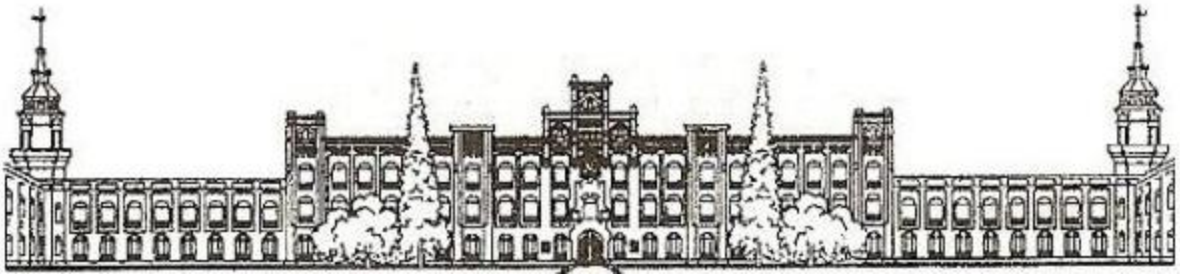


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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-74

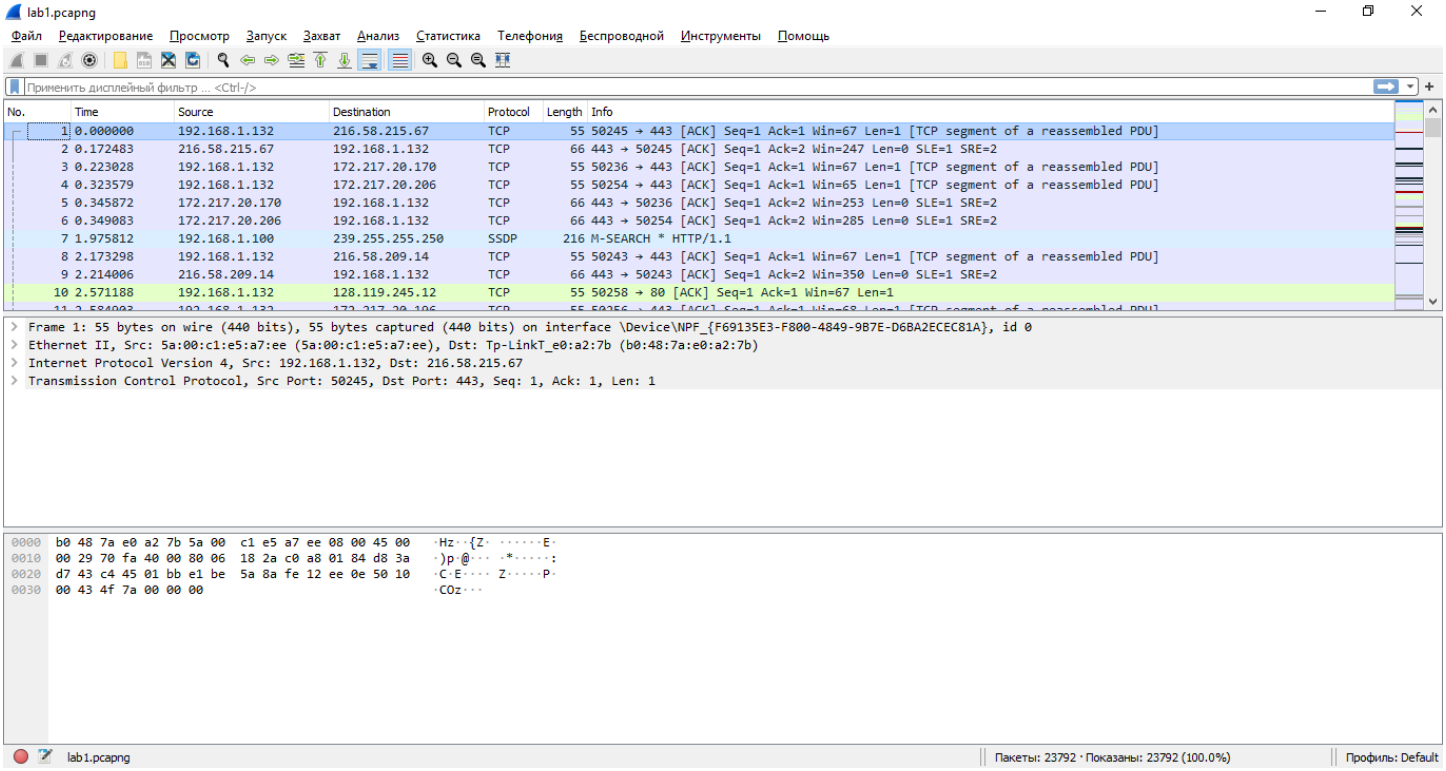
Ковальчук О. О.

