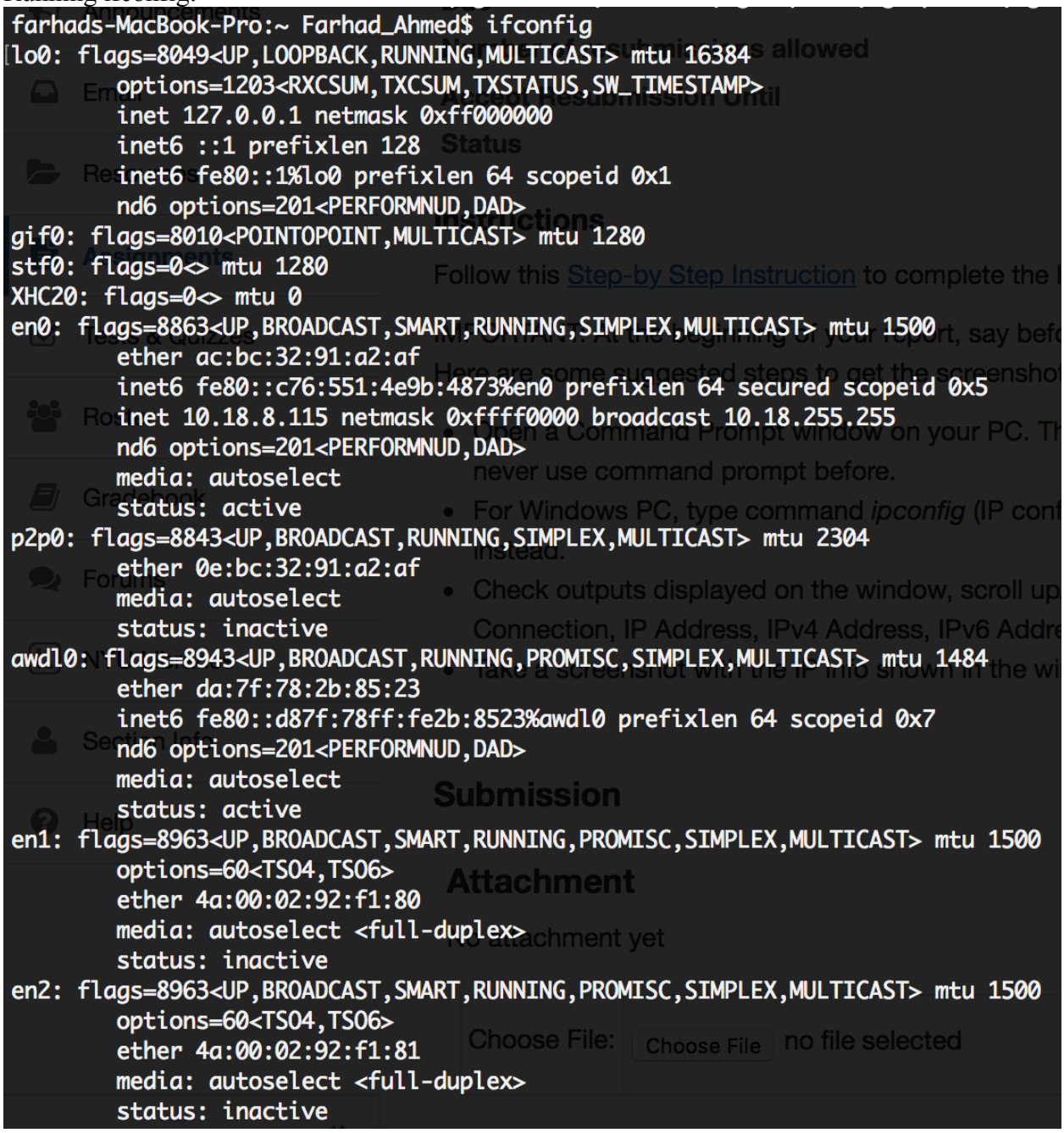
Farhad Ahmed
Computer Networking
10/01/18

Wireshark Lab: HTTP

Running ifconfig:



```
farhads-MacBook-Pro:~ Farhad_Ahmed$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:bc:32:91:a2:af
        inet6 fe80::c76:551:4e9b:4873%en0 prefixlen 64 secured scopeid 0x5
        inet 10.18.8.115 netmask 0xffff0000 broadcast 10.18.255.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 0e:bc:32:91:a2:af
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        ether da:7f:78:2b:85:23
        inet6 fe80::d87f:78ff:fe2b:8523%awdl0 prefixlen 64 scopeid 0x7
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=60<TSO4,TSO6>
        ether 4a:00:02:92:f1:80
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=60<TSO4,TSO6>
        ether 4a:00:02:92:f1:81
        media: autoselect <full-duplex>
        status: inactive
```

Part 1:

1. My browser is running HTTP version 1.1. The server is running HTTP version 1.1.
2. The languages accepted are en-us.
3. The IP Address of my computer is 10.18.8.115. The IP Address of the gaia.cs.umass.edu server is 128.119.245.12.
4. The status code returned from the server to the browser is 200 OK.
5. The last modified date of the HTML file Tue, 02 Oct 2018 05:59:02 GMT.
6. The content length is 128.
7. There are not any HTTP messages.

