

Lab Assignment-1

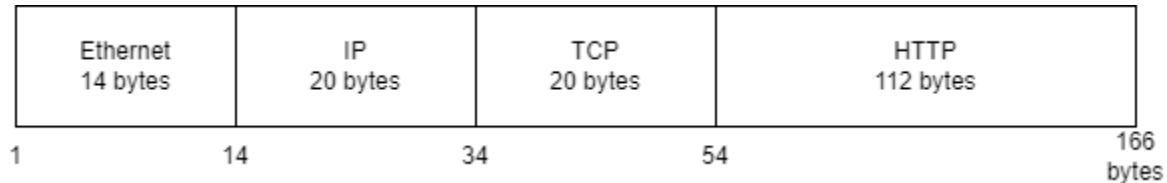
112001046

Vaibhav B Nagrale

Part 1

1. Hand in your packet drawing.

Ans.



Protocol layer structure of the HTTP GET packet

2. Estimate the download protocol overhead on packet 7 in the given trace.

Ans.

Frame size = 1484 bytes

Ethernet = 14 bytes

IP = 20 bytes

TCP = 20 bytes

$$\text{Total(Ethernet, IP, TCP)} = 14 + 20 + 20 = 54 \text{ bytes}$$

Overhead (on packet 7) = $(54/1484)*100 = 3.639$

3. Estimate the download protocol overhead for the entire HTTP response, as defined above.

Ans.

Frame size = 66 + 60 + 1484 + 1484 + 1282 + 1484 + 1484 + 1290 + 1484 + 1484 + 1290 + 1484 + 1281 + 60 = 15717 bytes

Total (Ethernet, IP, TCP) = (32+20+14) + (20+20+20) + (20+20+14) + (20+20+14) + (20+20+14)
+ (20+20+14) + (20+20+14) + (20+20+14) + (20+20+14) + (20+20+14) + (20+20+14) +
(20+20+14) + (20+20+14) + (20+20+20) = 780 bytes

$$\text{Overhead} = (780/15717) \times 100 = 4.963$$

4. Which Ethernet header field is the demultiplexing key indicating that the next higher layer is IP? What value is used in this field to indicate IP?

Ans.

The demultiplexing key for Ethernet is the Type field. It holds 0x800 when the higher layer is IP.

5. Which IP header field is the demultiplexing key indicating that the next higher layer is TCP? What value is used in this field to indicate TCP?

Ans.

The demultiplexing key for IP is the Protocol field. It has value 6 when the higher layer is TCP.

6. Why doesn't TCP's header contain a demultiplexing key? How can TCP know to deliver the data to HTTP on the receiving side?

Ans.

It doesn't have demultiplexing key because TCP relies on destination port number in the header to identify the receiving application. This port number serves as a means for TCP to accurately route the data on the receiving end.

Part 2

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Ans.

Both of them are version 1.1

```
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
```

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

Ans.

en-IN, en

```
Accept-Language: en-IN,en;q=0.9\r\n
```

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

Ans.

Computer IP: 10.128.8.173

Gaia.cs.umass.edu IP: 128.199.245.12

```
▼ Internet Protocol Version 4, Src: 10.128.8.173, Dst: 128.119.245.12
```

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

Ans.

Status code: 200 ok

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
```

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

Ans.

Wed, 30 August 2023

```
Last-Modified: Wed, 30 Aug 2023 05:59:01 GMT\r\n
```

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

Ans.

128

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
[Content length: 128]
```

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.

Ans.

No, I don't see any in the HTTP Message below

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?

Ans.

There is no IF-MODIFIED-SINCE in first GET

```
1233 4.996423 10.128.8.173 128.119.245.12 HTTP 526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file2.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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-IN,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/3]
[Response in frame: 1267]
[Next request in frame: 1278]
```

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

Ans.

```
1267 5.289242 128.119.245.12 10.128.8.173 HTTP 784 HTTP/1.1 200 OK (text/html)
Line-based text data: text/html (10 lines)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
</html>\r\n
```

10. Now inspect the contents of the second HTTP GET request from your browser to the

server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans.

