**Homework - HTTP network traffic analysis**

**IT210**

**Objectives:**

* Expose the nuts and bolts of the Hypertext Protocol, HTTP.
* Give experience with tools for troubleshooting network protocols.
* Teach problem solving skills for web-based systems.
* Give you experience looking under the hood of web services.

**Resources**

* PC with:
* Web Browser.
* Wireshark
* <http://tools.ietf.org/html/rfc2068> The IETF standard that defines HTTP 1.1.
* A [tutorial](http://www3.ntu.edu.sg/home/ehchua/programming/webprogramming/HTTP_Basics.html) on how HTTP works.
* <http://www.wireshark.org/> *Sniffing the packets going to or from your computer.*
* A brief [Wireshark](http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1334483,00.html) tutorial

**What to turn in:**

Write your answers to the questions as you go through this assignment.

**Procedure: Follow the instructions and write your answers in red to the questions throughout. Submit this word document to LearningSuite once finished.**

* Make sure the PC that you are using has the required software installed (see Resource 1). Follow the links if necessary to get the software. Open Wireshark.
* Start a live capture of network traffic on Wireshark, making sure you include the network you are currently on.
* Find your IP address (e.g., via ipconfig or some other technique – use google to find out how if you haven’t done it before)
* Create a filter that will listen to just HTTP traffic associated with your IP address by typing in the following into the filter: **(ip.addr == X.X.X.X) && (http)** - note that the X.X.X.X should be replaced with your IP address
* Try and visit the following website: [http://byu.edu](http://byu.edu/)
* Click on the http packet where your GET request for the page was sent. You should see the details of the packet in the middle section of Wireshark.
* Click on the Internet Protocol section to expand it. This section summarizes information about the IP packets. Remember, IP packets use IP addresses to route messages back and forth through the Internet.

What is the source IP address? **192.168.1.220**

What is the destination IP address? **128.187.16.98**

* Expand the Transmission Control Protocol (TCP) section. Answer the following questions based on what you see:

What is the destination port? **80**

Is the destination port what you would expect? Why? **Yes, because that is the port that is used for general web browsing.**

* Now Expand the Hypertext Transfer Protocol section. This shows a great deal of information that is sent via HTTP. Answer the following questions based on what you see:

What is the Host? (i.e., the host is the domain of the site being requested) **byu.edu**

What “User-Agent” information does your browser send with the HTTP request? **The Type of browser you are using, what OS you are using.**

Can your browser handle files from the server that have been gzip-ed? (Look in the “Accept-Encoding:” section to find out.) **Yes, it can.**

Was a cookie sent to the server? **Yes, it was.**

* Now look at the packet where the IP address you contacted responded to you.

What status did you receive? **200**

Explain what the number means. **This means that the page is okay, no errors.**

What type of server is BYU using? **Apache 2.2.15 (Red Hat)**

What URL did it end up sending you to? [**http://home.byu.edu**](http://home.byu.edu/)

* Look at the next several packets sent and received from your computer and answer the following questions:

List one of the sites (i.e., Hosts) that you were referred to by BYU’s site.

**cloud.typography.com**

Does it have a different IP address than BYU’s site? Why or why not? **Yes it does. Because it is a site different that BYU, it is not BYU.**

Did any of the packets sent from the server use Cache-Control? Briefly explain what Cache-Control is. **Yes they did. Cache-Control is a header field that specifies the rules that MUST be obeyed by all caching mechanisms along the request/response chain**.

* Refresh the BYU webpage after it’s fully loaded (without clearing your cache – hint, hint).

Do you notice any difference in the amount of messages that are sent to/from the server? Why? **There are tons of more packets. That is because someone anyone who goes to that site can be listened in on and they send a packet that I can watch.**

* Change the filter so it captures any data on the network that is http (i.e., change the filter so it just says HTTP). Note that this now shows everyone’s HTTP packet content. This is why you need to be careful when you use public networks (e.g., wireless networks at the airport). Even form data can be

List at least one website that someone other than you is visiting right now.

**facebook.com. This shows basically that anyone can see what anyone is on when it is a public network**.

This is why you need to be careful when you use public networks (e.g., wireless networks at the airport). Other data, such as email and form data can often be listened in on as well, if it’s not protected by HTTPS.