ELEC 5220 Information Networks and Technology  
Lab 6 Report

Robert Skelton

# Abstract

The main point of this lab was to get a basic introduction to two great network tools – nmap and Wireshark. I used the nmap GUI for Windows, called Zenmap, since I don’t like the Windows command prompt.

# Introduction

For this lab, I used the same setup as in previous labs. I am running the Apache server on my Windows 7 Ultimate 64-bit OS, using Google Chrome as my internet browser. Wireshark and Zenmap were both installed before completing any of the steps below.

# Design

**Wireshark Section**

All screenshots below are direct from my computer, via the instructions provided in this week’s lab writeup. I added a new column in my Wireshark display for the Round Trip Time for step 17. This section was fun because I learned more about packet sniffing. Wireshark is a tool that all hackers use for checking out network packets, so that was cool.

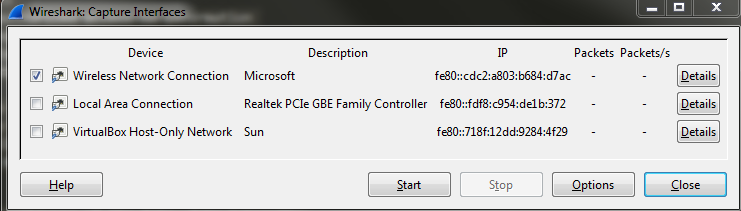


Figure 1. Choosing the wireless interface.

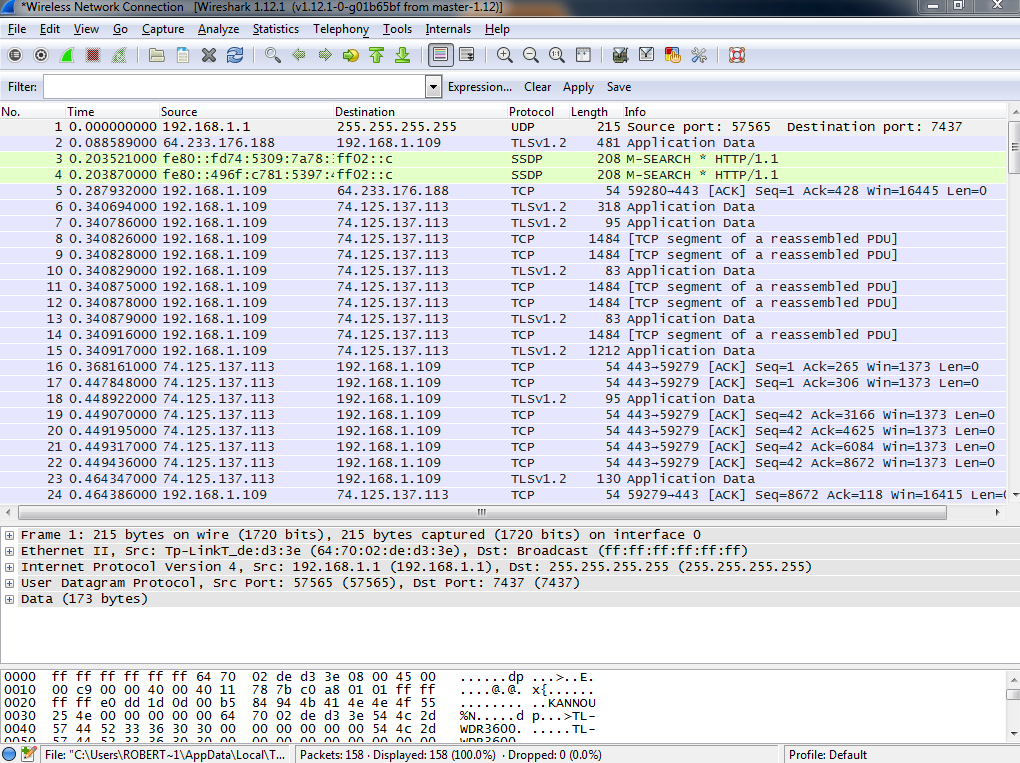


Figure 2. Before filtering any packets.

