

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

Завдання лабораторної роботи №2
З дисципліни «Комп'ютерні мережі»

Виконав: студент 3-го курсу

гр. КА-71

Возняк В. З.

Прийняв: Кухарєв С.О.

Київ 2020

lab_2(1).pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

No.	Time	Source	Destination	Protocol	Length	Info
72	6.326968	192.168.1.5	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
76	6.453069	128.119.245.12	192.168.1.5	HTTP	552	HTTP/1.1 200 OK (text/html)
78	6.529812	192.168.1.5	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
79	6.659777	128.119.245.12	192.168.1.5	HTTP	550	HTTP/1.1 404 Not Found (text/html)

> Frame 72: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{DA808D97-276E-43B7-99F5-2E540C9C4376}, id 0
 > Ethernet II, Src: LiteonTe_00:d6:0a (58:00:e3:00:d6:0a), Dst: Tp-LinkT_81:c9:ee (c0:25:e9:81:c9:ee)
 > Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 24670, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
 > Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 > [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 > [Severity level: Chat]
 > [Group: Sequence]
 > Request Method: GET
 > Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 > Request Version: HTTP/1.1
 > Host: gaia.cs.umass.edu\r\n
 > Connection: keep-alive\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/81.0.4044.129 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\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: 76]
 > [Next request in frame: 78]

Hypertext Transfer Protocol (request)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\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/81.0.4044.129
Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;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\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: 76]  
[Next request in frame: 78]
```

Hypertext Transfer Protocol (response)

```
HTTP/1.1 200 OK\r\n  
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]  
[HTTP/1.1 200 OK\r\n]  
[Severity level: Chat]  
[Group: Sequence]  
Response Version: HTTP/1.1  
Status Code: 200  
[Status Code Description: OK]  
Response Phrase: OK  
Date: Fri, 01 May 2020 14:24:52 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: Fri, 01 May 2020 05:59:02 GMT\r\n  
ETag: "80-5a48fe0c9953e"\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: 0.126101000 seconds]  
[Request in frame: 72]  
[Next request in frame: 78]  
[Next response in frame: 79]  
[Request URI: http://gaia.cs.umass.edu/favicon.ico]  
File Data: 128 bytes
```

ВІДПОВІДІ НА ПИТАННЯ 1-7

- 1) HTTP 1.1. Навряд чи зараз ще використовується 1.0, оскільки 1.1 було розроблено саме для того, щоб можна було встановити постійне з'єднання в рамках якого посилалося б більше одного запиту-відповіді.
- 2) Для цього дивимося в заголовок пакета запиту Accept-Language. Мови перераховуються в порядку пріоритетності. В нашому випадку такими є російська, англійська (американська) та англійська (британська).

- 3) IP мого ПК **Source: 192.168.1.5**. Серверу **Destination: 128.119.245.12**.
- 4) Status Code: 200. Означає успішний запит.
- 5) Last-Modified: Fri, 01 May 2020 05:59:02 GMT
- 6) Content-Length: 128. Розмір вказується в байтах.
- 7) У пакеті на запит все відповідає байтовому представленню. У пакеті-відповіді все також відповідає байтовому представленню.

lab_2(2).pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

No.	Time	Source	Destination	Protocol	Length	Info
23	0.936535	192.168.1.5	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
27	1.074293	128.119.245.12	192.168.1.5	HTTP	552	HTTP/1.1 200 OK (text/html)
29	1.117741	192.168.1.5	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
30	1.249519	128.119.245.12	192.168.1.5	HTTP	550	HTTP/1.1 404 Not Found (text/html)
34	3.551788	192.168.1.5	128.119.245.12	HTTP	663	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
35	3.689351	128.119.245.12	192.168.1.5	HTTP	304	HTTP/1.1 304 Not Modified

> Frame 23: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{DA808D97-276E-43B7-99F5-2E540C9C4376}, id 0

> Ethernet II, Src: LiteonTe_00:d6:0a (58:00:e3:00:d6:0a), Dst: Tp-LinkT_81:c9:ee (c0:25:e9:81:c9:ee)

> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 24715, Dst Port: 80, Seq: 1, Ack: 1, Len: 486

▼ Hypertext Transfer Protocol

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

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

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

 [Severity level: Chat]

 [Group: Sequence]

 Request Method: GET

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

 Request Version: HTTP/1.1

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

 Connection: keep-alive\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/81.0.4044.129 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\r\n

 \r\n

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

 [HTTP request 1/3]

 [Response in frame: 27]

 [Next request in frame: 29]

Hypertext Transfer Protocol (1st request)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\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/81.0.4044.129
Safari/537.36\r\n
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;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\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-
wireshark-file1.html]
[HTTP request 1/3]
[Response in frame: 27]
[Next request in frame: 29]
```