2nd GET has IF-MODIFIED-SINCE

```
1432 6.206759 10.128.8.173 128.119.245.12 HTTP 638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
If-None-Match: "173-60431bda1ad49"\r\n
If-Modified-Since: Thu, 31 Aug 2023 05:59:01 GMT\r\n
\r\n
```

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

Ans.

Status Code: 304

The file has not been modified. So the text of the file is not returned in HTTP message.

```
1478 6.501743 128.119.245.12 10.128.8.173 HTTP 293 HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
    Date: Thu, 31 Aug 2023 08:05:46 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=98\r\n
    ETag: "173-60431bda1ad49"\r\n
    \r\n
    [HTTP response 3/3]
```

12. 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?

Ans.

```
537 3.184443 10.128.8.173 128.119.245.12 HTTP 526 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
```

HTTP GET request message: 1

In the 537th packet message Bill or Rights was present.

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

Ans.

```
593 3.462603 128.119.245.12 10.128.8.173 TCP 1514 80 → 51565 [ACK] Seq=1 Ack=473 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
594 3.462603 128.119.245.12 10.128.8.173 TCP 1514 80 → 51565 [ACK] Seq=1461 Ack=473 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
595 3.462603 128.119.245.12 10.128.8.173 TCP 1514 80 → 51565 [ACK] Seq=2921 Ack=473 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
```

Packet 593

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

Ans.

```
596 3.462603 128.119.245.12 10.128.8.173 HTTP 535 HTTP/1.1 200 OK (text/html)
```

200 ok

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

Ans.

593	3.462603	128.119.245.12	10.128.8.173	TCP	1514	80 → 51565	[ACK] Seq=1 Ack=473 Win=30336 Len=1460	[TCP segment of a reassembled PDU]
594	3.462603	128.119.245.12	10.128.8.173	TCP	1514	80 → 51565	[ACK] Seq=1461 Ack=473 Win=30336 Len=1460	[TCP segment of a reassembled PDU]
595	3.462603	128.119.245.12	10.128.8.173	TCP	1514	80 → 51565	[ACK] Seq=2921 Ack=473 Win=30336 Len=1460	[TCP segment of a reassembled PDU]

Three packets were required to carry single HTTP response, they were 593, 594 and 595.

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

Ans.

401	2.446723	10.128.8.173	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
449	2.725159	128.119.245.12	10.128.8.173	HTTP	1355	HTTP/1.1 200 OK (text/html)
460	2.770994	10.128.8.173	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
536	3.019842	10.128.8.173	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1

3 HTTP GET packets: packet 401 (to get the base file), packet 460 (to get pearson.png) and packet 536 (to get 8E_cover_small.jpg)

Packet 401 was sent to 128.119.245.12, packet 460 to 128.119.245.12, and packet 536 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 websites in parallel? Explain.

Ans.

401	2.446723	10.128.8.173	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
449	2.725159	128.119.245.12	10.128.8.173	HTTP	1355	HTTP/1.1 200 OK (text/html)
460	2.770994	10.128.8.173	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
536	3.019842	10.128.8.173	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
552	3.049285	128.119.245.12	10.128.8.173	HTTP	745	HTTP/1.1 200 OK (PNG)
576	3.150217	10.128.8.173	23.60.169.25	HTTP	165	GET /connecttest.txt HTTP/1.1
604	3.206679	178.79.137.164	10.128.8.173	HTTP	225	HTTP/1.1 301 Moved Permanently
634	3.248990	23.60.169.25	10.128.8.173	HTTP	241	HTTP/1.1 200 OK (text/plain)

The downloads occurred in parallel. The two GET messages for the images are in packets 460 and 536. The 200 OK reply containing the images show up as packets 552 and 634. Thus the request for the second image file (packet 552) was made BEFORE packet 634, the first image file was received.

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

Ans.

381	2.737582	10.128.8.173	128.119.245.12	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
431	3.018910	128.119.245.12	10.128.8.173	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Packet 381 in the trace has first GET and packet 431 has the reply. The server response in packet 431 is '401 Unauthorized'.

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

Ans.

779	5.533265	10.128.8.173	128.119.245.12	HTTP	595	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
-----	----------	--------------	----------------	------	-----	--

```
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic Og==\r\n
```

The HTTP GET includes the Authorization: Basic Og==\r\n