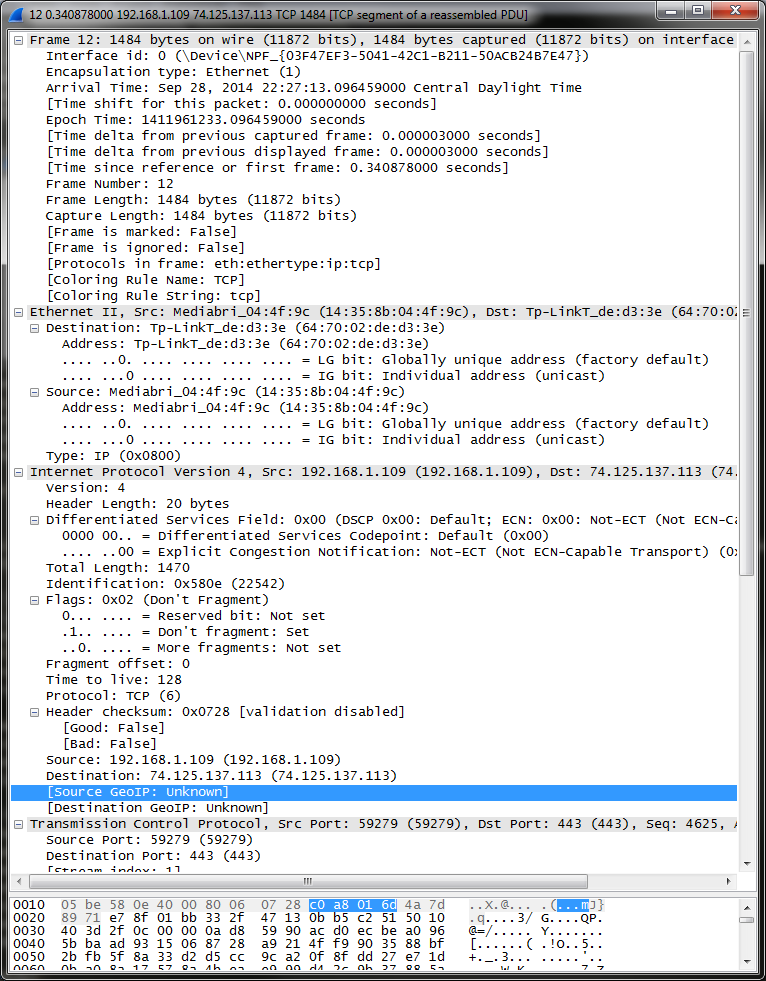


Figure 3. HTTPS packet, which is an HTTP request encrypted with TLS.

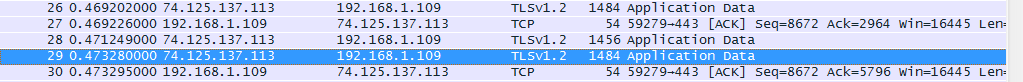


Figure 4. The three way handshake is three packets sent between the server and client to acknowledge each other.



Figure 5. Receiving (encrypted) images from Google images.

