

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

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №2
З дисципліни «Комп'ютерні мережі»

Виконала: студент 3-го курсу

гр. КА-77

Щедров М.О

Прийняв: Кухарев С.О

Київ 2020р.

No.	Time	Source	Destination	Protocol	Length	Info
55	5.047391	192.168.1.145	128.119.245.12	HTTP	536	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 55: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0 Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76) Internet Protocol Version 4, Src: 192.168.1.145, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 61614, Dst Port: 80, Seq: 1, Ack: 1, Len: 482 Hypertext Transfer Protocol						
98	5.182345	128.119.245.12	192.168.1.145	HTTP	540	HTTP/1.1 200 OK (text/html)
Frame 98: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0 Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.145 Transmission Control Protocol, Src Port: 80, Dst Port: 61614, Seq: 1, Ack: 483, Len: 486 Hypertext Transfer Protocol Line-based text data: text/html (4 lines)						
143	6.455126	192.168.1.145	128.119.245.12	HTTP	468	GET /favicon.ico HTTP/1.1
Frame 143: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0 Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76) Internet Protocol Version 4, Src: 192.168.1.145, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 61614, Dst Port: 80, Seq: 483, Ack: 487, Len: 414 Hypertext Transfer Protocol						
158	6.587569	128.119.245.12	192.168.1.145	HTTP	538	HTTP/1.1 404 Not Found (text/html)
Frame 158: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0 Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.145 Transmission Control Protocol, Src Port: 80, Dst Port: 61614, Seq: 487, Ack: 897, Len: 484 Hypertext Transfer Protocol Line-based text data: text/html (7 lines)						

Відповіді на контрольні запитання:

1. Яку версію протоколу HTTP використовує ваш браузер (1.0 чи 1.1)? **GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1**
Яку версію протоколу використовує сервер? **HTTP/1.1 200 OK**
2. Які мови (якщо вказано) браузер може прийняти від сервера? **Українська, американська англійська, а також будь-яка англійська та російська en-US,en;q=0.9,uk;q=0.8,ru;q=0.7**
3. Які IP-адреси вашого комп'ютера та цільового веб-сервера? **Адреса комп'ютера 192.168.1.145 цільова адреса веб-сервера 128.119.245.12**
4. Який статусний код сервер повернув у відповіді вашому браузеру? **200**
5. Коли на сервері в останній раз був модифікований файл, який запитується браузером? **Last-Modified: Tue, 11 Feb 2020 06:59:01 GMT**
6. Скільки байт контенту повертається сервером? **128 (Content-Length: 128)**
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.

No.	Time	Source	Destination	Protocol	Length	Info
12	3.489283	192.168.1.145	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 12: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0
 Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76)
 Internet Protocol Version 4, Src: 192.168.1.145, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 61765, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
 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
 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/80.0.3987.87 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,uk;q=0.8,ru;q=0.7\r\n
 If-None-Match: "80-59e4764024400"\r\n
 If-Modified-Since: Tue, 11 Feb 2020 06:59:01 GMT\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 [HTTP request 1/1]
 [Response in frame: 14]

No.	Time	Source	Destination	Protocol	Length	Info
14	3.620196	128.119.245.12	192.168.1.145	HTTP	293	HTTP/1.1 304 Not Modified

Frame 14: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0
 Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.145
 Transmission Control Protocol, Src Port: 80, Dst Port: 61765, Seq: 1, Ack: 594, Len: 239
 Hypertext Transfer Protocol
 HTTP/1.1 304 Not Modified\r\n
 Date: Tue, 11 Feb 2020 18:29:03 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: "80-59e4764024400"\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.130913000 seconds]
 [Request in frame: 12]
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

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?

