ECE3700 B02 – Lab 1

Nick McFadden

Due: January 25, 2023

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

   ARP, DB-LSP-DISC/JSON, DNS, ICMPv6, SSDP, TCP, TLSv1.2, UDP

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*.)

   17:40:22.148824 - 17:40:22.086583 = 0.062241 seconds

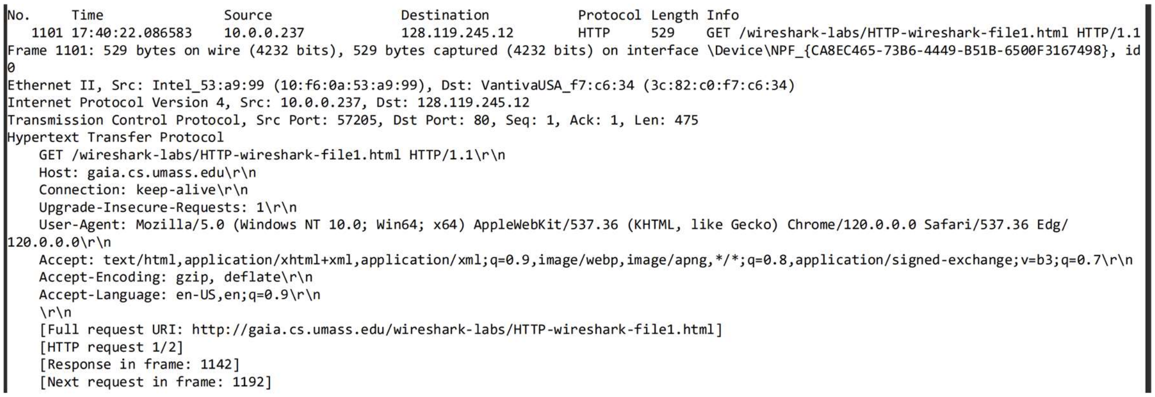
3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
   i. Print the two HTTP messages displayed in step 9 above. To do so, select *Print* from the Wireshark *File* command menu, and select "*Selected Packet Only"* and

"Print as displayed" and then click OK.

Internet address of gai.cs.umass.edu: 128.119.245.12

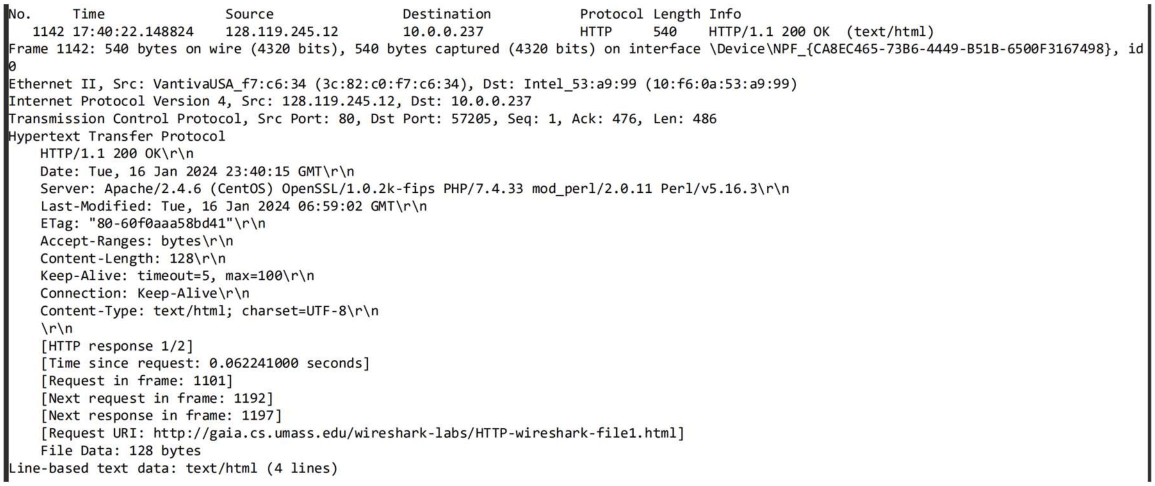
Internet address of computer: 10.0.0.237

