

Karthikeyan. G

Assignment-2

MTech - cybersecurity

Contents

1.Let's begin our exploration of HTTP by downloading a very simple HTML file - one that is very short and contains no embedded objects. Do the following: ----- 3

By looking at the information in the HTTP GET and response messages, answer the following questions. ----- 3

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?----- 3

What languages (if any) do 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? ----- 4

When was the HTML file that you are retrieving last modified at the server? ----- 4

How many bytes of content are being returned to your browser? ----- 5

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.----- 5

2. Before performing the steps below, ensure your browser's cache is empty. ----- 5

Answer the following questions: ----- 6

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? ----- 6

2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? ----- 6

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? What information follows the "IF-MODIFIED-SINCE:" header? ----- 7

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 file's contents? Explain.----- 7

Start up your web browser, and make sure your browser's cache is cleared, as discussed above. ----- 7

Answer the following questions: ----- 8

1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?----- 8

2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? ----- 8

3. What is the status code and phrase in the response? ----- 8

4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? ----- 9

Answer the following questions: -----10

1. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?-----10

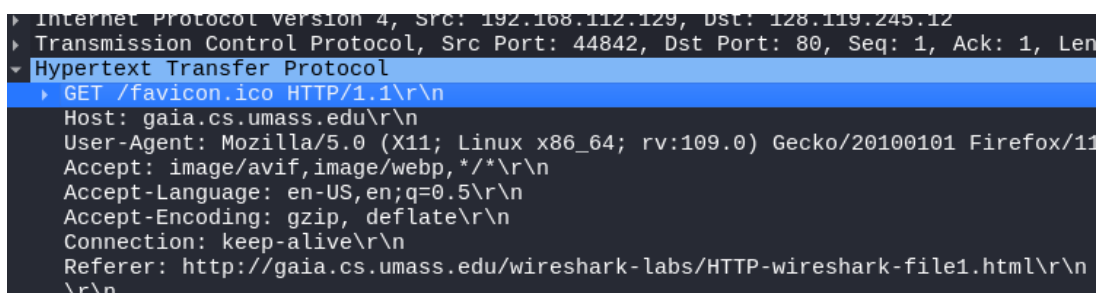
2. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? -----10

1. Let's begin our exploration of HTTP by downloading a very simple HTML file - one that is very short and contains no embedded objects. Do the following:

1. Start up your web browser.
2. Start the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
3. Wait more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
4. Enter the following into your browser
`http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html`
Your browser should display a very simple, one-line HTML file.
5. Stop Wireshark packet capture.

By looking at the information in the HTTP GET and response messages, answer the following questions.

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



A screenshot of a Wireshark packet capture. The packet list on the left shows three packets: Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol packet is selected and expanded, showing a GET request for /favicon.ico. The packet details pane on the right shows the following information: Host: gaia.cs.umass.edu\r\n, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/11, Accept: image/avif,image/webp,*/*\r\n, Accept-Language: en-US,en;q=0.5\r\n, Accept-Encoding: gzip, deflate\r\n, Connection: keep-alive\r\n, and Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\r\n.

```
Internet Protocol Version 4, Src: 192.168.112.129, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 44842, Dst Port: 80, Seq: 1, Ack: 1, Len
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/11
    Accept: image/avif,image/webp,*/*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\r\n
\r\n
```

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

```

Transmission Control Protocol, Src Port: 44842, Dst Port: 80, Seq: 1, Ack: 1, Len:
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115
    Accept: image/avif,image/webp,*/*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/favicon.ico]
    [HTTP request 1/1]
    [Response in frame: 539]

```

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

```

16 4.882263883 192.168.112.129 128.119.245.12 HTTP 435 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

```

The Source IP is **192.168.112.129** and Destination IP is **128.119.245.12**.

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

```

Transmission Control Protocol, Src Port:
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Mon, 05 Aug 2024 16:08:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1
    Last-Modified: Mon, 05 Aug 2024 05:59:0
    ETag: "80-61ee95fb824d4"\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

```

The status code returned from the server is **200 OK**.

