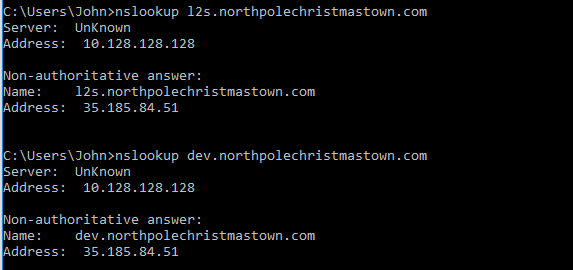
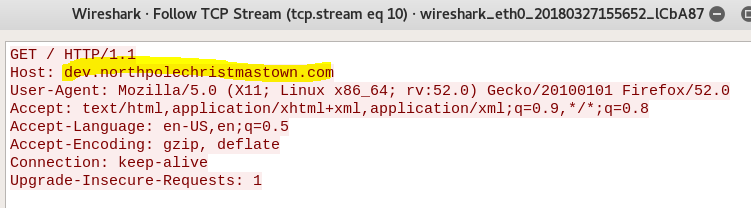
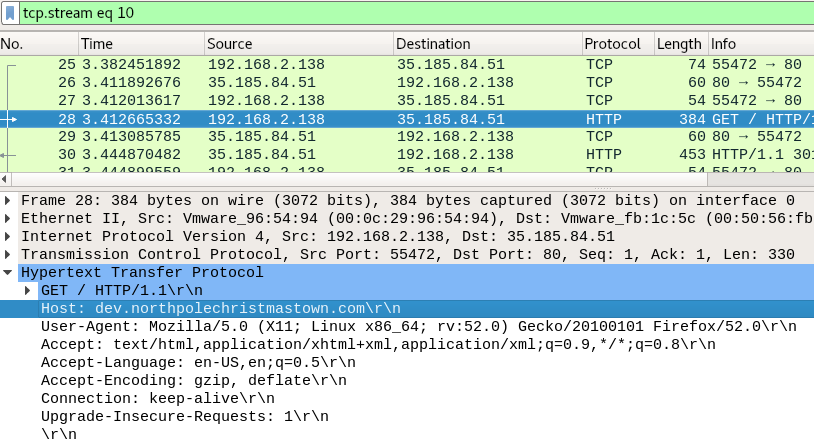
# Letters to Santa--a real world attack Part 3, More Reconnaissance

In the last section you should have found that the Letters to Santa site and the development site are both at the same IP address. The dev site is in scope!



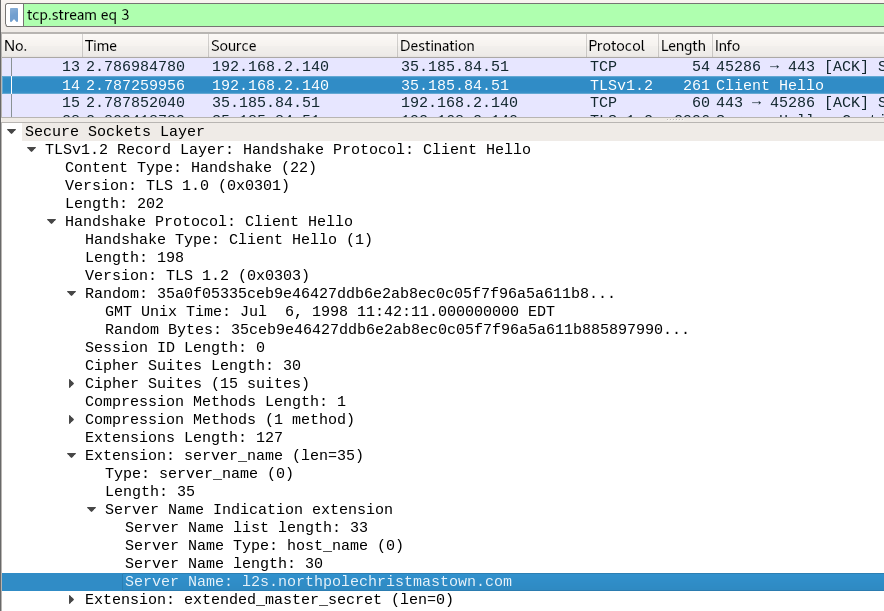
**<sidebar>**  
In case you are wondering how two web sites can be on the same IP address, HTTP and HTTPS allow the browser to specify the web site name in the request. Since IPv4 addresses are in short supply most ISPs put many sites on the same IP address. In fact, many modern web servers will not respond if the IP address is put into the browser address (or URL) bar instead of the domain name of the site. The browser puts the domain name of the web server in the HOST field of the HTTP request header. It is easy to see the HOST field in an unencrypted (HTTP) request header.





In an encrypted (HTTPS) request the name of the site is given, in clear text, in the Server Name Indication (SNI) when the TLS session is started. This allows the server to determine which site is being requested and present the matching certificate to the browser. More information is available [here](https://security.stackexchange.com/questions/86723/why-do-https-requests-include-the-host-name-in-clear-text) and [here](https://en.wikipedia.org/wiki/Server_Name_Indication).





**</sidebar>**

Examine the <http://dev.northpolechristmastown.com> site, and its source code. Remember the links about vulnerabilities you saw in Part 1, and Sparkle Redberry’s last two hints (especially the link she gives you.)

## Questions, part 3

1. What would be a promising attack to try in the next stage?
2. What evidence do you have to support this decision?