COMP2322 Computer Networking

Lab 2 Report: HTTP

Author
Wang Yuqi
[redacted]

Lecturer
Dr. LOU Wei

BsC in Computer Science
Academic year: 2024/2025 Sem 2

Trace Files

The trace files for this lab report are:

File Name	Parts	Questions
`./part1.pcapng`	The Basic HTTP GET/response interaction	2, 4, 6
`./part2.pcapng`	The HTTP CONDITIONAL GET/response interaction	8, 10
`./part3.pcapng`	Retrieving Long Documents	12, 14
`./part4.pcapng`	HTML Documents with Embedded Objects	16
`./part5.pcapng`	HTTP Authentication	18

DISCLAIMER To protect my **personal privacy**, only a selected subset of the original trace file is included. This partial trace retains lab-relevant traffic while scrubbing other sensitive data.

Sensitive Info The full trace contained these info that I do not wish to disclose:

- Public IPs of my private GPU compute nodes
- Public IPs of my private VPN network
- TLS handshake and key exchange messages
- Network activity that reveals my software usage and browsing habits

Questions

Part 1: *The Basic HTTP GET/response interaction*

HTTP GET

```
No.     Time               Source                Destination           Protocol Length Info
5096    21:05:22.110086837 172.20.131.34         128.119.245.12        HTTP     473    GET /wireshark-labs/HTTP-
wireshark-file1.html HTTP/1.1
Frame 5096: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 172.20.131.34, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57994, Dst Port: 80, Seq: 1, Ack: 1, Len: 405

Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [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
    User-Agent: [redacted]
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Sec-GPC: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\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: 5105]
    [Next request in frame: 5110]
```

HTTP OK

```
No.  Time               Source                Destination           Protocol Length Info
5105 21:05:22.397602215 128.119.245.12        172.20.131.34         HTTP     554    HTTP/1.1 200 OK  (text/html)
Frame 5105: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.131.34
Transmission Control Protocol, Src Port: 80, Dst Port: 57994, Seq: 1, Ack: 406, Len: 486

Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Fri, 14 Feb 2025 13:05:22 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: Fri, 14 Feb 2025 06:59:01 GMT\r\n
    ETag: "80-62e14b59e68f6"\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: 0.287515378 seconds]
    [Request in frame: 5096]
    [Next request in frame: 5110]
    [Next response in frame: 5118]
    [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)
```

Question 2

Q: What languages does your browser indicate that it can accept to the server?

Answer:

Source: Accept-Language header

Accept-Language:	**Language:**	**Quality Factor:**
`en-US`	English (US)	Relative quality factor 1.0
`en;q=0.5`	English	Relative quality factor 0.5

Summary: English (United States) is the most preferred language, followed by English. The latter is a general English language preference, which the server can use as a fallback option.

Question 4

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

Answer: 200

Source: HTTP Status Code in section HTTP OK

Question 6

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

Answer: 128 Bytes

Source: Content-Length header in section HTTP OK

(See Next Page)

Part 2: *The HTTP CONDITIONAL GET/response interaction*

HTTP GET (1st, No Cache)

```
No.     Time               Source               Destination          Protocol Length Info
245     21:17:43.957558559 172.20.131.34        128.119.245.12       HTTP     473    GET /wireshark-
labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 245: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 172.20.131.34, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49284, Dst Port: 80, Seq: 1, Ack: 1, Len: 405

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: [redacted]
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Sec-GPC: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 264]
    [Next request in frame: 272]
```

HTTP GET (2nd, w/ Cache)

```
No.     Time               Source               Destination          Protocol Length Info
798     21:17:53.580320537 172.20.131.34        128.119.245.12       HTTP     559    GET /wireshark-
labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 798: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 172.20.131.34, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58350, Dst Port: 80, Seq: 1, Ack: 1, Len: 491

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: [redacted]
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Sec-GPC: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Fri, 14 Feb 2025 06:59:01 GMT\r\n
    If-None-Match: "173-62e14b59e6126"\r\n
    Priority: u=0, i\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 807]
```

Questions 8

Q: 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?

Answer: No

The first HTTP GET request doesn’t contain an “IF-MODIFIED-SINCE” line, since browser cache was cleared earlier.

Questions 10

Q: 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?

Answer: Yes

The second HTTP GET request contains an “IF-MODIFIED-SINCE” line.
Source: `If-Modified-Since: Fri, 14 Feb 2025 06:59:01 GMT`

(See Next Page)

Part 3: *Retrieving Long Documents*

Questions 12

Q: 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?

Answer:
- 1 packet (258)
- 2 packets (258, 282) **if** counting `favicon.ico` request, returned 404 not found

Source: Packet number 258 & 282 in the tracefile

Questions 14

Q: What is the status code and phrase in the response?

Answer: 200 OK (404 Not Found)
- 404 Not Found, **if** counting `favicon.ico` request

Source: Packet 273 & 294

(See Next Page)

Part 4: *HTML Documents with Embedded Objects*

Questions 16

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

Answer: 4

No.	Time	Source	Destination	Protocol	Length	Info
74	22:02:53.509	172.20.131.34	128.119.245.12	HTTP	473	GET /wireshark-labs/HTTP...
90	22:02:53.903	172.20.131.34	128.119.245.12	HTTP	496	GET /pearson.png HTTP/1.1
104	22:02:54.107	172.20.131.34	128.119.245.12	HTTP	493	GET /favicon.ico HTTP/1.1
109	22:02:54.154	172.20.131.34	178.79.137.164	HTTP	463	GET /8E_cover_small.jpg HTTP/1.1

Source: Packet 74, 90, 104, 109

Part 5: *HTTP Authentication*

Question 18

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

Answer: 401 Unauthorized

- Status Code: 401
- Response Phrase: Unauthorized

Source: Packet 692