

Name:	Bodhisatya Ghosh
Class:	CSE DS
Batch:	B
UID:	2021700026
Experiment:	3

Aim: Experiment with Packet Analyzers – Wireshark. (Complete Various tasks given on website provided)

Task A: By looking at the information in the HTTP GET and response messages, answer the following (7) questions. When answering the following questions, you should print out the GET and response messages (to include the packet data in your own report, you may export the selected packet data as a text file. To do so, use the File->Export->File... window, select file type as Plain text, and choose "Selected packet" and indicate where in the message you've found the information that answers the following questions. (Note that the export procedure might differ based on the platform on which you are running Wireshark; e.g., SUN, Windows, etc.)

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? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?
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 bytes" pane, do you see any http headers within the data that are not displayed in the "packet details" pane? If so, name one.

Answers:

1. My browser is running HTTP version 1.1. The server is also running HTTP 1.1 version.

No.	Time	Source	Destination	Protocol	Length	Info
88	11.942717	192.168.0.104	103.88.220.83	HTTP	178	GET /ncsi.txt HTTP/1.1
90	11.944861	103.88.220.83	192.168.0.104	HTTP	233	HTTP/1.1 200 OK (text/plain)
121	15.678297	192.168.0.104	44.228.249.3	HTTP	674	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
126	15.967173	44.228.249.3	192.168.0.104	HTTP	330	HTTP/1.1 302 Found (text/html)
127	15.970420	192.168.0.104	44.228.249.3	HTTP	543	GET /login.php HTTP/1.1
137	16.328086	44.228.249.3	192.168.0.104	HTTP	1362	HTTP/1.1 200 OK (text/html)

2. The browser indicates that it can accept English (US).

No.	Time	Source	Destination	Protocol	Length	Info
84	7.369605	192.168.0.104	128.119.245.12	HTTP	499	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
90	7.648723	128.119.245.12	192.168.0.104	HTTP	540	HTTP/1.1 200 OK (text/html)
111	7.870594	192.168.0.104	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
118	8.137984	128.119.245.12	192.168.0.104	HTTP	538	HTTP/1.1 404 Not Found (text/html)
194	11.673061	192.168.0.104	103.88.220.42	HTTP	331	GET /appinfo/359550/sha/182c289a2932f10353aebd96f58d7effb922dd2c.txt.gz HTTP/1.1
195	11.673176	192.168.0.104	103.88.220.42	HTTP	331	GET /appinfo/555160/sha/9fefe1df6d76237abac3c969ba7284ec2d866908.txt.gz HTTP/1.1
196	11.673231	192.168.0.104	103.88.220.42	HTTP	332	GET /appinfo/1144200/sha/365d925b63e69cb45fee423684ee18340412d8.txt.gz HTTP/1.1
197	11.673278	192.168.0.104	103.88.220.42	HTTP	332	GET /appinfo/1324130/sha/ab93c677e94e81738cf745c5f311137616081b7c.txt.gz HTTP/1.1
216	11.677738	103.88.220.42	192.168.0.104	HTTP	1004	HTTP/1.1 200 OK (application/gzip)
222	11.678130	103.88.220.42	192.168.0.104	HTTP	1196	HTTP/1.1 200 OK (application/gzip)
224	11.678130	103.88.220.42	192.168.0.104	HTTP	926	HTTP/1.1 200 OK (application/gzip)
235	11.690331	103.88.220.42	192.168.0.104	HTTP	1047	HTTP/1.1 200 OK (application/gzip)

> [SEQ/ACK analysis]

TCP payload (445 bytes)

Hypertext Transfer Protocol

> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file1.html

Request Version: HTTP/1.1

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/60.0.3113.0 Safari/537.36

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

Accept-Encoding: gzip, deflate\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

[HTTP request 1/1]

```

0000 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65  Requests : 1..Use
0001 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61  r-Agent: Mozilla
0002 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54  /5.0 (Windows NT
0003 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36  10.0; Win64; x6
0004 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35  4) AppleWebKit/5
0005 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69  37.36 (KHTML, li
0006 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65  ke Gecko ) Chrome
0007 2f 31 31 30 2e 30 2e 30 2e 30 20 53 61 66 61 72  /110.0.0.0 Safar
0008 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74  i/537.36 - Accept
0009 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c  : text/html,appl
0010 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d  ication/ xhtml+xml
0011 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d  ,applic ation/xml
0012 6c 30 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76  i;q=0.9, image/ev
0013 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d  if,image /webp,im
0014 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30  age/apng /*;q=0
0015 2e 38 0d 0a 53 65 63 2d 47 50 43 3a 20 31 0d 0a  .8- Sec- GPC: 1
0016 01 23 65 65 70 74 2d 4c 61 6e 67 2f 61 67 65 68  Accept-Language:
0017 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 38 0d  en-US,en;q=0.8
0018 01 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67  Accept- Encoding
0019 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 6d  : gzip, deflate.
0020 0a 0d 0a

