Wireshark Lab #1

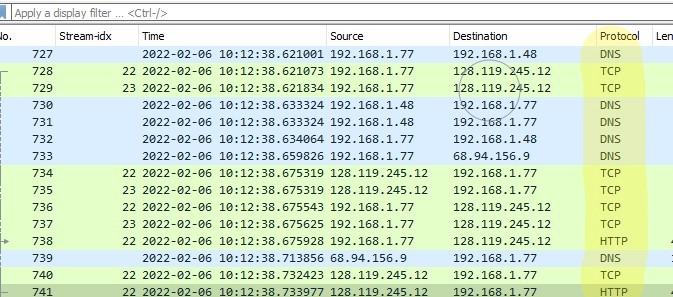
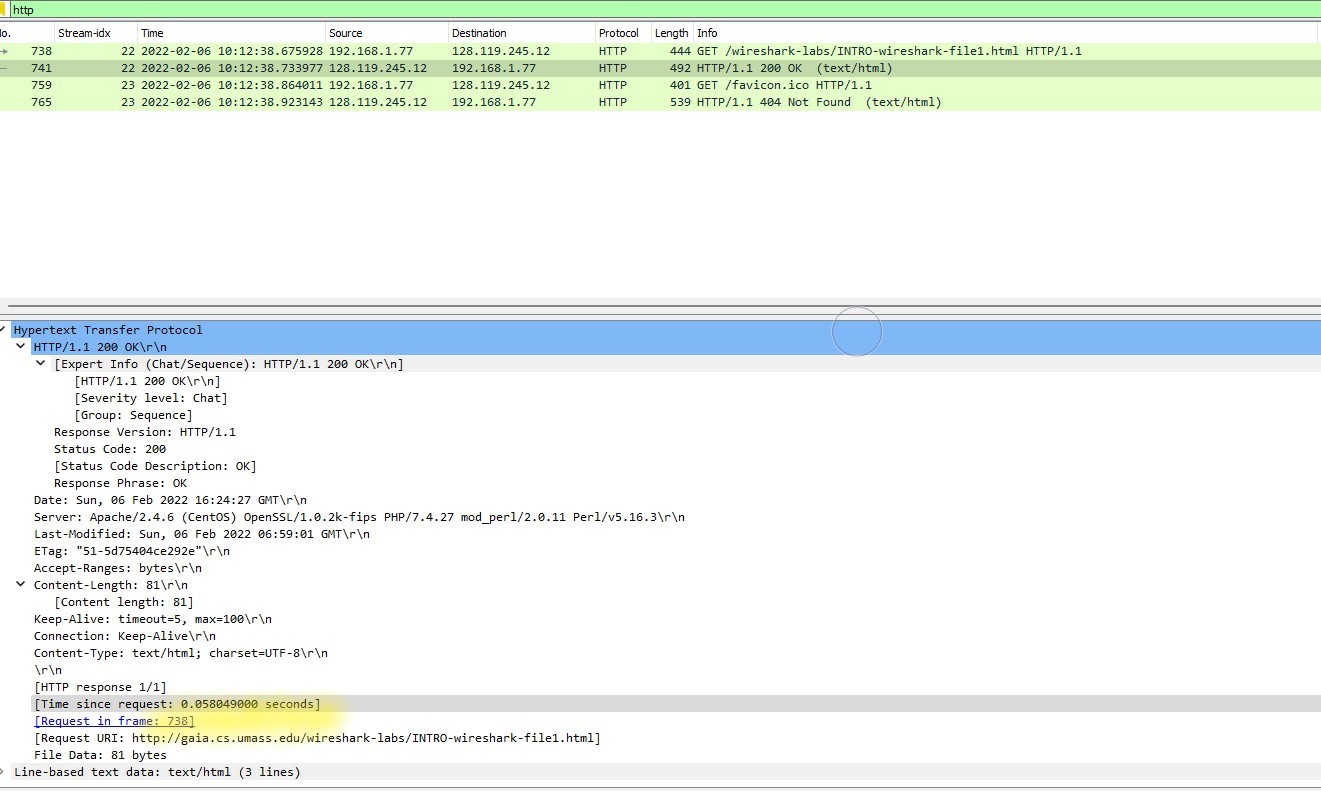
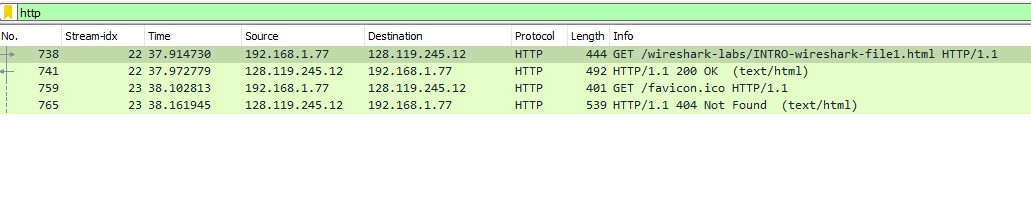
Mike Pendleton

Boralb Mimani

West Texas A@M University

Wireshark Lab #1

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you’ve been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   * DNS
   * TCP
   * HTTP
   * 
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)
   * .0580 Seconds
   * 
3. 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?
   * The address of www-net.cs.umass.edu is 128.119.254.12
   * My systems address is 192.168.1.77
   * 
4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the “*Selected Packet Only”* and *“Print as displayed”* radial buttons, and then click OK.
   * Get

No. Stream-idx Time Source Destination Protocol Length Info

TCP Length RTT Relative Time Ack Num Delta Time Sequesnce Number Next Exp Seq

738 22 37.914730 192.168.1.77 128.119.245.12 HTTP 444 GET /wireshark-labs/INTROwireshark-

file1.html HTTP/1.1 390 37.914730 1 0.000303 1 391

Frame 738: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface \Device\NPF\_{4A62DE4FBD32-

434A-9977-67972618DF59}, id 0

Ethernet II, Src: LiteonTe\_67:0f:7b (f8:28:19:67:0f:7b), Dst: e2:63:da:c5:01:0a (e2:63:da:c5:01:0a)

Internet Protocol Version 4, Src: 192.168.1.77, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 52468, Dst Port: 80, Seq: 1, Ack: 1, Len: 390

Hypertext Transfer Protocol

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

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

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\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: 741]
  + **OK**

No. Stream-idx Time Source Destination Protocol Length Info

TCP Length RTT Relative Time Ack Num Delta Time Sequesnce Number Next Exp Seq

741 22 37.972779 128.119.245.12 192.168.1.77 HTTP 492 HTTP/1.1 200 OK (text/html)

438 37.972779 391 0.001554 1 439

Frame 741: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{4A62DE4FBD32-

434A-9977-67972618DF59}, id 0

Ethernet II, Src: e2:63:da:c5:01:0a (e2:63:da:c5:01:0a), Dst: LiteonTe\_67:0f:7b (f8:28:19:67:0f:7b)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.77

Transmission Control Protocol, Src Port: 80, Dst Port: 52468, Seq: 1, Ack: 391, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 06 Feb 2022 16:24:27 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sun, 06 Feb 2022 06:59:01 GMT\r\n

ETag: "51-5d75404ce292e"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\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: 0.058049000 seconds]

[Request in frame: 738]

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

File Data: 81 bytes

Line-based text data: text/html (3 lines)

