

## Wireshark Lab 2

Jennifer Hurst

My IP address is shown below, 192.168.1.17 in this terminal screen shot.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
283	13:46:24.447071	192.168.1.17	128.119.245.12	HTTP	564	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
285	13:46:24.477066	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1118	13:48:19.525749	192.168.1.17	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1121	13:48:19.555170	128.119.245.12	192.168.1.17	HTTP	440	HTTP/1.1 200 OK (text/html)
1123	13:48:19.611393	192.168.1.17	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
1129	13:48:19.640120	128.119.245.12	192.168.1.17	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1147	13:48:19.692882	192.168.1.17	72.21.91.29	OCSP	506	Request
1150	13:48:19.710713	72.21.91.29	192.168.1.17	OCSP	842	Response

The packet details pane for the selected packet (1121) shows the following structure:

- Frame 1121: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
- Ethernet II, Src: Netgear\_bd:73:8c (50:6a:03:bd:73:8c), Dst: WistronI\_7e:38:bb (98:ee:cb:7e:38:bb)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.17
- Transmission Control Protocol, Src Port: 80, Dst Port: 55949, Seq: 1, Ack: 379, Len: 486
- Hypertext Transfer Protocol
- Line-based text data: text/html (4 lines)

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

1. Is your browser running HTTP version 1.0 or 1.1? My browser is running HTTP 1.1

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
283	13:46:24.447071	192.168.1.17	128.119.245.12	HTTP	564	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
285	13:46:24.477066	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1118	13:48:19.525749	192.168.1.17	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1121	13:48:19.555170	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1123	13:48:19.611393	192.168.1.17	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
1129	13:48:19.640120	128.119.245.12	192.168.1.17	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1147	13:48:19.692882	192.168.1.17	72.21.91.29	OCSP	506	Request
1150	13:48:19.710713	72.21.91.29	192.168.1.17	OCSP	842	Response

> Frame 1121: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0  
 > Ethernet II, Src: Netgear\_bd:73:8c (50:6a:03:bd:73:8c), Dst: WistronI\_7e:38:bb (98:ee:cb:7e:38:bb)  
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.17  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 55949, Seq: 1, Ack: 379, Len: 486  
 > Hypertext Transfer Protocol  
 > Line-based text data: text/html (4 lines)

0060 3a 34 38 3a 31 38 20 47 4d 54 0d 0a 53 65 72 76 :48:18 G MT--Serv  
 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6  
 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS  
 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH  
 00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod\_per  
 00b0 6c 2f 32 2e 30 2e 31 30 20 50 65 72 6c 2f 70 35 1.0.0-rc2-2/v5  
 00c0 2e 31 36 2e 33 0d 0a 6c 61 73 74 2d 4d 6f 64 69 16.3 Last-Modi  
 00d0 66 69 65 64 3a 20 53 61 74 2c 20 30 39 20 46 6f fied: Sa t, 09 Fe  
 00e0 62 20 32 30 31 39 20 30 36 3a 35 39 3a 30 31 20 b 2019.0 6:59:01  
 00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 35 Get-Data g: 500-5  
 0100 38 31 37 30 39 63 34 39 33 66 38 66 22 0d 0a 41 81709c49 3f8f--A  
 0110 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by  
 0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tes: Con tent-Len

Bytes 199-244: Last-Modified (http.last\_modified)

Packets: 1226 · Displayed: 8 (0.7%) · Dropped: 0 (0.0%) Profile: Default

1:49 PM 2/9/2019

2. When was the HTML file that you are retrieving last modified at the server? Sat, Feb 9, 2019, 6:59:01 GMT was the last modified date.

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
283	13:46:24.447071	192.168.1.17	128.119.245.12	HTTP	564	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
285	13:46:24.477066	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1118	13:48:19.525749	192.168.1.17	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1121	13:48:19.555170	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1123	13:48:19.611393	192.168.1.17	128.119.245.12	HTTP	373	GET /Favicon.ico HTTP/1.1
1129	13:48:19.640120	128.119.245.12	192.168.1.17	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1147	13:48:19.692882	192.168.1.17	72.21.91.29	OCSP	506	Request
1150	13:48:19.710713	72.21.91.29	192.168.1.17	OCSP	842	Response

> Frame 1118: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface 0  
 > Ethernet II, Src: WistronI\_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear\_bd:73:8c (50:6a:03:bd:73:8c)  
 > Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12  
 > Transmission Control Protocol, Src Port: 55949, Dst Port: 80, Seq: 1, Ack: 1, Len: 378  
 > Hypertext Transfer Protocol

0000 50 6a 03 bd 73 8c 98 ee cb 7e 38 bb 08 00 45 00 Pj...s...w8...E-  
 0010 01 a2 50 33 40 00 00 06 00 00 c0 a8 01 11 80 77 .P3@... ..w  
 0020 f5 0c da 8d 00 50 1a 0a a8 62 28 81 4d 5c 50 18 ....P...b(MVP-  
 0030 01 00 38 d2 00 00 47 45 54 20 2f 77 69 72 65 73 --8--GE T /wires  
 0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w  
 0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h  
 0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1: Ho  
 0070 73 74 3a 20 6f 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umass  
 0080 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e s.edu:U ser-Agen  
 0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozill la/5.0 (  
 00a0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;  
 00b0 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a Win64; x64; rv:  
 00c0 36 35 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 65.0) Ge cko/2010

wireshark\_42D18FF7-A89E-499A-98FC-6A16F8718B12\_20190209134607\_a09816.pcapng

Packets: 1226 · Displayed: 8 (0.7%) · Dropped: 0 (0.0%) Profile: Default

1:51 PM 2/9/2019

3. What is the IP address of the gaia.cs.umass.edu server? 128.119.045.12

Wireshark capture of HTTP traffic. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the HTTP request structure, including the Accept-Language header.