```

3. IP of computer: 192.168.0.104

IP of server: 128.119.245.12

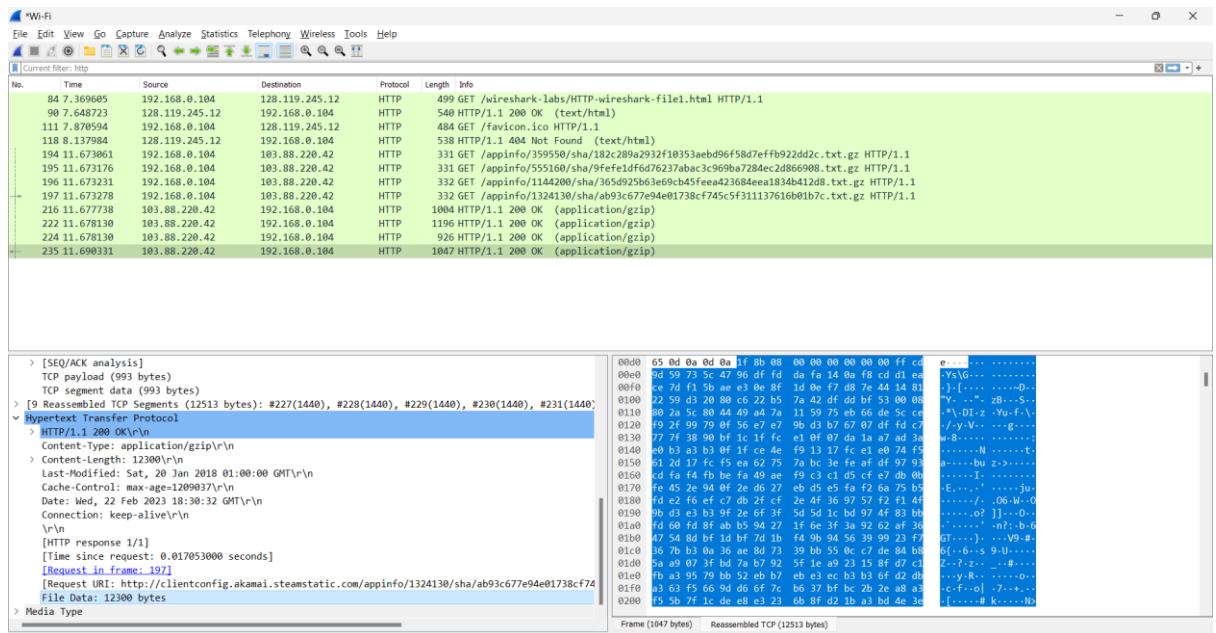
4. The returned status code is : 200

The image shows a Wireshark packet capture of an HTTP 200 OK response. The packet list on the left shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the response structure: Hypertext Transfer Protocol, [Expert Info (Chat/Sequence): HTTP/1.1 200 OK], Response Version: HTTP/1.1, Status Code: 200, [Status Code Description: OK], Response Phrase: OK, Content-Type: application/gzip, Content-Length: 12300, Last-Modified: Sat, 20 Jan 2018 01:00:00 GMT, Cache-Control: max-age=1209600, Date: Wed, 22 Feb 2023 18:30:32 GMT, Connection: keep-alive. The packet bytes pane shows the raw data of the response, including the status line: HTTP/1.1 200 OK.

5. The HTML file was last modified on Wednesday, 22 February 2023 18:30:29 GMT

The image shows a Wireshark packet capture of an HTTP 404 Not Found response. The packet list on the left shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the response structure: Hypertext Transfer Protocol, [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found], Response Version: HTTP/1.1, Status Code: 404, [Status Code Description: Not Found], Response Phrase: Not Found, Content-Type: text/html, Content-Length: 289, Last-Modified: Wed, 22 Feb 2023 18:30:29 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, Connection: Keep-Alive, Keep-Alive: timeout=5, max=99, Connection: Keep-Alive, Content-Type: text/html; charset=iso-8859-1. The packet bytes pane shows the raw data of the response, including the status line: HTTP/1.1 404 Not Found.

6. 12300 Bytes of total data is transferred.



7.

Task B: For questions 8-11, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

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

Answers:

8. No, there is no “IF-MODIFIED-SINCE” line in the first HTTP GET.
9. Yes, the server explicitly returned the contents of the file as seen below

Wireshark packet capture showing an HTTP GET request and its response. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file2.html. The packet details pane shows the Hypertext Transfer Protocol section with the 'Last-Modified' header.

```

> Frame 49: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{9FE73...}
> Ethernet II, Src: Tp-LinkT_20:5a:0a (ac:94:c6:20:5a:0a), Dst: Chongqin_47:4a:ae (c8:94:02:47:4a:ae)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103
> Transmission Control Protocol, Src Port: 80, Dst Port: 62295, Seq: 1, Ack: 446, Len: 730
> Hypertext Transfer Protocol
  Line-based text data: text/html (10 lines)
    <html>
    <h1>
    <p>
    <p>Congratulations again! Now you've downloaded the file lab2-2.html. <br>
    <p>This file's last modification date will not change. <br>
    <p>Thus if you download this multiple times on your browser, a complete copy <br>
    <p>will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
    <p>field in your browser's HTTP GET request to the server.<br>
    </html>
  
```

10. Yes, there is an “IF-MODIFIED-SINCE:” line in the second HTTP GET.

Wireshark packet capture showing an HTTP GET request and its response. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file2.html. The packet details pane shows the Hypertext Transfer Protocol section with the 'If-Modified-Since' header.

```

[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.6
If-None-Match: "173-5f580c7e90aea"
If-Modified-Since: Sat, 25 Feb 2023 06:59:02 GMT
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]
[Prev request in frame: 29]
  
```

This header shows the last date at which the file was last modified.

