

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Практична робота №2
з курсу «Комп'ютерні мережі»

Виконав студент 3 курсу
групи КА-72
Орел Євгеній
Прийняв Кухарев С.О.

Київ – 2020 р.

Контрольні запитання:

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

Мій браузер використовує версію: 1.1, сервер: 1.1.

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

Accept Language: en-US,en;q=0.9,ru;q=0.8

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

Internet Protocol Version 4, Src: 192.168.0.108, Dst: 128.119.245.12

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

HTTP/1.1 200 OK

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

Last-Modified: Tue, 07 Apr 2020 05:59:02 GMT\r\n

6. Скільки байт контенту повертається сервером?

Content-Length: 128\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.

Ні, такі заголовки відсутні.

Запит:

No.	Time	Source	Destination	Protocol	Length	Info
51	2.847474	192.168.0.108	128.119.245.12	HTTP	631	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 51: 631 bytes on wire (5048 bits), 631 bytes captured (5048 bits) on interface en0, id 0 Ethernet II, Src: Apple_d6:45:86 (a4:d1:8c:d6:45:86), Dst: Tp-LinkT_55:94:64 (14:cc:20:55:94:64)

Internet Protocol Version 4, Src: 192.168.0.108, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 63366, Dst Port: 80, Seq: 1, Ack: 1, Len: 565

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-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 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 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,ru;q=0.8\r\n

If-None-Match: "80-5a17f55135b28"\r\n

If-Modified-Since: Mon, 23 Mar 2020 05:59:03 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

[HTTP request 1/2]

[Response in frame: 53]

[Next request in frame: 55]

Відповідь:

No.	Time	Source	Destination	Protocol	Length	Info
53	2.975763	128.119.245.12	192.168.0.108	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 53: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_55:94:64 (14:cc:20:55:94:64), Dst: Apple_d6:45:86 (a4:d1:8c:d6:45:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.108

Transmission Control Protocol, Src Port: 80, Dst Port: 63366, Seq: 1, Ack: 566, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 07 Apr 2020 19:47:17 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: Tue, 07 Apr 2020 05:59:02 GMT\r\n

ETag: "80-5a2ad14a1b0ae"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\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 1/2]

[Time since request: 0.128289000 seconds]

[Request in frame: 51]

[Next request in frame: 55]

[Next response in frame: 56]

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

File Data: 128 bytes

Line-based text data: text/html (4 lines)

<html>\n

Congratulations. You've downloaded the file \n

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

</html>\n

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-MODIFIEDSINCE?

Якщо так, яке значення йому відповідає?

Ні

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

HTTP/1.1 200 OK\r\n

Так

Запит:

No.	Time	Source	Destination	Protocol	Length	Info
4018	7.959894	192.168.0.108	151.139.128.14	HTTP	362	GET / MFYwVKADAgEAME0wSzBJMAkGBSsOAwlaBQAEFEMl0g5PE3oabJGPJOXafjJNRzPIBBSNjF7EV K2K4Xfpm%2FmbBeG4AY1h4QIQCMsGSO%2F7DtZbcC%2BJGDJRAG%3D%3D HTTP/1.1

Frame 4018: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface en0, id 0
Ethernet II, Src: Apple_d6:45:86 (a4:d1:8c:d6:45:86), Dst: Tp-LinkT_55:94:64 (14:cc:20:55:94:64)
Internet Protocol Version 4, Src: 192.168.0.108, Dst: 151.139.128.14
Transmission Control Protocol, Src Port: 64598, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
Hypertext Transfer Protocol

GET /

MFYwVKADAgEAME0wSzBJMAkGBSsOAwlaBQAEFEMl0g5PE3oabJGPJOXafjJNRzPIBBSNjF7EV
K2K4Xfpm%2FmbBeG4AY1h4QIQCMsGSO%2F7DtZbcC%2BJGDJRAG%3D%3D HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /

MFYwVKADAgEAME0wSzBJMAkGBSsOAwlaBQAEFEMl0g5PE3oabJGPJOXafjJNRzPIBBSNjF7EV
K2K4Xfpm%2FmbBeG4AY1h4QIQCMsGSO%2F7DtZbcC%2BJGDJRAG%3D%3D HTTP/1.1\r\n]

Request Method: GET

Request URI: /

MFYwVKADAgEAME0wSzBJMAkGBSsOAwlaBQAEFEMl0g5PE3oabJGPJOXafjJNRzPIBBSNjF7EV
K2K4Xfpm%2FmbBeG4AY1h4QIQCMsGSO%2F7DtZbcC%2BJGDJRAG%3D%3D

Request Version: HTTP/1.1

Host: obsp.sectigo.com\r\n

Accept: */*\r\n

Accept-Language: ru\r\n

Connection: keep-alive\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: com.apple.trustd/2.0\r\n

\r\n

[Full request URI: http://osp.sectigo.com/

MFYwVKADAgEAME0wSzBJMAkGBSsOAwlaBQAEFEMl0g5PE3oabJGPJOXafjJNRzPIBBSNjF7EV
K2K4Xfpm%2FmbBeG4AY1h4QIQCMsGSO%2F7DtZbcC%2BJGDJRAG%3D%3D]

