

- 1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.**

- 2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)**

- 3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?**

- 4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.**

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

2. What languages (if any) does your browser indicate that it can accept to the server?

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

4. What is the status code returned from the server to your browser?

5. When was the HTML file that you are retrieving last modified at the server?

6. How many bytes of content are being returned to your browser?

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

IF-MODIFIED-SINCE در http get نیست

46	43.443174	192.168.39.196	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
50	43.676054	128.119.245.12	192.168.39.196	HTTP	784	HTTP/1.1 200 OK (text/html)
59	43.737994	192.168.39.196	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
75	43.945974	128.119.245.12	192.168.39.196	HTTP	539	HTTP/1.1 404 Not Found (text/html)
112	70.177261	192.168.39.196	23.58.222.83	HTTP	244	GET /titles/nvidiatech.html HTTP/1.1
178	72.836885	192.168.39.196	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
186	71.829858	128.119.245.12	192.168.39.196	HTTP	294	HTTP/1.1 304 Not Modified

Transmission Control Protocol, Src Port: 62618, Dst Port: 80, Seq: 1, Ack: 1, Len: 380

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Host: gaia.cs.umass.edu

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Upgrade-Insecure-Requests: 1

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

[HTTP request 1/1]

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

بله-سرور به وضوح محتویات فایل را نشان می دهد. و ایرشارک یک بخش line-based text data نشان می دهد سرور چه چیز را به مرورگر بر می گرداند.

Transmission Control Protocol, Src Port: 62618, Dst Port: 80, Seq: 1, Ack: 1, Len: 380						
Hypertext Transfer Protocol						
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1						
Host: gaia.cs.umass.edu						
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8						
Accept-Language: en-US,en;q=0.5						
Accept-Encoding: gzip, deflate						
Connection: keep-alive						
Upgrade-Insecure-Requests: 1						
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]						
[HTTP request 1/1]						

No.	Time	Source	Destination	Protocol	Length	Info
46	43.443174	192.168.39.196	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
50	43.656944	128.119.245.12	192.168.39.196	HTTP	784	HTTP/1.1 200 OK (text/html)
59	43.737994	192.168.39.196	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
75	43.945971	128.119.245.12	192.168.39.196	HTTP	539	HTTP/1.1 404 Not Found (text/html)
112	70.177261	192.168.39.196	23.58.222.83	HTTP	244	GET /titles/nvidiatech HTTP/1.1
178	72.838885	192.168.39.196	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
186	73.829858	128.119.245.12	192.168.39.196	HTTP	294	HTTP/1.1 304 Not Modified

>	Transmission Control Protocol, Src Port: 80, Dst Port: 62618, Seq: 1, Ack: 390, Len: 730
▼	Hypertext Transfer Protocol
>	HTTP/1.1 200 OK\r\n
	Date: Fri, 12 Nov 2021 15:03:48 GMT\r\n
	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
	Last-Modified: Fri, 12 Nov 2021 06:59:01 GMT\r\n
	ETag: "173-5d891f6799b0"\r\n
	Accept-Ranges: bytes\r\n
>	Content-Length: 573\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

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

بله IF-MODIFIED-SINCE هست. تاریخ و آخرین دسترسی ما را به وبسایت نشان می دهد.

46	43.443174	192.168.39.196	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
50	43.656944	128.119.245.12	192.168.39.196	HTTP	784	HTTP/1.1 200 OK (text/html)
59	43.737994	192.168.39.196	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
75	43.945971	128.119.245.12	192.168.39.196	HTTP	539	HTTP/1.1 404 Not Found (text/html)
112	70.177261	192.168.39.196	23.58.222.83	HTTP	244	GET /titles/nvidiatech HTTP/1.1
178	72.838885	192.168.39.196	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
186	73.829858	128.119.245.12	192.168.39.196	HTTP	294	HTTP/1.1 304 Not Modified

