CSE390 – Assignment 1

Warm up exercise using Wireshark to analyze a packet trace

**Hint: make use of Wireshark’s filtering capabilities to complete this assignment!**

**You might also find the following resources helpful:**

* Follow the Money: Understanding economics of online aggregation and advertising. P. Gill, V. Erramilli, A. Chaintreau, B. Krishnamurthy, D. Papgiannaki, and P. Rodriguez. Proc. of ACM Internet Measurement Conference 2013. <http://www.cs.stonybrook.edu/~phillipa/papers/GECK.pdf>
* RFC 2616 <https://www.ietf.org/rfc/rfc2616.txt>

**1. Consider packet 27. What is this packet?**

**2. What Web browser is being used?**

**3. What is the referer header value?**

**4. What do we learn from this value?**

**6. Use Wireshark’s filtering capabilities to see all requests refered by the target (ie., URL) of packet 27. How many requests are refered by this URL?**

**7. Consider the first 4 requests refered by this domain.**

**(a) What are the destination IP addresses of these requests?**

**(b) Use the ``whois’’ command line tool to determine who registered these IP addresses. Write the registrant next to the corresponding IP address in the table below:**

|  |  |  |
| --- | --- | --- |
| **IP address** | **Host name** | **Registrant** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**(c) Compare the host names and the IP registrants. What is strange here?**

**8. Find the DNS query and corresponding response for s1.huffpost.com (hint “dns.qry.name” filter will help).**

 **(a) What are the two CNAMES for this host?**

 **(b) Explain what a CNAME is.**

 **(c) Who manages these hostnames? Research this organization to explain the strange observation in 7c.**

**9. Consider packet 1832**

 **(a) What is the referer value?**

 **(b) What are the cookie values?**

**10. Use the http.host filter to find all requests for ``b.scorecardresearch.com”**

 **(a) What are the referers for each request? (you can just write/copy+paste the unique set of referer values)**

 **(b) What do you notice about the cookie values on each of these requests?**

 **(c) What has the host b.scorecardresearch.com learned based on the cookie and header values?**