

**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»**

**Виконала студентка 3 курсу
групи КА-71
Кічангіна О.Є.
Прийняв Кухарєв 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 – 1.1, сервер – 1.1.

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

Accept-Language: ru-RU\r\n

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

Internet Protocol Version 4, Src: 192.168.0.103, 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: Mon, 30 Mar 2020 05:59:03 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
1187	9.296384	192.168.0.103	128.119.245.12	HTTP	643	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 1187: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface en0, id 0
Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64327, Dst Port: 80, Seq: 1, Ack: 1, Len: 577
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_14_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.132 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

If-None-Match: "80-5a1f80826eccd"\r\n

If-Modified-Since: Sun, 29 Mar 2020 05:59:04 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: 1203]

No.	Time	Source	Destination	Protocol	Length	Info
1203	9.426893	128.119.245.12	192.168.0.103	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 1203: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103

Transmission Control Protocol, Src Port: 80, Dst Port: 64327, Seq: 1, Ack: 578, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Mon, 30 Mar 2020 19:18:59 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: Mon, 30 Mar 2020 05:59:03 GMT\r\n

ETag: "80-5a20c25eb0e37"\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 1/1]

[Time since request: 0.130509000 seconds]

[Request in frame: 1187]

[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)

8. Перевірте вміст першого запиту HTTP GET від вашого браузера до сервера. Чи є в ньому заголовок IF-MODIFIED-SINCE?

Відсутній.

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

Так, повернув.

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

Відсутній.

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, повернув

Запит:

No.	Time	Source	Destination	Protocol	Length	Info
776	5.782033	192.168.0.103	128.119.245.12	HTTP	558	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 776: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface en0, id 0
Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64575, Dst Port: 80, Seq: 1, Ack: 1, Len: 492

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_14_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.132 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 1/1]
[Response in frame: 813]

No.	Time	Source	Destination	Protocol	Length	Info
813	5.907593	128.119.245.12	192.168.0.103	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 813: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103
Transmission Control Protocol, Src Port: 80, Dst Port: 64575, Seq: 1, Ack: 493, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n
Date: Mon, 30 Mar 2020 19:34:40 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: Mon, 30 Mar 2020 05:59:03 GMT\r\n
ETag: "80-5a20c25eb0e37"\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 1/1]
[Time since request: 0.125560000 seconds]
[Request in frame: 776]
[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)

12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

Два повідомлення.

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

187

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

HTTP/1.1 200 OK (JPEG JFIF image)

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.

Запит:

No.	Time	Source	Destination	Protocol	Length	Info
3750	23.962515	192.168.0.103	92.53.114.59	HTTP	564	GET /_photos/gallery_160825/800x600/KV_letto_2016_22.jpg HTTP/1.1

Frame 3750: 564 bytes on wire (4512 bits), 564 bytes captured (4512 bits) on interface en0, id 0
Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 92.53.114.59

Transmission Control Protocol, Src Port: 64580, Dst Port: 80, Seq: 1, Ack: 1, Len: 498

Source Port: 64580

Destination Port: 80

[Stream index: 10]

[TCP Segment Len: 498]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 2975267245

[Next sequence number: 499 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 1955164005

1000 = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window size value: 2058

[Calculated window size: 131712]

[Window size scaling factor: 64]

Checksum: 0xa7d3 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

[Timestamps]

TCP payload (498 bytes)

Hypertext Transfer Protocol

GET /_photos/gallery_160825/800x600/KV_letto_2016_22.jpg HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /_photos/gallery_160825/800x600/KV_letto_2016_22.jpg HTTP/1.1\r\n]

Request Method: GET

Request URI: /_photos/gallery_160825/800x600/KV_letto_2016_22.jpg
Request Version: HTTP/1.1
Host: o-site.spb.ru\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 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://o-site.spb.ru/_photos/gallery_160825/800x600/KV_letto_2016_22.jpg]
[HTTP request 1/2]
[Response in frame: 4105]
[Next request in frame: 4109]

No.	Time	Source	Destination	Protocol	Length	Info
4105	24.211891	92.53.114.59	192.168.0.103	HTTP	1175	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 4105: 1175 bytes on wire (9400 bits), 1175 bytes captured (9400 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)

Internet Protocol Version 4, Src: 92.53.114.59, Dst: 192.168.0.103

Transmission Control Protocol, Src Port: 80, Dst Port: 64580, Seq: 269329, Ack: 499, Len: 1109

Source Port: 80

Destination Port: 64580

[Stream index: 10]

[TCP Segment Len: 1109]

Sequence number: 269329 (relative sequence number)

Sequence number (raw): 1955433333

[Next sequence number: 270438 (relative sequence number)]

Acknowledgment number: 499 (relative ack number)

Acknowledgment number (raw): 2975267743

1000 = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window size value: 253

[Calculated window size: 64768]

[Window size scaling factor: 256]

Checksum: 0xdbeb [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

[Timestamps]

TCP payload (1109 bytes)

TCP segment data (1109 bytes)

[187 Reassembled TCP Segments (270437 bytes): #3764(1448), #3765(1448), #3767(1448), #3768(1448), #3770(1448), #3771(1448), #3773(1448), #3774(1448), #3775(1448), #3778(1448), #3787(1448), #3789(1448), #3791(1448), #3792(1448), #3794(1448),]

