Tu Lam

CS 372 Lab

January 14th, 2021

Lab #0

(*Intro to WireShark*)

1. *List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window.*

Answer: There are more than 3 different protocols presented under the unfiltered packet-listing window. The 3 that were spotted was the **TCP**, **ARP**, and the **TLSv1.2**.

2. *How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?*

Answer: The HTTP GET got sent was around **12:05:33.276322 AM** while the HTTP OK was received at **12:05:33.371800 AM**. If we take the OK time minus the send time, we get:

$$33.371800 - 33.276322 = 0.095478$$

So, it took roughly around **12:05:33.095478 AM** from sent to received.

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?*

Answer: The Internet address of the gaia.cs.umass.edu is the following:

IP Address – 128.119.245.12

As for my internet address, I have:

IP Address – 192.168.1.5

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

Answer:

HTTP GET Messages:

```
No.     Time              Source                Destination           Protocol Length Info
     79 00:05:33.276322    192.168.1.5           128.119.245.12        HTTP     536    GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 79: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{9209EA0C-66BA-4D01-B635-66ECCAE28F1D},
id 0
Ethernet II, Src: HonHaiPr_75:c4:25 (f8:da:0c:75:c4:25), Dst: Netgear_df:c6:00 (8c:3b:ad:df:c6:00)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50300, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 Edg/
87.0.664.75\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 89]
    [Next request in frame: 101]
```

HTTP OK Messages:

```
No.     Time              Source                Destination           Protocol Length Info
     89 00:05:33.371800    128.119.245.12        192.168.1.5           HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 89: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{9209EA0C-66BA-4D01-B635-66ECCAE28F1D},
id 0
Ethernet II, Src: Netgear_df:c6:00 (8c:3b:ad:df:c6:00), Dst: HonHaiPr_75:c4:25 (f8:da:0c:75:c4:25)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 50300, Seq: 1, Ack: 483, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 14 Jan 2021 08:05:32 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.13 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 14 Jan 2021 06:59:01 GMT\r\n
    ETag: "51-5b8d6ca68306a"\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 1/2]
    [Time since request: 0.095478000 seconds]
    [Request in frame: 79]
    [Next request in frame: 101]
    [Next response in frame: 106]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```