No.	Time	Source	Destination	Protocol	Length	Info
283	13:46:24.447071	192.168.1.17	128.119.245.12	HTTP	564	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
285	13:46:24.477066	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1118	13:48:19.525749	192.168.1.17	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1121	13:48:19.555170	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1123	13:48:19.611393	192.168.1.17	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
1129	13:48:19.640120	128.119.245.12	192.168.1.17	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1147	13:48:19.692882	192.168.1.17	72.21.91.29	OCSP	506	Request
1150	13:48:19.710713	72.21.91.29	192.168.1.17	OCSP	842	Response

Frame 1118: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface 0  
 Ethernet II, Src: WistronI\_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear\_bd:73:8c (50:6a:03:bd:73:8c)  
 Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12  
 Transmission Control Protocol, Src Port: 55949, Dst Port: 80, Seq: 1, Ack: 1, Len: 378  
 Hypertext Transfer Protocol

0000 36 35 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 65.0) Ge cko/2010  
 0010 30 31 30 31 20 46 69 72 65 66 6f 78 2f 36 35 2e 0101 Fir efox/65.  
 0020 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 0 -Accept t: text/  
 0030 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e html,app lication  
 0040 2f 70 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 /xhtml+xml,appli  
 0050 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 cation/x ml;q=0.9  
 0060 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b -image/\*;q=0.8  
 0070 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8 -Accept-L  
 0080 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e language: en-US,en  
 0090 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5 -Accept-E  
 0100 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 6d ncoding: gzip, d  
 0110 65 66 6c 61 74 65 0d 0a 43 6f 6e 65 63 74 69 erlate connecti  
 0120 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep-alive..

4. What languages does your browser indicate that it can accept to the server? En for English

Wireshark capture of HTTP traffic. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the HTTP request structure, including the Date header.

No.	Time	Source	Destination	Protocol	Length	Info
283	13:46:24.447071	192.168.1.17	128.119.245.12	HTTP	564	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
285	13:46:24.477066	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1118	13:48:19.525749	192.168.1.17	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1121	13:48:19.555170	128.119.245.12	192.168.1.17	HTTP	540	HTTP/1.1 200 OK (text/html)
1123	13:48:19.611393	192.168.1.17	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
1129	13:48:19.640120	128.119.245.12	192.168.1.17	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1147	13:48:19.692882	192.168.1.17	72.21.91.29	OCSP	506	Request
1150	13:48:19.710713	72.21.91.29	192.168.1.17	OCSP	842	Response

Frame 1121: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0  
 Ethernet II, Src: Netgear\_bd:73:8c (50:6a:03:bd:73:8c), Dst: WistronI\_7e:38:bb (98:ee:cb:7e:38:bb)  
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.17  
 Transmission Control Protocol, Src Port: 80, Dst Port: 55949, Seq: 1, Ack: 379, Len: 486  
 Hypertext Transfer Protocol  
 Line-based text data: text/html (4 lines)

0000 98 ee cb 7e 38 bb 50 6a 03 bd 73 8c 08 00 45 20 ---8-Pj s---E  
 0010 02 0e fd 18 40 00 31 06 13 74 80 77 f5 0c c0 a8 ---@1 t w  
 0020 01 11 00 50 da 6d 28 01 4d 5c 1a 0a a9 dc 50 18 ---@1 t w  
 0030 00 ed 2c 16 00 00 48 54 54 50 2f 31 2e 31 20 20 ---HT P/1.1 2  
 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 6f 74 00 OK-ate: Sat  
 0050 2c 20 30 39 20 46 65 62 20 32 30 31 39 20 31 38 , 09 Feb 2019 18  
 0060 3a 34 38 3a 31 38 20 47 4d 54 0d 0a 53 65 72 76 :48:18 G MT- Serv  
 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 -t: Apac he/2.4.6  
 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS  
 0090 4c 2f 31 2e 30 2e 32 0b 2d 66 69 70 73 20 50 48 /1.0.2k -fips PH  
 00a0 50 2f 35 2a 3a 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod\_per  
 00b0 6c 2f 32 2e 30 2e 31 30 20 50 65 72 6c 2f 76 35 1/2.0.10 Perl/v5  
 00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3 -L ast-Modi

5. When was the HTML file that you are retrieving created at the server? The file appears to have been created today, Feb 9, 2019.

Screen shot of my Print message from the http OK

The screenshot shows the Wireshark network protocol analyzer interface. The main window displays a packet capture of an HTTP transaction. The packet list shows four packets: an OCSP request, an OCSP response, an HTTP GET request, and an HTTP 200 OK response. The packet details pane shows the structure of the selected HTTP 200 OK response, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw data of the selected packet.

A 'Wireshark - Print' dialog box is open, displaying the following options:

- Packet Format:**
  - ☒ Summary line
  - ☒ Include column headings
  - ☒ Details:
    - ☐ All collapsed
    - ☒ As displayed
    - ☐ All expanded
  - ☐ Bytes
  - ☐ Print each packet on a new page
- Packet Range:**
  - ☐ Captured
  - ☒ Displayed
  - ☐ All packets
  - ☒ Selected packets only
  - ☐ Marked packets only
  - ☐ First to last marked
  - ☐ Range: [ ]
  - ☐ Remove ignored packets
- Page Setup...** **Print...** **Cancel** **Help**

The status bar at the bottom indicates 'Packets: 2109 · Displayed: 4 (0.2%)' and 'Profile: Default'.