

Lab: 3

Understanding Working of HTTP Headers

Question: Understand working of HTTP headers Conditional Get: If-Modified-Since

HTTP Cookies: Cookie and Set-Cookie

Authentication: Auth-Basic

Design a web page that has one embedded page (e.g. image) and sets a cookie and enables authentication. You are required to configure the web server (e.g. apache) with authentication mechanism. Show the behavior of conditional get when embedded objects are modified and when it is not (you can just change the create date of the embedded object). Decode the BasicAuth header using Base64 mechanism as per the password setup.

Observation: Show the behavior of browser when cookie is set and when cookie is removed.

Solution: Analyzing Basic Authentication and Cookies

The three parts of experiment are: 1. Password Authentication 2. Cookie Setting
3. Conditional get

Steps of Execution (for Password Authentication) 1. Executing the below commands on the terminal.

--> Provide username and password to set authentication

sudo htpasswd -c /etc/apache2/.htpasswd netwo

--> View the authentication

sudo cat /etc/apache2/.htpasswd

Here “netwo” is the username. Also, password is entered twice.

2. To setup the authentication phase, execute the following commands. Configuring Access control within the Virtual Host Definition.

--> Opening the file for setting authentication

sudo nano /etc/apache2/sites-available/000-default.conf

```
<VirtualHost *:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined <Directory "/var/www/html">
```

AuthType Basic

AuthName "RESTRICTED" AuthUserFile /etc/apache2/.htpasswd Require valid-user >

```
</Directory> </VirtualHost>
```

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html


    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    <Directory "/var/www/html">
        AuthType Basic
        AuthName "RESTRICTED"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user
    </Directory>
    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

3. Password policy implementation is done by restarting the server as:

sudo service apache2 restart

4. The localhost is then accessed using the Firefox browser requiring a username and a password set during the authentication phase.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*/available/`

5. Wireshark is used to capture the packets sent upon the network.

No.	Time	Source	Destination	Protocol	Length	Info
121	4.222614	127.0.0.1	127.0.0.1	TCP	76	58912 → 80 [Syn] Seq=6544555555 Len=0 MSS=65535 SACK_PERM=1 TSval=1275876481, TSecr=0
122	4.222616	127.0.0.1	127.0.0.1	TCP	76	80 → 58912 [Syn, ACK] Seq=6544555555 Len=0 MSS=65535 SACK_PERM=1 TSval=1275876481, TSecr=1275876481
123	4.222616	127.0.0.1	127.0.0.1	TCP	60	58912 → 80 [ACK] Seq=1 ACK=1 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
124	4.222617	127.0.0.1	127.0.0.1	HTTP	361	GET / HTTP/1.1
125	4.222617	127.0.0.1	127.0.0.1	TCP	60	80 → 58912 [ACK] Seq=1 ACK=6544555555 Len=0 MSS=65535 SACK_PERM=1 TSval=1275876481, TSecr=1275876481
126	4.222617	127.0.0.1	127.0.0.1	HTTP	768	HTTP/1.1 200 OK (text/html)
127	4.222618	127.0.0.1	127.0.0.1	TCP	60	58912 → 80 [ACK] Seq=1 ACK=128 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
128	7.212621	127.0.0.1	127.0.0.1	HTTP	344	GET / HTTP/1.1
129	7.212621	127.0.0.1	127.0.0.1	TCP	60	80 → 58912 [ACK] Seq=729 ACK=128 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
130	7.212621	127.0.0.1	127.0.0.1	HTTP	344	GET / HTTP/1.1
131	7.212621	127.0.0.1	127.0.0.1	TCP	60	58912 → 80 [ACK] Seq=729 ACK=128 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
132	7.212621	127.0.0.1	127.0.0.1	HTTP	344	GET / HTTP/1.1
133	7.212621	127.0.0.1	127.0.0.1	TCP	60	80 → 58912 [ACK] Seq=729 ACK=128 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
134	7.212621	127.0.0.1	127.0.0.1	HTTP	344	GET / HTTP/1.1
135	7.212621	127.0.0.1	127.0.0.1	TCP	60	80 → 58912 [ACK] Seq=729 ACK=128 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
136	7.212621	127.0.0.1	127.0.0.1	HTTP	344	GET / HTTP/1.1
137	7.212621	127.0.0.1	127.0.0.1	TCP	60	80 → 58912 [ACK] Seq=729 ACK=128 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
138	7.212621	127.0.0.1	127.0.0.1	HTTP	344	GET / HTTP/1.1
139	7.212621	127.0.0.1	127.0.0.1	TCP	60	80 → 58912 [ACK] Seq=729 ACK=128 Win=65535 Len=0 TSval=1275876481, TSecr=1275876481
140	7.212621	127.0.0.1	127.0.0.1	HTTP	344	GET / HTTP/1.1

Frame 130: 3541 bytes on wire (28328 bits), 3541 bytes captured (28328 bits) on interface any, 10 B

- Ethernet II, Src: Linux cooked capture
- Internet Protocol Version 4, Src: 127.0.0.1, Dest: 127.0.0.1
- Transmission Control Protocol, Src Port: 80, Dest Port: 58912, Seq: 729, Ack: 128, Len: 3473
- Hypertext Transfer Protocol

Line-based text data: text/html (373 lines)

6. Using the “follow TCP stream” on the HTTP message segment the password was retrieved which was encrypted by the base64 algorithm and decryption could be done with same algorithm.

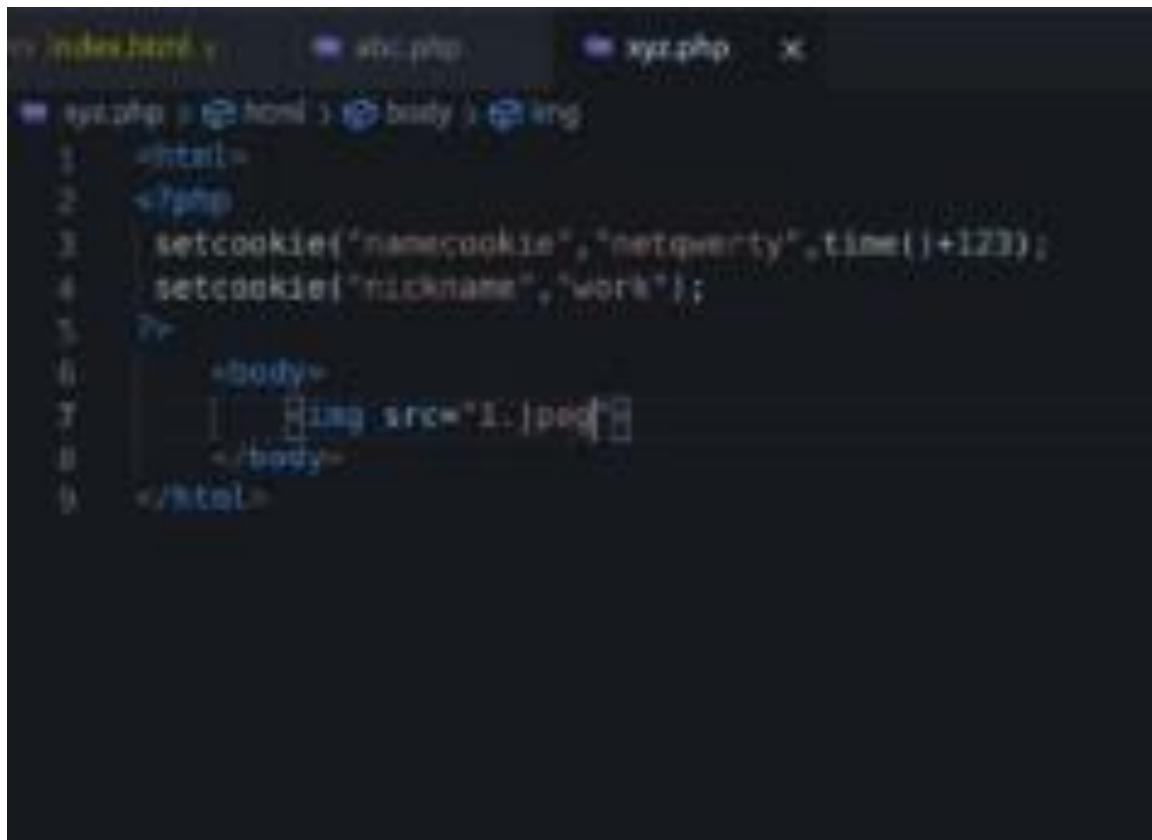
Steps of Execution (Cookie Setting)

