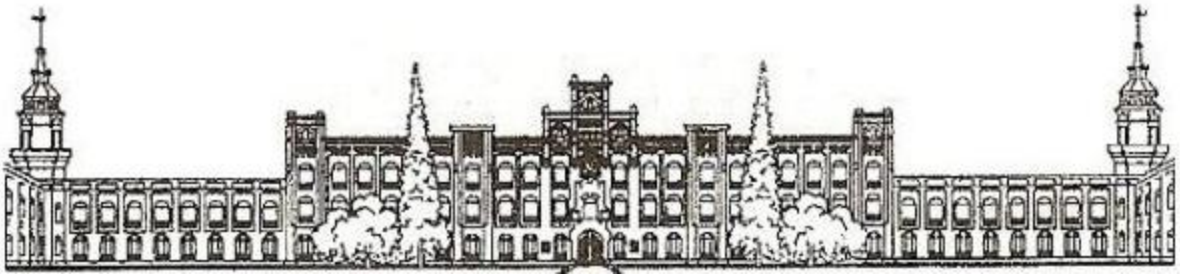


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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-72

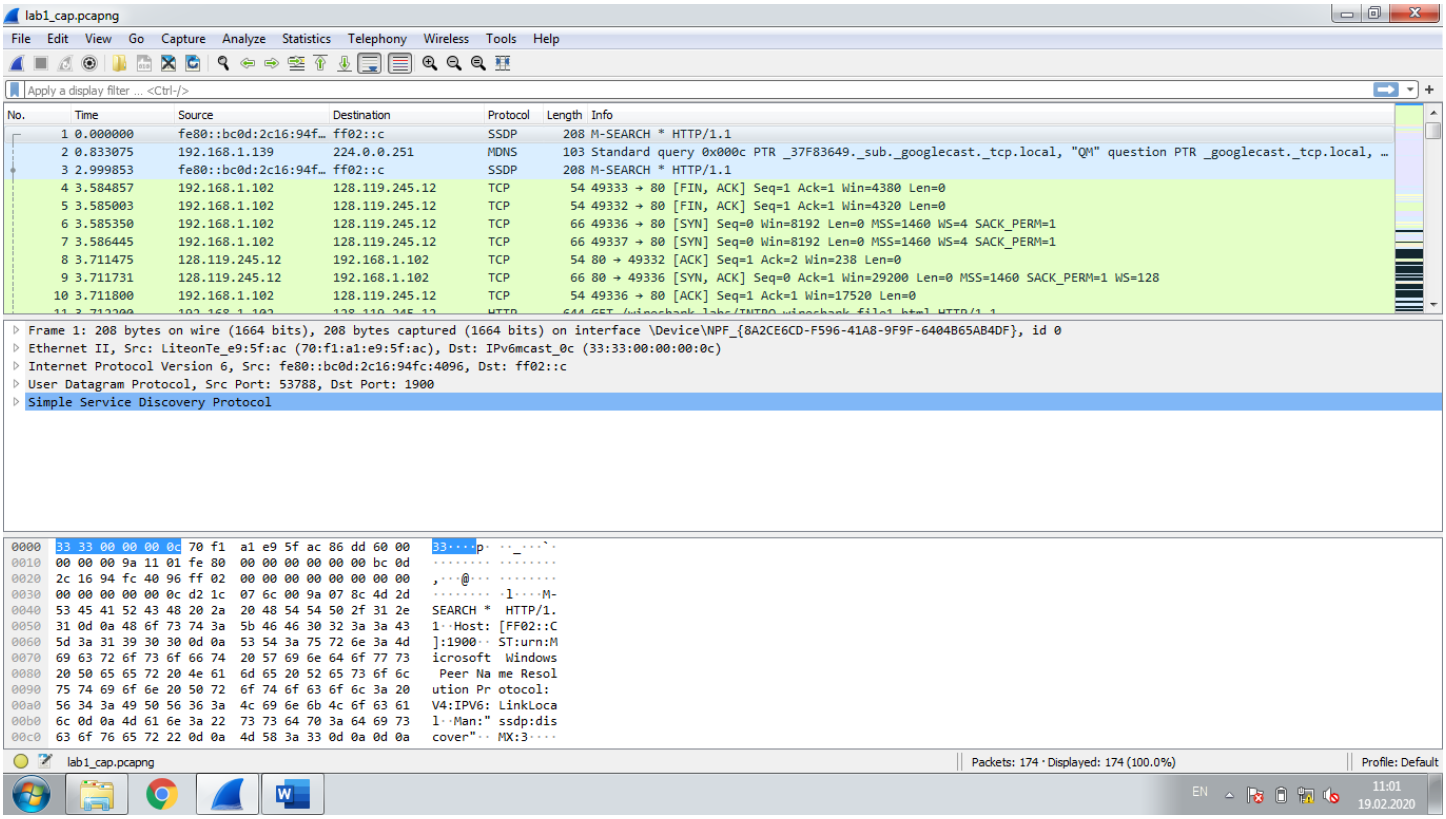
Жакулін Н. В.