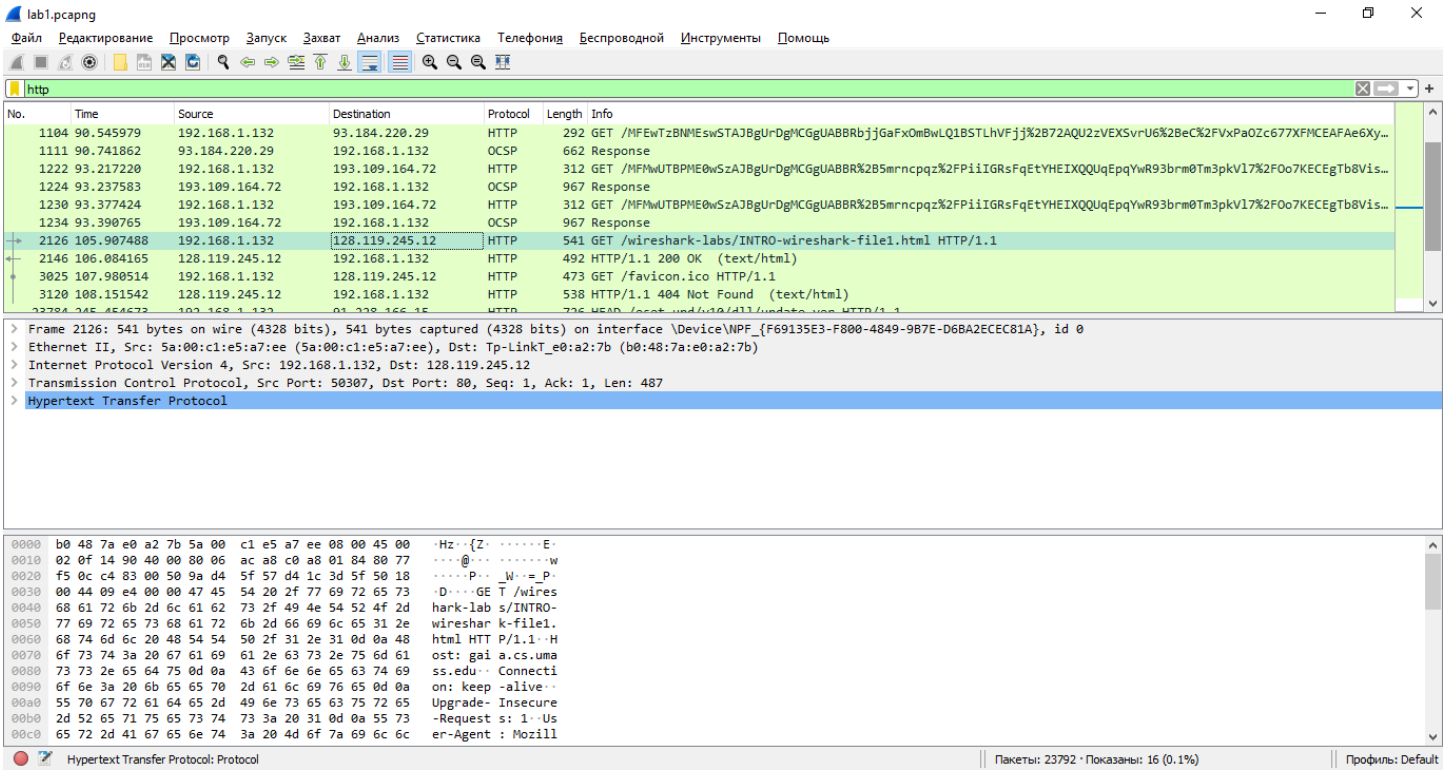
Перевірив: Кухарєв С. О.

