Chris Bamci

CS436

11/14/17

Wireshark Lab

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
2. Internet protocol
3. Transmission control protocol
4. Hypertext transfer protocol
5. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

5.878581 seconds

1. What is the Internet address of the gaia.cs.umass.edu (also known as www- net.cs.umass.edu)? What is the Internet address of your computer?

128.119.245.12 = www-net.cs.umass.edu

192.168.0.7 = my computer

1. Print the two HTTP messages (GET and OK) referred to in question 2 above.

(GET)

62 5.878581 192.168.0.7 128.119.245.12 HTTP 592 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 62: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits) on interface 0

Ethernet II, Src: GemtekTe\_4a:b8:17 (20:10:7a:4a:b8:17), Dst: ArrisGro\_ed:d2:27 (90:1a:ca:ed:d2:27)

Internet Protocol Version 4, Src: 192.168.0.7, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 2515, Dst Port: 80, Seq: 1, Ack: 1, Len: 538

Hypertext Transfer Protocol

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

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

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36\r\n

Upgrade-Insecure-Requests: 1\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=0.8\r\n

If-None-Match: "51-55e0009d96c54"\r\n

If-Modified-Since: Wed, 15 Nov 2017 06:59:01 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 64]

--------------------------------------------------------------------------------------------------

(OK)

64 6.046243 128.119.245.12 192.168.0.7 HTTP 293 HTTP/1.1 304 Not Modified

Frame 64: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0

Ethernet II, Src: ArrisGro\_ed:d2:27 (90:1a:ca:ed:d2:27), Dst: GemtekTe\_4a:b8:17 (20:10:7a:4a:b8:17)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.7

Transmission Control Protocol, Src Port: 80, Dst Port: 2515, Seq: 1, Ack: 539, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Thu, 16 Nov 2017 03:34:33 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=100\r\n

ETag: "51-55e0009d96c54"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.167662000 seconds]

[Request in frame: 62]