ELEC 5220 Information Networks and Technology  
Lab 10 Report

Robert Skelton

# Abstract

The goal of this lab was to further understand certificates, and create our own self-signed certificates and install them into the Root Certificate Authority on our local machines. We then checked if the certificate installation was correct by editing the hosts file and checking the website using the local Apache server, run by XAMPP.

# Introduction

Before I could start the lab, I installed ActivePerl 5.16 64-bit for Windows. Also I installed Win64 OpenSSL v1.0.1j and Visual C++ 2008 was also installed. I then added the OpenSSL bin to the Windows PATH environment variable. All configuration files were edited using Sublime Text 3, the browser used is Google Chrome, and the Operating System is Windows 7 64-bit. The Apache Server is being managed by XAMPP.

# Design

First, we had to establish a Certificate Authority (CA) and issue a certificate. This will make it a trusted CA root certificate in our computer. I created a new cert in the sslcert folder in OpenSSL, with my PEM pass phrase being “robert”. I later had to remake this to be AU-Authority certificate, for wareagle.com.

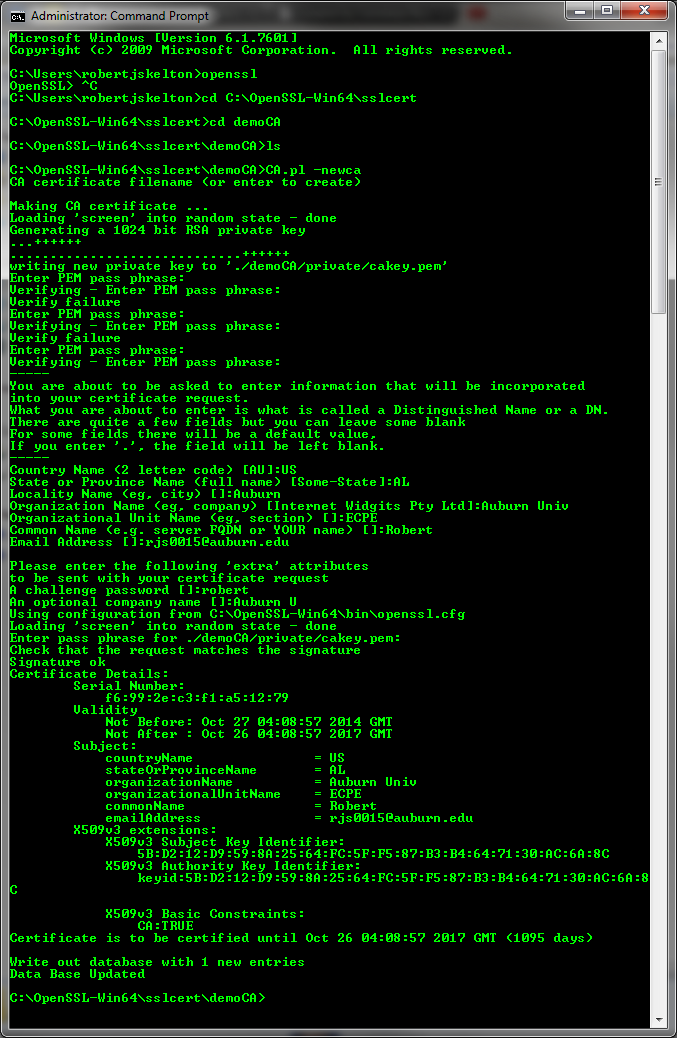


Figure 1. Created a new OpenSSL Certificate with the password “robert”.