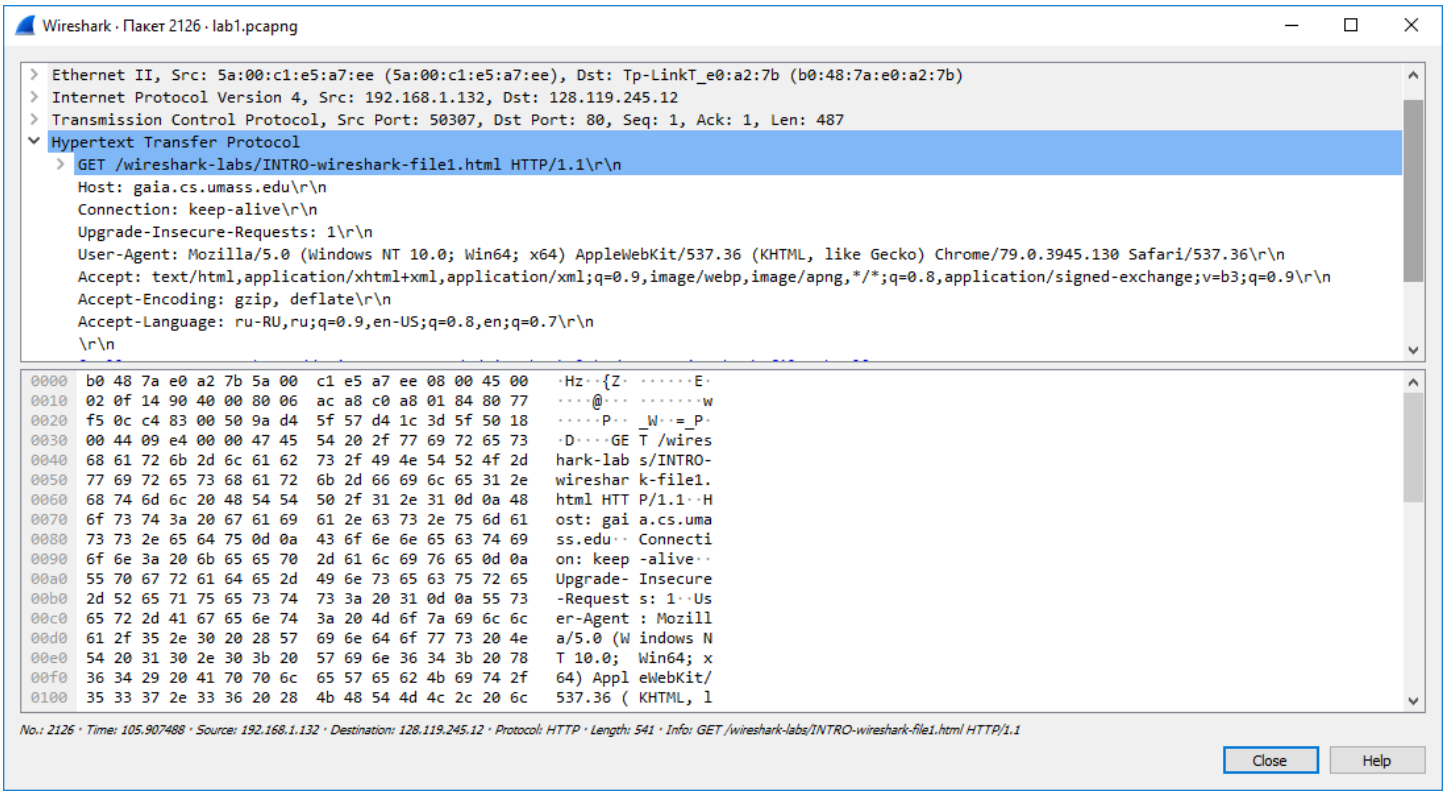
Київ 2020

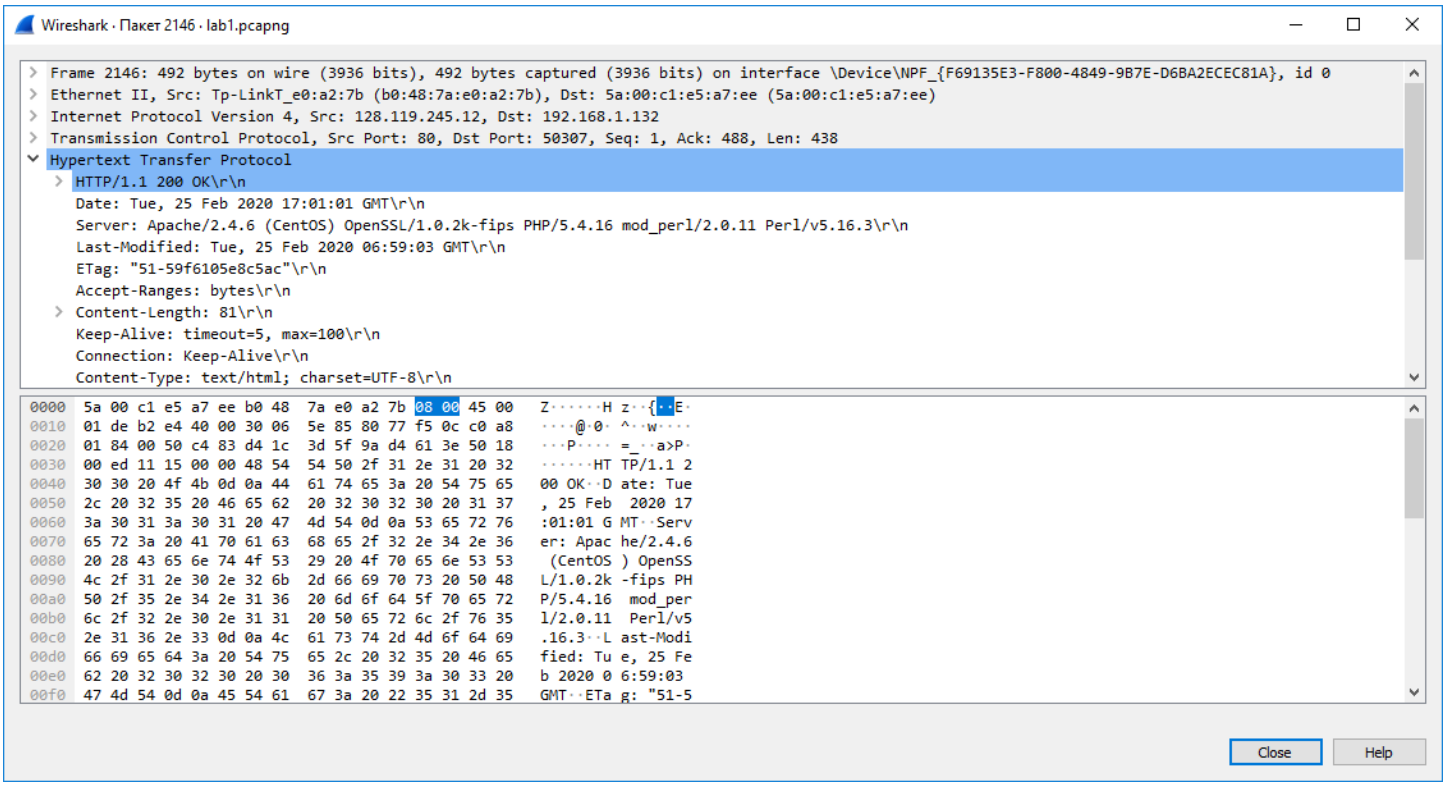
Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Хід виконання роботи