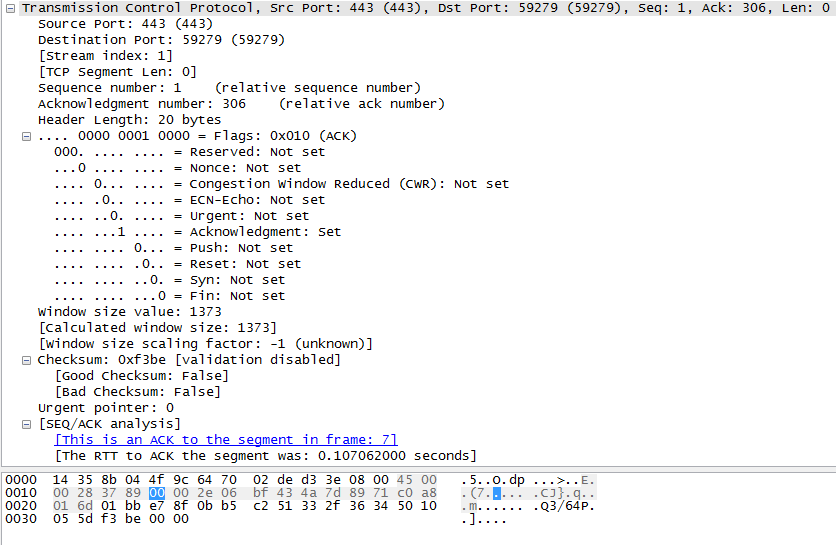


Figure 6. Showing the relationship between ACK, Sequence number, and flag. FTT also.

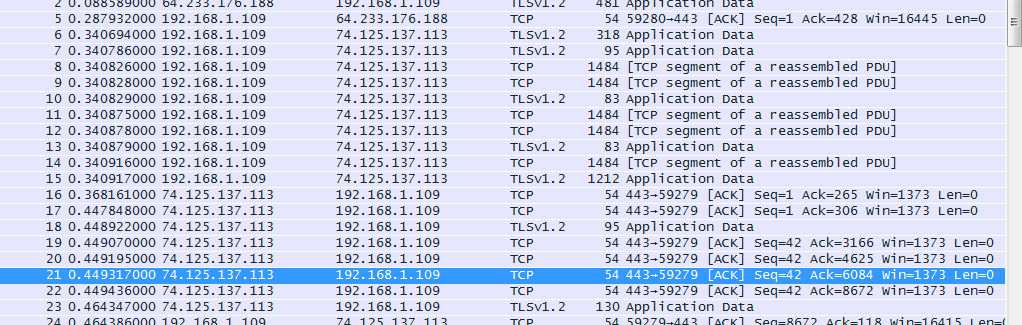


Figure 7. The number of connections opened.