Hypertext Transfer Protocol (1st response)

```
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 01 May 2020 14:29:34 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: Fri, 01 May 2020 05:59:02 GMT\r\n
ETag: "80-5a48fe0c9953e"\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 1/3]
[Time since request: 0.137758000 seconds]
[Request in frame: 23]
[Next request in frame: 29]
[Next response in frame: 30]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
file1.html]
File Data: 128 bytes
```

Hypertext Transfer Protocol (3d request)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-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/81.0.4044.129
Safari/537.36\r\n
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;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\r\n
If-None-Match: "80-5a48fe0c9953e"\r\n
If-Modified-Since: Fri, 01 May 2020 05:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-
wireshark-file1.html]
[HTTP request 3/3]
[Prev request in frame: 29]
[Response in frame: 35]
```

Hypertext Transfer Protocol (3d response)

```
HTTP/1.1 304 Not Modified\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
[HTTP/1.1 304 Not Modified\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Fri, 01 May 2020 14:29:37 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=98\r\n
ETag: "80-5a48fe0c9953e"\r\n
\r\n
[HTTP response 3/3]
[Time since request: 0.137563000 seconds]
[Prev request in frame: 29]
[Prev response in frame: 30]
[Request in frame: 34]
[Request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>]

ВІДПОВІДІ НА ПИТАННЯ 8-11

8) У першому запиті заголовок IF-MODIFIED-SINCE відсутній.

9) Так, повернув html:

<html>\n

Congratulations. You've downloaded the file \n

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

</html>\n

10) Так, є. Значення 3-го GET запиту для If-Modified-Since співпадає зі значенням 1-го response Last-Modified: Fri, 01 May 2020 05:59:02 GMT.

11) У третю відповідь сервер не вертав уже файл. Він повернув код 304, який відповідає статусу, що файл не був змінений. Таким чином спрацював механізм кешування в браузері. Оскільки сторінка не була змінена з часу останнього завантаження, то не було потреби додатково навантажувати мережу і заново її передавати.

lab_2(3).pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

No.	Time	Source	Destination	Protocol	Length	Info
35	3.814420	192.168.1.5	99.86.245.71	HTTP	612	GET /photographs/1080-tall/time-100-influential-photos-albert...
222	3.933666	99.86.245.71	192.168.1.5	HTTP	104	HTTP/1.1 200 OK (JPEG JFIF image)
225	3.983171	192.168.1.5	99.86.245.71	HTTP	555	GET /favicon.ico HTTP/1.1
257	4.128879	99.86.245.71	192.168.1.5	HTTP/X...	71	HTTP/1.1 403 Forbidden

> Frame 222: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{DA808D97-276E-43B7-99F5-2E540C9C4376}, id 0

> Ethernet II, Src: Tp-LinkT_81:c9:ee (c0:25:e9:81:c9:ee), Dst: LiteonTe_00:d6:0a (58:00:e3:00:d6:0a)

> Internet Protocol Version 4, Src: 99.86.245.71, Dst: 192.168.1.5

> Transmission Control Protocol, Src Port: 80, Dst Port: 27139, Seq: 182915, Ack: 547, Len: 38

> [128 Reassembled TCP Segments (182952 bytes): #38(466), #39(1448), #40(1448), #41(1448), #42(1448), #43(1448), #45(1448), #46(1448), #47(1448), #49(

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

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

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Content-Type: image/jpeg\r\n

> Content-Length: 182486\r\n

Connection: keep-alive\r\n

Date: Fri, 01 May 2020 10:27:07 GMT\r\n

Last-Modified: Fri, 18 Sep 2015 00:58:10 GMT\r\n

ETag: "cce4df7d8d27234217d6e54b8fbc2207"\r\n

Accept-Ranges: bytes\r\n

Server: AmazonS3\r\n

X-Cache: Hit from cloudfront\r\n

Via: 1.1 93f2a781416975f99355acc4c81d60d2.cloudfront.net (CloudFront)\r\n

X-Amz-Cf-Pop: VIE50-C1\r\n

X-Amz-Cf-Id: 0hWJD_3BPVFzo8iHQYr001Eny6pChwMwq0ZhCnJfMjgHYQP1DE14jw==\r\n

Age: 18510\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.119246000 seconds]

