

HTTP

Task1 by Vladimir Mikulin

Остортировано по фильтру: http.

1)Запрос для получения веб-странички протоколом HTTP:
Из какого адреса был запрос на какой(Source-Destination).

No.	Time	Source	Destination	Protocol	Length	Info
291	8.493599129	93.184.220.29	192.168.116.174	OCSP	853	Response
293	8.493624032	93.184.220.29	192.168.116.174	OCSP	854	Response
331	9.397192567	192.168.116.174	128.119.245.12	HTTP	452	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
346	9.770410329	128.119.245.12	192.168.116.174	HTTP	1139	HTTP/1.1 200 OK (text/html)
349	9.826975656	192.168.116.174	128.119.245.12	HTTP	420	GET /pearson.png HTTP/1.1
355	10.026160789	192.168.116.174	128.119.245.12	HTTP	344	GET /favicon.ico HTTP/1.1
369	10.335276409	128.119.245.12	192.168.116.174	HTTP	782	HTTP/1.1 200 OK (PNG)
382	10.452570289	128.119.245.12	192.168.116.174	HTTP	551	HTTP/1.1 404 Not Found (text/html)
396	10.770010275	192.168.116.174	128.119.245.12	HTTP	434	GET /-kurose/cover_5th_ed.jpg HTTP/1.1
456	11.549391310	192.168.116.174	93.184.220.29	OCSP	466	Request
478	11.654279936	192.168.116.174	93.184.220.29	OCSP	466	Request
518	11.855214739	93.184.220.29	192.168.116.174	OCSP	853	Response
530	11.879722086	93.184.220.29	192.168.116.174	OCSP	853	Response
605	12.056636654	128.119.245.12	192.168.116.174	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 331: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits) on interface 0

Ethernet II, Src: IntelCor_86:bb:22 (44:03:2c:86:bb:22), Dst: AsustekC_67:19:61 (00:18:f3:67:19:61)

Internet Protocol Version 4, Src: 192.168.116.174, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 40524, Dst Port: 80, Seq: 1, Ack: 1, Len: 386

Hypertext Transfer Protocol

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

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

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

\r\n

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

[HTTP request 1/1]

[Response in frame: 346]

Из Header line: *GET wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1*

- GET-запрос
- Используется версия HTTP — 1.1

Из Header key: мы видим что:

- соединение постоянное и не закрытыми,что позволяет выполнять последующие запросы на один и тот же сервер (Connection: keep-alive);
- сервер понимает русский,английский языки (Accept - Language);
- клиент готов принять и понять такие MIME типы,например html, xml(Accept);

Транспортный и сетевой уровни модели OSI(всего из 7): скрин ниже (IPv4)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
291	8.493599129	93.184.220.29	192.168.116.174	OCSP	853	Response
293	8.493624032	93.184.220.29	192.168.116.174	OCSP	854	Response
331	9.397192567	192.168.116.174	128.119.245.12	HTTP	452	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
346	9.770410329	128.119.245.12	192.168.116.174	HTTP	1139	HTTP/1.1 200 OK (text/html)
349	9.826975656	192.168.116.174	128.119.245.12	HTTP	420	GET /pearson.png HTTP/1.1
355	10.026160789	192.168.116.174	128.119.245.12	HTTP	344	GET /favicon.ico HTTP/1.1
369	10.335276409	128.119.245.12	192.168.116.174	HTTP	782	HTTP/1.1 200 OK (PNG)
382	10.452570289	128.119.245.12	192.168.116.174	HTTP	551	HTTP/1.1 404 Not Found (text/html)
396	10.770010275	192.168.116.174	128.119.245.12	HTTP	434	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
456	11.549391310	192.168.116.174	93.184.220.29	OCSP	466	Request
478	11.654279936	192.168.116.174	93.184.220.29	OCSP	466	Request
518	11.855214739	93.184.220.29	192.168.116.174	OCSP	853	Response
530	11.879722086	93.184.220.29	192.168.116.174	OCSP	853	Response
605	12.056636654	128.119.245.12	192.168.116.174	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

▶ Frame 331: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits) on interface 0

▶ Ethernet II, Src: IntelCor_86:bb:22 (44:03:2c:86:bb:22), Dst: AsustekC_67:19:61 (00:18:f3:67:19:61)

▼ Internet Protocol Version 4, Src: 192.168.116.174, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 438

