

PART 1

No.	Time	Source	Destination	Protocol	Length	Info
40	1.710261	10.204.51.30	128.119.245.12	HTTP	492	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 40: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: IntelCor_60:1e:36 (70:1c:e7:60:1e:36), Dst: ArubaNet_01:5d:d0 (00:1a:1e:01:5d:d0)
Internet Protocol Version 4, Src: 10.204.51.30, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65432, Dst Port: 80, Seq: 1, Ack: 1, Len: 438
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.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/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-GB,en-US;q=0.9,en;q=0.8\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 42]

No.	Time	Source	Destination	Protocol	Length	Info
42	1.747390	128.119.245.12	10.204.51.30	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 42: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Ethernet II, Src: ArubaNet_01:5d:d0 (00:1a:1e:01:5d:d0), Dst: IntelCor_60:1e:36 (70:1c:e7:60:1e:36)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.204.51.30
Transmission Control Protocol, Src Port: 80, Dst Port: 65432, Seq: 1, Ack: 439, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Tue, 02 Oct 2018 17:36:27 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
[HTTP response 1/1]
[Time since request: 0.037129000 seconds]
[Request in frame: 40]
File Data: 128 bytes
Line-based text data: text/html (4 lines)

7. No, I do not see any headers within the data that are not listed.

PART 2

Host: gaia.cs.umass.edu User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1 Accept-Language: en-us,en;q=0.50 Accept-Encoding: gzip, deflate, compress;q=0.9 Accept-Charset: ISO-8859-1, utf-8;q=0.66,*/*;q=0.66 Keep-Alive: 300 Connection: keep-alive	8 There is no IF-MODIFIED-SINCE in this initial GET
Date: Tue, 23 Sep 2003 05:35:50 GMT Server: Apache/2.0.40 (Red Hat Linux) Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT ETag: "1bfef-173-8f4ae900" Accept-Ranges: bytes Content-Length: 371 Keep-Alive: timeout=10, max=100 Connection: Keep-Alive Content-Type: text/html; charset=ISO-8859-1	9 Text from response to initial GET
<html>Congratulations again! Now you've downloaded the file lab2-2.html. This file's last modification date will not change. <p>Thus if you download t	
Host: gaia.cs.umass.edu User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1 Accept-Language: en-us,en;q=0.50 Accept-Encoding: gzip, deflate, compress;q=0.9 Accept-Charset: ISO-8859-1, utf-8;q=0.66,*/*;q=0.66 Keep-Alive: 300 Connection: keep-alive	10 Next GET has IF-MODIFIED-SINCE
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT If-None-Match: "1bfef-173-8f4ae900" Cache-Control: max-age=0	11 Has not been modified, so text is not returned
HTTP/1.1 304 Not Modified	

PART 3

Wireshark capture showing HTTP traffic. The packet list shows several packets, with packet 20 being a GET request. The packet details pane shows the full request URI and other headers.

No.	Time	Source	Destination	Protocol	Length	Info
20	0.969013	192.168.1.154	54.243.128.120	HTTP	596	GET /client.cgi/unblocking_rate?rmt_ver=1.108.99&ext_ver=1.108.99&...
21	1.000142	192.168.1.154	230.0.0.1	UDP	92	51715 → 6666 Len=50
22	1.017640	54.243.128.120	192.168.1.154	TCP	60	80 → 56394 [ACK] Seq=1 Ack=543 Win=28032 Len=0
23	1.017641	54.243.128.120	192.168.1.154	TCP	1514	80 → 56394 [ACK] Seq=1 Ack=543 Win=28032 Len=1460 [TCP segment of...]
24	1.017641	54.243.128.120	192.168.1.154	TCP	1514	80 → 56394 [ACK] Seq=1461 Ack=543 Win=28032 Len=1460 [TCP segment...]
25	1.017643	54.243.128.120	192.168.1.154	TCP	1514	80 → 56394 [ACK] Seq=2921 Ack=543 Win=28032 Len=1460 [TCP segment...]
26	1.017745	192.168.1.154	54.243.128.120	TCP	54	56394 → 80 [ACK] Seq=543 Ack=4381 Win=17408 Len=0
27	1.018226	54.243.128.120	192.168.1.154	TCP	1514	80 → 56394 [ACK] Seq=4381 Ack=543 Win=28032 Len=1460 [TCP segment...]
28	1.018226	54.243.128.120	192.168.1.154	HTTP	1097	HTTP/1.1 200 OK (application/json)