>	Transmission Control Protocol, Src Port: 62626, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
▼	Hypertext Transfer Protocol
>	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
	Host: gata.cs.umass.edu\r\n
	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
	Accept-Language: en-US;q=0.5\r\n
	Accept-Encoding: gzip, deflate\r\n
	Connection: keep-alive\r\n
	Upgrade-Insecure-Requests: 1\r\n
	If-Modified-Since: Fri, 12 Nov 2021 06:59:01 GMT\r\n
	If-None-Match: "173-5d891f6799b0"\r\n
	Cache-Control: max-age=0\r\n

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

کد: 304 not modified

سرور محتویات فایل را برنمی گرداند. چون محتویات فایل را از کش خودش بازیابی کرده است. آخرین باری که به فایل modified since پیدا کرده بود، محتویات فایل را نشان می دهد.

46	43.443174	192.168.39.196	128.119.245.12	HTTP	443 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
50	43.656044	128.119.245.12	192.168.39.196	HTTP	784 HTTP/1.1 200 OK (text/html)
59	43.737964	192.168.39.196	128.119.245.12	HTTP	460 GET /favicon.ico HTTP/1.1
75	43.945971	128.119.245.12	192.168.39.196	HTTP	539 HTTP/1.1 404 Not Found (text/html)
112	70.177261	192.168.39.196	23.58.222.83	HTTP	244 GET /titles/avidiatech HTTP/1.1
178	72.838889	192.168.39.196	128.119.245.12	HTTP	555 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
186	73.825858	128.119.245.12	192.168.39.196	HTTP	294 HTTP/1.1 304 Not Modified

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 62626, Seq: 1, Ack: 582, Len: 240
< Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 12 Nov 2021 15:04:05 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 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: "173-5d891fe799b6b"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.190973000 seconds]
    [Request in frame: 178]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and filtering. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. Packet 24 is selected, showing it as an HTTP GET request from 192.168.154.101 to 192.168.154.131.
- Packet Details:** Displays the structure of the selected packet. It shows the Ethernet II frame, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The HTTP status is 200 OK.
- Packet Bytes:** Shows the raw data of the packet in hexadecimal and ASCII.

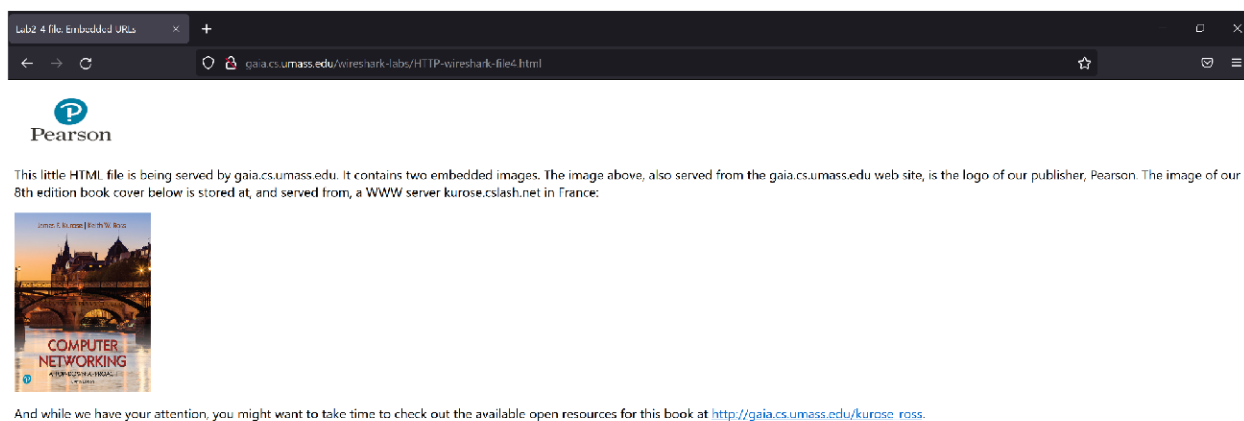
The selected packet (24) is a GET request for the file /favicon.ico. The response (200 OK) is shown in the details pane, indicating a successful retrieval of the favicon.

