Astrid Delestine

1/13/2023

ECE_372

Prof. Bechir Hamdaoui

Overview:

This lab is designed to introduce the concepts of how Wireshark works and how the student is expected to use it. In this lab the student primarily sets up Wireshark and analysis a HTTP protocol.

Content:

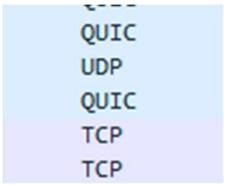
First the student installs Wireshark, then opens it. Once they have started Wireshark they must start capturing their network traffic, so the student makes sure they are connected to Wi-Fi or to Ethernet and uses the connection labeled as such. Next, while Wireshark is capturing, the student opens a particular webpage, this webpage then appears inside of the Wireshark program. The student then can stop the Wireshark capture and can analyze the HTTP protocol.

Requested Questions/Information:

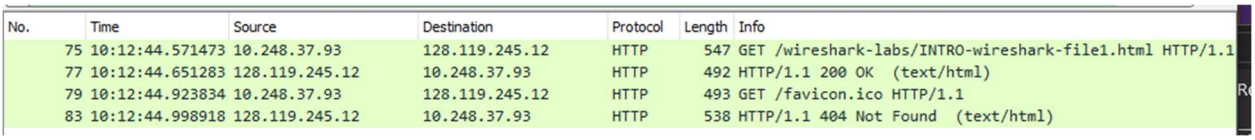
1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
    a. UDP, TCP, QUIC *
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?
    a. 0.07981 seconds *
3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?
    a. The address of gaia.cs.umass.edu is 128.199.245.12
4. What is the Internet address of your computer?
    a. The address of my computer is 10.248.37.93
5. 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.
    a. See appendix section

Appendix:

Different protocols seen:



Time Determined to receive message, source, and destination:



No.	Time	Source	Destination	Protocol	Length	Info
75	10:12:44.571473	10.248.37.93	128.119.245.12	HTTP	547	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
77	10:12:44.651283	128.119.245.12	10.248.37.93	HTTP	492	HTTP/1.1 200 OK (text/html)
79	10:12:44.923834	10.248.37.93	128.119.245.12	HTTP	493	GET /favicon.ico HTTP/1.1
83	10:12:44.998918	128.119.245.12	10.248.37.93	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Screenshot of printed document:

C:\Users\tgogo\AppData\Local\Temp\wireshark_Wi-Fi6Y0VY1.pcapng 121 total packets, 4 shown

```
No.     Time              Source                Destination           Protocol Length Info
     75 10:12:44.571473   10.248.37.93          128.119.245.12        HTTP     547    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 75: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{52A93EF6-8BB7-488A-
AA9F-46C9AA036E99}, id 0
Ethernet II, Src: IntelCor_d8:24:30 (f8:e4:e3:d8:24:30), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.248.37.93, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52947, Dst Port: 80, Seq: 1, Ack: 1, Len: 493
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
    DNT: 1\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/108.0.0.0 Safari/
537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
    sec-gpc: 1\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: 77]
    [Next request in frame: 79]
No.     Time              Source                Destination           Protocol Length Info
     77 10:12:44.651283   128.119.245.12        10.248.37.93          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 77: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{52A93EF6-8BB7-488A-
AA9F-46C9AA036E99}, id 0
Ethernet II, Src: HewlettP_45:60:de (40:b9:3c:45:60:de), Dst: IntelCor_d8:24:30 (f8:e4:e3:d8:24:30)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.248.37.93
Transmission Control Protocol, Src Port: 80, Dst Port: 52947, Seq: 1, Ack: 494, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 13 Jan 2023 18:12:43 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 13 Jan 2023 06:59:01 GMT\r\n
    ETag: "51-5f21fc4b9351b"\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: 0.079810000 seconds]
    [Request in frame: 75]
    [Next request in frame: 79]
    [Next response in frame: 83]
    [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)
```