1. A PHP file to set the cookie is created which also contains an image in it (placed under the HTML directory) to be accessed once the cookie is set. The following code helped to set the cookie:

```
<html> <?php
```

```
setcookie("namecookie","netqwerty",time()+123); setcookie("nickname","work"); ?>
```

```
<img src= “highres.png” width= “300” height= “300” title= “password” /> </html>
```



Note: The Image added is called **1.jpeg**

2. The combined file saved with a .php extension is placed under **/var/www/html** for accessing.



No.	Time	Source	Destination	Protocol	Length	Info
622	10.08652	127.0.0.1	127.0.0.53	DNS	362	Standard query query 20x20 A nav.smartscreen.microsoft.com OPT
623	10.08652	127.0.0.15	192.168.29.1	TCP	123	Standard query 20x20 A wd-prod-us-ss-south-east-1-fe.south-eastasia.cloudapp.a
624	10.08931	127.0.0.1	127.0.0.1	HTTP	806	GET /xyz.php HTTP/1.1
625	10.08934	127.0.0.1	127.0.0.1	TCP	60	80 -> 5782 [ACK] Seq=179 Min=6486 Len=0 TSval=2760826796 TSecr=2760
626	10.09048	127.0.0.1	127.0.0.1	HTTP	506	HTTP/1.1 200 OK (text/html)
627	10.09071	127.0.0.1	127.0.0.1	TCP	60	5782 -> 80 [ACK] Seq=1408 Min=6512 Len=0 TSval=2760826792 TSecr=276
628	10.09111	192.168.29.1	10.0.2.15	DNS	139	Standard query response 20x20 A wd-prod-us-ss-south-east-1-fe.south-eastasia.c
629	10.09117	127.0.0.1	127.0.0.1	TCP	233	Standard query response 20x20 A nav.smartscreen.microsoft.com CHAME wd-prod-
630	10.09566	192.168.2.15	40.90.184.82	TCP	76	80722 -> 443 [SVN] Seq=1 Acl=1 Len=0 Min=6553 Len=0 TSval=2760825222
631	10.11216	192.168.2.15	204.79.197.209	TLV1.2	173	Application data
632	10.11222	192.168.2.15	204.79.197.209	TLV1.2	779	Application data
633	10.11261	204.79.197.209	10.0.2.15	TCP	62	443 -> 4438 [ACK] Seq=135899 Acl=1000 Min=6553 Len=0
634	10.11261	204.79.197.209	10.0.2.15	TCP	62	443 -> 4438 [ACK] Seq=135899 Acl=1719 Min=6553 Len=0
635	10.13388	10.0.2.15	10.0.2.15	TCP	297	443 -> 5782 [ACK] Seq=1 Acl=518 Min=6553 Len=7939 [TCP segment of a reassemb
636	10.13991	10.0.2.15	20.197.71.89	TCP	50	52752 -> 443 [ACK] Seq=518 Acl=2921 Min=6770 Len=0
637	10.14027	20.197.71.89	10.0.2.15	TLV1.2	2801	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server He
638	10.14098	10.0.2.15	20.197.71.89	TCP	60	5782 -> 443 [ACK] Seq=1 Acl=5666 Min=6770 Len=0
639	10.14367	10.0.2.1	127.0.0.1	TCP	806	GET /dragon-ball-super-new-super-hero-movie-goku-tte-animation/1276900.webp
640	10.14468	127.0.0.1	127.0.0.1	TCP	60	5782 -> 5782 [ACK] Seq=1291 Acl=2146 Min=6486 Len=0 TSval=2760826845 TSecr=276
641	10.14566	127.0.0.1	127.0.0.1	HTTP	2794	HTTP/1.1 200 OK
642	10.14568	127.0.0.1	127.0.0.1	TCP	60	80 -> 5782 [FIN, ACK] Seq=29127 Acl=2146 Min=6553 Len=0 TSval=2760826847 TSecr=27
643	10.14568	127.0.0.1	127.0.0.1	TCP	60	5782 -> 80 [FIN, ACK] Seq=2146 Acl=29127 Min=6782 Len=0 TSval=2760826847 TSecr=27
644	10.14568	127.0.0.1	127.0.0.1	TCP	60	5782 -> 80 [FIN, ACK] Seq=2146 Acl=29128 Min=6553 Len=0 TSval=2760826849 TSecr=27
645	10.14966	127.0.0.1	127.0.0.1	TCP	60	80 -> 5782 [ACK] Seq=29128 Acl=2147 Min=6553 Len=0 TSval=2760826851 TSecr=27
646	10.15632	20.197.71.89	20.197.71.89	TLV1.2	214	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
647	10.15677	20.197.71.89	10.0.2.15	TCP	62	443 -> 5782 [ACK] Seq=5666 Acl=676 Min=6553 Len=0
648	10.16041	40.90.184.82	10.0.2.15	TCP	62	443 -> 80722 [SVN, ACK] Seq=1 Acl=1 Min=6553 Len=0 Min=1400
649	10.16446	10.0.2.15	40.90.184.82	TCP	60	80722 -> 443 [ACK] Seq=1 Acl=1 Acl=1 Len=0 Min=64240 Len=0
650	10.16446	10.0.2.15	40.90.184.82	TCP	60	80722 -> 443 [ACK] Seq=1 Acl=1 Acl=1 Len=0 Min=64240 Len=0

Frame 1: 1358 bytes on wire (10864 bits), 1358 bytes captured (10864 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 104.86.248.378, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 443, Dst Port: 43806, Seq: 1, Acl: 1, Len: 1382

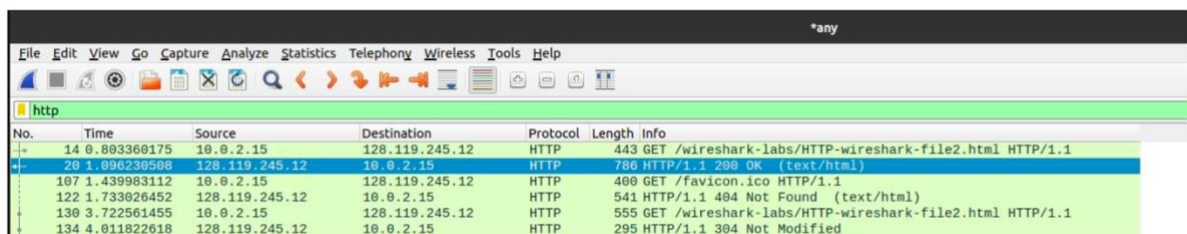
Transport Layer Security

[illegible]

The cookie is set as shown in the above screenshot.

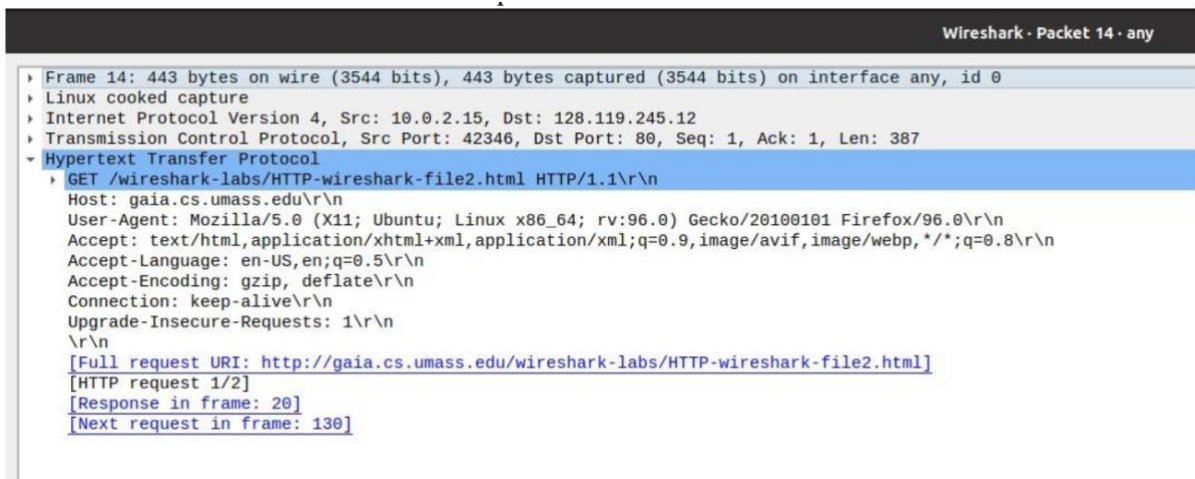
Observation: Understand and work out base 64 algorithm and write in your observation. Observe various parameters associated with Cookie in the wireshark capture. **Conditional Get: If-Modified-Since Observations:**