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

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Mon, 05 Aug 2024 16:08:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP
    Last-Modified: Mon, 05 Aug 2024 05:59:02 GMT\r\n
    ETag: "80-61ee95fb824d4"\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

```

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

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Mon, 05 Aug 2024 16:08:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP
    Last-Modified: Mon, 05 Aug 2024 05:59:02 GMT\r\n
    ETag: "80-61ee95fb824d4"\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: 0.306322894 s]
[Request in frame: 16]

```

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.

No.

2. Before performing the steps below, ensure your browser's cache is empty.

- a. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- b. Start up the Wireshark packet sniffer
- c. Enter the following URL into your browser
- d. <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>
- e. Your browser should display a very simple five-line HTML file.
- f. Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)

- g. Stop Wireshark packet capture and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Answer the following questions:

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?

The first time I have requested the resource, there might not be any cached data to compare against. Because I cleared all the cache. In such cases, the browser will send a normal GET request without the If-Modified-Since header.

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

```
HTTP/1.1 200 OK
Date: Mon, 05 Aug 2024 13:41:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Mon, 05 Aug 2024 05:59:02 GMT
ETag: "173-61ee95fb81d04"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations again! Now you've downloaded the file lab2-2.html. <br>
This file's last modification date will not change. <p>
Thus if you download this multiple times on your browser, a complete copy <br>
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
field in your browser's HTTP GET request to the server.
</html>
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
```

The server response included a Content-Type: text/html header, confirming the file type. The response body contained the actual HTML content of the file. This indicates that the server explicitly returned the file contents.

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? What information follows the “IF-MODIFIED-SINCE:” header?

```
Internet Protocol Version 4, Src: 192.168.112.129, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 43916, Dst Port: 80, Seq: 382, Ack: 731, Len: 467
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\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: Mon, 05 Aug 2024 05:59:02 GMT\r\n
    If-None-Match: "173-61ee95fb81d04"\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: 13]
    [Response in frame: 33]
```

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 file’s contents? Explain.

```
Frame 29: 293 bytes on wire (2344 bits), 293 bytes captured on interface
Ethernet II, Src: VMware_f0:02:c3 (00:50:56:f0:02:c3), Dst: 192.168.112.129
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.112.129
Transmission Control Protocol, Src Port: 80, Dst Port: 43916
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 06 Aug 2024 06:20:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-61efd7d80d84b"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.319866992 seconds]
    [Prev request in frame: 15]
```

The server confirmed that the file has not changed, and thus the server hasn’t resend the file’s contents.

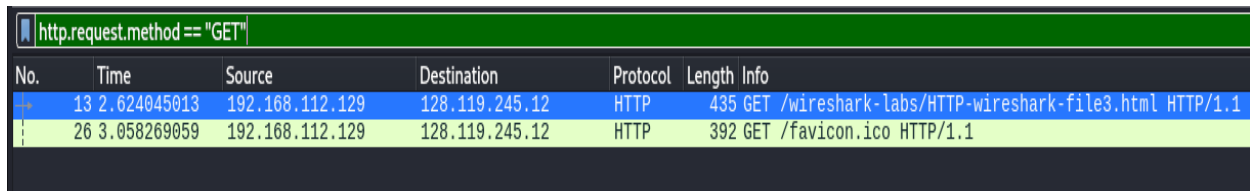
Start up your web browser, and make sure your browser’s cache is cleared, as discussed above.

- Start up the Wireshark packet sniffer
- Enter the following URL into your browser
- <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

- d. Your browser should display the rather lengthy US Bill of Rights.
- e. Stop Wireshark packet capture and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed.

Answer the following questions:

1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

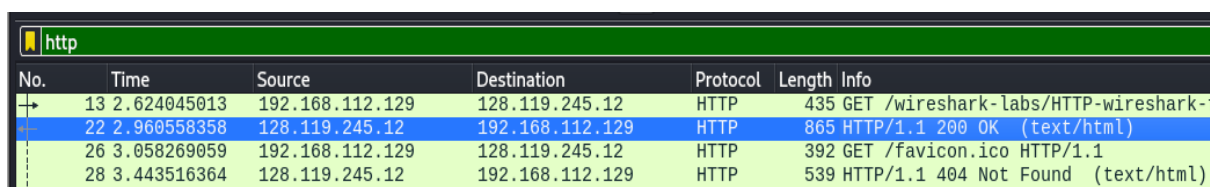


| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-----------------|----------------|----------|--------|--|
| 13 | 2.624045013 | 192.168.112.129 | 128.119.245.12 | HTTP | 435 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 26 | 3.058269059 | 192.168.112.129 | 128.119.245.12 | HTTP | 392 | GET /favicon.ico HTTP/1.1 |

There are 2 HTTP GET request messages set to the web server.

