

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №2
з курсу «Комп'ютерні мережі»
тема: «аналіз деталей роботи протоколу HTTP»

Виконав: студент 3 курсу
групи КА-77
Буханевич Р.М.
Прийняв: Кухарев С.О.

Київ – 2020р.

Вихідний пакет

No.	Time	Source	Destination	Protocol	Length	Info
344	76.749437	192.168.0.102	128.119.245.12	HTTP	661	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 344: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 0a:31:28:1d:9e:b5 (0a:31:28:1d:9e:b5), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 53586, Dst Port: 80, Seq: 1, Ack: 1, Len: 607

Hypertext Transfer Protocol

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

[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/INTRO-wireshark-file1.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\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/80.0.3987.106 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,uk;q=0.6\r\n

If-None-Match: "51-59ec017223662"\r\n

If-Modified-Since: Mon, 17 Feb 2020 06:59:02 GMT\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: 349]

Вхідний пакет

No.	Time	Source	Destination	Protocol	Length	Info
349	76.872251	128.119.245.12	192.168.0.102	HTTP	293	HTTP/1.1 304 Not Modified

Frame 349: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface
\\Device\\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 0a:31:28:1d:9e:b5
(0a:31:28:1d:9e:b5)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102

Transmission Control Protocol, Src Port: 80, Dst Port: 53586, Seq: 1, Ack: 608, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\\r\\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\\r\\n]

Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

Date: Mon, 17 Feb 2020 19:02:07 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: "51-59ec017223662"\\r\\n

\\r\\n

[HTTP response 1/1]

[Time since request: 0.122814000 seconds]

[Request in frame: 344]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

Контрольні запитання:

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

1.1 в обох

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

ru,en,uk.

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

192.168.0.102,

128.119.245.12.

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

304 not modified

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

21:00:57 19.02.2020

6. Скільки байт контенту повертається сервером?

239 bytes

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.

8. Перевірте вміст першого запиту HTTP GET від вашого браузера до сервера. Чи є в

ньому заголовок IF-MODIFIED-SINCE? Ні

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

Так

10. Перевірте вміст другого запиту HTTP GET. Чи є в ньому заголовок IF-MODIFIED-

SINCE? Якщо так, яке значення йому відповідає?

11. Який код та опис статусу другої відповіді сервера? Чи повернув сервер вміст файлу
безпосередньо у відповіді?
12. Скільки повідомлень HTTP GET було відправлено вашим браузером?
13. Скільки пакетів TCP було необхідно для доставки одної відповіді HTTP-сервера?
14. Який код та опис статусу був у відповіді сервера?
15. Чи зустрічаються у даних пакетів-продовжень протоколу TCP стрічки з кодом та
описом статусу відповіді, або ж якісь заголовки протоколу HTTP?
16. Скільки запитів HTTP GET було відправлено вашим браузером? Якими
були цільові
3 запити
IP-адреси запитів?
192.168.0.103
17. Чи можете ви встановити, чи були ресурси отримані паралельно чи
послідовно?
Яким чином?

Висновки

Оволодів методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих проколів.