1. 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?
 2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
 3. 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?
 4. 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.
- Wireshark containing the HTTP REQUESTS AND RESPONSES



No.	Time	Source	Destination	Protocol	Length	Info
14	0.803360175	10.0.2.15	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
20	1.096230508	128.119.245.12	10.0.2.15	HTTP	786	HTTP/1.1 200 OK (text/html)
107	1.439983112	10.0.2.15	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
122	1.733026452	128.119.245.12	10.0.2.15	HTTP	541	HTTP/1.1 404 Not Found (text/html)
130	3.722561455	10.0.2.15	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
134	4.011822618	128.119.245.12	10.0.2.15	HTTP	295	HTTP/1.1 304 Not Modified

1. IF-MODIFIED-SINCE is not present in the first HTTP GET



2. The server explicitly returned the contents on the first HTTP RESPONSE

Line-Based text data is the content returned by the **server** on **first HTTP RESPONSE**

```
Wireshark - Packet 20 - any
+ Frame 20: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface any, id 0
+ Linux cooked capture
+ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
+ Transmission Control Protocol, Src Port: 80, Dst Port: 42346, Seq: 1, Ack: 388, Len: 730
+ Hypertext Transfer Protocol
  + HTTP/1.1 200 OK\r\n
    Date: Sun, 13 Feb 2022 09:03:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 13 Feb 2022 06:59:02 GMT\r\n
    ETag: "173-5d7e0d5c000cb"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\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: 0.292870333 seconds]
    [Request in frame: 14]
    [Next request in frame: 130]
    [Next response in frame: 134]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
  + Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change. <p>\n
    Thus if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

3. Yes. IF-MODIFIED-SINCE is present in the second HTTP GET

```
Wireshark - Packet 130
+ Frame 130: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface any, id 0
+ Linux cooked capture
+ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
+ Transmission Control Protocol, Src Port: 42346, Dst Port: 80, Seq: 388, Ack: 731, Len: 499
+ Hypertext Transfer Protocol
  + GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0\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,en;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: Sun, 13 Feb 2022 06:59:02 GMT\r\n
    If-None-Match: "173-5d7e0d5c000cb"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 14]
    [Response in frame: 134]
```

4. The HTTP status code for the second HTTP GET is **304**.

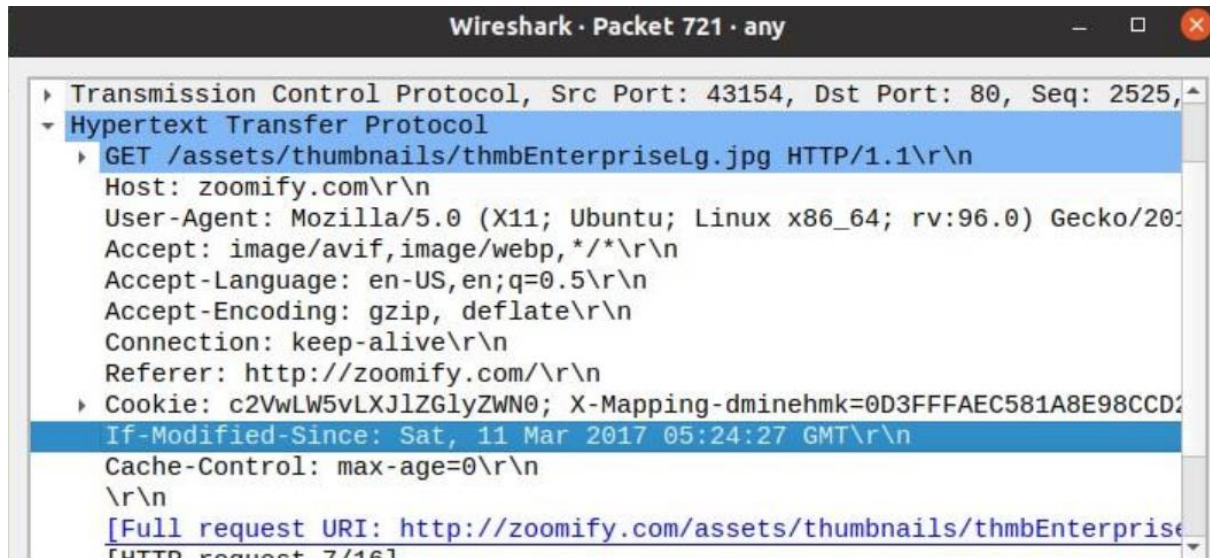
The Server does not return the file as they are already present from the time the first http get request was made. This time the contents are not modified.

```
Wireshark · Packet 134 · any
> Frame 134: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface any, id 0
> Linux cooked capture
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 42346, Seq: 731, Ack: 887, Len: 239
> Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 13 Feb 2022 09:03:59 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5d7e0d5c000cb"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.289261163 seconds]
    [Prev request in frame: 14]
    [Prev response in frame: 20]
    [Request in frame: 130]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

For a server with images (used the website www.zoomify.com)

No.	Time	Source	Destination	Protocol	Length	Info
172	4.715950801	10.0.2.15	98.129.229.158	HTTP	434	GET /ZV5/ZoomifyImageViewerExpress-min.js HTTP/1.1
177	4.721701850	98.129.229.158	10.0.2.15	HTTP	1039	HTTP/1.1 200 OK (application/x-javascript)
180	4.721702139	98.129.229.158	10.0.2.15	HTTP	945	HTTP/1.1 200 OK (application/x-javascript)
185	4.722773218	10.0.2.15	98.129.229.158	HTTP	458	GET /assets/logos/zoomify/v5Gold-isHere.jpg HTTP/1.1
187	4.725211301	10.0.2.15	98.129.229.158	HTTP	444	GET /assets/icons/circle3.gif HTTP/1.1
193	4.743240904	10.0.2.15	98.129.229.158	HTTP	458	GET /assets/thumbnails/thmbEnterpriseLg.jpg HTTP/1.1
194	4.743340732	10.0.2.15	98.129.229.158	HTTP	452	GET /assets/thumbnails/thmbFreeLg.jpg HTTP/1.1
205	4.948596554	98.129.229.158	10.0.2.15	HTTP	2085	HTTP/1.1 200 OK (JPEG JFIF image)
207	4.948783606	10.0.2.15	98.129.229.158	HTTP	486	GET /assets/dynamic/scripts.js?cb=1644745436431&fingerprint=c...
209	4.954276801	98.129.229.158	10.0.2.15	HTTP	1643	HTTP/1.1 200 OK (GIF89a)
211	4.954569568	10.0.2.15	98.129.229.158	HTTP	455	GET /assets/icons/checkmarkSmallBlue.gif HTTP/1.1
215	4.969083117	10.0.2.15	98.129.229.158	HTTP	455	GET /assets/thumbnails/thmbExpressLg.jpg HTTP/1.1
218	4.969853702	10.0.2.15	98.129.229.158	HTTP	451	GET /assets/thumbnails/thmbProLg.jpg HTTP/1.1
231	4.974536324	98.129.229.158	10.0.2.15	HTTP	3249	HTTP/1.1 200 OK (JPEG JFIF image)
233	4.974783718	10.0.2.15	98.129.229.158	HTTP	448	GET /assets/icons/flags/china.png HTTP/1.1
235	5.184532174	98.129.229.158	10.0.2.15	HTTP	2651	HTTP/1.1 200 OK (application/javascript)
237	5.184532632	98.129.229.158	10.0.2.15	HTTP	410	HTTP/1.1 200 OK (GIF89a)
239	5.185119668	10.0.2.15	98.129.229.158	HTTP	456	GET /assets/icons/flags/europeanUnion.png HTTP/1.1
240	5.185193592	10.0.2.15	98.129.229.158	HTTP	449	GET /assets/icons/flags/france.png HTTP/1.1
271	5.206431829	98.129.229.158	10.0.2.15	HTTP	1087	HTTP/1.1 200 OK (PNG)
273	5.206726069	10.0.2.15	98.129.229.158	HTTP	435	GET /assets/shim.gif HTTP/1.1
279	5.277259930	10.0.2.15	117.254.84.212	HTTP	467	GET /getjs?nadipdata=%7B%7D&screenheight=100&screenwidth=100&...
297	5.353219064	117.254.84.212	10.0.2.15	HTTP	5054	HTTP/1.1 200 OK (application/x-javascript)
299	5.411781172	98.129.229.158	10.0.2.15	HTTP	3905	HTTP/1.1 200 OK (PNG)

1. IF-MODIFIED-SINCE is not present in the first HTTP GET
2. The server returns the file explicitly.
3. Yes. IF-MODIFIED-SINCE is present in the second HTTP GET



4. The HTTP status code for the second HTTP GET is **304**.
The Server does not return the file as they are already present from the time the first http get request was made.

