

My IP address is 192.168.200.8

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows a packet from 128.119.245.12 to 192.168.200.8, which is highlighted in green. The packet details pane shows the following structure:

- Ethernet II, Src: Verizon_d0:13:e4 (20:c0:47:d0:13:e4), Dst: Intelcom_47:b8:32 (ac:ed:5c:47:b8:32)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.200.8
- TCP, Src Port: 80, Dst Port: 53130, Seq: 1, Ack: 312, Len: 486
- Hypertext Transfer Protocol (http), 358 bytes

The packet bytes pane shows the raw data of the HTTP response, starting with the status line: 200 OK (text/html).

Question 1: My Computer is running HTTP version 1.1

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
671	2019-02-10 11:56:02.134765	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1743	2019-02-10 11:57:17.111554	192.168.200.8	54.236.65.67	HTTP	712	GET /ping?h=en-us.msn.com&p=X2Fen-us&u=Bq8jA0p-sMYCejjKY&d=msn.com&g=42635&g0=homepage&g1=No%20Author&n=0&f=f0045&c
1745	2019-02-10 11:57:17.127106	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1946	2019-02-10 11:57:48.912527	192.168.200.8	128.119.245.12	HTTP	365	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1954	2019-02-10 11:57:48.951707	128.119.245.12	192.168.200.8	HTTP	540	HTTP/1.1 200 OK (text/html)
1968	2019-02-10 11:57:48.970468	192.168.200.8	40.114.54.223	HTTP	1410	GET /c.gif?rid=5201f9013d254db2b6150cca80c2388c&cts=1549817868956&idx=7&clid=3C73453A16A763490C594E7917786254&issc
1971	2019-02-10 11:57:48.984273	40.114.54.223	192.168.200.8	HTTP	582	HTTP/1.1 200 OK (GIF89a)
2092	2019-02-10 11:57:49.164712	77.234.42.247	192.168.200.8	HTTP	234	HTTP/1.1 200 OK
2093	2019-02-10 11:57:49.167070	192.168.200.8	77.234.42.247	HTTP	356	GET /R/A3gKIDdjZjHjYk3YmQ3ZjQ2NDc4ZWEhMDgyZjkZ2ZjAXNTHpYegQGCQIZGN8C1gECKgcIBBDd6Y7rKgcIAXC05KpqMgo1ABCQ7I7rGIACIOIY
2113	2019-02-10 11:57:49.187219	192.168.200.8	128.119.245.12	HTTP	287	GET /favicon.ico HTTP/1.1
2124	2019-02-10 11:57:49.207385	128.119.245.12	192.168.200.8	HTTP	539	HTTP/1.1 404 Not Found (text/html)

[Time since first frame in this TCP stream: 0.058050000 seconds]
[Time since previous frame in this TCP stream: 0.039180000 seconds]
TCP payload (486 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 10 Feb 2019 16:57:52 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n

Etag: "80-58184ba1f23f8"\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

ac ed 5c 47 b8 32 20 c0 47 d0 13 e4 08 00 45 20 ..\G-2..G.....E
02 0e c8 29 40 00 35 06 7d 6b 80 77 f5 0c c0 a8 ...@5:}k-w....
c8 08 00 50 cf 8a 34 c0 3a 23 94 5a a6 7c 50 18 ...P.:#-Z|P-
00 ed a3 5d 00 00 48 54 50 2f 31 2e 31 20 32 ...]HT TP/1.1 2
30 30 20 4f 4b 0d 0a 41 61 74 65 3a 20 53 75 6e 00 OK: Date: Sun
2c 20 31 30 20 46 65 62 20 32 30 31 39 20 31 36 , 10 Feb 2019 16
3a 35 37 3a 35 32 20 47 4d 54 0d 0a 53 65 72 76 :57:52 GMT- Serv
65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0800 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 76 35 l/2.0.10 Perl/v5
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3: Last-Modi
00d0 66 69 65 64 3a 20 53 75 6e 2c 20 31 30 20 46 65 fied: Su n, 10 Fe

Wireshark_87882E4A-E8B8-48D4-B0F8-13707C3D83D8_20190210115541_a17308.pcapng

Packets: 2164 · Displayed: 40 (1.8%) · Dropped: 0 (0.0%)

Profile: Default

12:10 PM
2/10/2019

Question 2: HTML file that I am retrieving was last-modified: Sun, 10 Feb 2019 06:59:01 GMT\r\n

