

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 2
З дисципліни: Комп'ютерні мережі

Протоколи HTTP

Виконала:
Студент III курсу
Групи КА-74
Вішталъ Д. В.
Перевірів: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу HTTP.

Хід виконання роботи

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows a single packet (No. 7) at time 0.174630, source 192.168.0.105, destination 128.119.245.12, protocol HTTP, length 549 bytes. The packet details pane shows the Hypertext Transfer Protocol section with the request line: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1. The packet bytes pane shows the raw data of the request, including the status bar at the bottom indicating 15 packets, 4 (26.7%) shown, and 0 (0.0%) lost.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.174630	192.168.0.105	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

> Frame 7: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{E7910711-2CFD-4CF3-A912-85B68977E86D}, id 0
> Ethernet II, Src: AzureNav_87:73:0d (74:c6:3b:87:73:0d), Dst: Tp-Link_f5:36:88 (78:4f:57:f5:36:88)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54036, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
> Hypertext Transfer Protocol

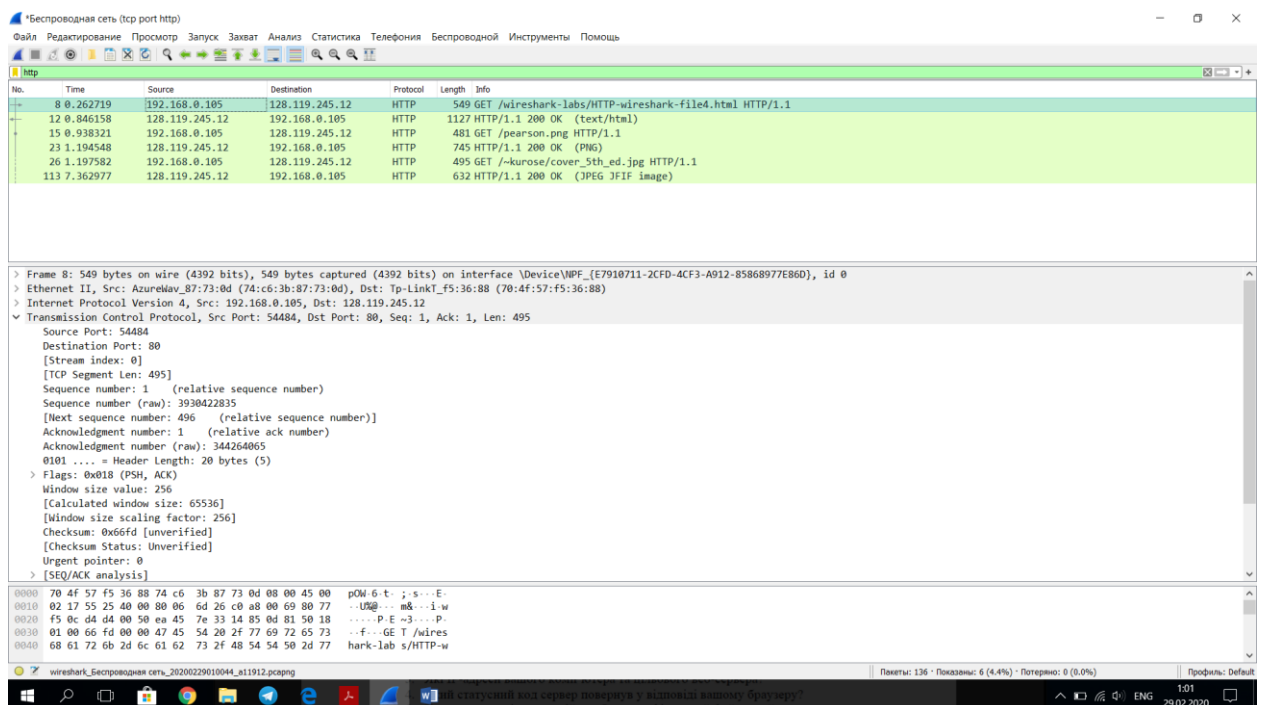
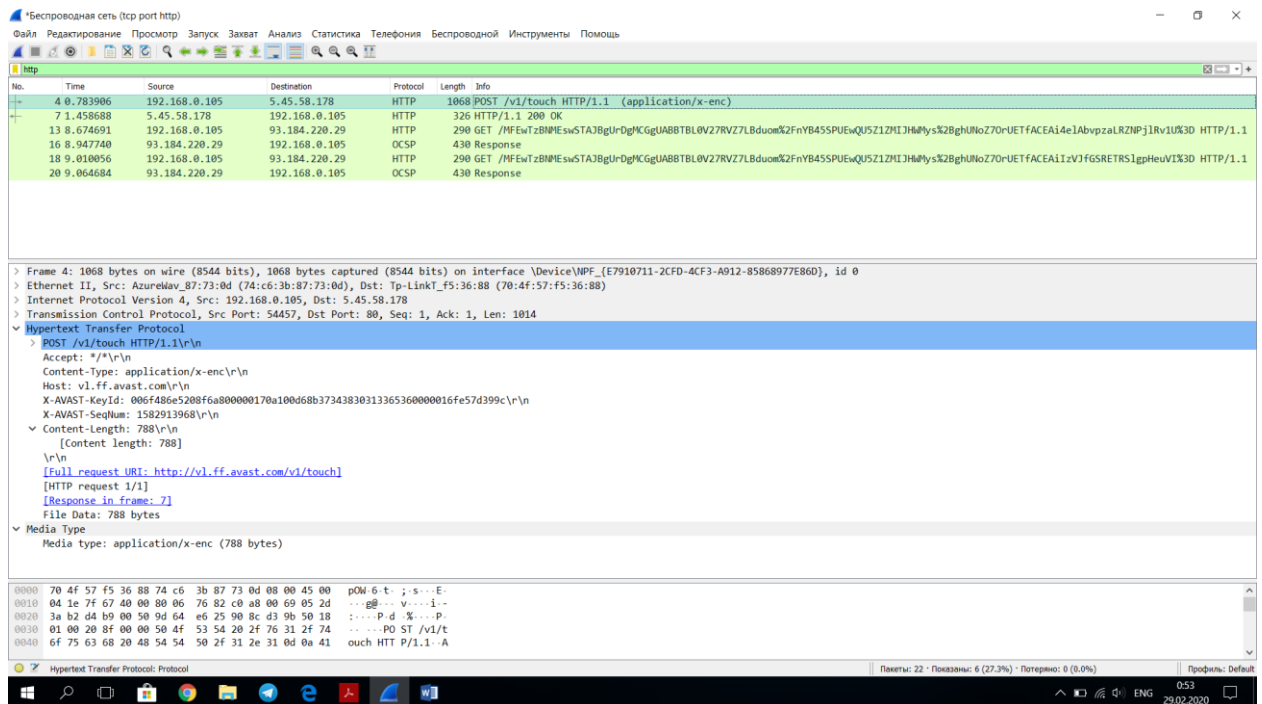
0000 70 4f 57 f5 36 88 74 c6 3b 87 73 0d 08 00 45 00 pOW 6 t ; s...E-
0010 02 17 54 40 40 00 80 06 6e 0b c0 a8 00 69 80 77 -T@... n...i w
0020 f5 0c d3 14 00 50 d3 0b 56 c f ff 5c 69 87 50 18P.. V...i.P.
0030 01 00 60 80 00 00 47 45 54 20 2f 77 69 72 65 73GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 reshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1. Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umass
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu -C connectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep-alive -U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1..Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; W in64; x6
00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows a single packet (No. 8) at time 0.260869, source 192.168.0.105, destination 128.119.245.12, protocol HTTP, length 549 bytes. The packet details pane shows the Hypertext Transfer Protocol section with the request line: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1. The packet bytes pane shows the raw data of the request, including the status bar at the bottom indicating 25 packets, 6 (24.0%) shown, and 0 (0.0%) lost.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.260869	192.168.0.105	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

