

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»**

**КАФЕДРА ММСА**

**Протокол до лабораторної роботи № 1**

**З теми: «Основи захоплення та аналізу пакетів»**

**Виконав:**

**Студент ІII курсу**

**Групи КА-73**

**Півень О. К.**

**Прийняв: Кухарєв С. О.**

**Київ 2020**

**Запит:**

/Users/aleksandr/Desktop/dump laba1.pcapng 329 всего пакетов, 43 показано

No. Time Source Destination Protocol Length Info

52 13.039929 172.20.10.2 128.119.245.12 HTTP 548 GET /

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

Frame 52: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface en0, id

0

Ethernet II, Src: Apple\_3c:2c:dd (8c:85:90:3c:2c:dd), Dst: f2:a3:5a:50:d0:64 (f2:a3:5a:

50:d0:64)

Internet Protocol Version 4, Src: 172.20.10.2, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 65249, Dst Port: 80, Seq: 1, Ack: 1, Len: 482

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]

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

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /wireshark-labs/INTRO-wireshark-file1.html

Request Version: HTTP/1.1

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

If-None-Match: "51-59f6105e8c5ac"\r\n

Upgrade-Insecure-Requests: 1\r\n

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

If-Modified-Since: Tue, 25 Feb 2020 06:59:03 GMT\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_6) 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: 54]

**Відповідь:**

/Users/aleksandr/Desktop/dump laba1.pcapng 329 всего пакетов, 43 показано

No. Time Source Destination Protocol Length Info

54 13.219916 128.119.245.12 172.20.10.2 HTTP 504 HTTP/1.1

200 OK (text/html)

Frame 54: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id

0

Ethernet II, Src: f2:a3:5a:50:d0:64 (f2:a3:5a:50:d0:64), Dst: Apple\_3c:2c:dd (8c:85:90:3c:

2c:dd)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.2

Transmission Control Protocol, Src Port: 80, Dst Port: 65249, Seq: 1, Ack: 483, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Wed, 26 Feb 2020 06:38:41 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: Wed, 26 Feb 2020 06:38:02 GMT\r\n

ETag: "51-59f74d891b4b4"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

[Content length: 81]

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: 0.179987000 seconds]

[Request in frame: 52]

[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 запитання:**

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

**DNS, HTTP, MDNS, TCP, TLSv1.2**

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

**HTTP**

1. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до

отримання першого пакету з відповіддю сервера?

**0,179987**

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

**Запит: вихідна - 172.20.10.2 цільова - 128.119.245.12**

**Відповідь: вихідна - 128.119.245.12 цільова - 172.20.10.2**

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

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

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

**HTTP/1.1 200 OK\r\n**

**Висновок:**В ході виконання даної лабораторної роботи, було покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та було проведено аналіз деталей роботи даних протоколів.