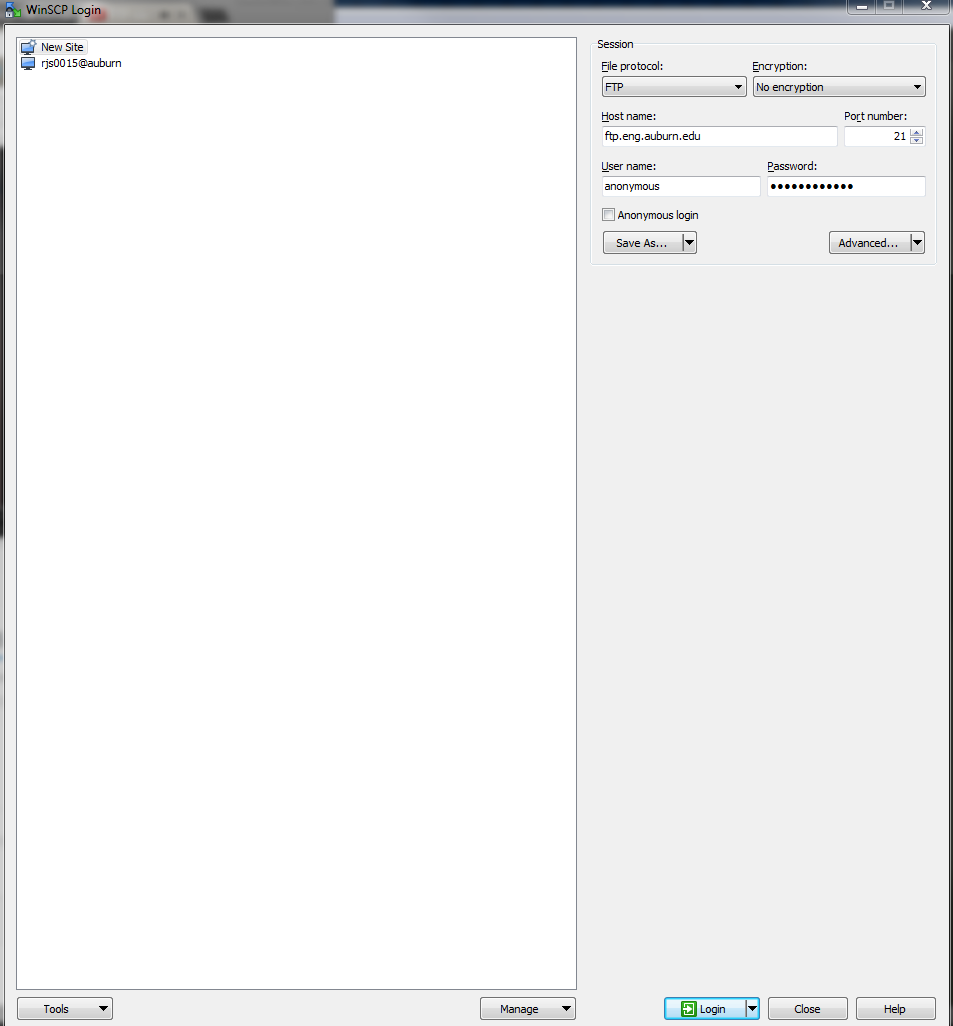


Figure 8. FTP settings for an anonymous user using WinSCP.

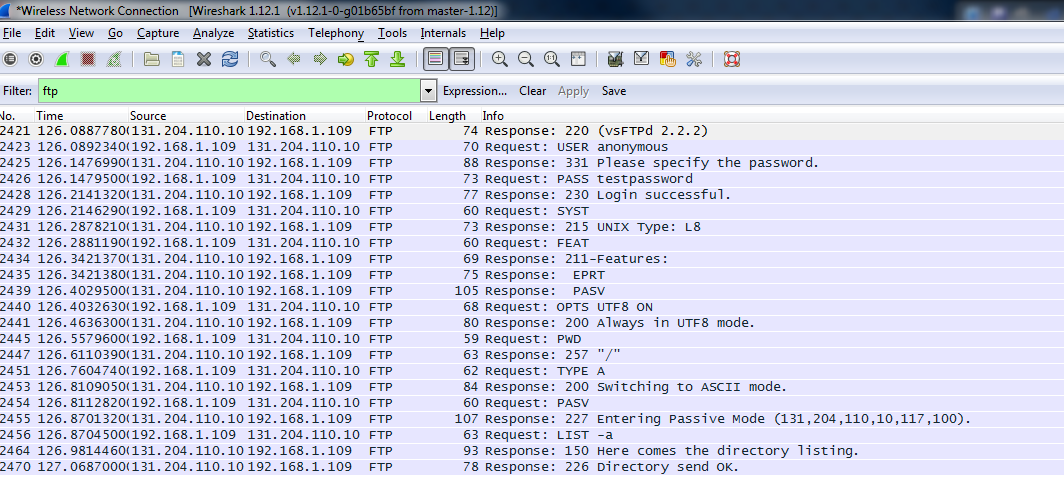


Figure 9. FTP packets captured by Wireshark.

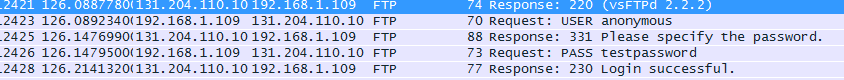


Figure 10. Three way handshake done with FTP.

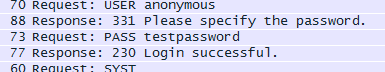


Figure 11. Password “testpassword” sniffed using Wireshark.

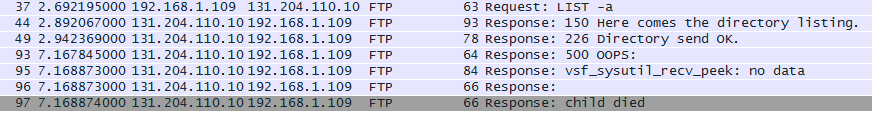


Figure 12. When an FTP connection is closed, the response tells you that a child died. Sad.