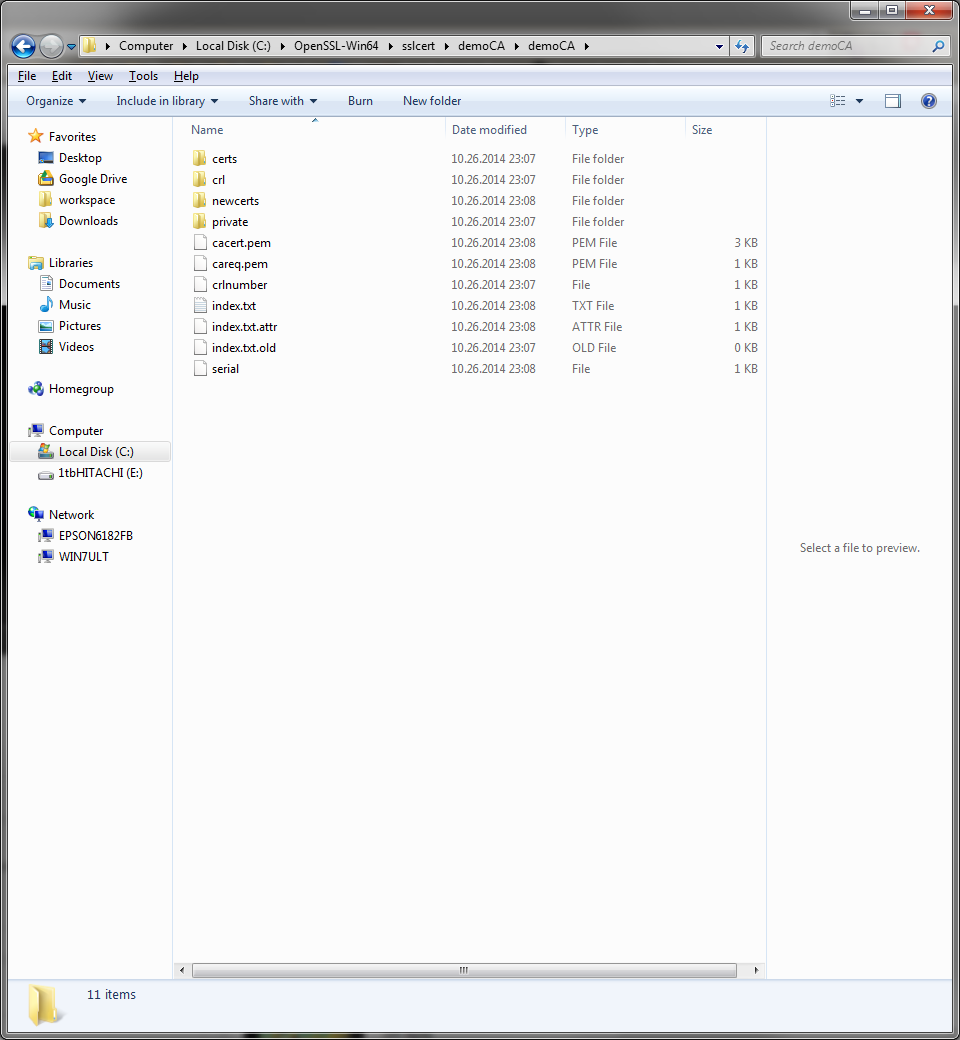


Figure 2. The directory where all the Certificate files were created and stored.

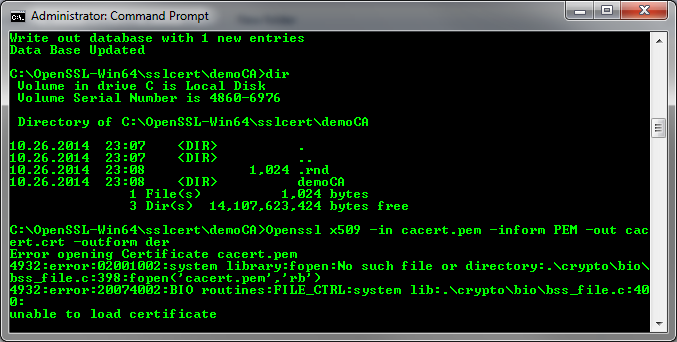


Figure 3. Converting the certificate to der format.