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
671	2019-02-10 11:56:02.134765	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1743	2019-02-10 11:57:17.111554	192.168.200.8	54.236.65.67	HTTP	712	GET /ping?h=en-us.msn.com&p=X2Fen-us&u=Bq8jA0p-sMYCejjKY&d=msn.com&g=42635&g0=homepage&g1=No%20Author&n=0&f=f0045&c
1745	2019-02-10 11:57:17.127106	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1946	2019-02-10 11:57:48.912527	192.168.200.8	128.119.245.12	HTTP	365	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1954	2019-02-10 11:57:48.951707	128.119.245.12	192.168.200.8	HTTP	540	HTTP/1.1 200 OK (text/html)
1968	2019-02-10 11:57:48.970468	192.168.200.8	40.114.54.223	HTTP	1410	GET /c.gif?rid=5201f9013d254db2b6150cca80c2388c&cts=1549817868956&idx=7&clid=3C73453A16A763490C594E7917786254&issc
1971	2019-02-10 11:57:48.984273	40.114.54.223	192.168.200.8	HTTP	582	HTTP/1.1 200 OK (GIF89a)
2092	2019-02-10 11:57:49.164712	77.234.42.247	192.168.200.8	HTTP	234	HTTP/1.1 200 OK
2093	2019-02-10 11:57:49.167070	192.168.200.8	77.234.42.247	HTTP	356	GET /R/A3gKIDdjZjHjYk3YmQ3ZjQ2NDc4ZWEhMDgyZjkZ2ZjAXNTHpYegQGCQIZGN8C1gECKgcIBBDd6Y7rKgcIAXC05KpqMgo1ABCQ7I7rGIACIOIY
2113	2019-02-10 11:57:49.187219	192.168.200.8	128.119.245.12	HTTP	287	GET /favicon.ico HTTP/1.1
2124	2019-02-10 11:57:49.207385	128.119.245.12	192.168.200.8	HTTP	539	HTTP/1.1 404 Not Found (text/html)

[Time since first frame in this TCP stream: 0.058050000 seconds]
[Time since previous frame in this TCP stream: 0.039180000 seconds]
TCP payload (486 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 10 Feb 2019 16:57:52 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n

Etag: "80-58184ba1f23f8"\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

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3: Last-Modi
00d0 66 69 65 64 3a 20 53 75 6e 2c 20 31 30 20 46 65 fied: Su n, 10 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 GMT: Etag g: "80-5
0100 38 31 38 34 62 61 31 66 32 33 66 38 22 0d 0a 41 8184ba1f 23f8".A
0110 63 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 4d 65 6e tes: Con tent-Len
0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 gth: 128 .-Keep-A
0140 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c live: ti meout=5,
0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 max=100 .-Connec
0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0170 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 .-Conten t-Type:
0180 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 text/htm l; chars
0190 65 74 3d 55 54 6d 2d 38 0d 0a 0d 0a 3c 68 74 6d et=UTF-8chtm

HTTP Last Modified (http.last_modified), 46 bytes

Packets: 2164 · Displayed: 40 (1.8%) · Dropped: 0 (0.0%)

