Firstname Lastname

September 28,2017

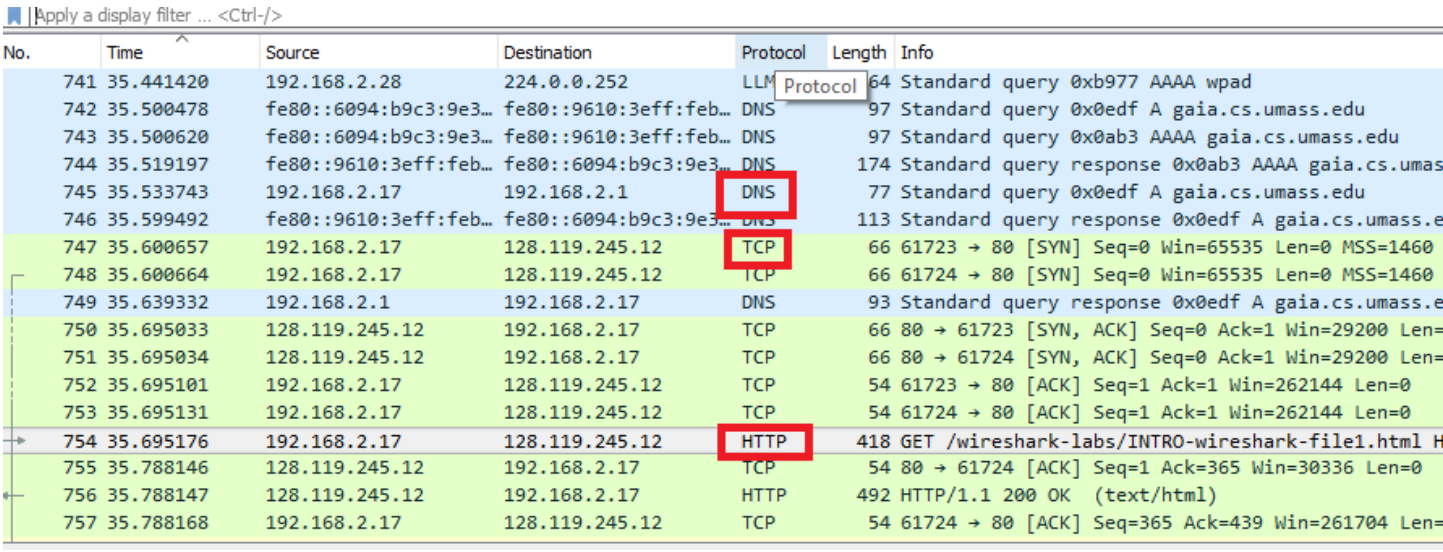
CSC 138-01

Lab 1

Intro to Wireshark

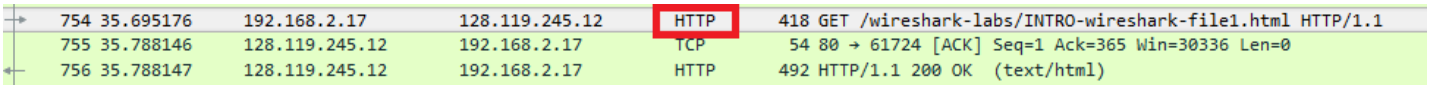
Due September 28,2017

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 packetlisting 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.)



35.695176 - 35.788147 = .092971 SECONDS

It took .092971 seconds for the HTTP GET messeage to be received by the other server and for it to send an OK message back to my computer.

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

gaia.cs.umass.edu = 128.119.245.12

My computer = 192.168.2.17

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.

HTTP GET

```
    754 35.695176      192.168.2.17          128.119.245.12        HTTP     418    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 754: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface 0
Ethernet II, Src: EdimaxTe_5b:71:4b (74:da:38:5b:71:4b), Dst: BelkinIn_b7:5f:0e (94:10:3e:b7:5f:0e)
    Destination: BelkinIn_b7:5f:0e (94:10:3e:b7:5f:0e)
    Source: EdimaxTe_5b:71:4b (74:da:38:5b:71:4b)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.2.17, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61724, Dst Port: 80, Seq: 1, Ack: 1, Len: 364
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-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; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/
14.14393\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/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 756]
```

HTTP OK

```
    756 35.788147      128.119.245.12        192.168.2.17          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 756: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: BelkinIn_b7:5f:0e (94:10:3e:b7:5f:0e), Dst: EdimaxTe_5b:71:4b (74:da:38:5b:71:4b)
    Destination: EdimaxTe_5b:71:4b (74:da:38:5b:71:4b)
    Source: BelkinIn_b7:5f:0e (94:10:3e:b7:5f:0e)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.17
Transmission Control Protocol, Src Port: 80, Dst Port: 61724, Seq: 1, Ack: 365, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 25 Sep 2017 01:22:56 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, 24 Sep 2017 05:59:01 GMT\r\n
    ETag: "51-559e9237e8bbd"\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: 0.092971000 seconds]
    [Request in frame: 754]
    File Data: 81 bytes
Line-based text data: text/html
```