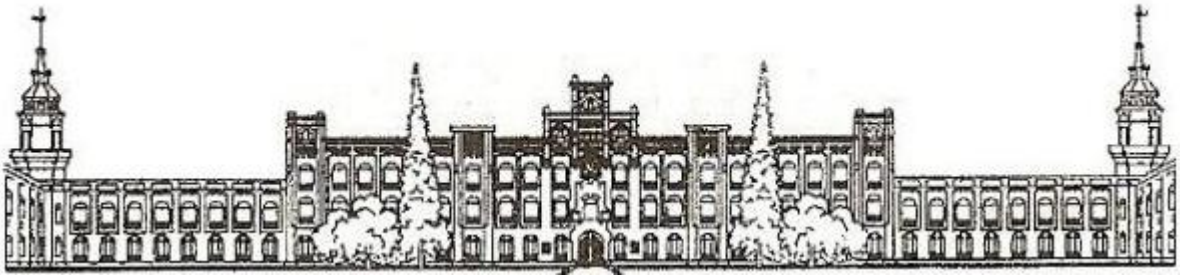


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

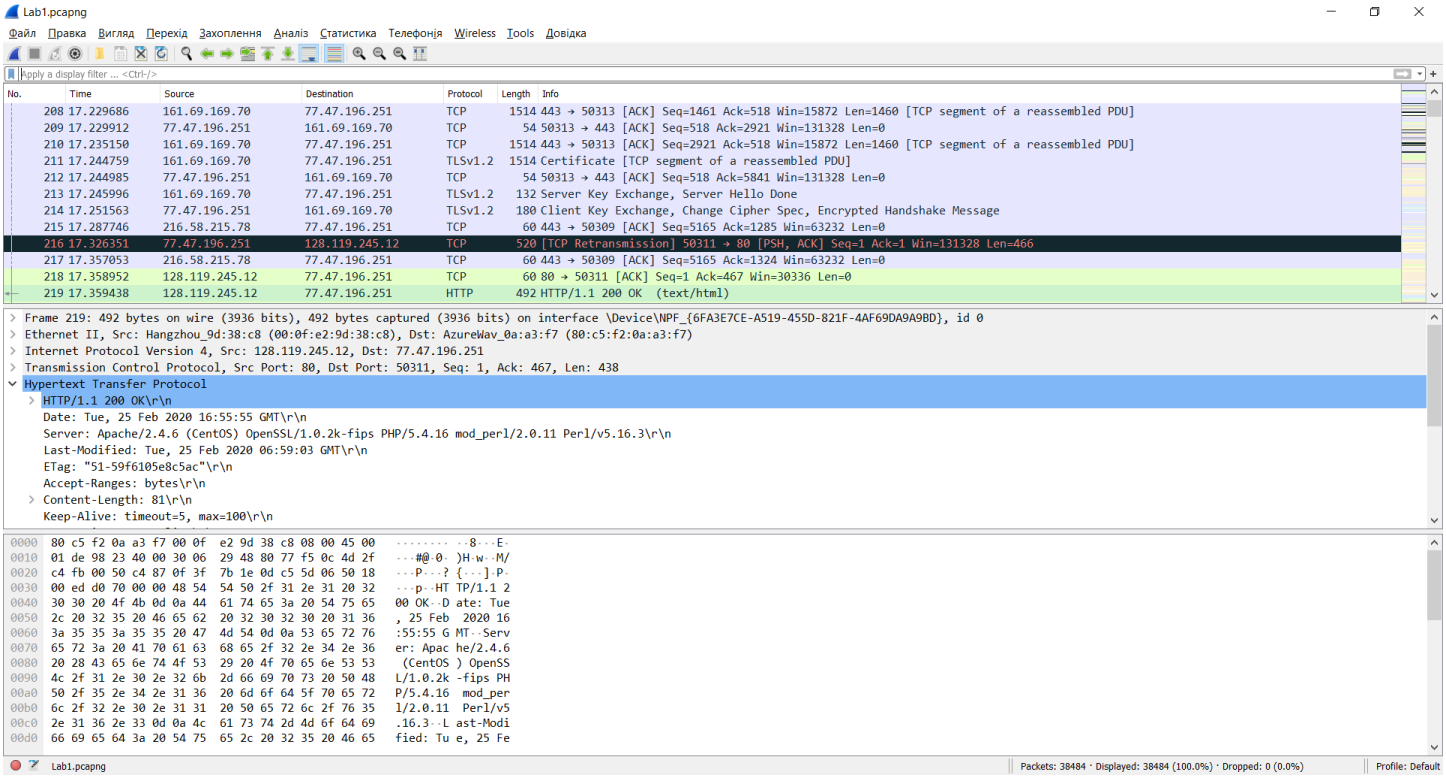
Соболь Н. О.