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

Server: nginx/1.14.1\r\n

Date: Mon, 30 Mar 2020 19:38:51 GMT\r\n

Content-Type: image/jpeg\r\n

Content-Length: 270121\r\n

Last-Modified: Fri, 26 Aug 2016 10:35:24 GMT\r\n

Connection: keep-alive\r\n

ETag: "57c01b6c-41f29"\r\n

Expires: Thu, 30 Apr 2020 19:38:51 GMT\r\n

Cache-Control: max-age=2678400\r\n

Accept-Ranges: bytes\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.249376000 seconds]

[Request in frame: 3750]

[Next request in frame: 4109]

[Next response in frame: 4112]

[Request URI: http://o-site.spb.ru/_photos/gallery_160825/800x600/KV_letto_2016_22.jpg]

File Data: 270121 bytes

JPEG File Interchange Format

No.	Time	Source	Destination	Protocol	Length	Info
4109	24.241400	192.168.0.103	92.53.114.59	HTTP	492	GET /favicon.ico HTTP/1.1

Frame 4109: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0

Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 92.53.114.59

Transmission Control Protocol, Src Port: 64580, Dst Port: 80, Seq: 499, Ack: 270438, Len: 426

Source Port: 64580

Destination Port: 80

[Stream index: 10]

[TCP Segment Len: 426]

Sequence number: 499 (relative sequence number)

Sequence number (raw): 2975267743

[Next sequence number: 925 (relative sequence number)]

Acknowledgment number: 270438 (relative ack number)

Acknowledgment number (raw): 1955434442

1000 = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window size value: 2048
[Calculated window size: 131072]
[Window size scaling factor: 64]
Checksum: 0xf066 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[Timestamps]
TCP payload (426 bytes)

Hypertext Transfer Protocol

GET /favicon.ico HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]

Request Method: GET

Request URI: /favicon.ico

Request Version: HTTP/1.1

Host: o-site.spb.ru\r\n

Connection: keep-alive\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/80.0.3987.132 Safari/537.36\r\n

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

Referer: http://o-site.spb.ru/_photos/gallery_160825/800x600/KV_letto_2016_22.jpg\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://o-site.spb.ru/favicon.ico]

[HTTP request 2/2]

[Prev request in frame: 3750]

[Response in frame: 4112]

No.	Time	Source	Destination	Protocol	Length	Info
4112	24.276994	92.53.114.59	192.168.0.103	HTTP	1309	HTTP/1.1 200 OK (image/x-icon)

Frame 4112: 1309 bytes on wire (10472 bits), 1309 bytes captured (10472 bits) on interface en0, id 0

Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)

Internet Protocol Version 4, Src: 92.53.114.59, Dst: 192.168.0.103

Transmission Control Protocol, Src Port: 80, Dst Port: 64580, Seq: 270438, Ack: 925, Len: 1243

Source Port: 80

Destination Port: 64580

[Stream index: 10]

[TCP Segment Len: 1243]

Sequence number: 270438 (relative sequence number)

Sequence number (raw): 1955434442

[Next sequence number: 271681 (relative sequence number)]

Acknowledgment number: 925 (relative ack number)

Acknowledgment number (raw): 2975268169

1000 = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window size value: 252
 [Calculated window size: 64512]
 [Window size scaling factor: 256]
 Checksum: 0xe848 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 [SEQ/ACK analysis]
 [Timestamps]
 TCP payload (1243 bytes)
 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
 Server: nginx/1.14.1\r\n
 Date: Mon, 30 Mar 2020 19:38:51 GMT\r\n
 Content-Type: image/x-icon\r\n
 Content-Length: 894\r\n
 Connection: keep-alive\r\n
 Last-Modified: Sat, 19 May 2012 20:21:10 GMT\r\n
 ETag: "37e-4c06968d91980"\r\n
 Accept-Ranges: bytes\r\n
 Cache-Control: max-age=0, no-store, no-cache, must-revalidate\r\n
 Expires: Mon, 30 Mar 2020 19:38:51 GMT\r\n
 \r\n
 [HTTP response 2/2]
 [Time since request: 0.035594000 seconds]
 [Prev request in frame: 3750]
 [Prev response in frame: 4105]
 [Request in frame: 4109]
 [Request URI: http://o-site.spb.ru/favicon.ico]
 File Data: 894 bytes
 Media Type

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

3

No.	Time	Source	Destination	Protocol	Length	Info
2026	11.062920	192.168.0.103	128.119.245.12	HTTP	558	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
No.	Time	Source	Destination	Protocol	Length	Info
2098	11.238321	192.168.0.103	128.119.245.12	HTTP	490	GET /pearson.png HTTP/1.1

No.	Time	Source	Destination	Protocol	Length	Info
2201	11.669600	192.168.0.103	128.119.245.12	HTTP	504	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

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

Яким чином?

Паралельно.

Висновки:

В цій лабораторній роботі я продовжила досліджувати протокол HTTP за допомогою середовища захоплення та аналізу пакетів протоколів Wireshark. Більш детально були досліджені старотовий рядок запиту та відповіді та деякі HTTP заголовки, а саме Accept-Language, Last-Modified, Content-Length, If-Modified-Since та ін. Було виявлено, що якщо сайт містить багато ресурсів, то всі вони отримуються послідовно; що для великих за розміром ресурсів може знадобитись велика кількість TCP пакетів для доставки відповіді сервера, і що в цих пакетах міститься також стрічки з кодом та описом статусу відповіді та заголовки HTTP.