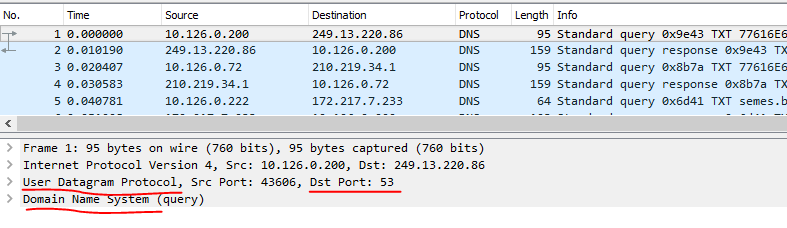
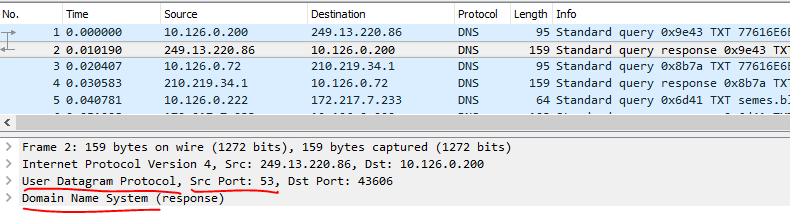
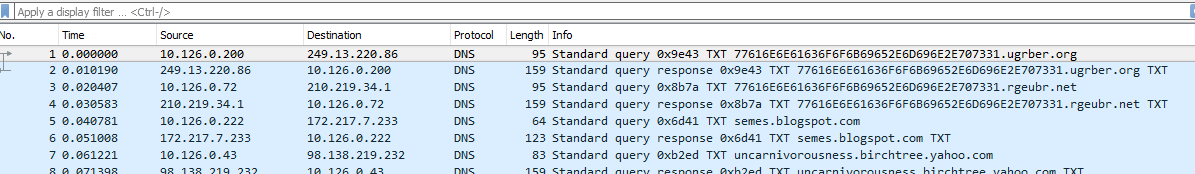
Terminal--Snort Challenge (Part 2)

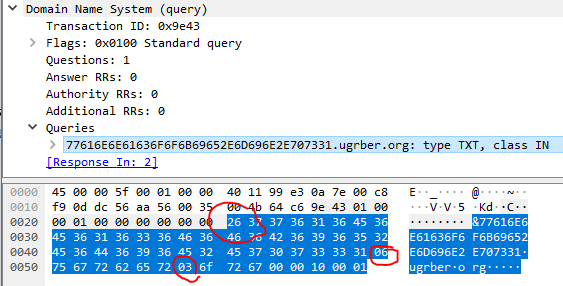
# Solution (examining the traffic in Wireshark)

When you look at the packet capture from the Snort sensor, you should immediately notice that it is all DNS, and it is all UDP. Also, every packet has port 53 in either the source or destination.  


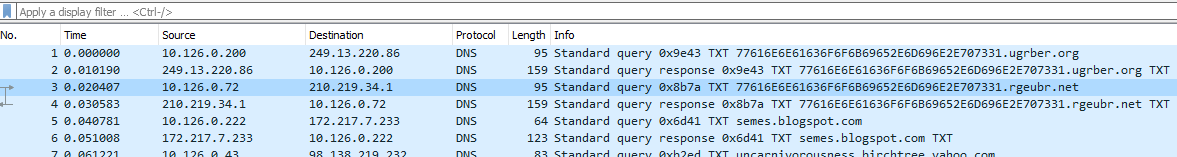
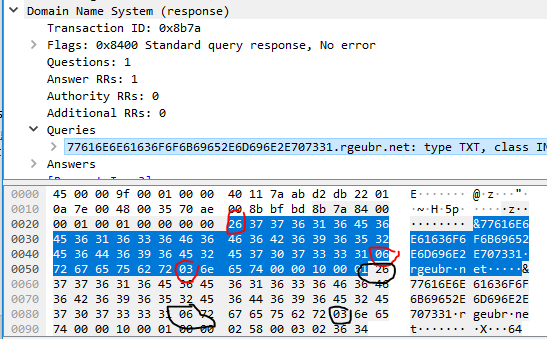
We can’t just block all DNS, though. None of Santa’s users would be able to connect to the Internet if we did that. We will have to fine tune our filter somewhat. We can quickly see that what appears to be the evil traffic all has a long hex string prepended to the domain name. We see things like  
[long hex string].ugrber.com  
[long hex string].rgeubr.net  
[long hex string].ugrber.org