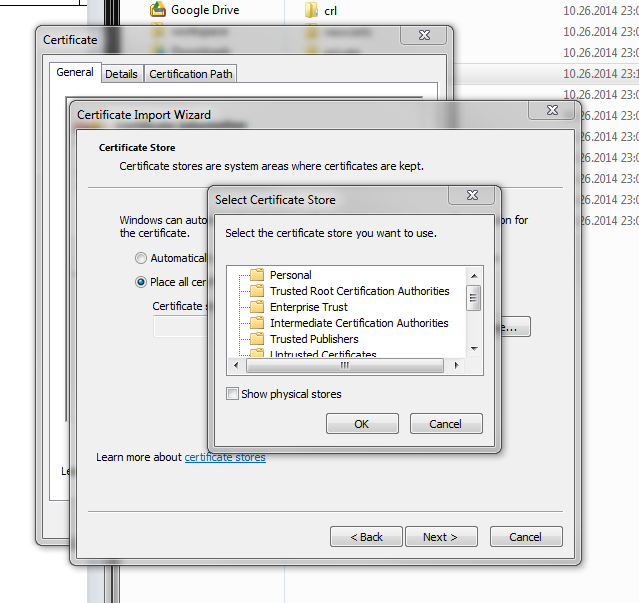


Figure 4. Importing the Certificate to be a Trusted Root Certificate.

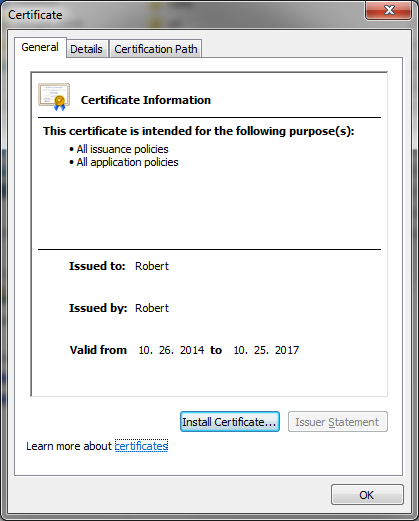


Figure 5. Post Installation of my Certificate.

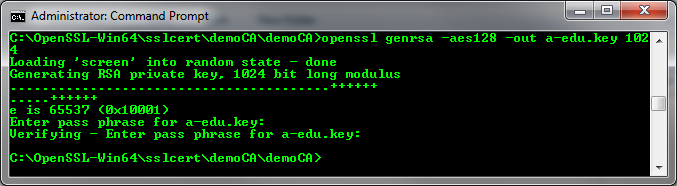


Figure 6. Created a website certificate with RSA.

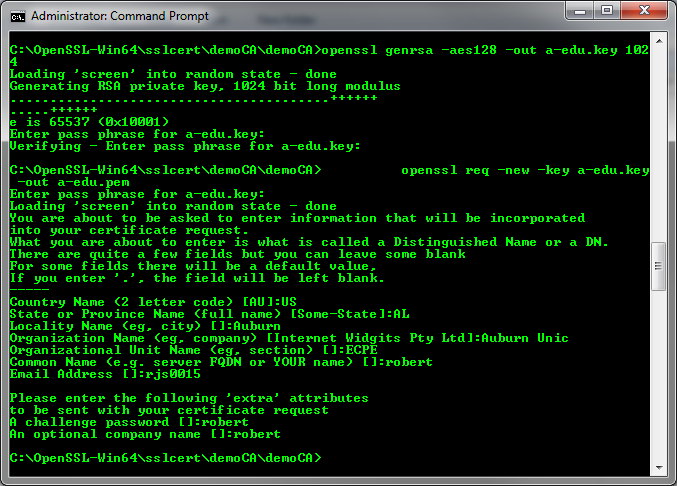


Figure 7. Converting the certificate to be a CSR in PEM format.

I created a cacaert.crt, and AU-Authority.pem and converted it to be in der format. I then placed the AU-Authority.key file in C:\xampp\apache\conf\ssl.key and cacert.crt in the C:\xampp\apache\conf\ssl.crt directory.