Hypertext Transfer Protocol (1st request)

GET /photographs/1080-tall/time-100-influential-photos-alberto-korda-guerillero-heroico-48.jpg HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /photographs/1080-tall/time-100-influential-photos-alberto-korda-guerillero-heroico-48.jpg HTTP/1.1\r\n]

[GET /photographs/1080-tall/time-100-influential-photos-alberto-korda-guerillero-heroico-48.jpg HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /photographs/1080-tall/time-100-influential-photos-alberto-korda-guerillero-heroico-48.jpg

Request Version: HTTP/1.1

Host: dujye7n3e5wj1.cloudfront.net\r\n

Connection: keep-alive\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/81.0.4044.129 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\r\n\r\n
[Full request URI:
http://dujye7n3e5wj1.cloudfront.net/photographs/1080-tall/time-100-
influential-photos-alberto-korda-guerillero-heroico-48.jpg]
[HTTP request 1/2]
[Response in frame: 222]
[Next request in frame: 225]

Hypertext Transfer Protocol (1st response)

HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Content-Type: image/jpeg\r\n
Content-Length: 182486\r\n
Connection: keep-alive\r\n
Date: Fri, 01 May 2020 10:27:07 GMT\r\n
Last-Modified: Fri, 18 Sep 2015 00:58:10 GMT\r\n
ETag: "cce4df7d8d27234217d6e54b8fbc2207"\r\n
Accept-Ranges: bytes\r\n
Server: AmazonS3\r\n
X-Cache: Hit from cloudfront\r\n
Via: 1.1 93f2a781416975f99355acc4c81d60d2.cloudfront.net
(CloudFront)\r\n
X-Amz-Cf-Pop: VIE50-C1\r\n
X-Amz-Cf-Id:
OWWJD_3BPVFzo8iHQYr001Eny6pChwMwq0ZhCnJfMjqHYQP1DEl4jw==\r\n
Age: 18510\r\n\r\n
[HTTP response 1/2]
[Time since request: 0.119246000 seconds]
[Request in frame: 35]
[Next request in frame: 225]
[Next response in frame: 257]
[Request URI: http://dujye7n3e5wj1.cloudfront.net/favicon.ico]
File Data: 182486 bytes

ВІДПОВІДІ НА ПИТАННЯ 12-15

- 12) Було 2 GET запити.
- 13) Для доставки малюнка необхідно було 128 TCP пакети (41 Reassembled TCP Segments)
- 14) Code: 200, Description: OK.
- 15) Так, зустрічалися у першому файлі, якщо клікнути по ньому ПКМ і вибрати «Показати Байти Пакета». Скріншот наводиться:

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with packet 222 selected. The middle pane shows the details of packet 222, which is an HTTP 200 OK response for a JPEG image. The bottom pane shows the raw bytes of the packet, which are the reassembled TCP segments.

No.	Time	Source	Destination	Protocol	Length	Info
35	3.814420	192.168.1.5	99.86.245.71	HTTP	612	GET /photographs/1080-tall/time-100-influential-photos-albert...
222	3.933666	99.86.245.71	192.168.1.5	HTTP	104	HTTP/1.1 200 OK (JPEG JFIF image)
225	3.983171	192.168.1.5	99.86.245.71	HTTP	555	GET /favicon.ico HTTP/1.1
257	4.128879	99.86.245.71	192.168.1.5	HTTP/X...	71	HTTP/1.1 403 Forbidden