The packet no. in the trace is 13.

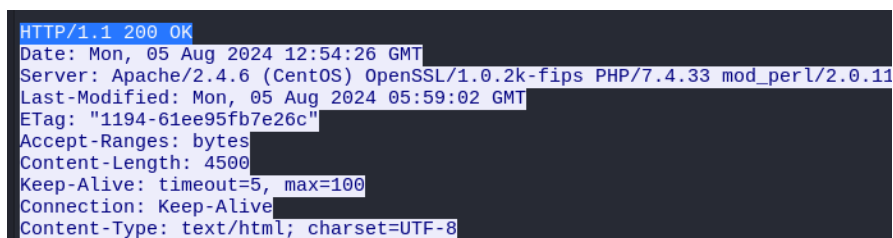
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-----------------|-----------------|----------|--------|-------------------------------------|
| 13 | 2.624045013 | 192.168.112.129 | 128.119.245.12 | HTTP | 435 | GET /wireshark-labs/HTTP-wireshark- |
| 22 | 2.960558358 | 128.119.245.12 | 192.168.112.129 | HTTP | 865 | HTTP/1.1 200 OK (text/html) |
| 26 | 3.058269059 | 192.168.112.129 | 128.119.245.12 | HTTP | 392 | GET /favicon.ico HTTP/1.1 |
| 28 | 3.443516364 | 128.119.245.12 | 192.168.112.129 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |

Here the packet number in the trace is **22**. And the status code is **200** and the phrase associated with the response is **OK**.

3. What is the status code and phrase in the response?



```

HTTP/1.1 200 OK
Date: Mon, 05 Aug 2024 12:54:26 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11
Last-Modified: Mon, 05 Aug 2024 05:59:02 GMT
ETag: "1194-61ee95fb7e26c"
Accept-Ranges: bytes
Content-Length: 4500
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

```

The status code is **200** and the phrase associated with the response is **OK**.

4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

```
▶ Frame 21: 2215 bytes on wire (17720 bits), 2
▶ Ethernet II, Src: VMware_f0:02:c3 (00:50:56:
▶ Internet Protocol Version 4, Src: 128.119.24
▼ Transmission Control Protocol, Src Port: 80,
    Source Port: 80
    Destination Port: 45542
    [Stream index: 0]
    ▶ [Conversation completeness: Complete, WITH
    [TCP Segment Len: 2161]
    Sequence Number: 2701      (relative sequenc
    Sequence Number (raw): 549008429
    [Next Sequence Number: 4862      (relative s
    Acknowledgment Number: 382      (relative ac
    Acknowledgment number (raw): 2184246041
    0101 .... = Header Length: 20 bytes (5)
    ▶ Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
```

4. Finally, let's try visiting a website that is password-protected and examining the sequence of HTTP messages exchanged for such a site. The URL http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html is password protected. The username is "Wireshark-students" (without the quotes), and the password is "network" (again, without the quotes). So, let's access this "secure" password-protected site.

Go Through this link before answering this question: HTTP Authentication Schemes (userland.com)

Answer the following questions:

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

```
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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

HTTP/1.1 401 Unauthorized
Date: Mon, 05 Aug 2024 06:07:26 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
WWW-Authenticate: Basic realm="wireshark-students only"
Content-Length: 381
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

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

```
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbmRzOm5ldHdvcm==

HTTP/1.1 200 OK
Date: Mon, 05 Aug 2024 06:07:51 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Mon, 05 Aug 2024 05:59:02 GMT
ETag: "84-61ee95fb8308c"
Accept-Ranges: bytes
Content-Length: 132
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

This page is password protected! If you're seeing this, you've downloaded the page correctly <br>
Congratulations!
</html>GET /favicon.ico HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
```