
Вихідний: 128.119.245.12  
Цільовий: 192.168.1.2

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

## **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.