Non- Persistent

Activities | Wireshark
Feb 12 17:03

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

933 Bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface em03, id 0
*enp0s3

Filter
 No. Time Source Destination Protocol Length Info

No.	Time	Source	Destination	Protocol	Length	Info
93	0.020311	10.0.2.15	98.129.229.158	HTTP	309	GET / HTTP/1.1
94	0.037610	10.0.2.15	98.129.229.158	HTTP	339	GET /Assets/dynamic/scripts.js HTTP/1.1
95	0.060904	98.129.229.158	10.0.2.15	HTTP	2749	HTTP/1.1 200 OK (text/html)
96	0.083174	98.129.229.158	10.0.2.15	HTTP	2071	HTTP/1.1 200 OK (application/javascript)
97	0.100210	10.0.2.15	98.129.229.158	HTTP	410	GET /2v0/ZoomifyImageViewerExpress.min.js HTTP/1.1
98	0.106228	98.129.229.158	10.0.2.15	HTTP	12676	HTTP/1.1 200 OK (application/javascript)
99	0.106742	10.0.2.15	98.129.229.158	HTTP	411	GET /Assets/show.gif HTTP/1.1
100	0.150789	98.129.229.158	10.0.2.15	HTTP	310	HTTP/1.1 200 OK (GIF89a)
101	0.172184	10.0.2.15	98.129.229.158	HTTP	454	GET /Images/folders/MichaelVonAichbergerBudapest/ImageProperties.xml?11644605...
102	0.161050	98.129.229.158	10.0.2.15	HTTP/XML	384	HTTP/1.1 200 OK
103	0.163769	10.0.2.15	98.129.229.158	HTTP	475	GET /Assets/fonts/poppins-vi-latin-regular.woff2 HTTP/1.1
104	0.187345	98.129.229.158	10.0.2.15	HTTP	21607	HTTP/1.1 200 OK (font/woff2)
105	0.187434	10.0.2.15	98.129.229.158	HTTP	412	GET /2v0/Assets/Skins/default/skinFiles.xml HTTP/1.1
106	0.184224	98.129.229.158	10.0.2.15	HTTP/XML	11081	HTTP/1.1 200 OK
107	0.142762	10.0.2.15	98.129.229.158	HTTP	471	GET /Assets/fonts/poppins-vi-latin-300.woff2 HTTP/1.1
108	0.140979	98.129.229.158	10.0.2.15	HTTP	2187	HTTP/1.1 200 OK (font/woff2)
109	0.143120	10.0.2.15	98.129.229.158	HTTP	438	GET /Assets/logos/zoomify/zoomifylogo200x61.gif HTTP/1.1
110	0.153693	98.129.229.158	10.0.2.15	HTTP	2087	HTTP/1.1 200 OK (GIF89a)
111	0.153695	10.0.2.15	98.129.229.158	HTTP	434	GET /Assets/logos/zoomify/v500id-iswerr.jpg HTTP/1.1
112	0.160083	98.129.229.158	10.0.2.15	HTTP	9183	HTTP/1.1 200 OK (JPEG JFIF image)
113	0.167308	10.0.2.15	98.129.229.158	HTTP	420	GET /Assets/icons/circle1.gif HTTP/1.1
114	0.167308	10.0.2.15	98.129.229.158	HTTP	1578	HTTP/1.1 200 OK (GIF89a)
115	0.166371	10.0.2.15	98.129.229.158	HTTP	420	GET /Assets/icons/circle2.gif HTTP/1.1
116	0.166371	10.0.2.15	98.129.229.158	HTTP	1628	HTTP/1.1 200 OK (GIF89a)
117	0.166371	10.0.2.15	98.129.229.158	HTTP	420	GET /Assets/icons/circle3.gif HTTP/1.1
118	0.166371	10.0.2.15	98.129.229.158	HTTP	1641	HTTP/1.1 200 OK (GIF89a)
119	0.166371	10.0.2.15	98.129.229.158	HTTP	431	GET /Assets/thumbnails/thumbExpress.jpg HTTP/1.1
120	0.166371	10.0.2.15	98.129.229.158	HTTP	2426	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 93: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface em03, id 0

Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158

Transmission Control Protocol, Src Port: 50732, Dst Port: 80, Seq: 1, Ack: 1, Len: 343

Hypertext Transfer Protocol

933 Bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface em03, id 0
*enp0s3

Filter
 No. Time Source Destination Protocol Length Info

No.	Time	Source	Destination	Protocol	Length	Info
800	34.588904	10.0.2.15	98.129.229.158	HTTP	456	GET /2v0/Assets/Skins/default/standard/fullViewExitDown.png HTTP/1.1
801	34.640904	98.129.229.158	10.0.2.15	HTTP	2273	HTTP/1.1 200 OK (Png)
802	34.849609	10.0.2.15	98.129.229.158	HTTP	466	GET /Images/folders/MichaelVonAichbergerBudapest/TileGroup184/10-347-46.jpg H...
803	34.849609	98.129.229.158	10.0.2.15	HTTP	5458	HTTP/1.1 200 OK (Image/jpeg)
804	35.101137	10.0.2.15	98.129.229.158	HTTP	466	GET /Images/folders/MichaelVonAichbergerBudapest/TileGroup187/10-347-47.jpg H...
805	35.359985	98.129.229.158	10.0.2.15	HTTP	21889	HTTP/1.1 200 OK (Image/jpeg)

Max Number of persistent Connections 2

The image displays two screenshots of Wireshark, a network protocol analyzer. The top screenshot shows a list of captured packets, specifically HTTP requests, with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom screenshot provides a detailed view of a selected packet (Frame 5), showing its structure across multiple layers: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet details pane shows the raw data and the parsed structure of the packet, including the HTTP request line and headers.

No.	Time	Source	Destination	Protocol	Length	Info
50	0.259414	10.0.2.15	98.129.229.158	HTTP	395	GET / HTTP/1.1
17	0.542147	10.0.2.15	98.129.229.158	HTTP	399	GET /assets/dynamic/scripts.js HTTP/1.1
21	0.778952	98.129.229.158	10.0.2.15	HTTP	2749	HTTP/1.1 200 OK (text/html)
23	0.789054	10.0.2.15	98.129.229.158	HTTP	410	GET /ZVS/zoomifyImageViewerExpress-min.js HTTP/1.1
25	0.867744	98.129.229.158	10.0.2.15	HTTP	2671	HTTP/1.1 200 OK (application/javascript)
89	1.810385	98.129.229.158	10.0.2.15	HTTP	2458	HTTP/1.1 200 OK (application/javascript)
91	1.810562	10.0.2.15	98.129.229.158	HTTP	434	GET /assets/logos/zoomify/v5Gold-isHere.jpg HTTP/1.1
92	1.810556	10.0.2.15	98.129.229.158	HTTP	429	GET /assets/icons/circle1.gif HTTP/1.1
93	1.060531	98.129.229.158	10.0.2.15	HTTP	1579	HTTP/1.1 200 OK (GIF89a)
97	2.065791	10.0.2.15	98.129.229.158	HTTP	454	GET /images/folders/MichaelVonaAichbergerBudapest/ImageProperties.xml?1644665 HTTP/1.1
101	2.073931	98.129.229.158	10.0.2.15	HTTP	4883	HTTP/1.1 200 OK (JPEG JFIF image)
103	2.074100	10.0.2.15	98.129.229.158	HTTP	475	GET /assets/fonts/poppins-v1-latin-regular.woff2 HTTP/1.1
105	2.329076	98.129.229.158	10.0.2.15	HTTP/XML	384	HTTP/1.1 200 OK
106	2.329375	10.0.2.15	98.129.229.158	HTTP	471	GET /assets/fonts/poppins-v1-latin-300.woff2 HTTP/1.1
112	2.343134	98.129.229.158	10.0.2.15	HTTP	2167	HTTP/1.1 200 OK (font/woff2)
114	2.343372	10.0.2.15	98.129.229.158	HTTP	411	GET /assets/shis.gif HTTP/1.1
116	2.502338	98.129.229.158	10.0.2.15	HTTP	13867	HTTP/1.1 200 OK (font/woff2)
118	2.502788	10.0.2.15	98.129.229.158	HTTP	412	GET /ZVS/Assets/Skins/Default/skinFiles.xml HTTP/1.1
120	2.607418	98.129.229.158	10.0.2.15	HTTP	310	HTTP/1.1 200 OK (GIF89a)
122	2.607671	10.0.2.15	98.129.229.158	HTTP	438	GET /assets/logos/zoomify/zoomifyLogo200x61.gif HTTP/1.1
124	2.606712	98.129.229.158	10.0.2.15	HTTP/XML	2241	HTTP/1.1 200 OK
128	2.857035	10.0.2.15	98.129.229.158	HTTP	420	GET /assets/icons/circle2.gif HTTP/1.1
130	2.872190	98.129.229.158	10.0.2.15	HTTP	2087	HTTP/1.1 200 OK (GIF89a)
132	2.872091	10.0.2.15	98.129.229.158	HTTP	429	GET /assets/icons/circle3.gif HTTP/1.1
134	3.117891	98.129.229.158	10.0.2.15	HTTP	1628	HTTP/1.1 200 OK (GIF89a)
136	3.118277	10.0.2.15	98.129.229.158	HTTP	431	GET /assets/thumbnails/thumbExpresslg.jpg HTTP/1.1
138	3.135102	98.129.229.158	10.0.2.15	HTTP	1641	HTTP/1.1 200 OK (GIF89a)
140	3.135434	10.0.2.15	98.129.229.158	HTTP	427	GET /assets/thumbnails/thumbProlog.jpg HTTP/1.1