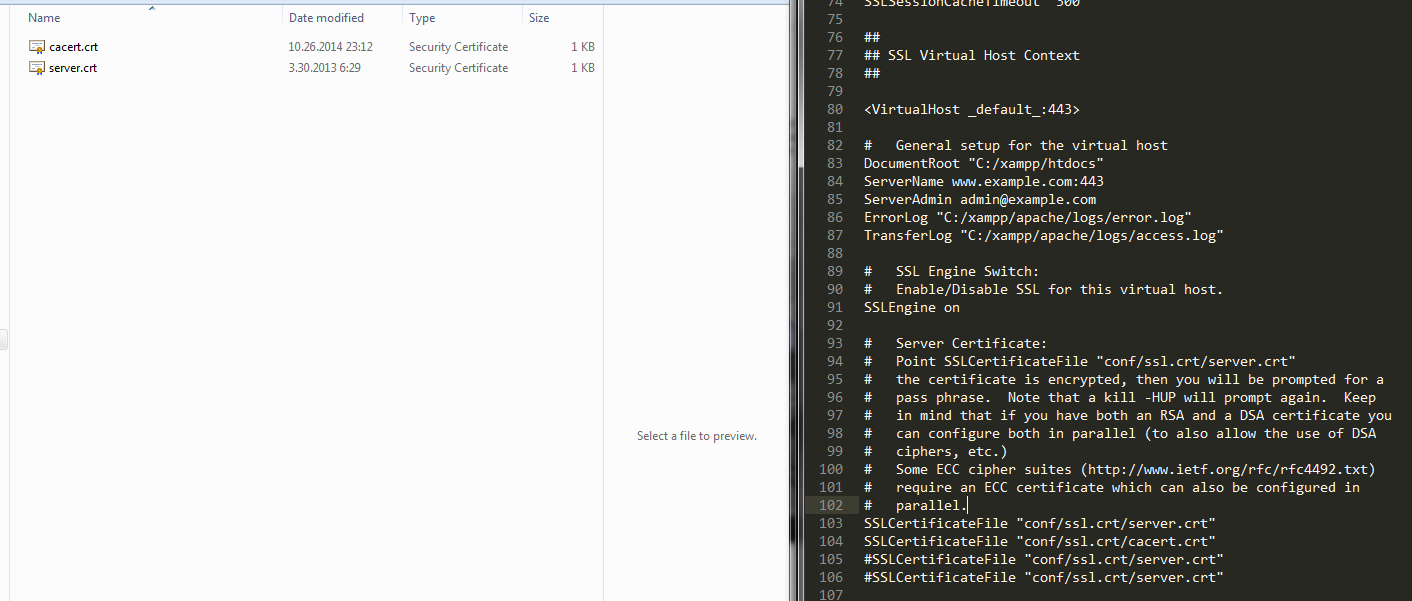


Figure 8. Editing the first part of the httpd-ssl.conf configuration file.