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

مرورگر 4 تا پیام درخواست http get ارسال کرده است.

15	6.101860	192.168.43.137	128.119.245.12	HTTP	443 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
21	6.382145	128.119.245.12	192.168.43.137	HTTP	1355 HTTP/1.1 200 OK (text/html)
24	6.368935	192.168.43.137	128.119.245.12	HTTP	400 GET /pearson.png HTTP/1.1
38	6.565647	192.168.43.137	128.119.245.12	HTTP	400 GET /favicon.ico HTTP/1.1
41	6.592139	192.168.43.137	178.79.137.164	HTTP	367 GET /8E_cover_small.jpg HTTP/1.1
52	6.680979	128.119.245.12	192.168.43.137	HTTP	866 HTTP/1.1 200 OK (PNG)
61	6.789565	178.79.137.164	192.168.43.137	HTTP	225 HTTP/1.1 301 Moved Permanently
68	6.765895	128.119.245.12	192.168.43.137	HTTP	539 HTTP/1.1 404 Not Found (text/html)

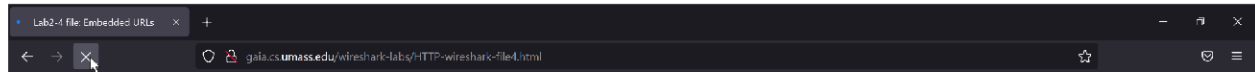
1. The initial page
2. Pearson logo
3. 8th-cover-small
4. favicon



17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

به صورت سریال دانلود کرده است. چون تصویر اول قبل از درخواست تصویر دوم توسط مرورگر در خواست و ارسال شده است و تصویر دوم بعد از برگشت تصویر اول در خواست شده است.

اگر به صورت موازی بود هر دو هم زمان در خواست و نشان داده می شدند.



This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:

And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.



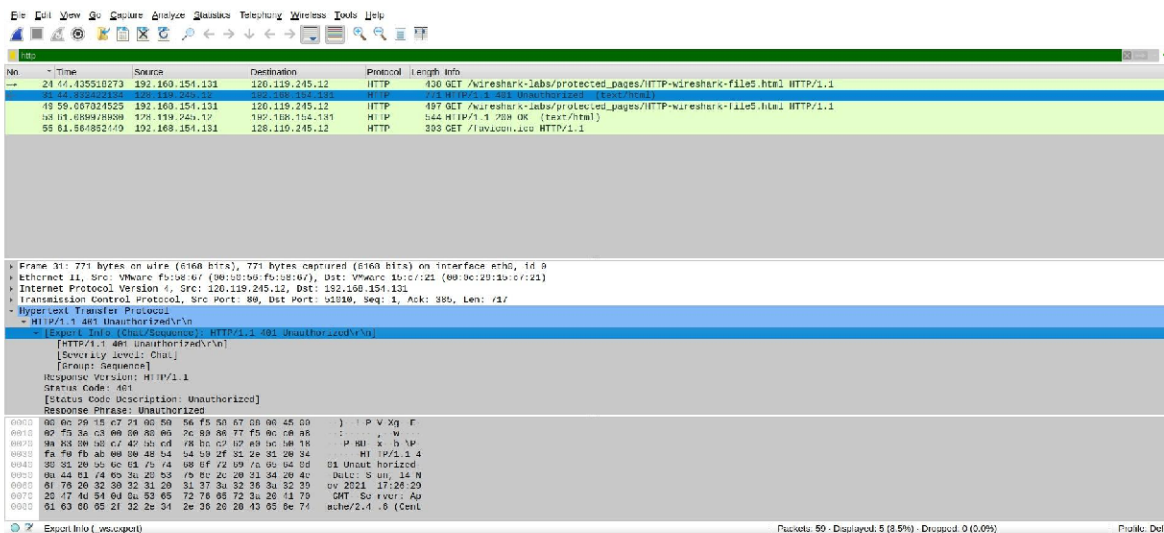
This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:



And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

HTTP/1.1 401 unauthorized



19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

wireshark-students:network

