

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

Лабораторна робота № 2
З дисципліни: Комп'ютерні мережі

Протокол HTTP

Виконав:
Студент III курсу
Групи КА-74
Микитенко О.В.
Перевірів: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу HTTP.

Хід роботи

Необхідно виконати наступні дії:

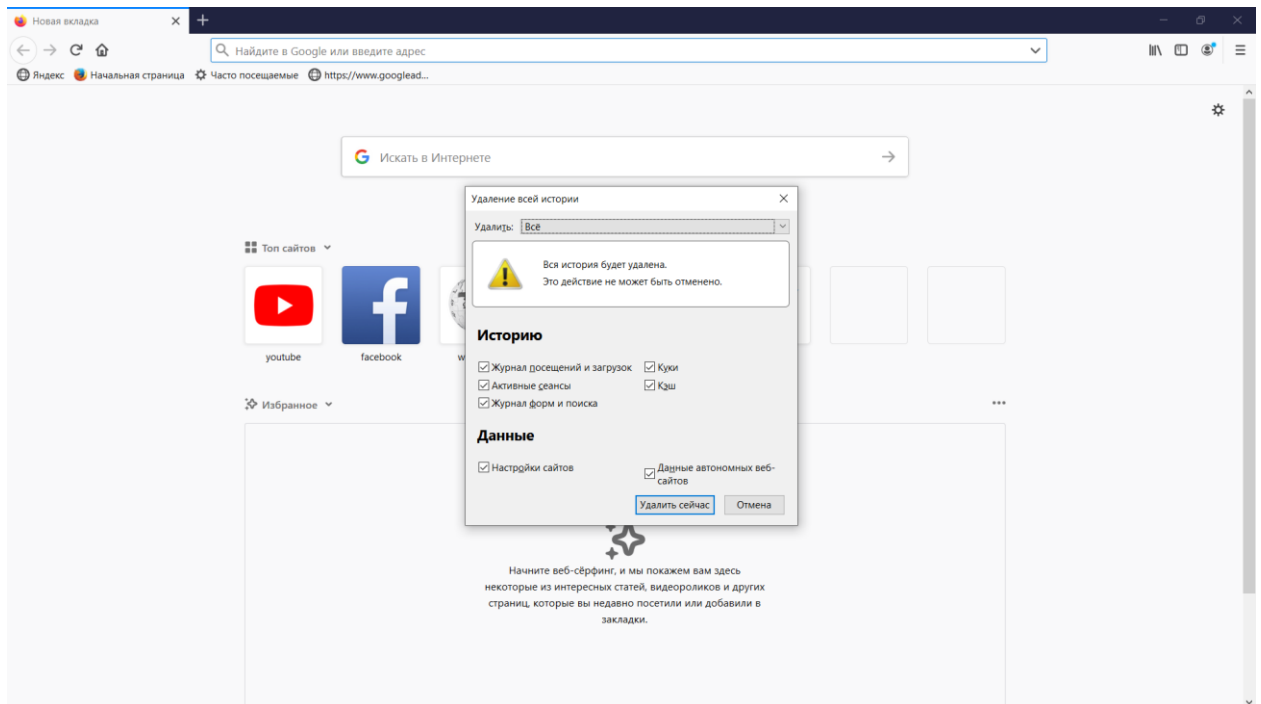
✓ Запустіть веб-браузер, очистіть кеш браузера:

а. для Firefox виконайте

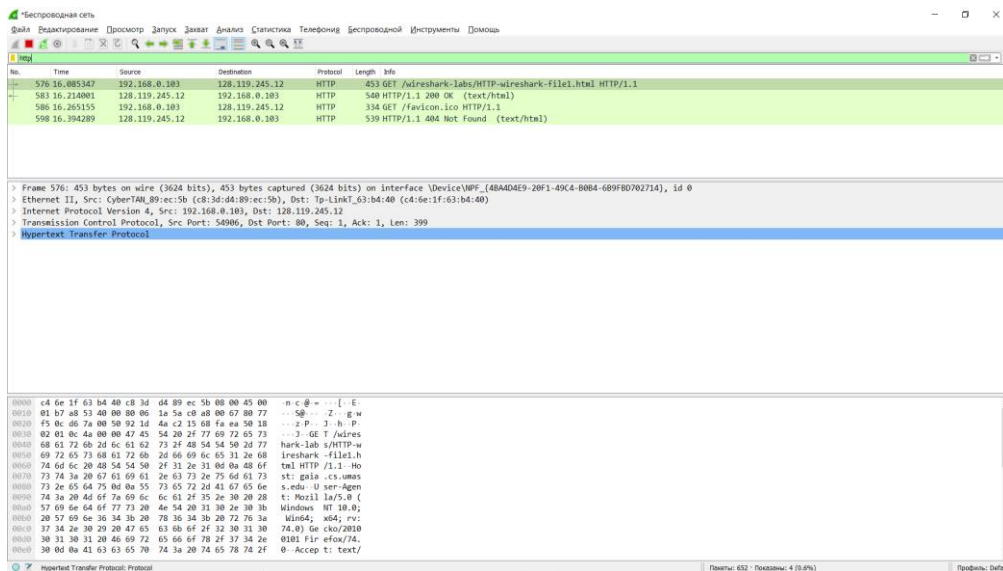
Tools >> Clear Private Data (або Ctrl + Shift + Del)

б. для MS IE виконайте

Tools >> Internet Options >> Delete File



✓ Запустіть Wireshark, введіть «http» в поле фільтрації, почніть захоплення пакетів.