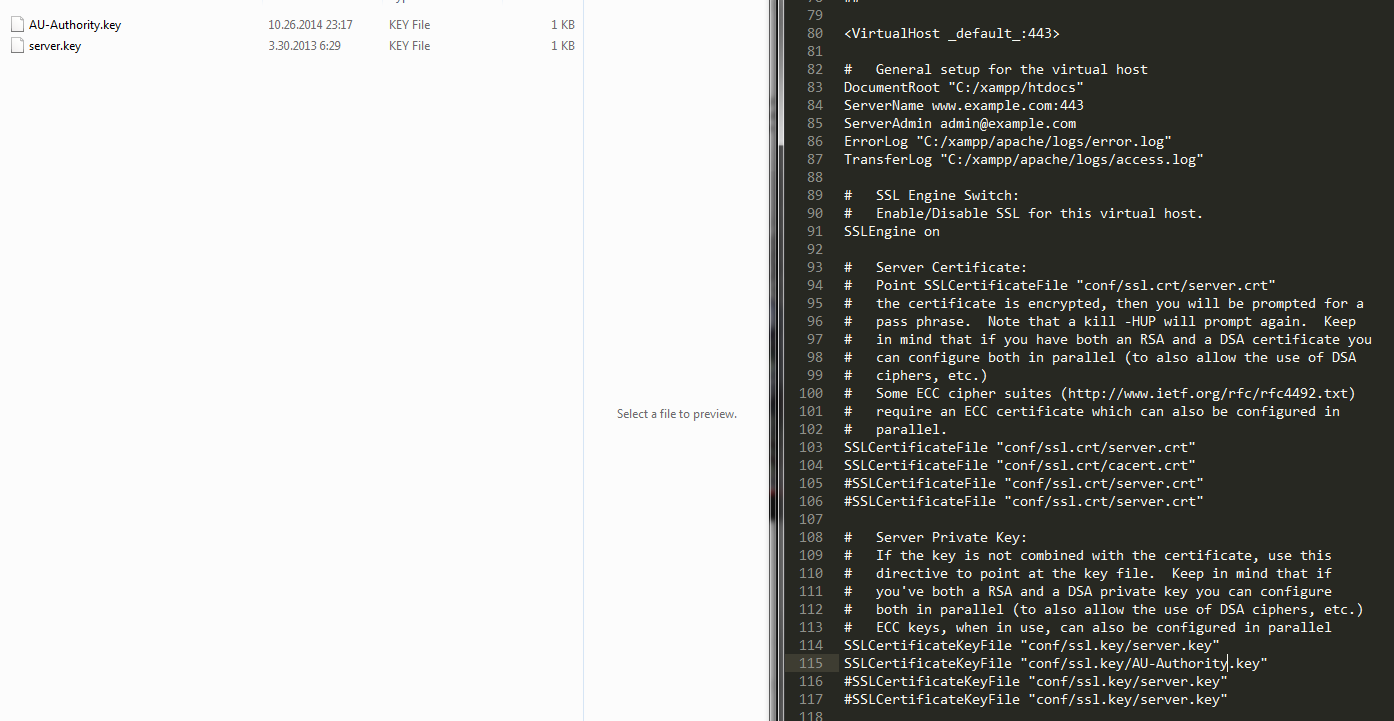


Figure 9. Editing the second part of httpd-ssl.conf.

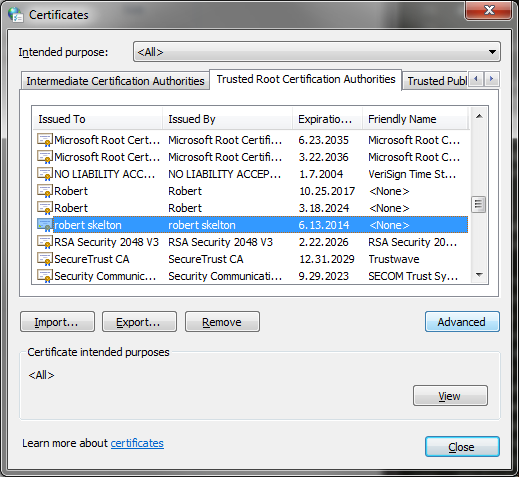


Figure 10. Verifying that the new certificates have been installed. The other certificate I installed was from Dr. Wu’s 5150 class.