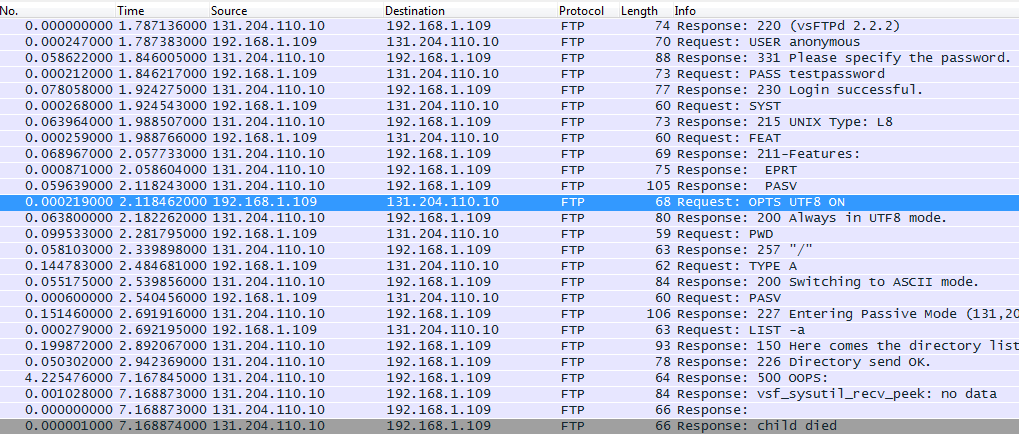


Figure 13. Round Trip Time (RTT) is displayed in the Time column.

