Ethan Taylor Behar
ebehar@iu.edu
8/27/2021
P538 Assignment 00 Wireshark

# Task 1 - Explore HTTP

***1. What is the IP address of your computer? Of the /gaia.cs.umass.edu/ server?***

Taken from packet-listing window. I do not see IP information in the HTTP portion of the packet-header details window.
PC IP - 192.168.1.2
/gaia.cs.umass.edu/ server - 128.119.245.12

***2. What is the status code and phrase returned from the server to your browser?***

Status Code = 200
Phrase = Ok\r\n

***3. What languages does your browser indicate to the server that it can accept? Which header line is used to indicate this information?***

Acceptable languages = en-US,en;q=0.5
This information is taken from the "Accept-Language" header line.

***4. How many bytes of content (size of file) are returned to your browser? Which header line is used to indicate this information?***

128 bytes.
This information is taken from the "Content-Length" header line.
We know it is bytes because of the "Accept-Ranges" header line.

***5. 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.)***

Crazy fast!
The GET was sent at 08:43:53.211370 and I received the response at 08:43:53.259751.
Time: 00:00:00.48381

# Task 2 - Capture a traceroute

Ethan Taylor Behar
ebehar@iu.edu
8/27/2021
P538 Assignment 00 Wireshark

***Step 3 Commandline Output:***

```
Microsoft Windows [Version 10.0.19042.1165]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\WINDOWS\system32>tracert yahoo.com

Tracing route to yahoo.com [74.6.143.26]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  www.routerlogin.com [192.168.1.1]
  2    13 ms    18 ms     8 ms  96.120.112.121
  3     7 ms     9 ms     7 ms  96.110.168.17
  4    15 ms    22 ms    14 ms  96.108.120.145
  5    22 ms    22 ms    22 ms  24.153.88.85
  6    23 ms    27 ms    23 ms  4.68.110.122
  7     *        *        *     Request timed out.
  8    59 ms    58 ms    59 ms  YAHOO-INC.ear2.NewYork1.Level3.net [4.14.4.250]
  9    56 ms    55 ms    55 ms  et-19-0-0.pat2.bfz.yahoo.com [209.191.64.187]
 10    57 ms    58 ms    58 ms  et-1-1-1.msr1.bf2.yahoo.com [72.30.223.53]
 11    59 ms    58 ms    63 ms  et-1-1-0.clr1-a-gdc.bf2.yahoo.com [74.6.122.53]
 12    58 ms    57 ms    56 ms  lo0.fab6-1-gdc.bf2.yahoo.com [74.6.123.239]
 13    55 ms    57 ms    57 ms  usw1-1-lbb.bf2.yahoo.com [74.6.98.138]
 14    62 ms    59 ms    61 ms  media-router-fp74.prod.media.vip.bf1.yahoo.com [74.6.143.26]

Trace complete.

C:\WINDOWS\system32>
```

Ethan Taylor Behar
ebehar@iu.edu
8/27/2021
P538 Assignment 00 Wireshark

***Step 6 Screenshots: (Png files can be found in GitHub Repo alongside other submission files)***