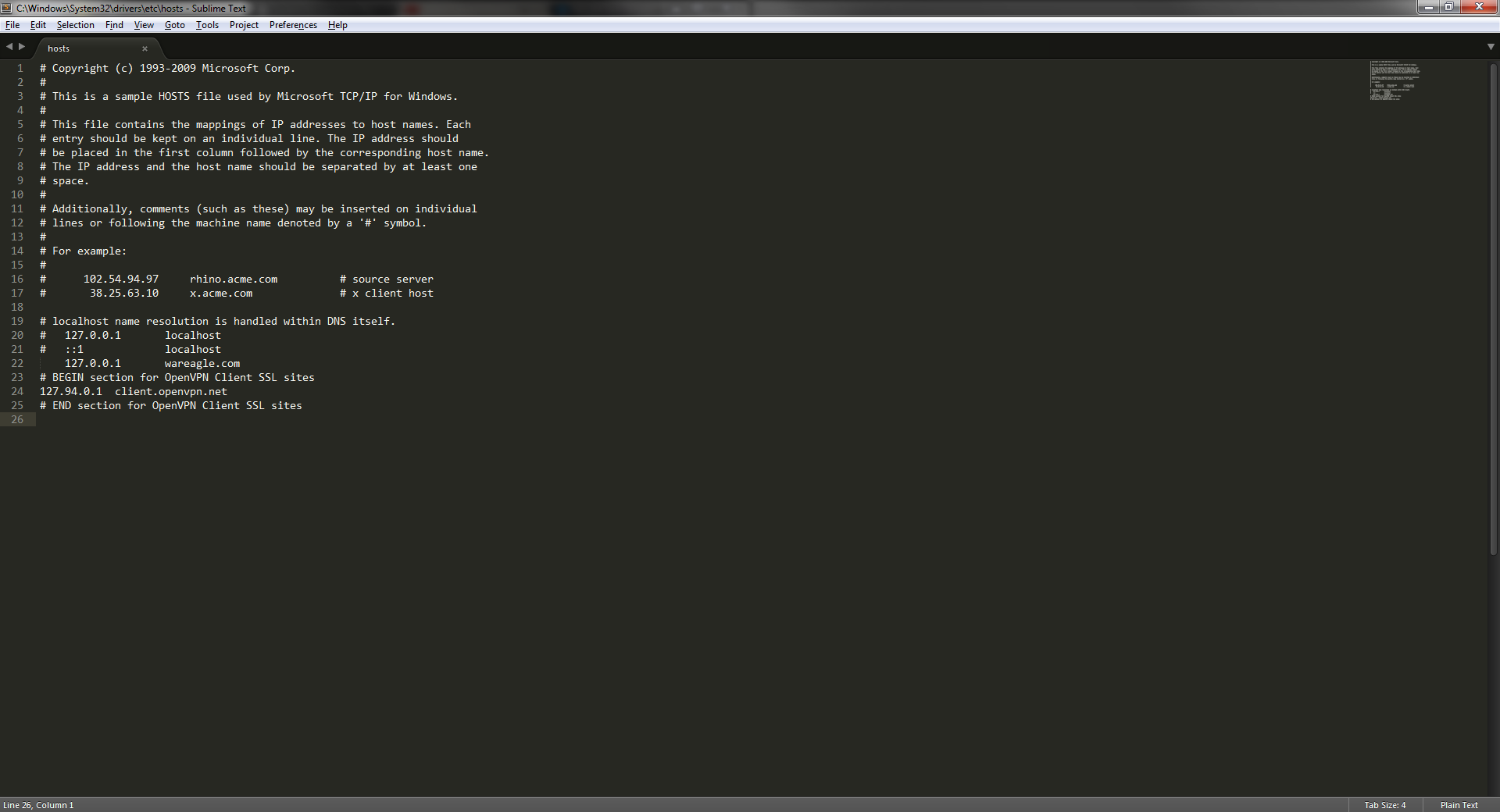


Figure 11. Editing the Windows Host file.