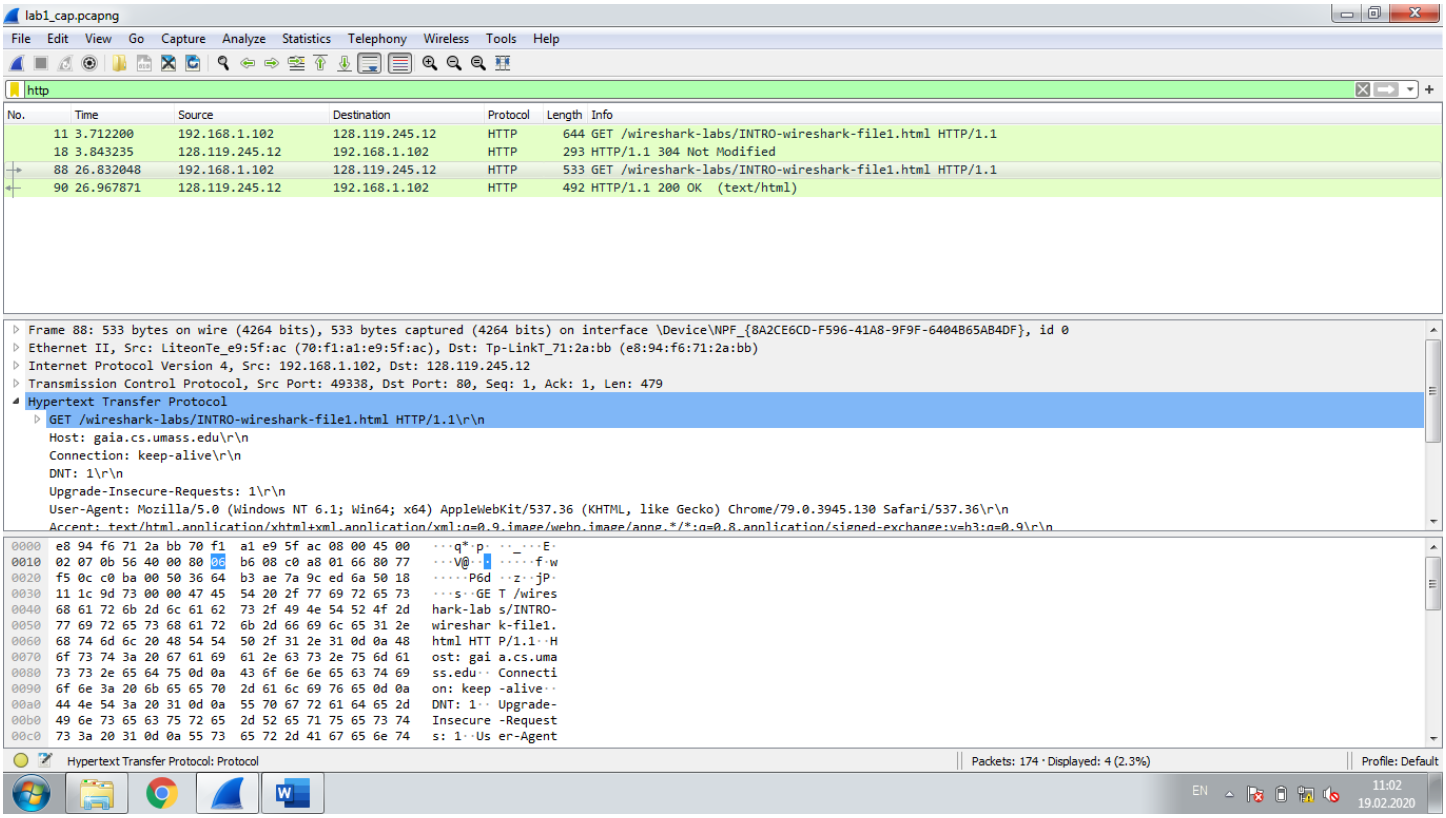
Перевірив: Кухарєв С. О.