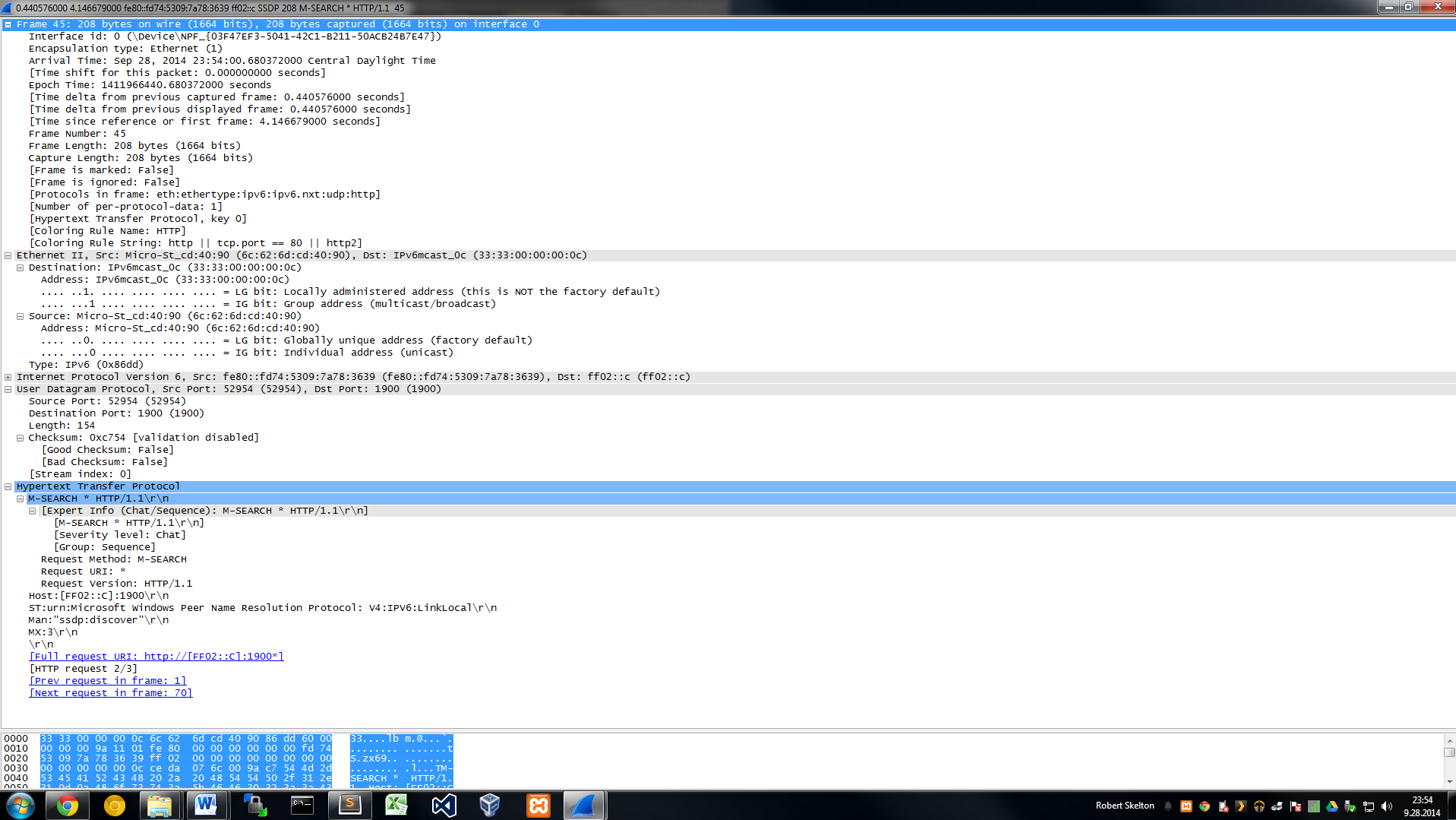


Figure 14. GET method in Wireshark.