Profile: Default

12:10 PM
2/10/2019

Question 3: The IP address of gaia.cs.umass.edu server is 128.119.245.12

The image shows a Wireshark packet capture of an HTTP session. The packet list pane at the top shows several HTTP packets. Packet 1954 is highlighted, showing a GET request from source IP 128.119.245.12 to destination IP 192.168.200.8. The packet details pane below shows the structure of this packet: Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The IP address 128.119.245.12 is circled in green in the packet details pane. The packet bytes pane at the bottom shows the raw data of the packet, with the first few bytes highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
637	2019-02-10 11:55:54.010632	65.202.184.107	192.168.200.8	HTTP	350	HTTP/1.1 200 OK (JPEG JFIF image)
670	2019-02-10 11:56:02.098580	192.168.200.8	54.236.65.67	HTTP	714	GET /ping?h=en-us.msn.com&p=%2Fen-us&u=Bq8jA0p-sMYCejjKY&d=msn.com&g=42635&g0=homepage&g1=No%20Author&n=0&f=f0045&c
671	2019-02-10 11:56:02.134765	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1743	2019-02-10 11:57:17.111554	192.168.200.8	54.236.65.67	HTTP	712	GET /ping?h=en-us.msn.com&p=%2Fen-us&u=Bq8jA0p-sMYCejjKY&d=msn.com&g=42635&g0=homepage&g1=No%20Author&n=0&f=f0045&c
1745	2019-02-10 11:57:17.127106	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1946	2019-02-10 11:57:48.912527	192.168.200.8	128.119.245.12	HTTP	365	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1954	2019-02-10 11:57:48.951707	128.119.245.12	192.168.200.8	HTTP	540	HTTP/1.1 200 OK (text/html)
1968	2019-02-10 11:57:48.970468	192.168.200.8	40.114.54.223	HTTP	1410	GET /c.gif?rid=5201f9013d254db2b6150cca80c2388c&cts=1549817868956&idx=7&clid=3C73453A16A763490C594E79177B6254&issc
1971	2019-02-10 11:57:48.984273	40.114.54.223	192.168.200.8	HTTP	582	HTTP/1.1 200 OK (GIF89a)
2092	2019-02-10 11:57:49.164712	77.234.42.247	192.168.200.8	HTTP	234	HTTP/1.1 200 OK
2093	2019-02-10 11:57:49.167070	192.168.200.8	77.234.42.247	HTTP	356	GET /R/A3gKIDdjZjhyjk3YmQ3JQ2NDc4ZWEhMDgyZjk2ZjAxNTIyEgQGCQIZGN8CIgECKgcIBBd6Y3rKgcIAXCD5KpQmgoIABCO7I7rGIAC01OY

Packet 1954 details:

- Ethernet II, Src: Verizon_d0:13:e4:20:c0:42:d0:13:e4, Dst: IntelCor_47:b8:32 (ac:ed:5c:47:b8:32)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.200.8
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 - Total Length: 526
 - Identification: 0xc829 (51241)
 - > Flags: 0x4000, Don't fragment
 - Time to live: 53
 - Protocol: TCP (6)
 - Header checksum: 0x7d6b [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 128.119.245.12
 - Destination: 192.168.200.8
- Transmission Control Protocol, Src Port: 80, Dst Port: 53130, Seq: 1, Ack: 312, Len: 486
- Hypertext Transfer Protocol (http), 358 bytes

Question 4: It accepts en-US\r\n language

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
671	2019-02-10 11:56:02.134765	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1743	2019-02-10 11:57:17.111554	192.168.200.8	54.236.65.67	HTTP	712	GET /ping?h=en-us.msn.com&p=%2Fen-us&u=Bq8jA0p-sMYCejjKY&d=msn.com&g=42635&g0=homepage&g1=No%20Author&n=0&f=f0045&c
1745	2019-02-10 11:57:17.127106	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1946	2019-02-10 11:57:48.912527	192.168.200.8	128.119.245.12	HTTP	365	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1954	2019-02-10 11:57:48.951707	128.119.245.12	192.168.200.8	HTTP	540	HTTP/1.1 200 OK (text/html)
1968	2019-02-10 11:57:48.970468	192.168.200.8	40.114.54.223	HTTP	1410	GET /c.gif?rid=5201f9013d254db2b6150cca80c2388c&cts=1549817868956&idx=7&clid=3C73453A16A763490C594E7917786254&issc
1971	2019-02-10 11:57:48.984273	40.114.54.223	192.168.200.8	HTTP	582	HTTP/1.1 200 OK (GIF89a)
2092	2019-02-10 11:57:49.164712	77.234.42.247	192.168.200.8	HTTP	234	HTTP/1.1 200 OK
2093	2019-02-10 11:57:49.167070	192.168.200.8	77.234.42.247	HTTP	356	GET /R/A3gKIDdjZjHjYjk3YmQ3ZjQ2NDc4ZWExMDgyZjk2ZjAxNTMyEgQGCQIZGN8CIgECKgcIBBDd6YjrKgcIAXCD5KpqMgoIABCQ7Ij-rGIACIOY
2113	2019-02-10 11:57:49.187219	192.168.200.8	128.119.245.12	HTTP	287	GET /favicon.ico HTTP/1.1
2124	2019-02-10 11:57:49.207385	128.119.245.12	192.168.200.8	HTTP	539	HTTP/1.1 404 Not Found (text/html)

[Time since previous frame in this TCP stream: 0.000768000 seconds]

TCP payload (311 bytes)

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

Accept: text/html,application/xhtml+xml,image/jxr,*/*\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

Host: gaia.cs.umass.edu\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]

0090 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 ml+xml, image/jx

00a0 72 2c 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c r, /*... Accept-L

00b0 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 0d 0a language: en-US...