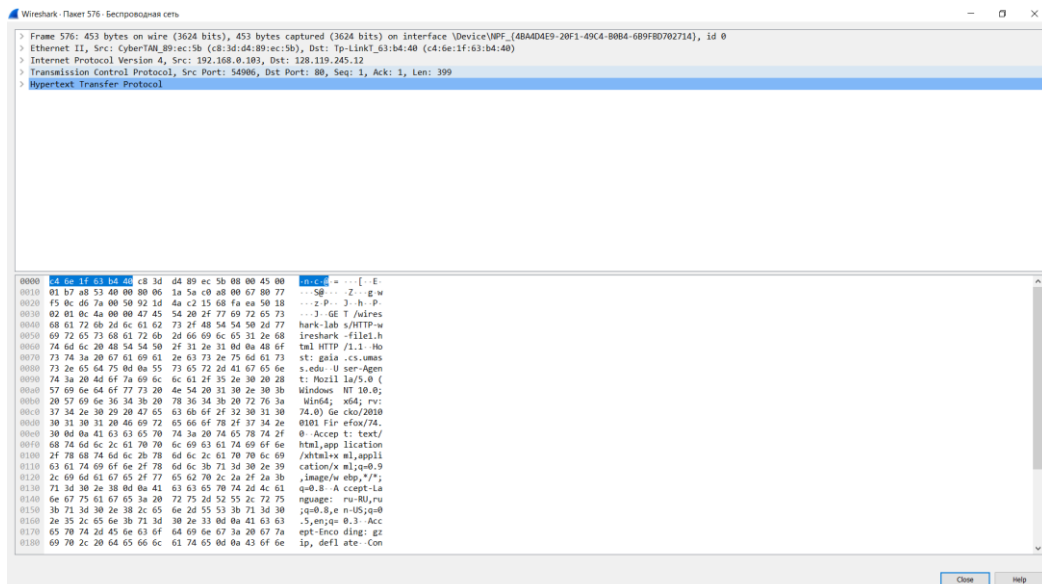
- ✓ Відкрийте за допомогою браузера одну із зазначених нижче адрес:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

<http://194.44.29.242/index.html>



- ✓ Зупиніть захоплення пакетів.
- ✓ Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім HTTP (за допомогою знаків +/-).



- ✓ Приготуйте відповіді на контрольні запитання 1-7, роздрукуйте необхідні для цього пакети.
- ✓ Почніть захоплення пакетів.
- ✓ Відкрийте у браузері ту ж саму сторінку, або ж просто натисніть F5 для її повторного завантаження. Якщо ви працюєте зі сторінкою на gaia.cs.umass.edu (ця сторінка регенерується кожну хвилину) – почніть спочатку та виконайте кроки 1,2,3 та 8.
- ✓ Зупиніть захоплення пакетів.
- ✓ Приготуйте відповіді на контрольні запитання 8-11, роздрукуйте необхідні для цього пакети.
- ✓ Виберіть адрес деякого ресурсу (наприклад, зображення), розмір якого перевищує 8192 байти. Можна, наприклад, використати

http://www.dilbert.com/dyn/str_strip/0000000000/00000000/00000000/000000/70000/3000

[/400/73435/73435.strip.gif](http://www.dilbert.com/dyn/str_strip/0000000000/00000000/00000000/000000/70000/3000)

http://www.dilbert.com/dyn/str_strip/0000000000/00000000/00000000/000000/70000/3000

[/300/77356/77356.strip.sunday.gif](http://www.dilbert.com/dyn/str_strip/0000000000/00000000/00000000/000000/70000/3000)

або будь-який не дуже великий файл з серверу 194.44.29.242.

- ✓ Почніть захоплення пакетів та очистіть кеш браузера.
- ✓ Відкрийте обраний ресурс браузером.
- ✓ Зупиніть захоплення пакетів.
- ✓ Приготуйте відповіді на запитання 12-15. При необхідності роздрукуйте деякі
- ✓ пакети з відповіді сервера.
- ✓ Почніть захоплення пакетів.
- ✓ Відкрийте сторінку за адресою

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

також можна використати будь-яку нескладну сторінку з невеликою кількістю зовнішніх ресурсів.

- ✓ Зупиніть захоплення пакетів.
- ✓ Приготуйте відповіді на запитання 16, 17. Роздрукуйте необхідні для цього пакети.
- ✓ Закрийте Wireshark.

Контрольні питання

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

протоколу використовує сервер?