Wireshark · Пакет 2126 · lab1.pcapng
Ethernet II, Src: 5a:00:c1:e5:a7:ee (5a:00:c1:e5:a7:ee), Dst: Tp-LinkT_e0:a2:7b (b0:48:7a:e0:a2:7b)
Internet Protocol Version 4, Src: 192.168.1.132, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50307, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
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/79.0.3945.130 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: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
0000 b0 48 7a e0 a2 7b 5a 00 c1 e5 a7 ee 08 00 45 00 ·Hz··{Z· ·····E·
0010 02 0f 14 90 40 00 80 06 ac a8 c0 a8 01 84 80 77 ····@··· ·····w
0020 f5 0c c4 83 00 50 9a d4 5f 57 d4 1c 3d 5f 50 18 ·····P·· _W··=_P·
0030 00 44 09 e4 00 00 47 45 54 20 2f 77 69 72 65 73 ·D····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 (W indows N
00e0 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x
00f0 36 34 29 20 41 70 70 6c 65 57 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
No.: 2126 · Time: 105.907488 · Source: 192.168.1.132 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 541 · Info: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Close
Help


Wireshark · Пакет 2146 · lab1.pcapng
Frame 2146: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{F69135E3-F800-4849-9B7E-D6BA2ECEC81A}, id 0
Ethernet II, Src: Tp-LinkT_e0:a2:7b (b0:48:7a:e0:a2:7b), Dst: 5a:00:c1:e5:a7:ee (5a:00:c1:e5:a7:ee)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.132
Transmission Control Protocol, Src Port: 80, Dst Port: 50307, Seq: 1, Ack: 488, Len: 438
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Tue, 25 Feb 2020 17:01:01 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: Tue, 25 Feb 2020 06:59:03 GMT\r\n
ETag: "51-59f6105e8c5ac"\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
0000 5a 00 c1 e5 a7 ee b0 48 7a e0 a2 7b 08 00 45 00 Z·····H z··{··E·
0010 01 de b2 e4 40 00 30 06 5e 85 80 77 f5 0c c0 a8 ····@·0· ^··w····
0020 01 84 00 50 c4 83 d4 1c 3d 5f 9a d4 61 3e 50 18 ···P···· =_··a>P·
0030 00 ed 11 15 00 00 48 54 54 50 2f 31 2e 31 20 32 ·····HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK··D ate: Tue
0050 2c 20 32 35 20 46 65 62 20 32 30 32 30 20 31 37 , 25 Feb 2020 17
0060 3a 30 31 3a 30 31 20 47 4d 54 0d 0a 53 65 72 76 :01:01 G MT··Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per
00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3··L ast-Modi
00d0 66 69 65 64 3a 20 54 75 65 2c 20 32 35 20 46 65 fied: Tu e, 25 Fe
00e0 62 20 32 30 32 30 20 30 36 3a 35 39 3a 30 33 20 b 2020 0 6:59:03
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 31 2d 35 GMT··ETa g: "51-5
Close
Help

Контрольні питання

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

   TCP, SSDR, HTTP, TLSv1.2, MDNS

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

IPV, 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 0,384879 с.

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

Запит:

Вихідна:192.168.1.132

Цільова:139.99.8.72

Відповідь:

Вихідний:139.99.8.72

Цільовий:192.168.1.132

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

GET / HTTP/1.1

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

HTTP/1.1 200 OK (text/html)

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.