Hypertext Transfer Protocol
 GET /client.cgi/unblocking_rate?rmt_ver=1.108.99&ext_ver=1.108.99&browser=chrome&product=cws&lccgi=1&src_country=ca&limit=200 HTTP/1.1\r\n
 Host: client.hola.org\r\n
 Connection: keep-alive\r\n
 Accept: application/json, text/javascript, */*; q=0.01\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
 Cookie: uuid=87fa114e13977a1e76ec9b2b37724603\r\n
 If-None-Match: W/"19d6-YA+2m8gPDsqSx+zt0kPQw"\r\n
 \r\n
 [Full request URI: http://client.hola.org/client.cgi/unblocking_rate?rmt_ver=1.108.99&ext_ver=1.108.99&browser=chrome&product=cws&lccgi=1&src...]
 [HTTP request 1/1]
 [Response in frame: 28]

12. There is 1 GET message numbered Packet 20.
13. Packet 23.
14. 200 (OK).
15. 4 (Packets 23, 24, 25, 27).

PART 4

Wireshark capture showing HTTP traffic. The packet list shows several packets, with packet 13 being a GET request. The packet details pane shows the full request URI and other headers.

No.	Time	Source	Destination	Protocol	Length	Info
13	2.934975	192.168.1.154	128.119.245.12	HTTP	492	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
15	2.969077	128.119.245.12	192.168.1.154	HTTP	1127	HTTP/1.1 200 OK (text/html)
16	2.986330	192.168.1.154	128.119.245.12	HTTP	463	GET /pearson.png HTTP/1.1
20	3.019448	128.119.245.12	192.168.1.154	HTTP	745	HTTP/1.1 200 OK (PNG)
24	3.020999	192.168.1.154	128.119.245.12	HTTP	477	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
115	3.193065	128.119.245.12	192.168.1.154	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

Hypertext Transfer Protocol
 GET /wireshark-labs/HTTP-wireshark-file4.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/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-GB,en-US;q=0.9,en;q=0.8\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
 [HTTP request 1/2]
 [Response in frame: 15]
 [Next request in frame: 16]

16. There were 3 GET messages all sent to the IP address 128.119.245.12.
17. The two images were downloaded serially, seen by the .png packet request and response being packets 16 and 20, whereas the .jpg pack request and response being packets 24 and 115. Since the response to the .png request came before the .jpg request, I can see that they were done serially.

PART 5

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
3	0.470278	81.161.59.128	10.204.51.30	HTTP	333	HTTP/1.1 200 OK (application/json)
4	0.470914	10.204.51.30	81.161.59.128	HTTP	149	GET /poll?push_id=d277e8a1-41f0-4b73-b11b-5803f5b83f87 HTTP/1.1
14	1.515906	10.204.51.30	128.119.245.12	HTTP	508	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
16	1.551796	128.119.245.12	10.204.51.30	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
40	9.960251	10.204.51.30	128.119.245.12	HTTP	567	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
43	9.998130	128.119.245.12	10.204.51.30	HTTP	544	HTTP/1.1 200 OK (text/html)
53	12.656230	81.161.59.89	10.204.51.30	HTTP	333	[TCP Previous segment not captured] HTTP/1.1 200 OK (application/json)
54	12.656231	81.161.59.89	10.204.51.30	HTTP	333	[TCP Previous segment not captured] HTTP/1.1 200 OK (application/json)
55	12.656546	10.204.51.30	81.161.59.89	HTTP	149	[TCP ACKed unseen segment] GET /poll?push_id=b020a454-f80e-4cb0-9395-80c
56	12.656682	10.204.51.30	81.161.59.89	HTTP	149	[TCP ACKed unseen segment] GET /poll?push_id=7412f270-e941-44de-a5de-dc8

GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Authorization: Basic dWlyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcm0=\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/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-GB,en-US;q=0.9,en;q=0.8\r\n

\r\n

18. Packet 14 contains the first GET and packet 16 contains the response, which is “401 Unauthorized.”
19. The following GET includes Authorization: Basic.