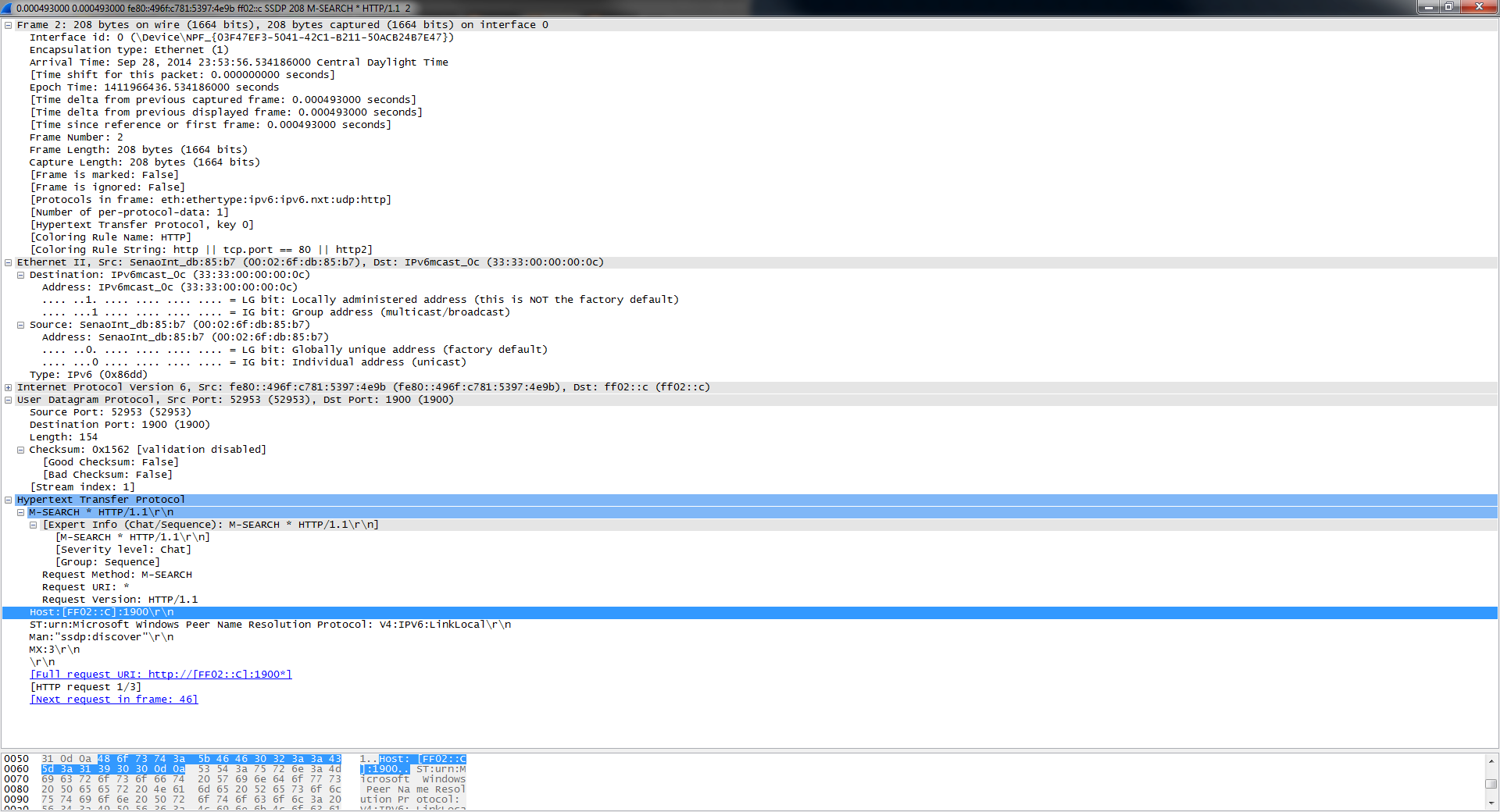


Figure 15. POST method in Wireshark.