If-Modified-Since: Tue, 11 Feb 2020 06:59:01 GMT\r\n

11. Який код та опис статусу другої відповіді сервера? Чи повернув сервер вміст файлу безпосередньо у відповіді? **304 Not Modified, ні**

```

No.      Time      Source      Destination      Protocol Length Info
  42 0.823284    192.168.1.145    104.28.24.14    HTTP      577      GET /r/i-guess.gif HTTP/1.1
Frame 42: 577 bytes on wire (4616 bits), 577 bytes captured (4616 bits) on interface \Device\NPF_{B7786215-
CC48-4D6B-89E8-7474D09ACEE0}, id 0
Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76)
Internet Protocol Version 4, Src: 192.168.1.145, Dst: 104.28.24.14
Transmission Control Protocol, Src Port: 50522, Dst Port: 80, Seq: 1, Ack: 1, Len: 523
Hypertext Transfer Protocol
No.      Time      Source      Destination      Protocol Length Info
 2244 2.609133    104.28.24.14    192.168.1.145    HTTP      120      HTTP/1.1 200 OK (GIF89a)
Frame 2244: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface \Device\NPF_{B7786215-
CC48-4D6B-89E8-7474D09ACEE0}, id 0
Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee)
Internet Protocol Version 4, Src: 104.28.24.14, Dst: 192.168.1.145
Transmission Control Protocol, Src Port: 80, Dst Port: 50522, Seq: 2076121, Ack: 524, Len: 66
[1425 Reassembled TCP Segments (2076186 bytes): #47(1460), #48(1460), #50(1460), #51(1460), #53(1460), #54(1460), #56(1460),
#57(1460), #59(1460), #60(1460), #63(1460), #64(1460), #66(1460), #67(1460), #69(1460), #70(1460), #72(1460), #73(1)]
Hypertext Transfer Protocol
Compuserve GIF, Version: GIF89a
No.      Time      Source      Destination      Protocol Length Info
 2264 2.863785    192.168.1.145    104.28.24.14    HTTP      552      GET /favicon.ico HTTP/1.1
Frame 2264: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{B7786215-
CC48-4D6B-89E8-7474D09ACEE0}, id 0
Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76)
Internet Protocol Version 4, Src: 192.168.1.145, Dst: 104.28.24.14
Transmission Control Protocol, Src Port: 50522, Dst Port: 80, Seq: 524, Ack: 2076187, Len: 498
Hypertext Transfer Protocol
No.      Time      Source      Destination      Protocol Length Info
 2273 3.172658    104.28.24.14    192.168.1.145    HTTP      393      HTTP/1.1 200 OK
Frame 2273: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface \Device\NPF_{B7786215-
CC48-4D6B-89E8-7474D09ACEE0}, id 0
Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee)
Internet Protocol Version 4, Src: 104.28.24.14, Dst: 192.168.1.145
Transmission Control Protocol, Src Port: 80, Dst Port: 50522, Seq: 2076187, Ack: 1022, Len: 339
Hypertext Transfer Protocol

```

12. Скільки повідомлень HTTP GET було відправлено вашим браузером? 2

13. Скільки пакетів TCP було необхідно для доставки одної відповіді HTTP-сервера? 2

14. Який код та опис статусу був у відповіді сервера? **200 OK (GIF89a) / 200 OK**

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

No. Info	Time	Source	Destination	Protocol	Length
	123 11.615824	192.168.1.145	128.119.245.12	HTTP	562
GET /wireshark-labs/HTTP-wireshark-file4.html					

HTTP/1.1

Frame 123: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{B7786215-

CC48-4D6B-89E8-7474D09ACEE0}, id 0

Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76)

Internet Protocol Version 4, Src: 192.168.1.145, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50573, Dst Port: 80, Seq: 1, Ack: 1, Len: 508

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

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/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,uk;q=0.8,ru;q=0.7\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: 127]

[Next request in frame: 128]

No.	Time	Source	Destination	Protocol	Length	Info
127	11.743612	128.119.245.12	192.168.1.145	HTTP	1127	HTTP/1.1 200 OK

Frame 127: 1127 bytes on wire (9016 bits), 1127 bytes captured (9016 bits) on interface \Device\NPF{CC48-4D6B-89E8-7474D09ACEE0}, id 0

Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.145

Transmission Control Protocol, Src Port: 80, Dst Port: 50573, Seq: 1, Ack: 509, Len: 1073

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 11 Feb 2020 21:08:10 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, 11 Feb 2020 06:59:01 GMT\r\n

ETag: "2ca-59e4764023078"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 714\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: 0.127788000 seconds]

[Request in frame: 123]

[Next request in frame: 128]

[Next response in frame: 135]

[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)

No.	Time	Source	Destination	Protocol	Length	Info
128	11.777911	192.168.1.145	128.119.245.12	HTTP	468	GET /pearson

Frame 128: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface \Device\NPF_{CC48-4D6B-89E8-7474D09ACEE0}, id 0

Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76)

Internet Protocol Version 4, Src: 192.168.1.145, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50573, Dst Port: 80, Seq: 509, Ack: 1074, Len: 414

Hypertext Transfer Protocol

GET /pearson.png HTTP/1.1\r\n

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

Connection: keep-alive\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/537.36\r\n

Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n

Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n

Accept-Encoding: gzip, deflate\r\n

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

\r\n

[Full request URI: http://gaia.cs.umass.edu/pearson.png]

[HTTP request 2/2]

[Prev request in frame: 123]

[Response in frame: 135]

No.	Time	Source	Destination	Protocol	Length	Info
135	11.916305	128.119.245.12	192.168.1.145	HTTP	745	HTTP/1.1 200

Frame 135: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0

Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.145

Transmission Control Protocol, Src Port: 80, Dst Port: 50573, Seq: 3994, Ack: 923, Len: 691

[3 Reassembled TCP Segments
(3611 bytes): #130(1460),
#133(1460), #135(691)] Hypertext
Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 11 Feb 2020 21:08:10 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, 06 Aug 2016 10:08:14 GMT\r\n

D:\Навчання\KM\lab2_damp_4.pcapng 278 total packets, 6 shown

Accept-Ranges: bytes\r\n

Content-Length: 3267\r\n

Keep-Alive: timeout=5, max=99\r\n

Connection: Keep-Alive\r\n

Content-Type: image/png\r\n

\r\n

[HTTP response 2/2]

[Time since request: 0.138394000 seconds]

[Prev request in frame: 123]

[Prev response in frame: 127]

[Request in frame: 128]

[Request URI: http://gaia.cs.umass.edu/pearson.png]

File Data: 3267 bytes

Portable Network Graphics

No.	Time	Source	Destination	Protocol	Length	Info
136	11.916488	192.168.1.145	128.119.245.12	HTTP	482	GET /~kurose

Frame 136: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface \Device\NPF_{CC48-4D6B-89E8-7474D09ACEE0}, id 0

Ethernet II, Src: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee), Dst: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76)

Internet Protocol Version 4, Src: 192.168.1.145, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50576, Dst Port: 80, Seq: 1, Ack: 1, Len: 428

Hypertext Transfer Protocol

GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n

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

Connection: keep-alive\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/537.36\r\n

Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n

Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n

Accept-Encoding: gzip, deflate\r\n

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

\r\n

[Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]

[HTTP request 1/1]

[Response in frame: 257]

No.	Time	Source	Destination	Protocol	Length	Info
257	12.478374	128.119.245.12	192.168.1.145	HTTP	632	HTTP/1.1 200

Frame 257: 632 bytes on wire (5056 bits), 632 bytes captured (5056 bits) on interface \Device\NPF_{B7786215-CC48-4D6B-89E8-7474D09ACEE0}, id 0

Ethernet II, Src: Tp-LinkT_f1:71:76 (f8:1a:67:f1:71:76), Dst: LiteonTe_f1:10:ee (74:df:bf:f1:10:ee)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.145

Transmission Control Protocol, Src Port: 80, Dst Port: 50576, Seq: 100741, Ack: 429, Len: 578

[70 Reassembled TCP Segments (101318 bytes): #139(1460), #140(1460), #142(1460), #143(1460), #145(1460), #146(1460), #148(1460), #149(1460), #151(1460),

#152(1460), #155(1460), #156(1460), #158(1460), #159(1460), #161(1460),
#162(1460), #16] Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 11 Feb 2020 21:08:11 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, 15 Sep 2009 18:23:27 GMT\r\n

ETag: "18a68-473a1e0e6e5c0"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 100968\r\n

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

Connection: Keep-Alive\r\n

Content-Type: image/jpeg\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.561886000 seconds]

[Request in frame: 136]

[Request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]

File Data: 100968 bytes

JPEG File Interchange Format

16. Скільки запитів HTTP GET було відправлено вашим браузером? Якими були
цільові IP-адреси запитів? **3, 192.168.1.145/ 128.119.245.12**

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

Висновки: Я ознайомився з середовищем Wireshark, його інтерфейсом та
оволоділа базовими методами перехоплення та аналізу пакетів, використовуваними
для дослідження мережевих протоколів а також зрозумів як саме передається
різноманітний контент.