11. The HTTP status code returned after second GET request is 304. No, the server did not return any file. The phrase returned was “NOT MODIFIED”.

No.	Time	Source	Destination	Protocol	Length	Info
29	3.678972	192.168.0.103	128.119.245.12	HTTP	499	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
49	4.318394	128.119.245.12	192.168.0.103	HTTP	784	HTTP/1.1 200 OK (text/html)
72	6.342299	192.168.0.103	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
74	6.599132	128.119.245.12	192.168.0.103	HTTP	293	HTTP/1.1 304 Not Modified
1517	143.550202	192.168.0.103	103.88.220.82	HTTP	178	GET /ncsl.txt HTTP/1.1
1519	143.556599	103.88.220.82	192.168.0.103	HTTP	233	HTTP/1.1 200 OK (text/plain)
1732	180.903760	192.168.0.103	192.168.0.1	HTTP	250	GET /gatedesc.xml HTTP/1.1
1738	180.908098	192.168.0.1	192.168.0.103	HTTP/X	513	HTTP/1.1 200 OK

<pre> > Frame 74: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{9FE73...} > Ethernet II, Src: Tp-Link T_20:5a:0a (ac:84:c6:20:5a:0a), Dst: Chongjin_47:4a:ae (c8:94:02:47:4a:ae) > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103 > Transmission Control Protocol, Src Port: 80, Dst Port: 62295, Seq: 731, Ack: 1003, Len: 239 > Hypertext Transfer Protocol > HTTP/1.1 304 Not Modified\r\n Date: Sun, 26 Feb 2023 05:48:40 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 Connection: Keep-Alive\r\n Keep-Alive: timeout=5, max=99\r\n ETag: "173-5f580c7e90aea"\r\n \r\n [HTTP response 2/2] [Time since request: 0.256833000 seconds] [Prev request in frame: 29] [Prev response in frame: 49] [Request in frame: 72] [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html] </pre>	<pre> 0000 c8 94 02 47 4a ae ac 84 c6 20 5a 0a 08 00 45 20 ...G...Z...E 0010 01 17 c5 c3 40 00 2a 06 53 6a 00 77 f5 0c c0 a8 ...@...Sjw... 0020 00 67 00 50 f3 57 3a de 8f 2d cd c7 a0 1c 50 18 ...g.P.W:....P. 0030 00 f6 12 46 00 00 48 54 54 50 2f 31 2e 31 20 33 ...F..HT TP/1.1 3 0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not Modified. 0050 0a 44 61 74 65 3a 20 53 75 6e 2c 20 32 36 20 46 :Date: S un, 26 F 0060 65 62 20 32 30 32 33 20 30 35 3a 34 38 3a 34 30 eb 2023 05:48:40 0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT-Se rver: Ap 0080 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/2.4 .6 (Cent 0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0. 00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e 2k-fips PHP/7.4. 00b0 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 33 mod_p erl/2.0. 00c0 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 11 Perl/ v5.16.3 00d0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 .Connect ion: Kee 00e0 70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6c p-Alive- iKeep-AL 00f0 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 ive: tim eout=5, 0100 6d 61 78 3d 39 39 0d 0a 45 54 61 67 3a 20 22 31 max=99 .ETag: "1 0110 37 33 2d 35 66 35 38 30 63 37 65 39 30 61 65 61 73-5f580 c7e90aea 0120 22 0d 0a 0d 0a </pre>
---	--

Task C: For questions 12-15, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

- How many HTTP GET request messages were sent by your browser?
- How many data-containing TCP segments were needed to carry the single HTTP response?
- What is the status code and phrase associated with the response to the HTTP GET request?
- Is there any HTTP header information in the transmitted data associated with TCP segmentation?

Answers:

- 1 HTTP GET request was sent by the browser.
- 4 data-containing TCP segments were needed to carry the single HTTP response.
- Status code returned : 200(OK)
- NAA

Task D: For questions 16-17, first write a brief but precise answer for each of the above questions, then write a paragraph explaining and

discussing your observations from the above practice questions.
Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

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

Answers:

16. 3 HTTP GET messages were sent by my browser. The addresses to which they were sent to are
 - i. wireshark-labs/HTTP-wireshark-file4.html
 - ii. /8E_cover_small.jpg
 - iii. /pearson.png
 17. As we can see, the last modified date and time of both files are exactly the same. Therefore, we can say both responses were enacted parallelly.
-

Conclusion: In this experiment I have learnt how to analyze a network and it's components using a packet sniffer like WireShark.