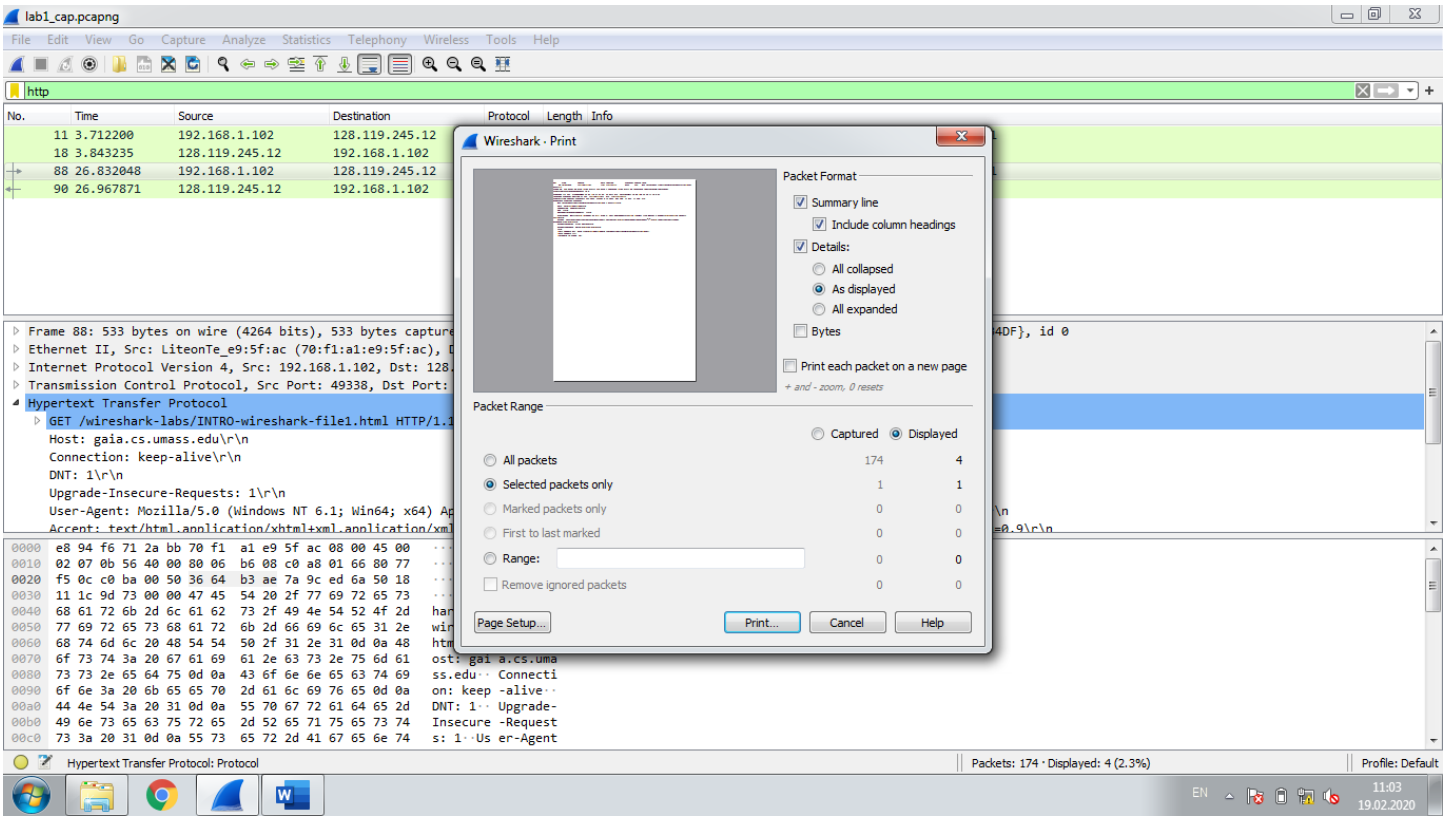
Київ 2020

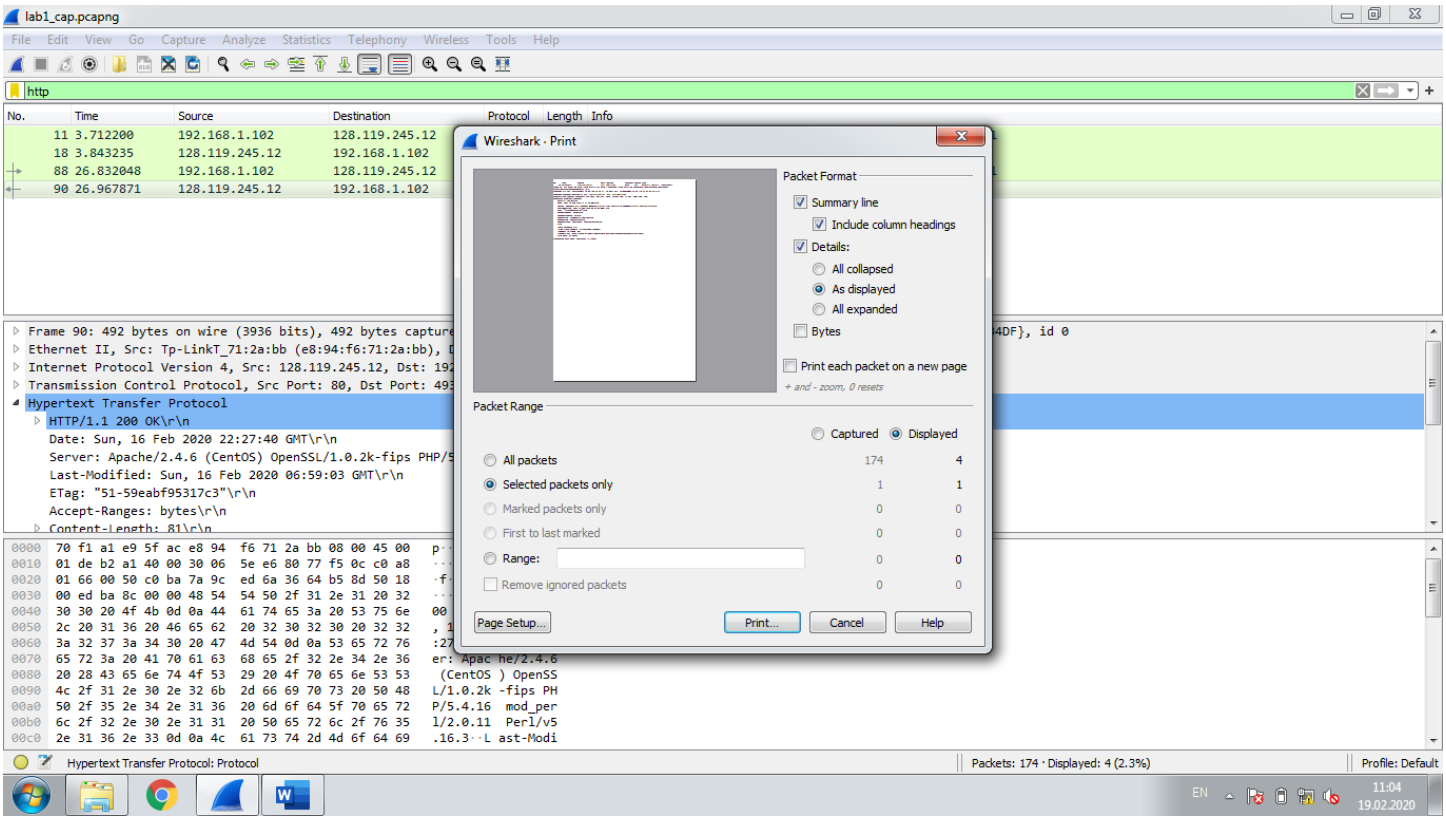
Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Хід виконання роботи






lab1_cap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
11 3.712200 192.168.1.102 128.119.245.12
18 3.843235 128.119.245.12 192.168.1.102
88 26.832048 192.168.1.102 128.119.245.12
90 26.967871 128.119.245.12 192.168.1.102
Wireshark · Print
Packet Format
Summary line
Include column headings
Details:
All collapsed
As displayed
All expanded
Bytes
Print each packet on a new page
+ and - zoom, 0 resets
Packet Range
Captured
Displayed
All packets 174 4
Selected packets only 1 1
Marked packets only 0 0
First to last marked 0 0
Range: 0 0
Remove ignored packets 0 0
Page Setup...
Print...
Cancel
Help
Frame 88: 533 bytes on wire (4264 bits), 533 bytes capture
Ethernet II, Src: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac),
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.
Transmission Control Protocol, Src Port: 49338, Dst Port:
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
DNT: 1\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) Ap
Accept: text/html,application/xhtml+xml,application/xml
0000 e8 94 f6 71 2a bb 70 f1 a1 e9 5f ac 08 00 45 00
0010 02 07 0b 56 40 00 80 06 b6 08 c0 a8 01 66 80 77
0020 f5 0c c0 ba 00 50 36 64 b3 ae 7a 9c ed 6a 50 18
0030 11 1c 9d 73 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a
00a0 44 4e 54 3a 20 31 0d 0a 55 70 67 72 61 64 65 2d
00b0 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74
00c0 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74
Hypertext Transfer Protocol: Protocol
Packets: 174 · Displayed: 4 (2.3%)
Profile: Default
11:03
19.02.2020