Identification: 0xd35f (54111)

▶ Flags: 0x4000, Don't fragment

Time to live: 64

Protocol: TCP (6)

Header checksum: 0xbb07 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.116.174

Destination: 128.119.245.12

▼ Transmission Control Protocol, Src Port: 40524, Dst Port: 80, Seq: 1, Ack: 1, Len: 386

Source Port: 40524

Destination Port: 80

[Stream index: 23]

[TCP Segment Len: 386]

Sequence number: 1 (relative sequence number)

[Next sequence number: 387 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

1000 = Header Length: 32 bytes (8)

▶ Flags: 0x018 (PSH, ACK)

Window size value: 502

[Calculated window size: 64256]

[Window size scaling factor: 128]

Checksum: 0x8141 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

2) Ответ на get-запрос получения страницы:

http						
No.	Time	Source	Destination	Protocol	Length	Info
291	8.493599129	93.184.220.29	192.168.116.174	OCSP	853	Response
293	8.493624032	93.184.220.29	192.168.116.174	OCSP	854	Response
331	9.397192567	192.168.116.174	128.119.245.12	HTTP	452	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
346	9.770410329	128.119.245.12	192.168.116.174	HTTP	1139	HTTP/1.1 200 OK (text/html)
349	9.826975656	192.168.116.174	128.119.245.12	HTTP	420	GET /pearson.png HTTP/1.1
355	10.026160789	192.168.116.174	128.119.245.12	HTTP	344	GET /favicon.ico HTTP/1.1
369	10.335276409	128.119.245.12	192.168.116.174	HTTP	782	HTTP/1.1 200 OK (PNG)
382	10.452570289	128.119.245.12	192.168.116.174	HTTP	551	HTTP/1.1 404 Not Found (text/html)
396	10.770010275	192.168.116.174	128.119.245.12	HTTP	434	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
456	11.549391310	192.168.116.174	93.184.220.29	OCSP	466	Request
478	11.654279936	192.168.116.174	93.184.220.29	OCSP	466	Request
518	11.855214739	93.184.220.29	192.168.116.174	OCSP	853	Response
530	11.879722086	93.184.220.29	192.168.116.174	OCSP	853	Response
605	12.056636654	128.119.245.12	192.168.116.174	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

▶	Frame 346: 1139 bytes on wire (9112 bits), 1139 bytes captured (9112 bits) on interface 0
▶	Ethernet II, Src: AsustekC_67:19:61 (00:18:f3:67:19:61), Dst: IntelCor_86:bb:22 (44:03:2c:86:bb:22)
▶	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.116.174
▶	Transmission Control Protocol, Src Port: 80, Dst Port: 40524, Seq: 1, Ack: 387, Len: 1073
▼	Hypertext Transfer Protocol
▶	HTTP/1.1 200 OK\r\n
	Date: Thu, 07 Nov 2019 18:14:44 GMT\r\n
	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
	Last-Modified: Thu, 07 Nov 2019 06:59:01 GMT\r\n
	Etag: "2ca-596bc33423538"\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 1/1]
	[Time since request: 0.373217762 seconds]
	[Request in frame: 331]
	[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

0040	47 bc	48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f	6-HTTP/1.1 200 0
------	-------	---	------------------

Header line: HTTP/1.1 200 OK

- Response
- Код 200 OK — успех

из **Header key**: мы видим что:

- дату и дата последнего изменения на страничке(Date, Last-modified);
- Etag — он позволяет отправлять серверу не весь ответ , если содержимое не изменилось после кеширования.
- Также, в самом низу мы видим , что сервер прислал нам HTML

3) На нашей веб-страничке также была картинка, по-этому мы использовали еще один GET-запрос на ее получение.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
291	8.493599129	93.184.220.29	192.168.116.174	OCSP	853	Response
293	8.493624032	93.184.220.29	192.168.116.174	OCSP	854	Response
331	9.397192567	192.168.116.174	128.119.245.12	HTTP	452	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
346	9.770410329	128.119.245.12	192.168.116.174	HTTP	1139	HTTP/1.1 200 OK (text/html)
349	9.826975656	192.168.116.174	128.119.245.12	HTTP	420	GET /pearson.png HTTP/1.1
355	10.026160789	192.168.116.174	128.119.245.12	HTTP	344	GET /favicon.ico HTTP/1.1
369	10.335276409	128.119.245.12	192.168.116.174	HTTP	782	HTTP/1.1 200 OK (PNG)
382	10.452570289	128.119.245.12	192.168.116.174	HTTP	551	HTTP/1.1 404 Not Found (text/html)
396	10.770010275	192.168.116.174	128.119.245.12	HTTP	434	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
456	11.549391310	192.168.116.174	93.184.220.29	OCSP	466	Request
478	11.654279936	192.168.116.174	93.184.220.29	OCSP	466	Request
518	11.855214739	93.184.220.29	192.168.116.174	OCSP	853	Response
530	11.879722086	93.184.220.29	192.168.116.174	OCSP	853	Response
605	12.056636654	128.119.245.12	192.168.116.174	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