/var/folders/66/1ts8yhy171x7y1wx1t_4__fr0000gn/T//wireshark_pcapng_en0_20181002173847_DOZ6EI 128 total packets, 6 shown

```
      6 0.019883       10.18.8.115           128.119.245.12        HTTP     463    GET /wireshark-
labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 6: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface 0
Ethernet II, Src: Apple_91:a2:af (ac:bc:32:91:a2:af), Dst: IETF-VRRP-VRID_32 (00:00:5e:00:01:32)
Internet Protocol Version 4, Src: 10.18.8.115, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51376 (51376), Dst Port: 80 (80), Seq: 1, Ack: 1, Len:
397
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]
            [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/11.1 Safari/605.1.15\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 8]
      8 0.048516       128.119.245.12        10.18.8.115           HTTP     552    HTTP/1.1 200 OK
(text/html)
Frame 8: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: CiscoInc_25:4f:40 (24:01:c7:25:4f:40), Dst: Apple_91:a2:af (ac:bc:32:91:a2:af)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.18.8.115
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 51376 (51376), Seq: 1, Ack: 398, Len:
486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Tue, 02 Oct 2018 21:38:50 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Tue, 02 Oct 2018 05:59:02 GMT\r\n
    ETag: "80-577389e5a7acb"\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: 0.028633000 seconds]
    [Request in frame: 6]
Line-based text data: text/html
```

client IP

Server IP

client running 1.1

languages accepted

status code

server running 1.1

Last Modified Date

Content Length

Part 2:

8. There is no IF-MODIFIED-SINCE in the first GET.
9. The contents of the server response is displayed within the packet and can be seen
10. Second Get has a IF-MODIFIED-SINCE.
11. Since the file wasn't modified, the contents of the file were not displayed.

```
   1401 3.785433       10.18.8.115           128.119.245.12        HTTP     498    GET /wireshark-
labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 1401: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0
Ethernet II, Src: Apple_91:a2:af (ac:bc:32:91:a2:af), Dst: IETF-VRRP-VRID_32 (00:00:5e:00:01:32)
Internet Protocol Version 4, Src: 10.18.8.115, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52282 (52282), Dst Port: 80 (80), Seq: 1, Ack: 1, Len:
432
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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8\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-file2.html]
    [HTTP request 1/3]
    [Response in frame: 1403]
    [Next request in frame: 1570]
   1403 3.799533       128.119.245.12        10.18.8.115           HTTP     796    HTTP/1.1 200 OK
(text/html)
Frame 1403: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface 0
Ethernet II, Src: CiscoInc_25:4f:40 (24:01:c7:25:4f:40), Dst: Apple_91:a2:af (ac:bc:32:91:a2:af)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.18.8.115
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 52282 (52282), Seq: 1, Ack: 433, Len:
730
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Tue, 02 Oct 2018 22:22:01 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Tue, 02 Oct 2018 05:59:02 GMT\r\n
    ETag: "173-577389e5a6f13"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\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 1/3]
    [Time since request: 0.014100000 seconds]
    [Request in frame: 1401]
    [Next request in frame: 1570]
    [Next response in frame: 1572]
Line-based text data: text/html
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
```

Text

```
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
   1574 6.911834       10.18.8.115           128.119.245.12        HTTP     610    GET /wireshark-
labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 1574: 610 bytes on wire (4880 bits), 610 bytes captured (4880 bits) on interface 0
Ethernet II, Src: Apple_91:a2:af (ac:bc:32:91:a2:af), Dst: IETF-VRRP-VRID_32 (00:00:5e:00:01:32)
Internet Protocol Version 4, Src: 10.18.8.115, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52282 (52282), Dst Port: 80 (80), Seq: 836, Ack: 1215,
Len: 544
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
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-577389e5a6f13"\r\n
    If-Modified-Since: Tue, 02 Oct 2018 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 3/3]
    [Prev request in frame: 1570]
    [Response in frame: 1575]
   1575 6.935372       128.119.245.12        10.18.8.115           HTTP     305    HTTP/1.1 304
Not Modified
Frame 1575: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0
Ethernet II, Src: CiscoInc_25:4f:40 (24:01:c7:25:4f:40), Dst: Apple_91:a2:af (ac:bc:32:91:a2:af)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.18.8.115
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 52282 (52282), Seq: 1215, Ack: 1380,
Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Request Version: HTTP/1.1
        Status Code: 304
        Response Phrase: Not Modified
    Date: Tue, 02 Oct 2018 22:22:04 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
    ETag: "173-577389e5a6f13"\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.023538000 seconds]
    [Prev request in frame: 1570]
    [Prev response in frame: 1572]
    [Request in frame: 1574]
```

IF-Modified-Since

Not Modified

Part 3:

12. 1 packet sent from browser, 8th packet number gets message for bill of rights.
13. Packet 12 has the status code and phrase associated with the response.
14. Status Code 200 OK.
15. 3 packets were necessary to carry the single HTTP response.

Part 4:

16. The browser sent 3 HTTP GET messages, each message was sent to a different IP Address. Packet 12 was sent to 128.119.245.12, Packet 19 was sent to 165.193.123.218, and packet 22 was sent to 134.241.6.82.
17. The images were downloaded in parallel. The GET messages are in packets 19 and 22. But the replies with the images in them are in packets 27 and 56. The request for packet 20 was made before the first image was even finished.
18. The server's response is 401 Authorization required.
19. When sending the HTTP GET message a second time a new field appears in the message. The field is Authorization: Basic.