

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №1
з курсу «Комп'ютерні мережі»
тема: «Основи захоплення та аналізу пакетів»

Виконала: студентка 3 курсу
групи КА-77
Наконечна В.А
Прийняв: Кухарєв С.О.

Київ – 2020р.

Вихідний пакет:

```
No.      Time      Source      Destination      Protocol Length Info
16 0.656559 192.168.88.252 128.119.245.12  HTTP      649      GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 16: 649 bytes on wire (5192 bits), 649 bytes captured (5192 bits) on interface \Device\NPF_{1C9B56D7-3A48-4DEC-BD07-
E0C12FC11D8E}, id 0
Ethernet II, Src: HewlettP_4a:ea:d7 (40:b0:34:4a:ea:d7), Dst: Routerbo_24:f5:fa (b8:69:f4:24:f5:fa)
Internet Protocol Version 4, Src: 192.168.88.252, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59414, Dst Port: 80, Seq: 1, Ack: 1, Len: 595
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
Cache-Control: max-age=0\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/80.0.3987.122 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
If-None-Match: "51-59fedd6cb932e"\r\n
If-Modified-Since: Tue, 03 Mar 2020 06:59:03 GMT\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: 19]
```

Вхідні пакет:

```
No.      Time      Source      Destination      Protocol Length Info
19 0.775458 128.119.245.12 192.168.88.252  HTTP      293      HTTP/1.1 304 Not Modified
Frame 19: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{1C9B56D7-3A48-4DEC-BD07-
E0C12FC11D8E}, id 0
Ethernet II, Src: Routerbo_24:f5:fa (b8:69:f4:24:f5:fa), Dst: HewlettP_4a:ea:d7 (40:b0:34:4a:ea:d7)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.88.252
Transmission Control Protocol, Src Port: 80, Dst Port: 59414, Seq: 1, Ack: 596, Len: 239
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Tue, 03 Mar 2020 18:06:51 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
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "51-59fedd6cb932e"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.118899000 seconds]
[Request in frame: 16]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

Контрольні запитання:

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

TCP, HTTP, SSDP, MDSN

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

Ethernet II, Internet Protocol Version 4, Transmission Control Protocol.

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

отримання першого пакету з відповіддю сервера?

0.775458-0.656559=0.118899

4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
Вхідна - 192.168.88.252
Цільова - 128.119.245.12
5. Яким був перший рядок запиту на рівні протоколу HTTP?
GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
6. Яким був перший рядок відповіді на рівні протоколу HTTP?
HTTP/1.1 304 Not Modified

Висновки:

Оволоділи методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих проколів.