Below is the HTTP message of the HTTP GET message



```
No.     Time               Source                Destination           Protocol Length Info
   1101 17:40:22.086583    10.0.0.237            128.119.245.12        HTTP     529    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 1101: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{CA8EC465-73B6-4449-B51B-6500F3167498}, id
0
Ethernet II, Src: Intel_53:a9:99 (10:f6:0a:53:a9:99), Dst: VantivaUSA_f7:c6:34 (3c:82:c0:f7:c6:34)
Internet Protocol Version 4, Src: 10.0.0.237, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57205, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/
120.0.0.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 1142]
    [Next request in frame: 1192]
```

Below is the HTTP message of the HTTP OK message

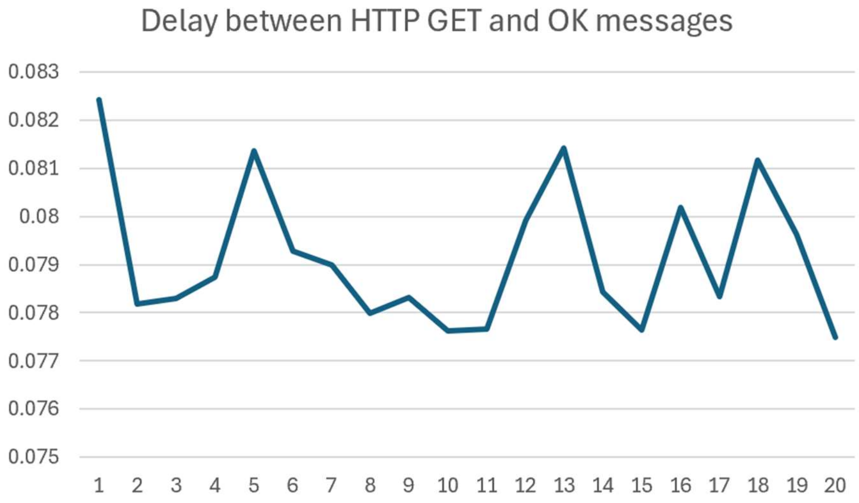


```
No.     Time                Source                Destination           Protocol Length Info
   1142 17:40:22.148824     128.119.245.12        10.0.0.237            HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 1142: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CA8EC465-73B6-4449-B51B-6500F3167498}, id
0
Ethernet II, Src: VantivaUSA_f7:c6:34 (3c:82:c0:f7:c6:34), Dst: Intel_53:a9:99 (10:f6:0a:53:a9:99)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.237
Transmission Control Protocol, Src Port: 80, Dst Port: 57205, Seq: 1, Ack: 476, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 16 Jan 2024 23:40:15 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 16 Jan 2024 06:59:02 GMT\r\n
    ETag: "80-60f0aaa58bd41"\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 1/2]
    [Time since request: 0.062241000 seconds]
    [Request in frame: 1101]
    [Next request in frame: 1192]
    [Next response in frame: 1197]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

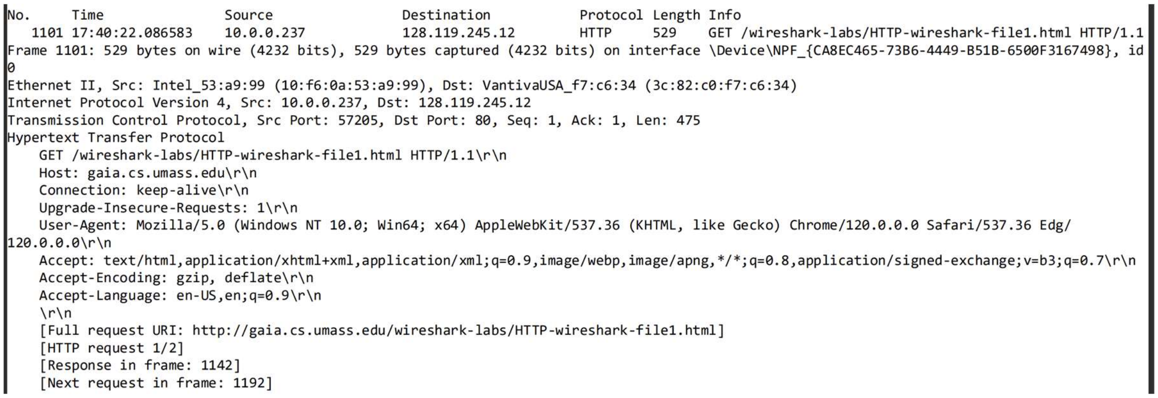
4. Plot a graph representing the results of the delay between HTTP GET and OK for 20 different HTTP requests and then calculate the average delay. (HINT: You can save Wireshark capture into a text file and write a Java program to extract the data by reading the text file. Then use MATLAB to plot the graphs).

Trial values (in seconds)

1. 0.082413
2. 0.078190
3. 0.078296
4. 0.078750
5. 0.081361
6. 0.079278
7. 0.078997
8. 0.077997
9. 0.078311
10. 0.077627
11. 0.077667
12. 0.079915
13. 0.081423
14. 0.078439
15. 0.077645
16. 0.080193
17. 0.078331
18. 0.081177
19. 0.079628
20. 0.077495

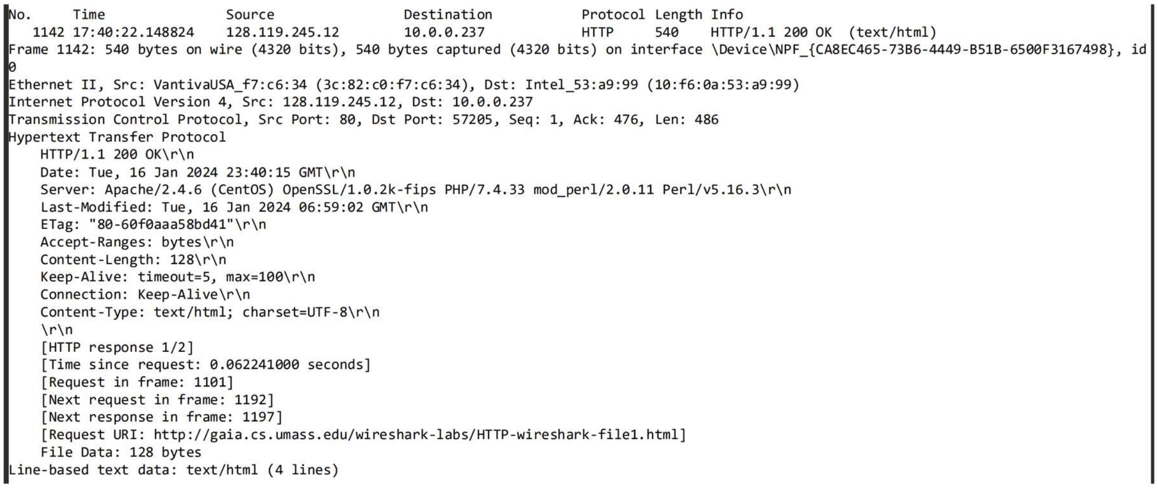


The average delay between the 20 different HTTP requests was 0.07915665