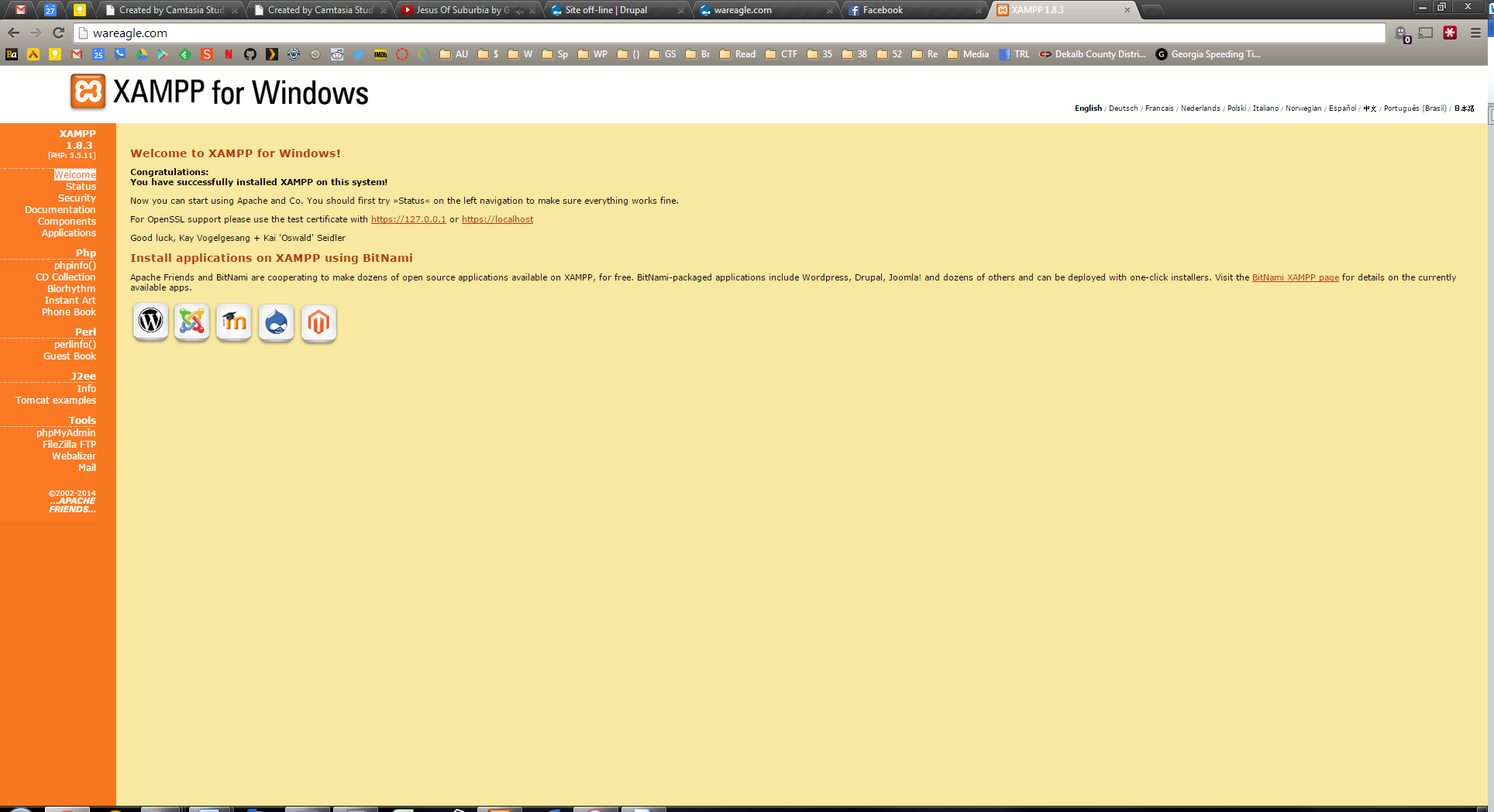


Figure 12. Xampp on wareagle.com.

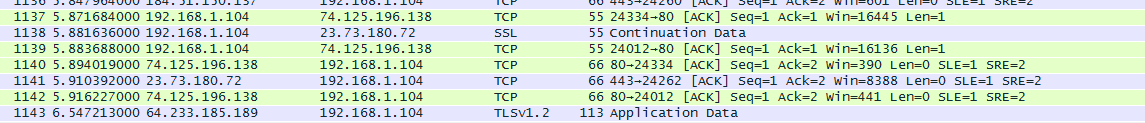


Figure 13. Wireshark capture of SSL on the local machine.

# Result

By the end of this lab, I had created a self-signed certificate called AU-Authority for wareagle.com, and then edited the Apache hosts file to reflect this. I then verified that the certificate was beng recognized using OpenSSL in Wireshark.

# Conclusion

This was a useful because it helped me better understand what certificates are, and how to create and sign your own certificates. Of course, there are companies that will create and digitially sign a better and more reliable certificate, such as Verisign, but no one has money for that. I’ll just make my own certs, thanks.

# References

* Dr. Wu’s included slides and lab materials