[HTTP request 1/1]

[Response in frame: 4032]

No.	Time	Source	Destination	Protocol	Length	Info
4032	8.001062	151.139.128.14	192.168.0.108	OCSP	982	Response

Frame 4032: 982 bytes on wire (7856 bits), 982 bytes captured (7856 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_55:94:64 (14:cc:20:55:94:64), Dst: Apple_d6:45:86 (a4:d1:8c:d6:45:86)
Internet Protocol Version 4, Src: 151.139.128.14, Dst: 192.168.0.108
Transmission Control Protocol, Src Port: 80, Dst Port: 64598, Seq: 1, Ack: 297, Len: 916
Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK
Date: Tue, 07 Apr 2020 21:09:28 GMT\r\n
Accept-Ranges: bytes\r\n
Content-Type: application/ocsp-response\r\n
Last-Modified: Tue, 07 Apr 2020 18:22:17 GMT\r\n
Server: Apache\r\n
ETag: 0B4BA9DB6F7F9B068909DAD1EA739C72FA6ECA0E\r\n
Cache-Control: max-age=595817,s-maxage=1800,public,no-transform,must-revalidate\r\n
X-OCSP-Responder-ID: mcdpcaocsp8\r\n
X-HW: 1586293768.cds002.wa1.h2,1586293768.cds010.wa1.c\r\n
Connection: keep-alive\r\n
Content-Length: 471\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.041168000 seconds]
[Request in frame: 4018]
[Request URI: http://ocsp.sectigo.com/
MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFEML0g5PE3oabJGPJOXafjJNRzPIBBSNjF7EV
K2K4Xfpm%2FmbBeG4AY1h4QIQCMMSGSO%2F7DtZbcC%2BJGDJRAG%3D%3D]
File Data: 471 bytes
Online Certificate Status Protocol
responseStatus: successful (0)
responseBytes
 ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
 BasicOCSPResponse
 tbsResponseData
 signatureAlgorithm (sha256WithRSAEncryption)
 Padding: 0
 signature: 75a322e7cfb22d720cc90dcff98bd9f5be53978b450fea43...

12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

Чотири

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

146

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?

Так, зустрічаються як код та опис статусу відповіді, так і всі заголовки HTTP.

No.	Time	Source	Destination	Protocol	Length	Info
97	2.781079	192.168.0.108	128.119.245.12	HTTP	546	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1

Frame 97: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface en0, id 0
Ethernet II, Src: Apple_d6:45:86 (a4:d1:8c:d6:45:86), Dst: Tp-LinkT_55:94:64 (14:cc:20:55:94:64)
Internet Protocol Version 4, Src: 192.168.0.108, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 64749, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file4.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 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 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,ru;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
[HTTP request 1/2]
[Response in frame: 110]
[Next request in frame: 221]

No.	Time	Source	Destination	Protocol	Length	Info
110	2.922516	128.119.245.12	192.168.0.108	HTTP	1139	HTTP/1.1 200 OK (text/html)

Frame 110: 1139 bytes on wire (9112 bits), 1139 bytes captured (9112 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_55:94:64 (14:cc:20:55:94:64), Dst: Apple_d6:45:86 (a4:d1:8c:d6:45:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.108
Transmission Control Protocol, Src Port: 80, Dst Port: 64749, Seq: 1, Ack: 481, Len: 1073
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Tue, 07 Apr 2020 21:20:14 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: Tue, 07 Apr 2020 05:59:02 GMT\r\n
ETag: "2ca-5a2ad14a1628d"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 714\r\n
[Content length: 714]
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 1/2]
[Time since request: 0.141437000 seconds]
[Request in frame: 97]
[Next request in frame: 221]
[Next response in frame: 230]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
File Data: 714 bytes
Line-based text data: text/html (17 lines)
<html>\n
<head>\n
<title>Lab2-4 file: Embedded URLs</title>\n

```

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">\n
</head>\n
\n
<body bgcolor="#FFFFFF" text="#000000">\n
\n
<p>\n
 </p>\n
<p>This little HTML file is being served by gaia.cs.umass.edu. \n
It contains two embedded images. <br> The image above, also served from the \n
gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. <br>\n
The image of our 5th edition book cover below is stored at, and served from, the www server
caite.cs.umass.edu:</p>\n
<p align="left"></p>\n
</body>\n
</html>\n

```

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

3

No.	Time	Source	Destination	Protocol	Length	Info
97	2.781079	192.168.0.108	128.119.245.12	HTTP	546	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
221	3.538007	192.168.0.108	128.119.245.12	HTTP	478	GET /pearson.png HTTP/1.1
268	3.882962	192.168.0.108	128.119.245.12	HTTP	492	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

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

Послідовно, це зрозуміло за часом

Висновки:

В цій лабораторній роботі я продовжив досліджувати протокол HTTP за допомогою середовища захоплення та аналізу пакетів протоколів Wireshark.