Wireshark Lab 2: HTTP

Trevor Bramwell
CS372 - Introduction to Computer Networks
Professor Bechir Hamdaoui

April 24, 2012

1 The Basic HTTP GET/response interation

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

   Answer My browser is running HTTP 1.1, and the server is running HTTP 1.1.

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

   Answer US English and English.

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

   Answer My computer's IP address is **10.0.1.21**, and the *gaia.cs.umass.edu* IP address is **128.119.245.12**.

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

   Answer 200

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

   Answer Tue, 24 Apr 2012 03:26:01 GMT

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

   Answer 128 Bytes

7. **Question** 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.

   Answer No, I do not. Every header is accounted for in the raw data.

```
No.     Time        Source                Destination           Protocol
    Length Info
      6 0.811425    10.0.1.21             128.119.245.12        HTTP      758
            GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 6: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: AppleCom_c1:5f
    :50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.21 (10.0.1.21), Dst: 128.119.245.12
    (128.119.245.12)
Transmission Control Protocol, Src Port: 38089 (38089), Dst Port: http (80),
    Seq: 1, Ack: 1, Len: 692
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    Host: gaia.cs.umass.edu
    Connection: keep-alive
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.19 (KHTML,
        like Gecko) Chrome/18.0.1025.162 Safari/535.19
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Referer: http://web.engr.oregonstate.edu/~hamdaoui/teaching/372Spring12/
        labs/WiresharkLab-HTTP-Ch2.pdf
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    Cookie: __utma=198765611.63021047.1334475645.1334475645.1334475645.1;
        __utmz=198765611.1334475645.1.1.utmcsr=google|utmccn=(organic)|utmcmd=
        organic|utmctr=umass%20amherst
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
        file1.html]
```

```
No.     Time        Source                Destination           Protocol
   Length Info
      8 1.219879    128.119.245.12        10.0.1.21             HTTP      494
          HTTP/1.1 200 OK  (text/html)

Frame 8: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af:71:6
   b (00:22:75:af:71:6b)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
   10.0.1.21 (10.0.1.21)
Transmission Control Protocol, Src Port: http (80), Dst Port: 38089 (38089),
   Seq: 1, Ack: 693, Len: 428
Hypertext Transfer Protocol
    HTTP/1.1 200 OK
    Date: Tue, 24 Apr 2012 03:26:27 GMT
    Server: Apache/2.2.3 (CentOS)
    Last-Modified: Tue, 24 Apr 2012 03:26:01 GMT
    ETag: "8734d-80-505b2440"
    Accept-Ranges: bytes
    Content-Length: 128
    Keep-Alive: timeout=10, max=100
    Connection: Keep-Alive
    Content-Type: text/html; charset=UTF-8
Line-based text data: text/html
```

2 The HTTP CONDITIONAL GET/response interaction

8. **Question** 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 Yes. It contains the current time.

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

   Answer Yes. The file is explicitly displayed below the packet.

10. **Question** 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 same date and time listed from the previous "IF-MODIFIED-SINCE" header is listed.

11. **Question** 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.