00c0 55 73 65 72 2d 41 67 65 6e 7a 3a 20 4d 6f 7a 69 User-Age nt: Mozil

00d0 6c 6c 61 2f 35 2e 30 20 20 57 69 6e 64 6f 77 78 illz/5.0 (Windows

00e0 20 4e 54 20 31 30 2e 30 3b 20 57 4f 57 36 34 3b NT 10.0 ; WOW64;

00f0 20 54 72 69 64 65 6e 7a 2f 37 2e 30 3b 20 54 6f Trident (7.0; To

0100 75 63 68 3b 20 72 76 3a 31 31 2e 30 29 20 6e 6e uch; rv:11.0) li

0110 6b 65 29 47 65 63 6b 6f 0d 0a 41 63 63 65 70 74 ke Gecko ..Accept

0120 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,

0130 20 64 65 66 6e 61 74 65 0d 0a 48 6f 73 74 3a 20 deflate ..Host:

0140 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed

0150 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b u--Conne ction: K

0160 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a eep-Aliv e....

HTTP Accept Language (http.accept_language), 24 bytes

Packets: 2164 · Displayed: 40 (1.8%) · Dropped: 0 (0.0%)

Profile: Default

12:09 PM 2/10/2019

Question 5: HTML file was created : Sun, 10 Feb 2019 16:57:52 GMT\r\n

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
671	2019-02-10 11:56:02.134765	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1743	2019-02-10 11:57:17.111554	192.168.200.8	54.236.65.67	HTTP	712	GET /ping?h=en-us.msn.com&p=%2Fen-us&u=Bq8jA0p-sMYCejjKY&d=msn.com&g=42635&g0=homepage&g1=No%20Author&n=0&f=f0045&c
1745	2019-02-10 11:57:17.127106	54.236.65.67	192.168.200.8	HTTP	304	HTTP/1.1 200 OK (GIF89a)
1946	2019-02-10 11:57:48.912527	192.168.200.8	128.119.245.12	HTTP	365	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1954	2019-02-10 11:57:48.951707	128.119.245.12	192.168.200.8	HTTP	540	HTTP/1.1 200 OK (text/html)
1968	2019-02-10 11:57:48.970468	192.168.200.8	40.114.54.223	HTTP	1410	GET /c.gif?rid=5201f9013d254db2b6150cca80c2388c&cts=1549817868956&idx=7&clid=3C73453A16A763490C594E7917786254&issc
1971	2019-02-10 11:57:48.984273	40.114.54.223	192.168.200.8	HTTP	582	HTTP/1.1 200 OK (GIF89a)
2092	2019-02-10 11:57:49.164712	77.234.42.247	192.168.200.8	HTTP	234	HTTP/1.1 200 OK
2093	2019-02-10 11:57:49.167070	192.168.200.8	77.234.42.247	HTTP	356	GET /R/A3gKIDdjZjHjYjk3YmQ3ZjQ2NDc4ZWExMDgyZjk2ZjAxNTMyEgQGCQIZGN8CIgECKgcIBBDd6YjrKgcIAXCD5KpqMgoIABCQ7Ij-rGIACIOY
2113	2019-02-10 11:57:49.187219	192.168.200.8	128.119.245.12	HTTP	287	GET /favicon.ico HTTP/1.1
2124	2019-02-10 11:57:49.207385	128.119.245.12	192.168.200.8	HTTP	539	HTTP/1.1 404 Not Found (text/html)

[Time since previous frame in this TCP stream: 0.039180000 seconds]

TCP payload (486 bytes)

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: Sun, 10 Feb 2019 16:57:52 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n

ETag: "80-58184baf23f8"\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: 0.039180000 seconds]

[Request in frame: 1946]

File Data: 128 bytes

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 75 6e 00 OK..Date: Sun

0050 2c 20 31 30 20 40 65 62 20 32 30 31 30 20 31 36 , 10 Feb 2019 16

0060 6a 35 37 20 35 32 20 47 4d 54 0d 0a 53 65 72 76 16:57:52 GMT. Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6

HTTP Date (http.date), 37 bytes

Packets: 2164 · Displayed: 40 (1.8%) · Dropped: 0 (0.0%)

Profile: Default

12:23 PM 2/10/2019

HTTP OK PRINT is attached separately. Thank you.