Frame 5: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface empo3s, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50742, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

Frame 5: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface empo3s, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50742, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

$$20.238-0.2594=19.9786$$

Max Number of persistent Connections 4

No.	Time	Source	Destination	Protocol	Length	Info
5	0.057283	10.0.2.15	10.129.229.158	HTTP	395	GET / HTTP/1.1
11	0.351090	10.0.2.15	10.129.229.158	HTTP	399	[TCP Previous segment not captured] GET /assets/dynamic/scripts.js HTTP/1.1
13	0.352755	10.0.2.15	10.129.229.158	HTTP	410	[TCP Previous segment not captured] GET /ZVS/zoomifyImageViewerExpress-610.js
17	0.586056	10.129.229.158	10.0.2.15	HTTP	2749	HTTP/1.1 200 OK (text/html)
23	0.628814	10.129.229.158	10.0.2.15	HTTP	2671	HTTP/1.1 200 OK (application/javascript)
64	1.685214	10.129.229.158	10.0.2.15	HTTP	6188	HTTP/1.1 200 OK (application/javascript)
66	1.685678	10.0.2.15	10.129.229.158	HTTP	411	GET /assets/shiv.gif HTTP/1.1
68	1.685983	10.0.2.15	10.129.229.158	HTTP	438	GET /assets/logos/zoomify/zoomifylogo280x61.gif HTTP/1.1
69	1.686174	10.0.2.15	10.129.229.158	HTTP	427	GET /assets/thumbnails/thumbProfp.jpg HTTP/1.1
73	1.943465	10.129.229.158	10.0.2.15	HTTP	310	HTTP/1.1 200 OK (GIF89a)
74	1.943710	10.0.2.15	10.129.229.158	HTTP	454	GET /images/folders/MichaelvonAichbergerBudapest/ImageProperties.xml?1644665..
79	1.952176	10.0.2.15	10.129.229.158	HTTP	431	GET /assets/thumbnails/thumbExpressd.jpg HTTP/1.1
81	1.953904	10.129.229.158	10.0.2.15	HTTP	36027	HTTP/1.1 200 OK (JPEG JFIF image)
83	1.954194	10.0.2.15	10.129.229.158	HTTP	479	GET /assets/fonts/poppins-v1-latin-regular.woff2 HTTP/1.1
85	1.955338	10.129.229.158	10.0.2.15	HTTP	2087	HTTP/1.1 200 OK (GIF89a)
87	1.955620	10.0.2.15	10.129.229.158	HTTP	471	GET /assets/fonts/poppins-v1-latin-300.woff2 HTTP/1.1
89	2.209079	10.129.229.158	10.0.2.15	HTTP/XML	384	HTTP/1.1 200 OK
90	2.209334	10.0.2.15	10.129.229.158	HTTP	434	GET /assets/logos/zoomify/v5Gold-isHere.jpg HTTP/1.1
104	2.224636	10.129.229.158	10.0.2.15	HTTP	2167	HTTP/1.1 200 OK (font/woff2)
106	2.224973	10.0.2.15	10.129.229.158	HTTP	420	GET /assets/icons/circles.gif HTTP/1.1
110	2.229804	10.129.229.158	10.0.2.15	HTTP	2187	HTTP/1.1 200 OK (font/woff2)
112	2.229889	10.0.2.15	10.129.229.158	HTTP	420	GET /assets/icons/circles2.gif HTTP/1.1
114	2.261488	10.0.2.15	10.129.229.158	HTTP	460	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup0/0-0-0.jpg HTTP/1.1
116	2.472445	10.129.229.158	10.0.2.15	HTTP	9183	HTTP/1.1 200 OK (JPEG JFIF image)
122	2.479790	10.129.229.158	10.0.2.15	HTTP	3086	HTTP/1.1 200 OK (JPEG JFIF image)
124	2.480142	10.0.2.15	10.129.229.158	HTTP	412	GET /ZVS/Assets/Skins/Default/skinFiles.xml HTTP/1.1
126	2.480610	10.129.229.158	10.0.2.15	HTTP	1578	HTTP/1.1 200 OK (GIF89a)
128	2.495599	10.0.2.15	10.129.229.158	HTTP	420	GET /assets/icons/circles.gif HTTP/1.1

Frame 5: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface emp0s3, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.129.229.158
Transmission Control Protocol, Src Port: 50750, Dst Port: 80, Seq: 1, Len: 341
Hypertext Transfer Protocol

Packets: 758 - Displayed: 266 (35.1%) - Dropped: 0 (0.0%)

No.	Time	Source	Destination	Protocol	Length	Info
655	9.548024	10.129.229.158	10.0.2.15	HTTP	15068	HTTP/1.1 200 OK (Image/jpeg)
657	9.548958	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup184/10-334-46.jpg M..
659	9.602735	10.129.229.158	10.0.2.15	HTTP	12548	HTTP/1.1 200 OK (Image/jpeg)
661	9.603120	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup187/10-334-47.jpg M..
665	9.607906	10.129.229.158	10.0.2.15	HTTP	4808	HTTP/1.1 200 OK (Image/jpeg)
667	9.608190	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup184/10-346-46.jpg M..
671	9.784248	10.129.229.158	10.0.2.15	HTTP	1947	HTTP/1.1 200 OK (Image/jpeg)
673	9.784388	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup187/10-346-47.jpg M..
675	9.789918	10.129.229.158	10.0.2.15	HTTP	15776	HTTP/1.1 200 OK (Image/jpeg)
677	9.800299	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup182/10-334-45.jpg M..
681	9.947533	10.129.229.158	10.0.2.15	HTTP	4857	HTTP/1.1 200 OK (Image/jpeg)
683	9.947938	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup190/10-334-48.jpg M..
687	9.964685	10.129.229.158	10.0.2.15	HTTP	6018	HTTP/1.1 200 OK (Image/jpeg)
689	9.964377	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup182/10-346-45.jpg M..
692	10.05276	10.129.229.158	10.0.2.15	HTTP	5296	HTTP/1.1 200 OK (Image/jpeg)
694	10.05320	10.0.2.15	10.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup190/10-346-48.jpg M..
700	10.05944	10.129.229.158	10.0.2.15	HTTP	3884	HTTP/1.1 200 OK (Image/jpeg)
702	10.05962	10.0.2.15	10.129.229.158	HTTP	448	GET /ZVS/Assets/Skins/Default/standard/fullViewExitUp.png HTTP/1.1
706	10.21070	10.129.229.158	10.0.2.15	HTTP	2433	HTTP/1.1 200 OK (Image/jpeg)
708	10.21092	10.0.2.15	10.129.229.158	HTTP	450	GET /ZVS/Assets/Skins/Default/standard/fullViewExitOver.png HTTP/1.1
710	10.23044	10.129.229.158	10.0.2.15	HTTP	17971	HTTP/1.1 200 OK (Image/jpeg)
712	10.23103	10.0.2.15	10.129.229.158	HTTP	450	GET /ZVS/Assets/Skins/Default/standard/fullViewExitDown.png HTTP/1.1
714	10.31810	10.129.229.158	10.0.2.15	HTTP	2421	HTTP/1.1 200 OK (PNG)
716	10.31988	10.129.229.158	10.0.2.15	HTTP	15024	HTTP/1.1 200 OK (Image/jpeg)
718	10.47387	10.129.229.158	10.0.2.15	HTTP	2248	HTTP/1.1 200 OK (PNG)
720	10.49811	10.129.229.158	10.0.2.15	HTTP	2273	HTTP/1.1 200 OK (PNG)
722	10.50180	10.0.2.15	10.129.229.158	HTTP	407	GET /favicon.ico HTTP/1.1
724	10.76079	10.129.229.158	10.0.2.15	HTTP	2544	HTTP/1.1 200 OK (Image/vnd.microsoft.icon)