lab1_cap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
11 3.712200 192.168.1.102 128.119.245.12
18 3.843235 128.119.245.12 192.168.1.102
88 26.832048 192.168.1.102 128.119.245.12
90 26.967871 128.119.245.12 192.168.1.102
Wireshark · Print
Packet Format
Summary line
Include column headings
Details:
All collapsed
As displayed
All expanded
Bytes
Print each packet on a new page
+ and - zoom, 0 resets
Packet Range
Captured
Displayed
All packets 174 4
Selected packets only 1 1
Marked packets only 0 0
First to last marked 0 0
Range: 0 0
Remove ignored packets 0 0
Page Setup...
Print...
Cancel
Help
Frame 90: 492 bytes on wire (3936 bits), 492 bytes capture
Ethernet II, Src: Tp-LinkT_71:2a:bb (e8:94:f6:71:2a:bb),
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192
Transmission Control Protocol, Src Port: 80, Dst Port: 493
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 16 Feb 2020 22:27:40 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5
Last-Modified: Sun, 16 Feb 2020 06:59:03 GMT\r\n
ETag: "51-59eabf95317c3"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
0000 70 f1 a1 e9 5f ac e8 94 f6 71 2a bb 08 00 45 00
0010 01 de b2 a1 40 00 30 06 5e e6 80 77 f5 0c c0 a8
0020 01 66 00 50 c0 ba 7a 9c ed 6a 36 64 b5 8d 50 18
0030 00 ed ba 8c 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 75 6e
0050 2c 20 31 36 20 46 65 62 20 32 30 32 30 20 32 32
0060 3a 32 37 3a 34 30 20 47 4d 54 0d 0a 53 65 72 76
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48
00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72
00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69
Hypertext Transfer Protocol: Protocol
Packets: 174 · Displayed: 4 (2.3%)
Profile: Default
11:04
19.02.2020

Request:

```
No.     Time           Source                Destination           Protocol Length Info
     88 26.832048      192.168.1.102         128.119.245.12        HTTP     533    GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 88: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{8A2CE6CD-
F596-41A8-9F9F-6404B65AB4DF}, id 0
Ethernet II, Src: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac), Dst: Tp-LinkT_71:2a:bb (e8:94:f6:71:2a:bb)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49338, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
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
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; 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,ru;q=0.9,uk;q=0.8\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: 90]
```

Response:

```
No.     Time           Source                Destination           Protocol Length Info
     90 26.967871      128.119.245.12        192.168.1.102         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 90: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{8A2CE6CD-
F596-41A8-9F9F-6404B65AB4DF}, id 0
Ethernet II, Src: Tp-LinkT_71:2a:bb (e8:94:f6:71:2a:bb), Dst: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 49338, Seq: 1, Ack: 480, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 16 Feb 2020 22:27:40 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: Sun, 16 Feb 2020 06:59:03 GMT\r\n
    ETag: "51-59eabf95317c3"\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 1/1]
    [Time since request: 0.135823000 seconds]
    [Request in frame: 88]
    [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)
```

Відповіді на контрольні запитання:

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
   ARP, BROWSER, HTTP, LLMNR, SSDP, MDNS, TCP, NBNS, TLSv1.2.
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
   Ethernet II, IPv4, TCP, HTTP.
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Пройшло 136 мс.

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

   Запит:

   Вихідна: 192.168.1.102

   Цільова: 128.119.245.12

   Відповідь:

   Вихідний: 128.119.245.12

   Цільовий: 192.168.1.102

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

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

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

   HTTP/1.1 200 OK\r\n

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Був проведений аналіз отриманих пакетів, період часу, що пройшов між запитом та відповіддю, а також було розглянуто інформацію, що містить в собі протокол HTTP.