Frame 222: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{DA808D97-276E-43B7-99F5-2E540C9C4376}, id 0
Ethernet II, Src: Tp-LinkT_81:c9:ee (c0:25:e9:81:c9:ee), Dst: LiteonTe_00:d6:0a (58:00:e3:00:d6:0a)
Internet Protocol Version 4, Src: 99.86.245.71, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 27139, Seq: 182915, Ack: 547, Len: 38
128 Reassembled TCP Segments (182952 bytes): #38(466), #39(1448), #40(1448), #41(1448), #42(1448), #43(1448), #45(1448), #46(1448), #47(1448), #49(1448), #50(1448), #51(1448), #52(1448), #53(1448), #54(1448), #55(1448), #56(1448), #57(1448), #58(1448), #59(1448), #60(1448), #61(1448), #62(1448), #63(1448), #64(1448), #65(1448), #66(1448), #67(1448), #68(1448), #69(1448), #70(1448), #71(1448), #72(1448), #73(1448), #74(1448), #75(1448), #76(1448), #77(1448), #78(1448), #79(1448), #80(1448), #81(1448), #82(1448), #83(1448), #84(1448), #85(1448), #86(1448), #87(1448), #88(1448), #89(1448), #90(1448), #91(1448), #92(1448), #93(1448), #94(1448), #95(1448), #96(1448), #97(1448), #98(1448), #99(1448), #100(1448), #101(1448), #102(1448), #103(1448), #104(1448), #105(1448), #106(1448), #107(1448), #108(1448), #109(1448), #110(1448), #111(1448), #112(1448), #113(1448), #114(1448), #115(1448), #116(1448), #117(1448), #118(1448), #119(1448), #120(1448), #121(1448), #122(1448), #123(1448), #124(1448), #125(1448), #126(1448), #127(1448), #128(1448)

Wireshark · Reassembled TCP Segments (tcp.segments) · lab_2(3).pcapng

HTTP/1.1 200 OK
Content-Type: image/jpeg
Content-Length: 182486
Connection: keep-alive
Date: Fri, 01 May 2020 10:27:07 GMT
Last-Modified: Fri, 18 Sep 2015 00:58:10 GMT
ETag: "cce4df7d8d27234217d6e54b8fbc2207"
Accept-Ranges: bytes
Server: AmazonS3
X-Cache: Hit from cloudfront
Via: 1.1 93f2a781416975f99355acc4c81d60d2.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: VIE50-C1
X-Amz-Cf-Id: OWMJD_3BPVfZo8iHQYr001Eny6pChwMmq0ZhCnJfMjqHYQP1DE14jw==
Age: 18510

.... .Exif II*DuckyAPhotoshop 3.0 8BIM.%
....
.....
.....8.H.....
.....!..1.AQ".aq.....2....B..R#.b...r3....C\$U.....4%Esc.DT.....
...&...A.4...e..?h.../...Z;L ..O../... c..7}'l..@..}..@.?:.....G...4...=.4. i.G5...@...r
3@...>.a.....?.....qxt.x0

ВІДПОВІДІ НА ПИТАННЯ 16-17

- 16) Усього було 3 GET запити, один на завантаження HTML сторінки і два на завантаження малюнків. Цільова адреса серверу 128.119.245.12, моя адреса – 192.168.1.5 .
- 17) Ресурси були отримані паралельно. Про це вказує часова послідовність запитів, де спочатку йдуть два GET запити на завантаження малюнків і аж потім ідуть запити-відповіді сервера.

lab_2(4).pcapng

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь



http

No.	Time	Source	Destination	Protocol	Length	Info
56	2.823454	192.168.1.5	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
61	2.947832	128.119.245.12	192.168.1.5	HTTP	1139	HTTP/1.1 200 OK (text/html)
62	2.963631	192.168.1.5	128.119.245.12	HTTP	484	GET /pearson.png HTTP/1.1
66	3.088288	192.168.1.5	128.119.245.12	HTTP	498	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
69	3.092095	128.119.245.12	192.168.1.5	HTTP	781	HTTP/1.1 200 OK (PNG)
151	3.502686	128.119.245.12	192.168.1.5	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

> Frame 56: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{DA808D97-276E-43B7-99F5-2E540C9C4376}, id 0

> Ethernet II, Src: LiteonTe_00:d6:0a (58:00:e3:00:d6:0a), Dst: Tp-LinkT_81:c9:ee (c0:25:e9:81:c9:ee)

> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 26587, Dst Port: 80, Seq: 1, Ack: 1, Len: 486

▼ Hypertext Transfer Protocol

 > GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n

 > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]

 Request Method: GET

 Request URI: /wireshark-labs/HTTP-wireshark-file4.html

 Request Version: HTTP/1.1

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

Connection: keep-alive\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/81.0.4044.129 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\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]

[HTTP request 1/3]

[Response in frame: 61]

[Next request in frame: 62]