    Answer The returned response is **304 Not Modified**. The server did not return the contents of the file because the file had not changed since it was last accessed.

```
No.     Time        Source                Destination           Protocol
    Length Info
     15 2.629401    10.0.1.21             128.119.245.12        HTTP      845
            GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 15: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: AppleCom_c1:5f
    :50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.21 (10.0.1.21), Dst: 128.119.245.12
    (128.119.245.12)
Transmission Control Protocol, Src Port: 38102 (38102), Dst Port: http (80),
    Seq: 1, Ack: 1, Len: 779
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    Host: gaia.cs.umass.edu
    Connection: keep-alive
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.19 (KHTML,
        like Gecko) Chrome/18.0.1025.162 Safari/535.19
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Referer: http://web.engr.oregonstate.edu/~hamdaoui/teaching/372Spring12/
        labs/WiresharkLab-HTTP-Ch2.pdf
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    Cookie: __utma=198765611.63021047.1334475645.1334475645.1334475645.1;
        __utmz=198765611.1334475645.1.1.utmcsr=google|utmccn=(organic)|utmcmd=
        organic|utmctr=umass%20amherst
    If-None-Match: "d6c96-173-623cc740"
    If-Modified-Since: Tue, 24 Apr 2012 03:31:01 GMT
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
        file2.html]
```

```
No.     Time        Source                Destination           Protocol
    Length Info
     19 2.743596    128.119.245.12        10.0.1.21             HTTP      738
          HTTP/1.1 200 OK  (text/html)

Frame 19: 738 bytes on wire (5904 bits), 738 bytes captured (5904 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af:71:6
    b (00:22:75:af:71:6b)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
    10.0.1.21 (10.0.1.21)
Transmission Control Protocol, Src Port: http (80), Dst Port: 38102 (38102),
    Seq: 1, Ack: 780, Len: 672
Hypertext Transfer Protocol
    HTTP/1.1 200 OK
    Date: Tue, 24 Apr 2012 03:32:32 GMT
    Server: Apache/2.2.3 (CentOS)
    Last-Modified: Tue, 24 Apr 2012 03:32:02 GMT
    ETag: "d6c96-173-65df9080"
    Accept-Ranges: bytes
    Content-Length: 371
    Keep-Alive: timeout=10, max=100
    Connection: Keep-Alive
    Content-Type: text/html; charset=UTF-8
Line-based text data: text/html
```

```
No.     Time        Source                Destination           Protocol
    Length Info
     24 4.025892    10.0.1.21             128.119.245.12        HTTP      871
            GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 24: 871 bytes on wire (6968 bits), 871 bytes captured (6968 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: AppleCom_c1:5f
    :50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.21 (10.0.1.21), Dst: 128.119.245.12
    (128.119.245.12)
Transmission Control Protocol, Src Port: 38102 (38102), Dst Port: http (80),
    Seq: 1107, Ack: 1183, Len: 805
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    Host: gaia.cs.umass.edu
    Connection: keep-alive
    Cache-Control: max-age=0
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.19 (KHTML,
        like Gecko) Chrome/18.0.1025.162 Safari/535.19
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Referer: http://web.engr.oregonstate.edu/~hamdaoui/teaching/372Spring12/
        labs/WiresharkLab-HTTP-Ch2.pdf
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    Cookie: __utma=198765611.63021047.1334475645.1334475645.1334475645.1;
        __utmz=198765611.1334475645.1.1.utmcsr=google|utmccn=(organic)|utmcmd=
        organic|utmctr=umass%20amherst
    If-None-Match: "d6c96-173-65df9080"
    If-Modified-Since: Tue, 24 Apr 2012 03:32:02 GMT
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
        file2.html]
```

```
No.     Time        Source                Destination           Protocol
    Length Info
     25 4.505268    128.119.245.12        10.0.1.21             HTTP      247
            HTTP/1.1 304 Not Modified

Frame 25: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af:71:6
    b (00:22:75:af:71:6b)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
    10.0.1.21 (10.0.1.21)
Transmission Control Protocol, Src Port: http (80), Dst Port: 38102 (38102),
    Seq: 1183, Ack: 1912, Len: 181
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified
    Date: Tue, 24 Apr 2012 03:32:33 GMT
    Server: Apache/2.2.3 (CentOS)
    Connection: Keep-Alive
    Keep-Alive: timeout=10, max=98
    ETag: "d6c96-173-65df9080"
```

3 Retrieving Long Documents

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

    Answer One HTTP GET request was sent by my browser.

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

    Answer 4 TCP segments were needed to carry the response.

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

    Answer 200 OK

15. **Question** Are there any HTTP status lines in the transmitted data associated with a TCPinduced "Continuation"?

    Answer There are no HTTP status lines in the data associated with "Continuation"

```
No.     Time        Source                Destination           Protocol
    Length Info
     14 0.688831    128.119.245.12        10.0.1.21             HTTP      525
          HTTP/1.1 200 OK  (text/html)

Frame 14: 525 bytes on wire (4200 bits), 525 bytes captured (4200 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af:71:6
    b (00:22:75:af:71:6b)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
    10.0.1.21 (10.0.1.21)
Transmission Control Protocol, Src Port: http (80), Dst Port: 38107 (38107),
    Seq: 4345, Ack: 693, Len: 459
[4 Reassembled TCP Segments (4803 bytes): #8(1448), #10(1448), #12(1448), #14(459)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK
    Date: Tue, 24 Apr 2012 03:35:42 GMT
    Server: Apache/2.2.3 (CentOS)
    Last-Modified: Tue, 24 Apr 2012 03:35:01 GMT
    ETag: "d6c97-1194-708ae340"
    Accept-Ranges: bytes
    Content-Length: 4500
    Keep-Alive: timeout=10, max=100
    Connection: Keep-Alive
    Content-Type: text/html; charset=UTF-8
Line-based text data: text/html
```

4 HTML Documents with Embeded Objects

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

    Answer 3 seperate GET requests were sent by my browser:

    1) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
    2) http://manic.cs.umass.edu/ kurose/cover_5th_ed.jpg
    3) http://www.pearsonhighered.com/assets/hip/us/hip_us_pearson highered/images/pearson_logo.gif

17. **Question** Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

    Answer The two images were downloaded serially. There is a 23 millisecond difference between the GET requests.

```
No.     Time        Source                Destination           Protocol
    Length Info
     21 0.758114    10.0.1.21             165.193.140.14        HTTP      524
        GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif
        HTTP/1.1

Frame 21: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: AppleCom_c1:5f
    :50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.21 (10.0.1.21), Dst: 165.193.140.14
    (165.193.140.14)
Transmission Control Protocol, Src Port: 40928 (40928), Dst Port: http (80),
    Seq: 1, Ack: 1, Len: 458
Hypertext Transfer Protocol
    GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif HTTP/1.1
    Host: www.pearsonhighered.com
    Connection: keep-alive
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.19 (KHTML,
        like Gecko) Chrome/18.0.1025.162 Safari/535.19
    Accept: */*
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    [Full request URI: http://www.pearsonhighered.com/assets/hip/us/
        hip_us_pearsonhighered/images/pearson_logo.gif]
```

```
No.     Time        Source                Destination           Protocol
    Length Info
     34 0.982627    10.0.1.21             128.119.240.90        HTTP      655
        GET /~kurose/cover_5th_ed.jpg HTTP/1.1

Frame 34: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: AppleCom_c1:5f
    :50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.21 (10.0.1.21), Dst: 128.119.240.90
    (128.119.240.90)
Transmission Control Protocol, Src Port: 60965 (60965), Dst Port: http (80),
    Seq: 1, Ack: 1, Len: 589
Hypertext Transfer Protocol
    GET /~kurose/cover_5th_ed.jpg HTTP/1.1
    Host: manic.cs.umass.edu
    Connection: keep-alive
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.19 (KHTML,
        like Gecko) Chrome/18.0.1025.162 Safari/535.19
    Accept: */*
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    Cookie: __utma=198765611.63021047.1334475645.1334475645.1334475645.1;
        __utmz=198765611.1334475645.1.1.utmcsr=google|utmccn=(organic)|utmcmd=
        organic|utmctr=umass%20amherst
    [Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]
```

5 HTTP Authentication

18. **Question** What is the servers response (status code and phrase) in response to the initial HTTP GET message from your browser?

    Answer 401 Authorization Required

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

    Answer The Authorization field. It's value is:
    Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

```
No.     Time        Source                Destination           Protocol
    Length Info
     12 0.376650    128.119.245.12        10.0.1.21             HTTP      839
            HTTP/1.1 401 Authorization Required  (text/html)

Frame 12: 839 bytes on wire (6712 bits), 839 bytes captured (6712 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af:71:6
    b (00:22:75:af:71:6b)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
    10.0.1.21 (10.0.1.21)
Transmission Control Protocol, Src Port: http (80), Dst Port: 38145 (38145),
    Seq: 1, Ack: 708, Len: 773
Hypertext Transfer Protocol
    HTTP/1.1 401 Authorization Required
    Date: Tue, 24 Apr 2012 03:47:24 GMT
    Server: Apache/2.2.3 (CentOS)
    WWW-Authenticate: Basic realm="wireshark-students only"
    Content-Length: 486
    Keep-Alive: timeout=10, max=100
    Connection: Keep-Alive
    Content-Type: text/html; charset=iso-8859-1
Line-based text data: text/html
```

```
No.     Time        Source                Destination           Protocol
   Length Info
    17 5.978273    10.0.1.21             128.119.245.12        HTTP      832
          GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP
       /1.1

Frame 17: 832 bytes on wire (6656 bits), 832 bytes captured (6656 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: AppleCom_c1:5f
   :50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.21 (10.0.1.21), Dst: 128.119.245.12
   (128.119.245.12)
Transmission Control Protocol, Src Port: 38145 (38145), Dst Port: http (80),
   Seq: 708, Ack: 774, Len: 766
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
    Host: gaia.cs.umass.edu
    Connection: keep-alive
    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.19 (KHTML,
       like Gecko) Chrome/18.0.1025.162 Safari/535.19
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Referer: http://web.engr.oregonstate.edu/~hamdaoui/teaching/372Spring12/
       labs/WiresharkLab-HTTP-Ch2.pdf
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    Cookie: __utma=198765611.63021047.1334475645.1334475645.1334475645.1;
       __utmz=198765611.1334475645.1.1.utmcsr=google|utmccn=(organic)|utmcmd=
       organic|utmctr=umass%20amherst
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages
       /HTTP-wiresharkfile5.html]
```