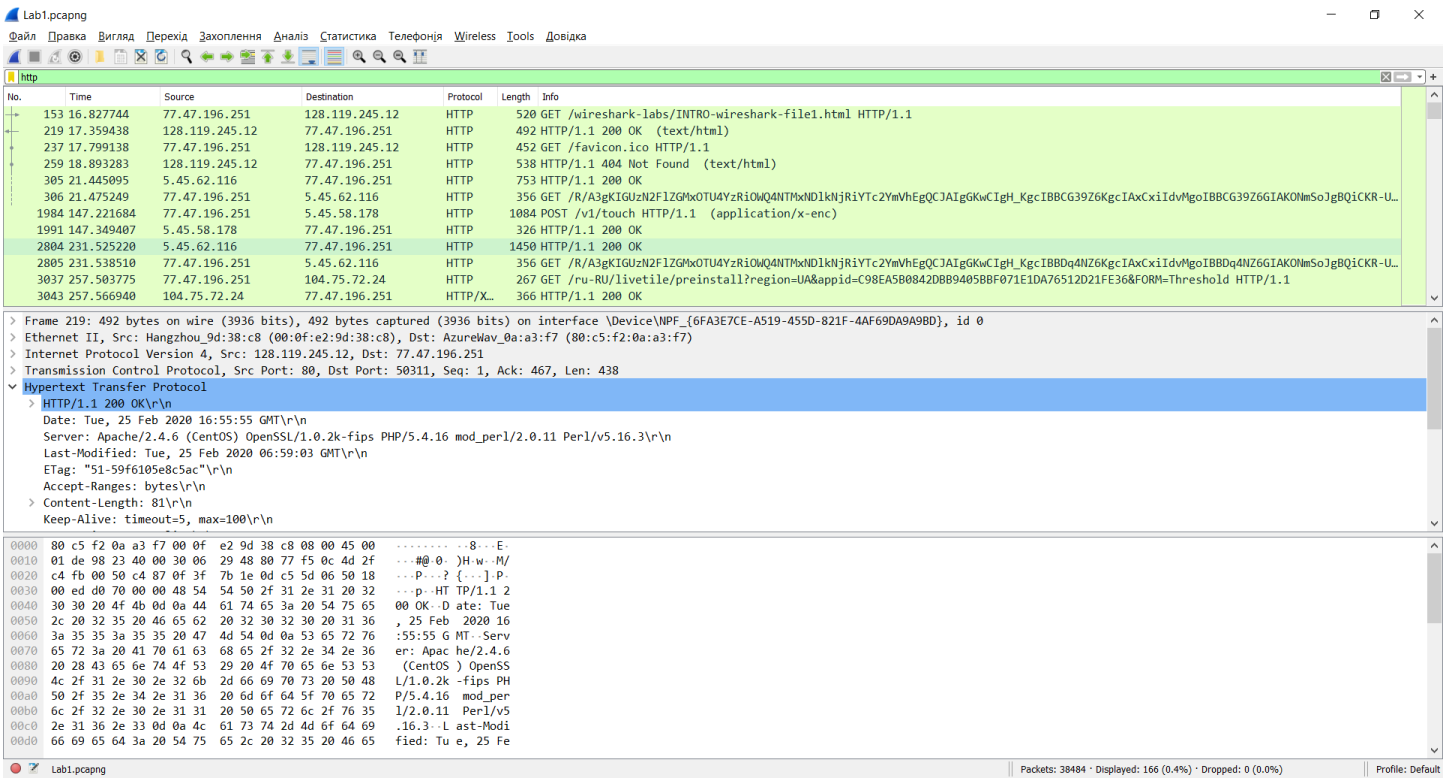
Перевірив: Кухарєв С. О.

