



**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

Виконав:
Студент III курсу
Групи КА-74
Іванов С. І.
Перевірів: Кухарєв С.О.

Київ 2020

No.	Time	Source	Destination	Protocol	Length	Info
54	4.361751	192.168.0.101	128.119.245.12	HTTP	546	GET /wireshark-labs/INTRO-wireshark-file1.html

HTTP/1.1
 Frame 54: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{FBB4350A-F432-460E-AF29-78556EA89AE6}, id 0
 Ethernet II, Src: ASUSTekC_80:15:84 (74:d0:2b:80:15:84), Dst: Tp-LinkT_04:32:30 (e8:94:f6:04:32:30)
 Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 53825, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
 Hypertext Transfer Protocol

```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Wed, 11 Mar 2020 05:18:02 GMT\r\n
If-None-Match: "51-5a08d5c417098"\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 57]
[Next request in frame: 64]
```

No.	Time	Source	Destination	Protocol	Length	Info
57	4.492413	128.119.245.12	192.168.0.101	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 57: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{FBB4350A-F432-460E-AF29-78556EA89AE6}, id 0
 Ethernet II, Src: Tp-LinkT_04:32:30 (e8:94:f6:04:32:30), Dst: ASUSTekC_80:15:84 (74:d0:2b:80:15:84)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.101
 Transmission Control Protocol, Src Port: 80, Dst Port: 53825, Seq: 1, Ack: 493, Len: 438
 Hypertext Transfer Protocol

```
HTTP/1.1 200 OK\r\n
Date: Wed, 11 Mar 2020 05:19:39 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, 11 Mar 2020 05:19:03 GMT\r\n
ETag: "51-5a08d5fe96c99"\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 1/2]
[Time since request: 0.130662000 seconds]
[Request in frame: 54]
[Next request in frame: 64]
[Next response in frame: 79]
[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)

No.	Time	Source	Destination	Protocol	Length	Info
64	4.601061	192.168.0.101	128.119.245.12	HTTP	401	GET /favicon.ico HTTP/1.1

Frame 64: 401 bytes on wire (3208 bits), 401 bytes captured (3208 bits) on interface \Device\NPF_{FBB4350A-F432-460E-AF29-78556EA89AE6}, id 0
 Ethernet II, Src: ASUSTekC_80:15:84 (74:d0:2b:80:15:84), Dst: Tp-LinkT_04:32:30 (e8:94:f6:04:32:30)
 Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 53825, Dst Port: 80, Seq: 493, Ack: 439, Len: 347
 Hypertext Transfer Protocol

```
GET /favicon.ico HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/favicon.ico]
[HTTP request 2/2]
[Prev request in frame: 54]
[Response in frame: 79]
```

No.	Time	Source	Destination	Protocol	Length	Info
79	4.727839	128.119.245.12	192.168.0.101	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 79: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{FBB4350A-F432-460E-AF29-78556EA89AE6}, id 0
 Ethernet II, Src: Tp-LinkT_04:32:30 (e8:94:f6:04:32:30), Dst: ASUSTekC_80:15:84 (74:d0:2b:80:15:84)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.101
 Transmission Control Protocol, Src Port: 80, Dst Port: 53825, Seq: 439, Ack: 841, Len: 484
 Hypertext Transfer Protocol

```
HTTP/1.1 404 Not Found\r\n
Date: Wed, 11 Mar 2020 05:19:39 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
Content-Length: 209\r\n
Keep-Alive: timeout=5, max=99\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
```

```
\r\n
[HTTP response 2/2]
[Time since request: 0.126778000 seconds]
[Prev request in frame: 54]
[Prev response in frame: 57]
[Request in frame: 64]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 209 bytes
Line-based text data: text/html (7 lines)
```

Контрольні питання

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

Здебільшого TCP, також HTTP, DNS, TLS і т.д.

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

HTTP

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

0,130662000 seconds

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

192.168.0.101	128.119.245.12
128.119.245.12	192.168.0.101

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

GET /wireshark-labs/INTRO-wireshark_file1.html

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

HTTP/1.1 200 OK

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