Lab #2 – Inspecting TCP/IP Traffic

Overview

In this lab, you will explore the TCP/IP protocol through packet capture, and gain some hands on skills with this type of technology. There are multiple tools that can be used to do packet capture, including libraries that can be used by scripting tools and programming language both for analysis and capture. We are going to use the tool Wireshark and look at traffic that happens when we connect to a website. You can refer to the example exercise posted to the course for guidance on basic Wireshark usage.

Preparation

Download and install Wireshark from:
https://www.wireshark.org/download.html

Lab

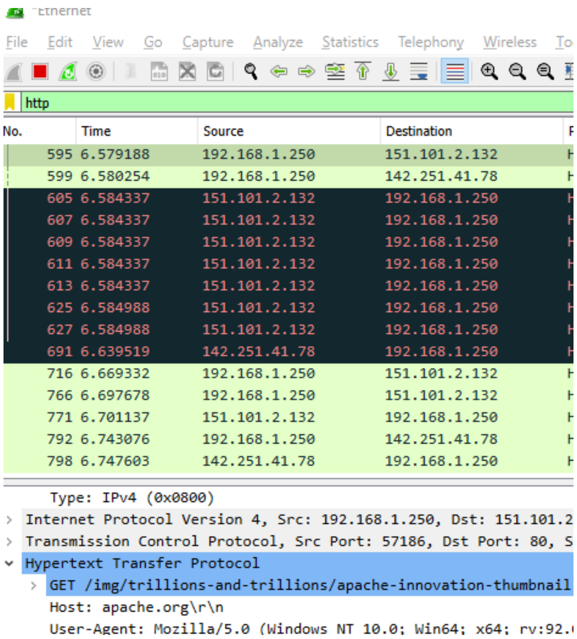
Part 1

For Part 1, you will connect to the main website of the Apache Foundation (which hosts projects for open source webservers, and many other software applications) which is available as http as http://apache.org. In order to personalize the content, please enter http://apache.org?1234, where 1234 are the last four digits of your student number (this is simulating a POST to the website; we will see this plain text traffic being sent).

With Wireshark enabled, capture the packets when you load that http://apache.org?1234 url (again, with your own unique ID numbers) and find the following information.

- What is the User-Agent (type of web browser) reported for your session?
- What is the Current Time as reported by the webserver?
- What does the webserver report for the “Referer” for the webpage?

Hint: After filtering for http packets as per the practice exercise in class, highlight the first line shown by Wireshark and then look in the middle frame of the window for the “Hypertext Transfer Protocol” dropdown, and expand it to see the HTTP traffic contents. It would look similar to what is shown to the right (with further info below).



http

```
No.     Time      Source          Destination
595 6.579188   192.168.1.250   151.101.2.132
599 6.580254   192.168.1.250   142.251.41.78
605 6.584337   151.101.2.132   192.168.1.250
607 6.584337   151.101.2.132   192.168.1.250
609 6.584337   151.101.2.132   192.168.1.250
611 6.584337   151.101.2.132   192.168.1.250
613 6.584337   151.101.2.132   192.168.1.250
625 6.584988   151.101.2.132   192.168.1.250
627 6.584988   151.101.2.132   192.168.1.250
691 6.639519   142.251.41.78   192.168.1.250
716 6.669332   192.168.1.250   151.101.2.132
766 6.697678   192.168.1.250   151.101.2.132
771 6.701137   151.101.2.132   192.168.1.250
792 6.743076   192.168.1.250   142.251.41.78
798 6.747603   142.251.41.78   192.168.1.250
```

```
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.250, Dst: 151.101.2
> Transmission Control Protocol, Src Port: 57186, Dst Port: 80, S
v Hypertext Transfer Protocol
  > GET /img/trillions-and-trillions/apache-innovation-thumbnail
    Host: apache.org\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.
```

Observations

As per the Lab Book Template instructions, provide observations/notes about your experience and work to complete this lab.

Screenshots

Include a screenshot that **shows the answers to all of the above** from Wireshark**. Ensure the referrer line is visible in the screenshot, and take only one screenshot to illustrate this. Also include a screenshot to support reflection #2.**

Reflections

1. Provide the written answer to the questions asked for the Lab section:
    a. What is the User-Agent (type of web browser) reported for your session?
    b. What is the Current Time as reported by the webserver?
    c. What does the webserver report for the "Referer" for the webpage?

2. Imagine you are sitting on free wireless at the local coffee shop while you are done this. Instead of looking at the filter for http, change that filter line to say "dns" (no quotes) instead.
    a. What do you feel is the implication of what you are seeing in that context?
    b. What is the DNS information you are seeing? What is DNS?
    c. Is there anything that would be visible to others in the coffeeshop, and if so, is there anything that would be a concern?
    d. Share a screenshot you are comfortable with that demonstrates your viewpoint.
    e. If you feel there was an issue with the visible DNS traffic, suggest a method to prevent any issues while still being able to look up DNS addresses.