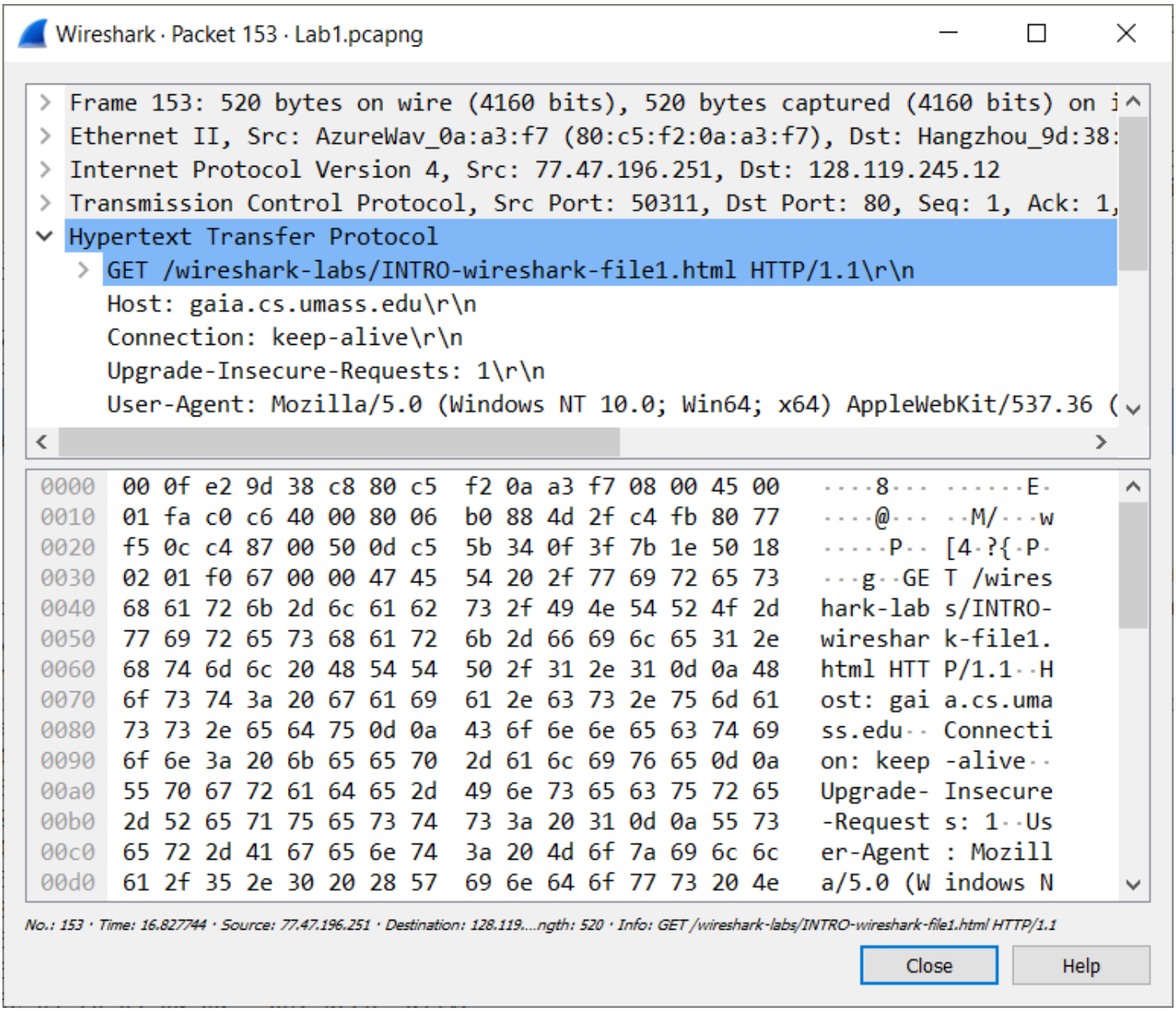
Київ 2020

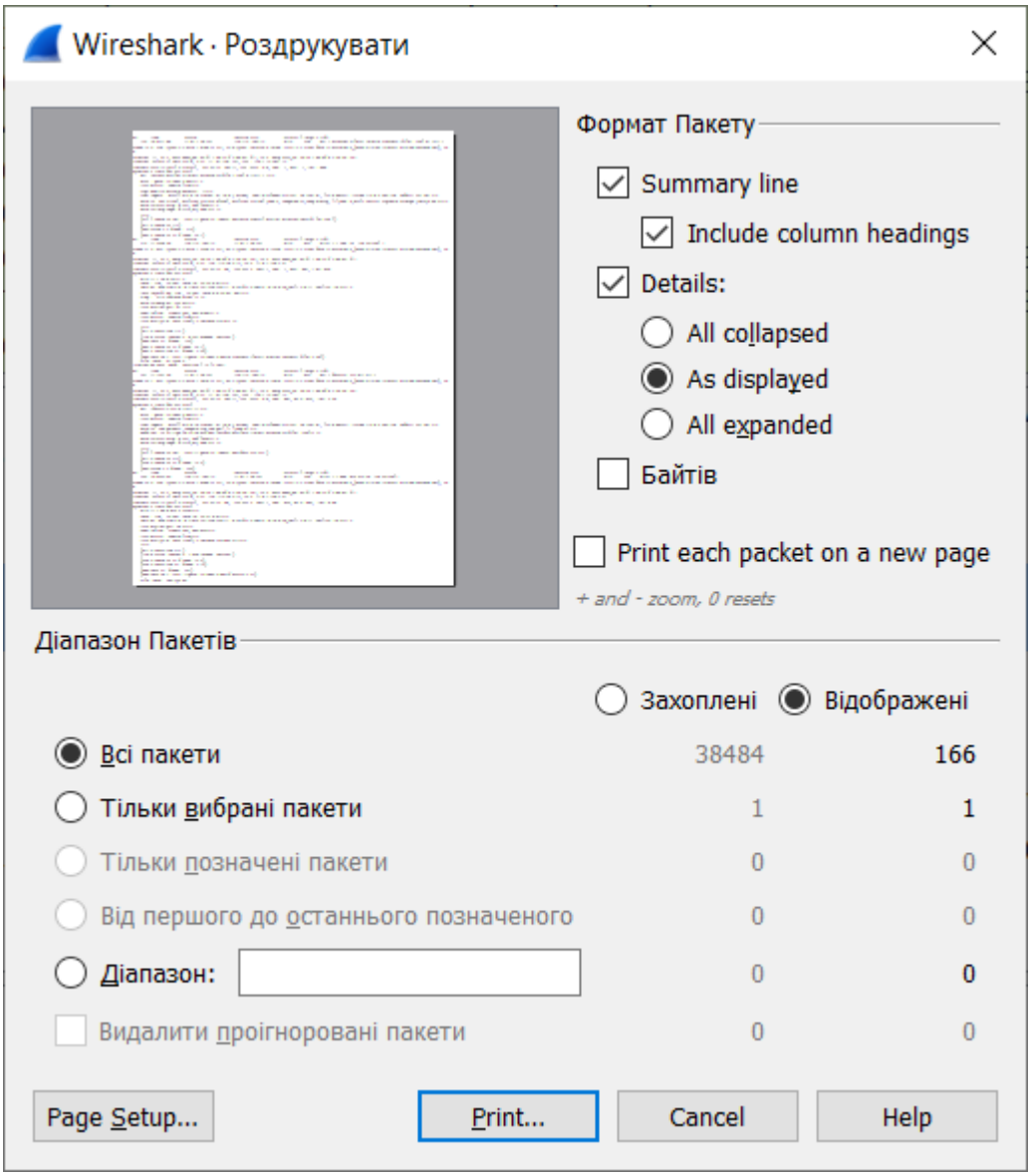
Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Хід виконання роботи






Wireshark · Packet 153 · Lab1.pcapng
Frame 153: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on i
Ethernet II, Src: AzureWav_0a:a3:f7 (80:c5:f2:0a:a3:f7), Dst: Hangzhou_9d:38:
Internet Protocol Version 4, Src: 77.47.196.251, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50311, Dst Port: 80, Seq: 1, Ack: 1,
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 (
0000 00 0f e2 9d 38 c8 80 c5 f2 0a a3 f7 08 00 45 00 ····8··· ·····E·
0010 01 fa c0 c6 40 00 80 06 b0 88 4d 2f c4 fb 80 77 ····@··· ··M/···w
0020 f5 0c c4 87 00 50 0d c5 5b 34 0f 3f 7b 1e 50 18 ·····P·· [4·?{·P·
0030 02 01 f0 67 00 00 47 45 54 20 2f 77 69 72 65 73 ···g··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
No.: 153 · Time: 16.827744 · Source: 77.47.196.251 · Destination: 128.119....ngth: 520 · Info: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Close
Help




```
No.     Time           Source                Destination           Protocol Length Info
    153 16.827744      77.47.196.251         128.119.245.12        HTTP     520    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 153: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{6FA3E7CE-A519-455D-821F-4AF69DA9A9BD}, id
0
Ethernet II, Src: AzureWav_0a:a3:f7 (80:c5:f2:0a:a3:f7), Dst: Hangzhou_9d:38:c8 (00:0f:e2:9d:38:c8)
Internet Protocol Version 4, Src: 77.47.196.251, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50311, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
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: en-US,en;q=0.9\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: 219]
    [Next request in frame: 237]
```

Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
   ARP, HTTP, IGMPv2, NBNS, MDNS, LLMNR, LOOP,TCP,TLSv1.2, BROWSER, DNS, TLSv1.3
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
   ARP, HTTP, IGMPv2, NBNS, MDNS, LLMNR, LOOP,TCP,TLSv1.2, BROWSER, DNS, TLSv1.3

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

Пройшло 0,531698 с.

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

Запит:

Вихідна:77.47.196.251

Цільова:128.119.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 77.47.196.251

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/1.1 200 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.