

**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-77**  
**Яцько Я. В.**  
**Перевірів: Кухарєв С. О.**

**Київ 2020**

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

## Хід виконання роботи

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Файл', 'Редактирование', 'Просмотр', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводной', 'Инструменты', and 'Помощь'. The main window shows a packet list on the left, a packet details pane in the middle, and a packet bytes pane on the right.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
243	86.397091	192.168.1.106	128.119.245.12	HTTP	562	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
247	86.531169	128.119.245.12	192.168.1.106	HTTP	492	HTTP/1.1 200 OK (text/html)
249	86.594967	192.168.1.106	128.119.245.12	HTTP	494	GET /favicon.ico HTTP/1.1
250	86.835147	128.119.245.12	192.168.1.106	HTTP	538	HTTP/1.1 404 Not Found (text/html)

**Packet Details (Frame 243):**

- Frame 243: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF\_{C26B40B3-DE2B-49AB-989F-CFF2109D2AF0}, id 0
- Ethernet II, Src: IntelCor\_3e:cc:2c (34:41:5d:3e:cc:2c), Dst: Tp-LinkT\_3f:9c:44 (ec:08:6b:3f:9c:44)
- Internet Protocol Version 4, Src: 192.168.1.106, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 53038, Dst Port: 80, Seq: 1, Ack: 1, Len: 508
- Hypertext Transfer Protocol

**Packet Bytes:**

0000 ec 08 6b 3f 9c 44 34 41 5d 3e cc 2c 08 00 45 00 ...k? D4A ]>...E-  
0010 02 24 89 2a 40 00 80 06 38 13 c0 a8 01 6a 80 77 ...\$\*@... 8...j-w  
0020 f5 0c cf 2e 00 50 4d 79 17 d2 fe b3 e7 58 50 18 ...PMY .....XP-  
0030 02 01 e8 c3 00 00 47 45 54 20 2f 77 69 72 65 73 .....GE T /wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-  
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.  
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1..H  
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma  
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu.. Connecti  
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..  
00a0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure  
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request s: 1..Us

**Wireshark - Filter 243 · dump.pcapng**

> Frame 243: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF\_{C26B40B3-DE2B-49AB-989F-CFF2109D2AF0}, id 0  
> Ethernet II, Src: IntelCor\_3e:cc:2c (34:41:5d:3e:cc:2c), Dst: Tp-LinkT\_3f:9c:44 (ec:08:6b:3f:9c:44)  
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 53038, Dst Port: 80, Seq: 1, Ack: 1, Len: 508  
> Hypertext Transfer Protocol

**Packet Bytes:**

0020 f5 0c cf 2e 00 50 4d 79 17 d2 fe b3 e7 58 50 18 ...PMY .....XP-  
0030 02 01 e8 c3 00 00 47 45 54 20 2f 77 69 72 65 73 .....GE T /wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-  
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.  
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1..H  
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma  
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu.. Connecti  
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..  
00a0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure  
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request s: 1..Us  
00c0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent: Mozill  
00d0 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (Windows N  
00e0 54 20 31 30 2e 30 30 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x  
00f0 36 34 29 20 41 70 70 6c 65 7f 65 62 4b 69 74 2f 64) Appl eWebKit/  
0100 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML, l  
0110 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Gecko o) Chrom  
0120 65 2f 38 30 2e 30 2e 33 39 38 37 2e 31 34 39 20 e/80.0.3 987.149  
0130 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 Safari/5 37.36..A  
0140 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html  
0150 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applicat ion/xht

No.: 243 · Time: 86.397091 · Source: 192.168.1.106 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 562 · Info: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Close Help

## Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?  
TCP, DNS, HTTP, TLSv1.3, SSL, ICMPv6, UDP, ARP
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?  
Ethernet II, IPV4, TCP, HTTP,
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Прошло 0,004625 с.

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

Запит:

Вихідна: 192.168.1.106

Цільова: 128.19.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 192.168.1.106

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

```
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/INTRO-wireshark-file1.html
    Request Version: HTTP/1.1
```

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

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

## Висновок

В ході виконання лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було визначено за який час було відправлено перший запит та отримано відповідь.