Frame 5: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface emp0s3, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.129.229.158
Transmission Control Protocol, Src Port: 50750, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

Packets: 758 - Displayed: 266 (35.1%) - Dropped: 0 (0.0%)

$$10.762-0.057=10.705$$

Max Number of persistent Connections 6

Feb 12 17:27
*enp0s3

No.	Time	Source	Destination	Protocol	Length	Info
50	0.263985	10.0.2.15	98.129.229.158	HTTP	399	GET / HTTP/1.1
19	0.556321	10.0.2.15	98.129.229.158	HTTP	399	GET /assets/dynamic/scripts.js HTTP/1.1
27	0.759690	98.129.229.158	10.0.2.15	HTTP	2749	HTTP/1.1 200 OK (text/html)
30	0.824781	98.129.229.158	10.0.2.15	HTTP	2671	HTTP/1.1 200 OK (application/javascript)
36	0.825645	10.0.2.15	98.129.229.158	HTTP	419	GET /ZVS/zoomifyImageViewerExpress-min.js HTTP/1.1
95	2.136677	98.129.229.158	10.0.2.15	HTTP	7648	HTTP/1.1 200 OK (application/javascript)
98	2.137327	10.0.2.15	98.129.229.158	HTTP	427	GET /assets/thumbnails/thmbProlg.jpg HTTP/1.1
99	2.137444	10.0.2.15	98.129.229.158	HTTP	424	GET /assets/icons/flags/japan.png HTTP/1.1
100	2.137478	10.0.2.15	98.129.229.158	HTTP	429	GET /assets/icons/flags/poland.png HTTP/1.1
104	2.137661	10.0.2.15	98.129.229.158	HTTP	430	GET /assets/icons/flags/switzerland.png HTTP/1.1
105	2.137694	10.0.2.15	98.129.229.158	HTTP	425	GET /assets/icons/flags/taiwan.png HTTP/1.1
108	2.137708	10.0.2.15	98.129.229.158	HTTP	432	GET /assets/icons/flags/unitedkingdom.png HTTP/1.1
112	2.397661	98.129.229.158	10.0.2.15	HTTP	1039	HTTP/1.1 200 OK (PNG)
114	2.398066	10.0.2.15	98.129.229.158	HTTP	454	GET /images/folders/MichaelvonAichbergerBudapest/ImageProperties.xml?1644667...
118	2.464225	98.129.229.158	10.0.2.15	HTTP	2431	HTTP/1.1 200 OK (PNG)
124	2.464226	98.129.229.158	10.0.2.15	HTTP	4085	HTTP/1.1 200 OK (PNG)
132	2.464504	98.129.229.158	10.0.2.15	HTTP	1044	HTTP/1.1 200 OK (PNG)
134	2.464504	98.129.229.158	10.0.2.15	HTTP	1007	HTTP/1.1 200 OK (PNG)
142	2.468226	10.0.2.15	98.129.229.158	HTTP	475	GET /assets/fonts/poppins-v1-latin-regular.woff2 HTTP/1.1
143	2.468326	10.0.2.15	98.129.229.158	HTTP	471	GET /assets/fonts/poppins-v1-latin-300.woff2 HTTP/1.1
144	2.468382	10.0.2.15	98.129.229.158	HTTP	411	GET /assets/shin.gif HTTP/1.1
145	2.468424	10.0.2.15	98.129.229.158	HTTP	438	GET /assets/logos/zoomify/zoomifyLogo200x61.gif HTTP/1.1
152	2.669556	98.129.229.158	10.0.2.15	HTTP/XML	384	HTTP/1.1 200 OK
156	2.669704	98.129.229.158	10.0.2.15	HTTP	2447	HTTP/1.1 200 OK (JPEG JFIF image)
158	2.669873	10.0.2.15	98.129.229.158	HTTP	434	GET /assets/logos/zoomify/v5Gold-isHere.jpg HTTP/1.1
159	2.670896	10.0.2.15	98.129.229.158	HTTP	429	GET /assets/icons/circle1.gif HTTP/1.1
162	2.670403	98.129.229.158	10.0.2.15	HTTP	2087	HTTP/1.1 200 OK (GIF89a)
164	2.670766	10.0.2.15	98.129.229.158	HTTP	428	GET /assets/icons/circle2.gif HTTP/1.1

Frame 5: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50768, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

Packets: 786 - Displayed: 266 (33.8%)

Feb 12 17:27
*enp0s3

No.	Time	Source	Destination	Protocol	Length	Info
710	7.473207	98.129.229.158	10.0.2.15	HTTP	60	HTTP/1.1 200 OK (Image/jpeg)
711	7.473481	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup187/10-334-47.jpg H...
715	7.478990	98.129.229.158	10.0.2.15	HTTP	4188	HTTP/1.1 200 OK (Image/jpeg)
717	7.479258	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup184/10-346-46.jpg H...
719	7.663462	98.129.229.158	10.0.2.15	HTTP	16288	HTTP/1.1 200 OK (Image/jpeg)
723	7.663583	98.129.229.158	10.0.2.15	HTTP	3788	HTTP/1.1 200 OK (Image/jpeg)
725	7.663917	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup187/10-346-47.jpg H...
726	7.664086	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup182/10-334-45.jpg H...
731	7.670559	98.129.229.158	10.0.2.15	HTTP	1947	HTTP/1.1 200 OK (Image/jpeg)
733	7.670811	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup190/10-334-48.jpg H...
735	7.724764	98.129.229.158	10.0.2.15	HTTP	13776	HTTP/1.1 200 OK (Image/jpeg)
737	7.725178	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup182/10-346-45.jpg H...
739	7.739412	98.129.229.158	10.0.2.15	HTTP	16537	HTTP/1.1 200 OK (Image/jpeg)
741	7.739557	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup190/10-346-48.jpg H...
745	7.745797	98.129.229.158	10.0.2.15	HTTP	6018	HTTP/1.1 200 OK (Image/jpeg)
747	7.745997	10.0.2.15	98.129.229.158	HTTP	448	GET /ZVS/Assets/Skins/Default/standard/fullViewExitUp.png HTTP/1.1
751	7.922902	98.129.229.158	10.0.2.15	HTTP	2378	HTTP/1.1 200 OK (Image/jpeg)
753	7.923215	10.0.2.15	98.129.229.158	HTTP	450	GET /ZVS/Assets/Skins/Default/standard/fullViewExitOver.png HTTP/1.1
757	7.925520	98.129.229.158	10.0.2.15	HTTP	3984	HTTP/1.1 200 OK (Image/jpeg)
759	7.925715	10.0.2.15	98.129.229.158	HTTP	450	GET /ZVS/Assets/Skins/Default/standard/fullViewExitDown.png HTTP/1.1
763	7.933954	98.129.229.158	10.0.2.15	HTTP	2431	HTTP/1.1 200 OK (Image/jpeg)
767	7.968973	98.129.229.158	10.0.2.15	HTTP	3371	HTTP/1.1 200 OK (Image/jpeg)
771	8.007087	98.129.229.158	10.0.2.15	HTTP	3344	HTTP/1.1 200 OK (Image/jpeg)
773	8.009725	98.129.229.158	10.0.2.15	HTTP	2421	HTTP/1.1 200 OK (PNG)
775	8.163532	98.129.229.158	10.0.2.15	HTTP	2248	HTTP/1.1 200 OK (PNG)
777	8.166267	98.129.229.158	10.0.2.15	HTTP	2273	HTTP/1.1 200 OK (PNG)
779	8.169525	10.0.2.15	98.129.229.158	HTTP	407	GET /favicon.ico HTTP/1.1
783	8.450647	98.129.229.158	10.0.2.15	HTTP	2544	HTTP/1.1 200 OK (Image/vnd.microsoft.icon)

Frame 5: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50768, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

Packets: 786 - Displayed: 266 (33.8%)

Feb 12 17:27
*enp0s3

$$8.45-0.263=8.187$$

Max Number of persistent Connections 8

The image displays two screenshots of a Wireshark network traffic analysis. The top screenshot shows a list of HTTP GET requests to various assets and logos. The bottom screenshot shows a list of HTTP GET requests for images and logos, including a favicon. Both screenshots show a high number of persistent connections to the same destination IP address.