```
No.     Time               Source                Destination           Protocol Length Info
   1101 17:40:22.086583    10.0.0.237            128.119.245.12        HTTP     529    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 1101: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{CA8EC465-73B6-4449-B51B-6500F3167498}, id
0
Ethernet II, Src: Intel_53:a9:99 (10:f6:0a:53:a9:99), Dst: VantivaUSA_f7:c6:34 (3c:82:c0:f7:c6:34)
Internet Protocol Version 4, Src: 10.0.0.237, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57205, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/
120.0.0.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 1142]
    [Next request in frame: 1192]
```

Figure 1: HTTP Get Message



```
No.     Time               Source                Destination           Protocol Length Info
   1142 17:40:22.148824    128.119.245.12        10.0.0.237            HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 1142: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CA8EC465-73B6-4449-B51B-6500F3167498}, id
0
Ethernet II, Src: VantivaUSA_f7:c6:34 (3c:82:c0:f7:c6:34), Dst: Intel_53:a9:99 (10:f6:0a:53:a9:99)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.237
Transmission Control Protocol, Src Port: 80, Dst Port: 57205, Seq: 1, Ack: 476, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 16 Jan 2024 23:40:15 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 16 Jan 2024 06:59:02 GMT\r\n
    ETag: "80-60f0aaa58bd41"\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 1/2]
    [Time since request: 0.062241000 seconds]
    [Request in frame: 1101]
    [Next request in frame: 1192]
    [Next response in frame: 1197]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

Figure 2: HTTP OK Message

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

   Underneath the Hypertext Transfer Protocol section of both my browser and the server, it indicates "HTTP/1.1" meaning that both are running HTTP version 1.1 (it is also indicated underneath the Info header).