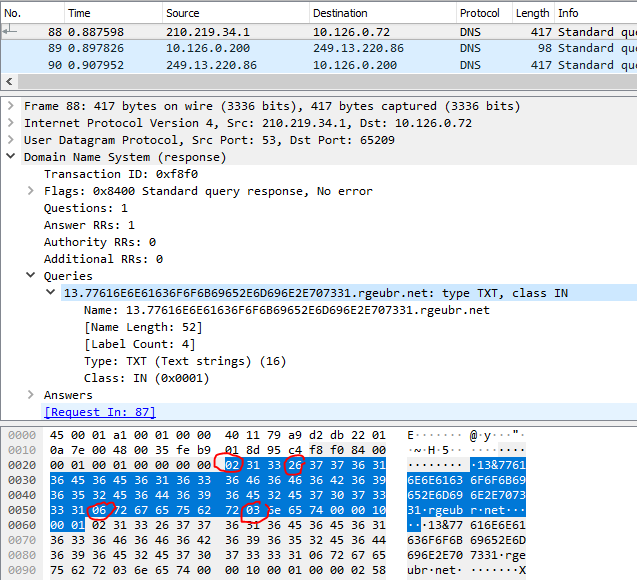
The domain names obviously change. If you look at the IP addresses, you will see that the IP address of the server changes as well.

That long text string seems to be in every packet. If we look at the first packet in the capture in detail, we see something interesting.  


Where the periods would be in the domain name, there are numbers. We can use that to get an idea of how many digits are in each section. For example, in this query, the name is  
77616E6E61636F6F6B69652E6D696E2E707331.ugrber.org  


There are 0x26 characters in the hex section, 0x06 in the next (ugrber) and 0x03 in the last (net).

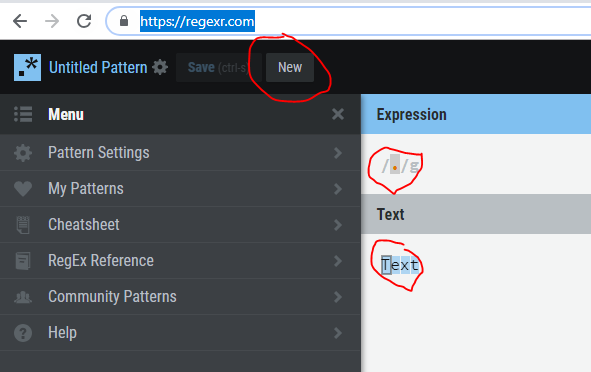
Here is a response. Again, the hex section of the address has 0x26 characters.  
  


There is some variation in the format. Here we see that there are two digits at the beginning before the long hex string. The hex string is still 0x26 characters long, however.  


If we can write something that finds long strings of hex, we are half the way there. This is a simple task for regular expressions.

First, read about character classes. We want to make one that alerts on hex digits. Not only that, the malware does not appear to use lower case letters. You need a short expression that will alert on one hex digit, comprised of either numbers or the letters A through F.  
<https://www.regular-expressions.info/charclass.html>

Next, we need to alert on a long string of hex instead of one character. The article below talks about “limiting” the number of matches, which is not quite what we want. Instead of matching something like one to four characters {1,4} we want to match on a big number {big number}. The number should not be so big that we miss packets, however.  
<https://www.regular-expressions.info/repeat.html>

Finally, you can [go to this site](https://regexr.com/) and test your regex if you like.  


Click on New to clear the page, put your regex in Expression, copy data from the packet into Text, and see what happens. Test some that should not match ([www.freddeadbeef.com](http://www.freddeadbeef.com) or something) to make sure you do not have false positives.

# Hand in

1. What is the regular expression you will use to detect the evil traffic?