No.	Time	Source	Destination	Protocol	Length	Info
80	2.63473	10.0.2.15	98.129.229.158	HTTP	395	GET / HTTP/1.1
120	4.48083	10.0.2.15	35.232.111.17	HTTP	143	GET / HTTP/1.1
240	5.60486	10.0.2.15	98.129.229.158	HTTP	389	GET /assets/dynamic/scripts.js HTTP/1.1
320	7.26244	35.232.111.17	10.0.2.15	HTTP	202	HTTP/1.1 204 No Content
400	7.94779	98.129.229.158	10.0.2.15	HTTP	2749	HTTP/1.1 200 OK [text/html]
450	8.821380	10.0.2.15	98.129.229.158	HTTP	419	GET /ZV9/zoomify/imageviewerExpress-min.js HTTP/1.1
470	8.821691	98.129.229.158	10.0.2.15	HTTP	2671	HTTP/1.1 200 OK (application/javascript)
1312	1.119752	98.129.229.158	10.0.2.15	HTTP	9188	HTTP/1.1 200 OK (application/javascript)
1332	1.119970	10.0.2.15	98.129.229.158	HTTP	427	GET /assets/thumbnails/thmbProlg.jpg HTTP/1.1
1342	1.20105	10.0.2.15	98.129.229.158	HTTP	431	GET /assets/thumbnails/thmbExpressig.jpg HTTP/1.1
1352	1.201052	10.0.2.15	98.129.229.158	HTTP	424	GET /assets/icons/flags/china.png HTTP/1.1
1362	1.201051	10.0.2.15	98.129.229.158	HTTP	431	GET /assets/icons/flags/germany.png HTTP/1.1
1412	1.20504	10.0.2.15	98.129.229.158	HTTP	428	GET /assets/thumbnails/thmbFreig.jpg HTTP/1.1
1422	1.20505	10.0.2.15	98.129.229.158	HTTP	425	GET /assets/icons/flags/taiwan.png HTTP/1.1
1432	1.20648	10.0.2.15	98.129.229.158	HTTP	428	GET /assets/icons/flags/france.png HTTP/1.1
1452	1.20736	10.0.2.15	98.129.229.158	HTTP	425	GET /assets/icons/flags/france.png HTTP/1.1
1512	1.376480	98.129.229.158	10.0.2.15	HTTP	488	HTTP/1.1 200 OK (GIF89a)
1532	1.376711	10.0.2.15	98.129.229.158	HTTP	454	GET /images/folders/MichaelvonAichbergerBudapest/ImageProperties.xml?t1644667.. HTTP/1.1
1552	1.377387	98.129.229.158	10.0.2.15	HTTP	3903	HTTP/1.1 200 OK (PNG)
1572	1.377617	10.0.2.15	98.129.229.158	HTTP	475	GET /assets/fonts/poppins-v1-latin-regular.woff2 HTTP/1.1
1712	1.379014	98.129.229.158	10.0.2.15	HTTP	1005	HTTP/1.1 200 OK (PNG)
1732	1.379736	10.0.2.15	98.129.229.158	HTTP	471	GET /assets/fonts/poppins-v1-latin-300.woff2 HTTP/1.1
1832	1.389653	98.129.229.158	10.0.2.15	HTTP	983	HTTP/1.1 200 OK (PNG)
1852	1.389923	10.0.2.15	98.129.229.158	HTTP	411	GET /assets/shin.gif HTTP/1.1
1892	1.391923	98.129.229.158	10.0.2.15	HTTP	3247	HTTP/1.1 200 OK (JPEG JFIF image)
1912	1.392081	10.0.2.15	98.129.229.158	HTTP	438	GET /assets/logos/zoomify/zoomifyLogo200x61.gif HTTP/1.1
1952	1.403037	98.129.229.158	10.0.2.15	HTTP	1039	HTTP/1.1 200 OK (PNG)
1972	1.404286	10.0.2.15	98.129.229.158	HTTP	434	GET /assets/logos/zoomify/v5Gold-isHere.jpg HTTP/1.1

Frame 8: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface emp03, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50780, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

Wireshark emp03_20220212172806_wky3t.pcapng

Packets: 884 - Displayed: 268 (30.3%)

Feb 12 17:28

*emp03

Activities Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

HTTP

No.	Time	Source	Destination	Protocol	Length	Info
800	0.195307	98.129.229.158	10.0.2.15	HTTP	3206	HTTP/1.1 200 OK (Image/jpeg)
802	0.195592	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup184/10-346-46.jpg HTTP/1.1
808	0.204949	98.129.229.158	10.0.2.15	HTTP	60	HTTP/1.1 200 OK (Image/jpeg)
809	0.205476	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup187/10-346-47.jpg HTTP/1.1
813	0.275804	98.129.229.158	10.0.2.15	HTTP	4188	HTTP/1.1 200 OK (Image/jpeg)
815	0.275880	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup182/10-334-45.jpg HTTP/1.1
819	0.292728	98.129.229.158	10.0.2.15	HTTP	3789	HTTP/1.1 200 OK (Image/jpeg)
821	0.297488	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup190/10-334-48.jpg HTTP/1.1
825	0.308228	98.129.229.158	10.0.2.15	HTTP	4088	HTTP/1.1 200 OK (Image/jpeg)
827	0.309099	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup182/10-346-45.jpg HTTP/1.1
831	0.379305	98.129.229.158	10.0.2.15	HTTP	1947	HTTP/1.1 200 OK (Image/jpeg)
833	0.379459	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelvonAichbergerBudapest/TileGroup190/10-346-48.jpg HTTP/1.1
837	0.459415	98.129.229.158	10.0.2.15	HTTP	2096	HTTP/1.1 200 OK (Image/jpeg)
839	0.459708	10.0.2.15	98.129.229.158	HTTP	449	GET /ZV9/Assets/Skins/Default/standard/fullViewExitOver.png HTTP/1.1
843	0.461132	98.129.229.158	10.0.2.15	HTTP	6317	HTTP/1.1 200 OK (Image/jpeg)
845	0.461568	10.0.2.15	98.129.229.158	HTTP	450	GET /ZV9/Assets/Skins/Default/standard/fullViewExitDown.png HTTP/1.1
849	0.478500	98.129.229.158	10.0.2.15	HTTP	6918	HTTP/1.1 200 OK (Image/jpeg)
851	0.478795	10.0.2.15	98.129.229.158	HTTP	450	GET /ZV9/Assets/Skins/Default/standard/fullViewExitOver.png HTTP/1.1
857	0.524526	98.129.229.158	10.0.2.15	HTTP	918	HTTP/1.1 200 OK (Image/jpeg)
860	0.535004	98.129.229.158	10.0.2.15	HTTP	3884	HTTP/1.1 200 OK (Image/jpeg)
862	0.559322	98.129.229.158	10.0.2.15	HTTP	17831	HTTP/1.1 200 OK (Image/jpeg)
867	0.576642	98.129.229.158	10.0.2.15	HTTP	3371	HTTP/1.1 200 OK (Image/jpeg)
871	0.635341	98.129.229.158	10.0.2.15	HTTP	3344	HTTP/1.1 200 OK (Image/jpeg)
873	0.728025	98.129.229.158	10.0.2.15	HTTP	2421	HTTP/1.1 200 OK (PNG)
875	0.732652	98.129.229.158	10.0.2.15	HTTP	2248	HTTP/1.1 200 OK (PNG)
877	0.740739	98.129.229.158	10.0.2.15	HTTP	2273	HTTP/1.1 200 OK (PNG)
879	0.748859	10.0.2.15	98.129.229.158	HTTP	407	GET /favicon.ico HTTP/1.1
881	0.000199	98.129.229.158	10.0.2.15	HTTP	2544	HTTP/1.1 200 OK (Image/vnd.microsoft.icon)

Frame 8: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface emp03, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50780, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

Wireshark emp03_20220212172806_wky3t.pcapng

Packets: 884 - Displayed: 268 (30.3%)

Feb 12 17:28

*emp03

Activities Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

HTTP

$$7.006-0.263=6.743$$

Max Number of persistent Connections 10

The top screenshot shows a list of HTTP GET requests to various assets on a website. The bottom screenshot shows a list of HTTP GET requests for image files, including thumbnails and logos. Both screenshots show the packet list, packet details, and packet bytes panes.