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

   As shown in Figure 1, in the Hypertext Transfer Protocol section, we can see Accepted-Languages and it indicates en-US. Meaning English (the US keyboard version).

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

   Internet address of computer: 10.0.0.237
   Internet address of gai.cs.umass.edu: 128.119.245.12

This is shown in Figure 1 (the HTTP Get Message), which labels the source IP as 10.0.0237 and the destination as 128.119.245.12. We know that the computer sends the GET message and gai.cs.umass.edu receives it.

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

   Status code: 200
   Phrase: OK

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

   Under the Last Modified section of the Hypertext Transfer Protocol section, it indicates that the HTML file was last modified at the server on January 16, 2024, 6:59:02 GMT.

Note: In your answer to question 5 above, you might have been surprised to find that the document you just retrieved was last modified within a minute before you downloaded the document. That's because (for this particular file), the gaia.cs.umass.edu server is setting the file's last-modified time to be the current time, and is doing so once per minute. Thus, if you wait a minute between accesses, the file will appear to have been recently modified, and hence your browser will download a "new" copy of the document.

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

   128 bytes as indicated by the File Data entry under the Hypertext Transfer Protocol section.

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.

   No

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?

   No

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

   Yes, in the Content-Length subfield, we are given a result of 371 and are given the Line-based text data field, indicating that the server returned the contents of the file.

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?

    Yes, it is followed with the time of the first HTTP GET request.

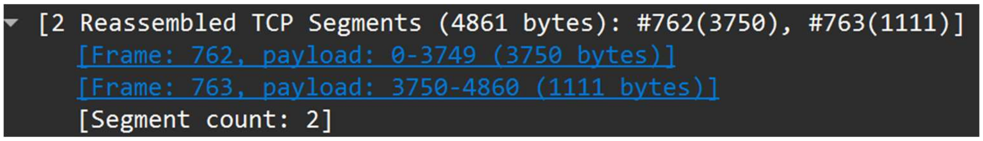
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

    304 is the status code and Not Modified is the phrase returned from the server in response to the second HTTP GET. The server did not explicitly return the contents of the file as there the file was not modified.

12. How many HTTP GET request messages were sent by your browser?

    1

13. How many data-containing TCP segments were needed to carry the single HTTP response?

    ```
    ▾ [2 Reassembled TCP Segments (4861 bytes): #762(3750), #763(1111)]
          [Frame: 762, payload: 0-3749 (3750 bytes)]
          [Frame: 763, payload: 3750-4860 (1111 bytes)]
          [Segment count: 2]
    ```

    2 TCP segments were needed, carrying up to 3750 bytes.

14. What is the status code and phrase associated with the response to the HTTP GET request?

    The response to the HTTP GET request was a “200” status code and an “OK” phrase.

15. Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?

    No

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

    3 HTTP GET request messages were sent by my browser. Two of the GET requests were sent to 128.119.245.12 and one was sent to 178.79.137.164.

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.

    The two images were downloaded from the two web sites serially as the time stamps for each differ by approximately 0.5 seconds, indicating that the action did not occur in parallel.

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

    The initial HTTP GET message received a 200 (status code) OK (phrase) response from the browser.

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

    The second HTTP GET message received a 401 (status code) Unauthorized (phrase) response from the browser.

1. To which layer in the TCP/IP protocol stack does HTTP belong?

   Application layer

2. What is the underlying transport layer protocol used by HTTP?

   TCP

3. What is the HTTP response code returned by the web server if the server is found and returns the requested content successfully?

   Status code: 200

   Phrase: OK

4. How are the files that exceed the packet's size (i.e., large files) sent to the client?

   Large files are sent to the client via multiple packets. These packets carry the large message and the client can piece the packets together to reform the message.

5. What are the components of an HTTP status line?

   HTTP protocol version, status code and phrase

6. What is the encoding method used in HTTP authentication?

   UTF-8 Encoding

7. Why is basic HTTP authentication not secure enough?

   Basic HTTP authentication is not secure enough as it is still vulnerable to attacks which is why https is more commonly used as it requires a username and password authentication which adds an extra layer of security.