CS 524 Homework #4

Due: March 17, 2020

This homework contains both technical and business-related DNS problems, for the total of **100** points.

Reading assignment: Chapter 5 (and references).

1. **(5 points)** Find out the exact number of all top domain names. Make sure you put a date and time of your finding. (Hint: use the information given at the lecture to locate the list of names at IANA.)

2. **(5 points)** Experiment with http://whois.domaintools.com (and also take a look at www.internic.net) and

   a. Find the information about the *stevens.edu* domain as well as the domain of some other school (for instance, the school you had studied at before you came to *Stevens*). Who are the administrative contacts for the domains listed there?

   b. Now, what happens when you try to find the administrative contact for the *.xxx* domain? Explain what you have found.

3. **(5 points)** Look up www.cs.*stevens.edu* https://network-tools.com/nslookup/ with different options and explain all the entries in the responses.

   Then use the returned CNAME entry to find the exact IP address. (Now, just for fun, do the *reverse DNS lookup* using the services of the http://dnsquery.org and find the geographic location of the host!)

   Does Stevens specify IPV6 addresses to any of its hosts? Does Google?

4. **(5 points)** Find your PC's IP address (preferably at home, if you have an Internet connection there.) Can you find your domain with the reverse look up? If you can, what is the domain name? If you cannot, explain why.

5. (**10 points)** Research the responsibilities and structure of *IANA (*www.iana.com) and ICANN (www.icann.com). What are the differences in responsibilities between these two organizations? Search the web for the information and then describe the controversy in ICANN concerning *Whois?*

6. (**50 points)** The *Spamhaus* attack

   a. (5 points) Read https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal-conspiracy-2/ . Describe (in no more than a couple of paragraphs) the *Spamhaus* attack and explain the dangers of open recursive resolvers.

b. (45 points) Find out (you will need to search the Web and sort a lot of information out!) how cloud services were used to mitigate this attack.

7. **(10 points)** Study the *Amazon Route 53* service and answer the following questions

   a. What does *Route 53* do?

   b. Why is it called *Route 53?*

   c. What other Amazon services is it designed to work with (please explain how it happens with one or two examples)?

   d. What is the difference between the domain name and *hosted zone*?

   e. Does *Route 53* have a default for the *Time-to-live (TTL)* value*?*

   f. What is the pricing of the service?

8. **(10 points)** Take a look at https://www.twistlock.com/2018/11/13/open-source-cloud-discovery-tool/ and learn what the Cloud Discovery service is. Explain how the tool works. What does it do? (Just research your answer and explain how you understand it.)

   Incidentally, this is the tool Amazon uses. Does *Route 53* provide a similar service? If so, how? What are the differences?