No.	Time	Source	Destination	Protocol	Length	Info
40	2.506230	10.0.2.15	98.129.229.158	HTTP	399	GET / HTTP/1.1
17	0.532626	10.0.2.15	98.129.229.158	HTTP	399	GET /assets/dynamic/scripts.js HTTP/1.1
27	0.762279	98.129.229.158	10.0.2.15	HTTP	2748	HTTP/1.1 200 OK (text/html)
32	0.791095	10.0.2.15	98.129.229.158	HTTP	410	GET /ZVS/zoomifyImageViewerExpress-min.js HTTP/1.1
34	0.801829	98.129.229.158	10.0.2.15	HTTP	2671	HTTP/1.1 200 OK (application/javascript)
112	2.075375	98.129.229.158	10.0.2.15	HTTP	10389	HTTP/1.1 200 OK (application/javascript)
114	2.083554	10.0.2.15	98.129.229.158	HTTP	431	GET /assets/thumbnails/thmbExpresslg.jpg HTTP/1.1
115	2.083635	10.0.2.15	98.129.229.158	HTTP	438	GET /assets/logos/zoomify/zoomifylogo280x61.gif HTTP/1.1
116	2.083694	10.0.2.15	98.129.229.158	HTTP	424	GET /assets/icons/flags/china.png HTTP/1.1
117	2.083748	10.0.2.15	98.129.229.158	HTTP	432	GET /assets/icons/flags/unitedkingdom.png HTTP/1.1
118	2.083891	10.0.2.15	98.129.229.158	HTTP	431	GET /assets/icons/flags/unitedStates.png HTTP/1.1
124	2.084026	10.0.2.15	98.129.229.158	HTTP	429	GET /assets/icons/circles.gif HTTP/1.1
125	2.084751	10.0.2.15	98.129.229.158	HTTP	434	GET /assets/logos/zoomify/v5Gold-isHere.jpg HTTP/1.1
128	2.085097	10.0.2.15	98.129.229.158	HTTP	428	GET /assets/thumbnails/thmbFreeig.jpg HTTP/1.1
130	2.088084	10.0.2.15	98.129.229.158	HTTP	427	GET /assets/icons/flags/hongkong.png HTTP/1.1
133	2.335985	98.129.229.158	10.0.2.15	HTTP	6167	HTTP/1.1 200 OK (JPEG JFIF image)
135	2.335959	10.0.2.15	98.129.229.158	HTTP	454	GET /images/folders/MichaelVonaIchbergerBudapest/ImageProperties.xml?1644667..
141	2.343271	98.129.229.158	10.0.2.15	HTTP	1083	HTTP/1.1 200 OK (JPEG JFIF image)
143	2.343449	10.0.2.15	98.129.229.158	HTTP	475	GET /assets/fonts/poppins-v1-Latin-regular.woff2 HTTP/1.1
145	2.346486	98.129.229.158	10.0.2.15	HTTP	2087	HTTP/1.1 200 OK (GIF89a)
147	2.346976	10.0.2.15	98.129.229.158	HTTP	471	GET /assets/fonts/poppins-v1-Latin-300.woff2 HTTP/1.1
151	2.347291	98.129.229.158	10.0.2.15	HTTP	1005	HTTP/1.1 200 OK (PNG)
153	2.347478	10.0.2.15	98.129.229.158	HTTP	411	GET /assets/shin.gif HTTP/1.1
164	2.351884	98.129.229.158	10.0.2.15	HTTP	1058	HTTP/1.1 200 OK (PNG)
166	2.352274	10.0.2.15	98.129.229.158	HTTP	420	GET /assets/icons/circle2.gif HTTP/1.1
168	2.355471	98.129.229.158	10.0.2.15	HTTP	3972	HTTP/1.1 200 OK (PNG)
170	2.355471	98.129.229.158	10.0.2.15	HTTP	1578	HTTP/1.1 200 OK (GIF89a)
174	2.355666	98.129.229.158	10.0.2.15	HTTP	1165	HTTP/1.1 200 OK (PNG)

Frame 4: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface emp03, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50812, Dst Port: 80, Seq: 1, Len: 341
Hypertext Transfer Protocol

The bottom screenshot shows a list of HTTP GET requests for image files, including thumbnails and logos. Both screenshots show the packet list, packet details, and packet bytes panes.

No.	Time	Source	Destination	Protocol	Length	Info
707	5.576312	98.129.229.158	10.0.2.15	HTTP	2057	HTTP/1.1 200 OK (Image/jpeg)
769	5.576530	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelVonaIchbergerBudapest/TileGroup187/10-346-47.jpg M-
775	5.607591	98.129.229.158	10.0.2.15	HTTP	68	HTTP/1.1 200 OK (Image/jpeg)
776	5.607993	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelVonaIchbergerBudapest/TileGroup182/10-334-45.jpg M-
780	5.614341	98.129.229.158	10.0.2.15	HTTP	7586	HTTP/1.1 200 OK (Image/jpeg)
782	5.614730	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelVonaIchbergerBudapest/TileGroup190/10-334-48.jpg M-
786	5.615433	98.129.229.158	10.0.2.15	HTTP	4188	HTTP/1.1 200 OK (Image/jpeg)
788	5.615579	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelVonaIchbergerBudapest/TileGroup182/10-346-45.jpg M-
792	5.620023	98.129.229.158	10.0.2.15	HTTP	3780	HTTP/1.1 200 OK (Image/jpeg)
794	5.620883	10.0.2.15	98.129.229.158	HTTP	466	GET /images/folders/MichaelVonaIchbergerBudapest/TileGroup190/10-346-48.jpg M-
798	5.638987	98.129.229.158	10.0.2.15	HTTP	4668	HTTP/1.1 200 OK (Image/jpeg)
800	5.639291	10.0.2.15	98.129.229.158	HTTP	448	GET /ZVS/Assets/Skins/Default/standard/fullViewExitUp.png HTTP/1.1
804	5.667844	98.129.229.158	10.0.2.15	HTTP	1947	HTTP/1.1 200 OK (Image/jpeg)
806	5.668395	10.0.2.15	98.129.229.158	HTTP	450	GET /ZVS/Assets/Skins/Default/standard/fullViewExitOver.png HTTP/1.1
810	5.697649	98.129.229.158	10.0.2.15	HTTP	2096	HTTP/1.1 200 OK (Image/jpeg)
812	5.698021	10.0.2.15	98.129.229.158	HTTP	450	GET /ZVS/Assets/Skins/Default/standard/fullViewExitDown.png HTTP/1.1
818	5.773421	98.129.229.158	10.0.2.15	HTTP	1937	HTTP/1.1 200 OK (Image/jpeg)
822	5.782955	98.129.229.158	10.0.2.15	HTTP	11858	HTTP/1.1 200 OK (Image/jpeg)
826	5.839957	98.129.229.158	10.0.2.15	HTTP	5298	HTTP/1.1 200 OK (Image/jpeg)
830	5.873913	98.129.229.158	10.0.2.15	HTTP	3884	HTTP/1.1 200 OK (Image/jpeg)
834	5.881124	98.129.229.158	10.0.2.15	HTTP	3344	HTTP/1.1 200 OK (Image/jpeg)
838	5.888205	98.129.229.158	10.0.2.15	HTTP	1431	HTTP/1.1 200 OK (Image/jpeg)
843	5.888983	98.129.229.158	10.0.2.15	HTTP	3371	HTTP/1.1 200 OK (Image/jpeg)
845	5.904853	98.129.229.158	10.0.2.15	HTTP	2421	HTTP/1.1 200 OK (PNG)
847	5.929756	98.129.229.158	10.0.2.15	HTTP	2248	HTTP/1.1 200 OK (PNG)
849	5.953231	98.129.229.158	10.0.2.15	HTTP	2273	HTTP/1.1 200 OK (PNG)
851	5.956517	10.0.2.15	98.129.229.158	HTTP	407	GET /favicon.ico HTTP/1.1
855	6.214586	98.129.229.158	10.0.2.15	HTTP	2544	HTTP/1.1 200 OK (Image/vnd.microsoft.icon)

Frame 4: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface emp03, id 0
Ethernet II, Src: PcsCompu 2e:ee:5a (08:00:27:2e:ee:5a), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 98.129.229.158
Transmission Control Protocol, Src Port: 50812, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

$$6.214-0.250=5.964$$