> Frame 8: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{E7910711-2CFD-4CF3-A912-85B68977E86D}, id 0
> Ethernet II, Src: AzureNav_87:73:0d (74:c6:3b:87:73:0d), Dst: Tp-Link_f5:36:88 (78:4f:57:f5:36:88)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54206, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
> Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-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\nAccept: 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\nAccept-Encoding: gzip, deflate\r\nAccept-Language: uk-UA,uk;q=0.9,ru;q=0.8,en-US;q=0.7,en;q=0.6\r\n\r\n[Full] request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
[Full] request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu -C connectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep-alive -U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1..Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; W in64; x6
00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome
0120 2f 38 30 2e 30 2e 33 39 38 37 2e 31 32 32 20 53 /80.0.39 87.122 S
0130 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 afari/53 7.36 -Ac
0140 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,
0150 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhta
0160 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,ap plicatio
0170 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 n/xml;q= 0.9,imag



Контрольні питання

1. Яку версію протоколу НТТР використовує ваш браузер (1.0 чи 1.1)? Яку версію протоколу використовує сервер?

Браузер та сервер використовують протоколи 1.1

2. Які мови (якщо вказано) браузер може прийняти від сервера?

Accept-Encoding: gzip, deflate\r\n

Accept-Language: uk-UA,uk;q=0.9,ru;q=0.8,en-US;q=0.7,en;q=0.6\r\n\r\n

[Full request URI: <http://eaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

3. Які IP-адреси вашого комп'ютера та цільового веб-сервера?

Мій комп'ютер: 192.168.0.105

Сервер: 128.119.245.12

4. Який статусний код сервер повернув у відповіді вашому браузеру?

200 OK

5. Коли на сервері в останній раз був модифікований файл, який запитується браузером?

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.1

Last-Modified: Fri, 28 Feb 2020 06:59:01 GMT\r\n

ETag: "80-59f9d5f544acc"\r\n

6. Скільки байт контенту повертається сервером?

Content-Length: 128\r\n

> Content-Length: 128\r\n

Keep-Alive: timeout=5, max=100\r\n

7. Переглядаючи нерозібраний байтовий потік пакету, чи бачите ви деякі заголовки в

потоці, які не відображаються у вікні деталей пакету? Якщо так, назвіть один з них.

Всі відображаються.

8. Перевірте вміст першого запиту HTTP GET від вашого браузера до сервера. Чи є в ньому заголовок IF-MODIFIED-SINCE?

Такого заголовку немає.

9. Перевірте вміст першої відповіді сервера. Чи повернув сервер вміст файлу безпосередньо у відповіді?

i

<html>\n

Congratulations. You've downloaded the file \n

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n

</html>\n

10. Перевірте вміст другого запиту HTTP GET. Чи є в ньому заголовок IF-MODIFIEDSINCE? Якщо так, яке значення йому відповідає?

If-None-Match: "80-59f9d5f544acc"\r\n

If-Modified-Since: Fri, 28 Feb 2020 06:59:01 GMT\r\n

\r\n

11. Який код та опис статусу другої відповіді сервера? Чи повернув сервер вміст файлу безпосередньо у відповіді?

304 Not Modified. Ні не повернув.

12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

2 повідомлення

13. Скільки пакетів TCP було необхідно для доставки одної відповіді HTTP-сервера?

```
> Internet Protocol Version 4, Src: 5.45.58.178, Dst: 192.168.0.105
  Transmission Control Protocol, Src Port: 80, Dst Port: 54457, Seq: 1, Ack: 1015, Len: 272
    Source Port: 80
    Destination Port: 54457
    [Stream index: 0]
    [TCP Segment Len: 272]
    Sequence number: 1 (relative sequence number)
    Sequence number (raw): 2425148315
    [Next sequence number: 273 (relative sequence number)]
    Acknowledgment number: 1015 (relative ack number)
    Acknowledgment number (raw): 2640636443
    0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
```

14. Який код та опис статусу був у відповіді сервера?

HTTP/1.1 200 OK

15. Чи зустрічаються у даних пакетів-продовжень протоколу TCP стрічки з кодом та описом статусу відповіді, або ж якісь заголовки протоколу HTTP?

Не зустрічаються

16. Скільки запитів HTTP GET було відправлено вашим браузером? Якими були цільові IP-адреси запитів?

3 запити.

Цільовий адрес: 128.119.245.12.

17. Чи можете ви встановити, чи були ресурси отримані паралельно чи послідовно? Яким чином?

Вони були отримані паралельно, це ми можемо дослідити подивившись на час коли вони були отримані.

Висновок

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