Браузер та сервер використовують протоколи 1.1

HTTP/1.1

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

00c0	37 34 2e 30 0d 0a 41 63	63 65 70 74 3a 20 69 6d	74.0..Ac cept: im
00d0	61 67 65 2f 77 65 62 70	2c 2a 2f 2a 0d 0a 41 63	age/webp , /*..Ac
00e0	63 65 70 74 2d 4c 61 6e	67 75 61 67 65 3a 20 72	cept-Lan guage: r
00f0	75 2d 52 55 2c 72 75 3b	71 3d 30 2e 38 2c 65 6e	u-RU,ru; q=0.8,en
0100	2d 55 53 3b 71 3d 30 2e	35 2c 65 6e 3b 71 3d 30	-US;q=0. 5,en;q=0
0110	2e 33 0d 0a 41 63 63 65	70 74 2d 45 6e 63 6f 64	.3..Acce pt-Encod
0120	69 6e 67 3a 20 67 7a 69	70 2c 20 64 65 66 6c 61	ing: gzi p, defla
0130	74 65 0d 0a 43 6f 6e 6e	65 63 74 69 6f 6e 3a 20	te..Conn ection:
0140	6b 65 65 70 2d 61 6c 69	76 65 0d 0a 0d 0a	keep-ali ve....

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

Мій комп'ютер: 192.168.0.103

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?

[Time since previous frame in this TCP stream: 0.006877000 seconds]

TCP payload (486 bytes)

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Sat, 04 Apr 2020 15:26:31 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Per

Last-Modified: Sat, 04 Apr 2020 05:59:02 GMT\r\n

ETag: "80-5a270bb15be41"\r\n

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 53 61	74 2c 20 30 34 20 41 70	fied: Sa t, 04 Ap
00e0	72 20 32 30 32 30 20 30	35 3a 35 39 3a 30 32 20	r 2020 0 5:59:02
00f0	47 4d 54 0d 0a 45 54 61	67 3a 20 22 38 30 2d 35	GMT..ETa g: "80-5
0100	61 32 37 30 62 62 31 35	62 65 34 31 22 0d 0a 41	a270bb15 be41"..A

6. Скільки байт контенту повертається сервером?

```

TCP payload (486 bytes)
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Sat, 04 Apr 2020 15:26:31 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: Sat, 04 Apr 2020 05:59:02 GMT\r\n
    ETag: "80-5a270bb15be41"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e  test content-len
0130 57 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41  th: 128, Keep-A
0140 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c  live: t1 meout=5,
0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63  max=100 --Conne
0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65  tion: Keep-Alive

```

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?

Ні, не повернув.

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

Такого заголовку немає.

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

```

Wireshark - Пакет 61 - Беспроводная сеть
[SEQ/ACK analysis]
  [IRTT: 0.121163000 seconds]
  [Bytes in flight: 239]
  [Bytes sent since last PSH flag: 239]
[Timestamps]
  [Time since first frame in this TCP stream: 0.249142000 seconds]
  [Time since previous frame in this TCP stream: 0.000822000 seconds]
TCP payload (239 bytes)
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 04 Apr 2020 15:47:26 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "80-5a270bb15be41"\r\n
    \r\n
  [HTTP response 1/1]
  [Time since request: 0.126385000 seconds]
  [Request in frame: 53]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
0000 c8 3d d4 89 ec 5b c4 6e 1f 63 b4 40 08 00 45 00  ....[.m.c.@@.E.
0010 01 17 3e b6 40 00 2d 06 d7 97 80 77 f5 0c c0 a8  -->@...w....
0020 00 67 00 50 de 11 a5 0b 0a 96 00 be 4b 5e 50 18  g.P....KpP.
0030 00 ed b2 ca 00 00 43 5a 54 50 2f 31 2e 31 20 33  ....H TP/1.1
0040 00 2d 2c 0f 74 20 4d 6f 24 69 6e 69 65 64 0a  0d Not Modified
0050 0a 44 61 74 65 3a 20 53 61 74 2c 20 30 3a 20 41  Date: Sat, 04 A
0060 70 72 20 32 30 32 30 20 31 35 3a 3a 37 3a 32 36  pr 2020 15:47:26
0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70  GMT..Se rver: Ap
0080 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74  ache/2.4.6 (Cent
0090 4f 53 20 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e  OS) Open SSL/1.0.
00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e  2k-fips PHP/5.4.
00b0 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e  16 mod_p erl/2.0.
00c0 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d  11 Perl/ v5.16.3.
00d0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65  .Connect ion: Kee
00e0 70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6c  p-Alive. Keep-Al
00f0 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20  live: tim eout=5,
0100 6d 61 78 3d 31 30 30 0d 0a 45 54 61 67 3a 20 22  max=100. ETag: "
0110 38 30 2d 35 61 32 37 30 62 62 31 35 62 65 34 31  80-5a270 bb15be41
0120 22 0d 0a 0d 0a  ....

```

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?

```

> Transmission Control Protocol, Src Port: 80, Dst Port: 58559, Seq: 1, Ack: 320, Len: 384

```

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

HTTP/1.1

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

Ні, не зустрічаються.

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

4 запити.

Цільовий адрес: 128.119.245.12

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

Вони були отримані послідовно, 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.