▶ Frame 396: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface 0
 ▶ Ethernet II, Src: IntelCor_86:bb:22 (44:03:2c:86:bb:22), Dst: AsustekC_67:19:61 (00:18:f3:67:19:61)
 ▶ Internet Protocol Version 4, Src: 192.168.116.174, Dst: 128.119.245.12
 ▶ Transmission Control Protocol, Src Port: 40536, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
 ▶ Hypertext Transfer Protocol

▾ GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n
 ▶ [Expert Info (Chat/Sequence): GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n]

Request Method: GET

Request URI: /~kurose/cover_5th_ed.jpg

Request Version: HTTP/1.1

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

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0\r\n

Accept: image/webp,*/*\r\n

Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

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

\r\n

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

[HTTP request 1/1]

[Response in frame: 605]

4) Response , на Get-запрос получения картинки. Картинка успешно отобразилась на веб-странице.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
291	8.493599129	93.184.220.29	192.168.116.174	OCSP	853	Response
293	8.493624032	93.184.220.29	192.168.116.174	OCSP	854	Response
331	9.397192567	192.168.116.174	128.119.245.12	HTTP	452	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
346	9.770410329	128.119.245.12	192.168.116.174	HTTP	1139	HTTP/1.1 200 OK (text/html)
349	9.826975656	192.168.116.174	128.119.245.12	HTTP	420	GET /pearson.png HTTP/1.1
355	10.026160789	192.168.116.174	128.119.245.12	HTTP	344	GET /favicon.ico HTTP/1.1
369	10.335276409	128.119.245.12	192.168.116.174	HTTP	782	HTTP/1.1 200 OK (PNG)
382	10.452570289	128.119.245.12	192.168.116.174	HTTP	551	HTTP/1.1 404 Not Found (text/html)
396	10.770010275	192.168.116.174	128.119.245.12	HTTP	434	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
456	11.549391310	192.168.116.174	93.184.220.29	OCSP	466	Request
478	11.654279936	192.168.116.174	93.184.220.29	OCSP	466	Request
518	11.855214739	93.184.220.29	192.168.116.174	OCSP	853	Response
530	11.879722086	93.184.220.29	192.168.116.174	OCSP	853	Response
605	12.056636654	128.119.245.12	192.168.116.174	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

▶ Frame 605: 1472 bytes on wire (11776 bits), 1472 bytes captured (11776 bits) on interface 0

▶ Ethernet II, Src: AsustekC.67:19:61 (00:18:f3:67:19:61), Dst: IntelCor_86:bb:22 (44:03:2c:86:bb:22)

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.116.174

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 40536, Seq: 99913, Ack: 369, Len: 1406

▶ [63 Reassembled TCP Segments (101318 bytes): #425(2896), #427(1448), #429(1448), #431(1448), #433(1448), #435(1448), #437(1448), #439(2896),

▼ **Hypertext Transfer Protocol**

▶ HTTP/1.1 200 OK\r\n

Date: Thu, 07 Nov 2019 18:14:45 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 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: 1.286626379 seconds]

[Request in frame: 396]

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

File Data: 100968 bytes

▼ **JPEG File Interchange Format**

Marker: Start of Image (0xffd8)

▶ Marker segment: Reserved for application segments - 0 (0xFFE0)

▶ Marker segment: Reserved for application segments - 1 (0xFFE1)

▶ Marker segment: Reserved for application segments - 13 (0xFFED)

▶ Marker segment: Reserved for application segments - 1 (0xFFE1)

▶ Marker segment: Reserved for application segments - 2 (0xFFE2)

▶ Marker segment: Reserved for application segments - 14 (0xFFEE)