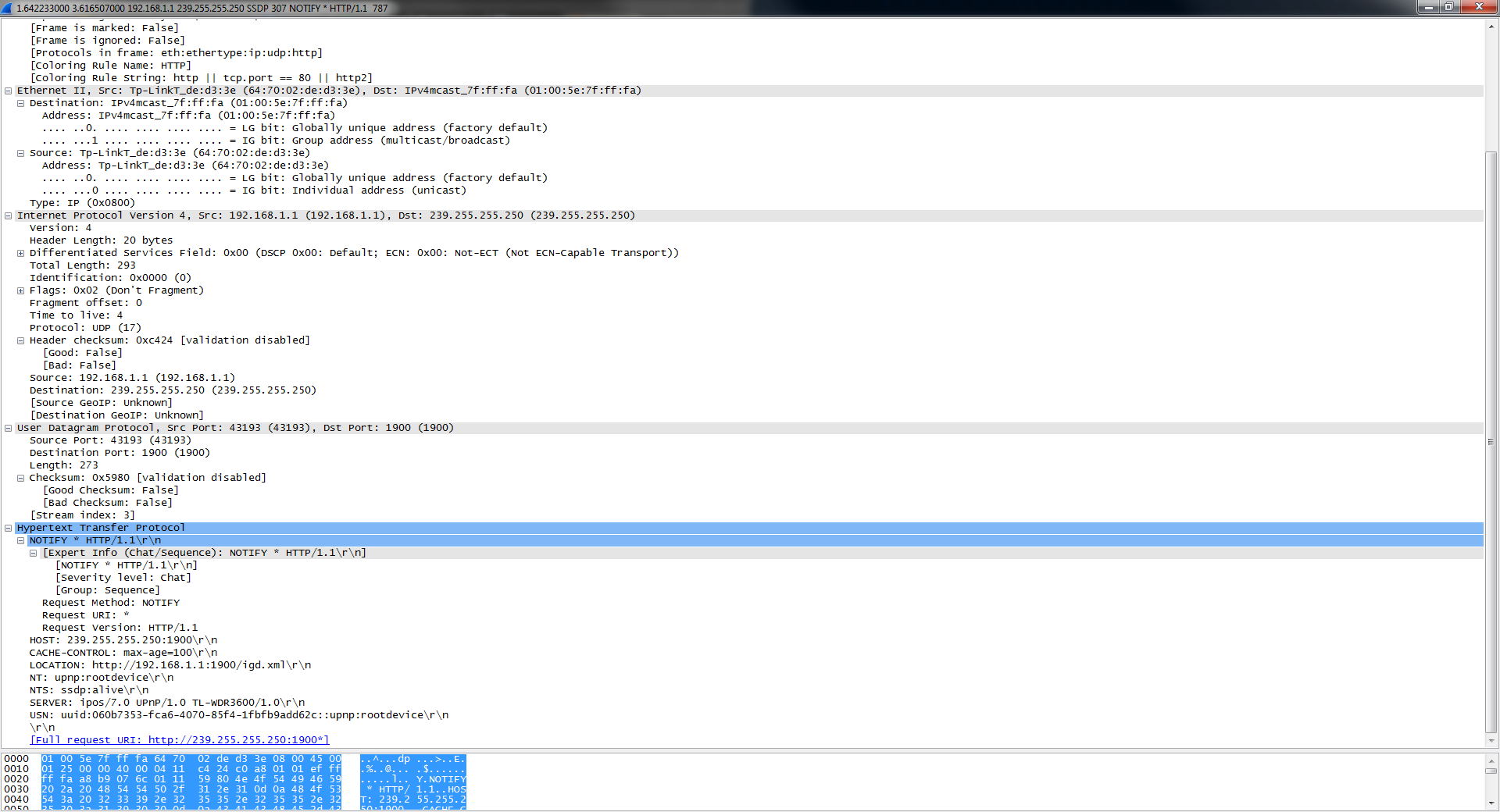


Figure 16. XMLhttpRequest from Lab4 in books.php for an XML file.

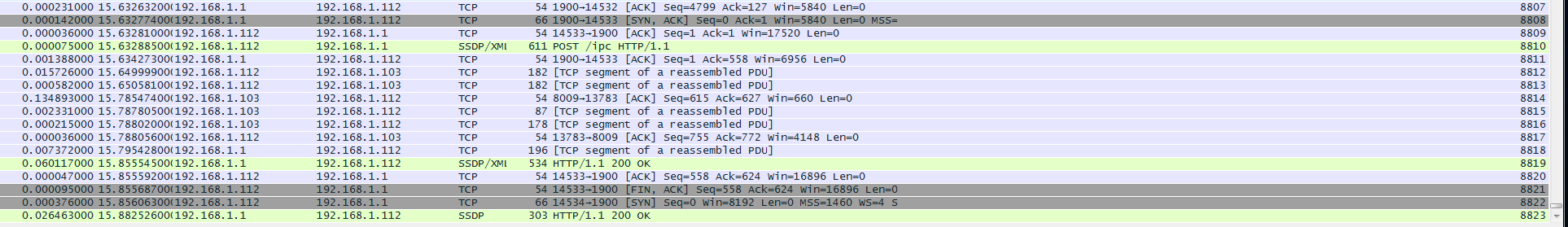


Figure 17. Setting cookies by a server and a browser for Facebook.com.

**Zenmap Section**

In addition to the Wireshark part, I installed Zenmap, the Windows GUI for nmap, to complete the following steps. Nmap is useful port scanning application that can help assess the security or your router/network/computer/server/anything. It’s another one of those tools of the trade that no hacker goes without. For this step, I scanned my Macbook Air laptop, running OS X 10.10. I ran a quick scan, intense scan, intense scan plus UDP, and intense scan plus TCP. Nmap can also run intense scan, no ping, ping scan, traceroute, and a comprehensive scan. The intense scan with TCP took the longest, at about 10 minutes.

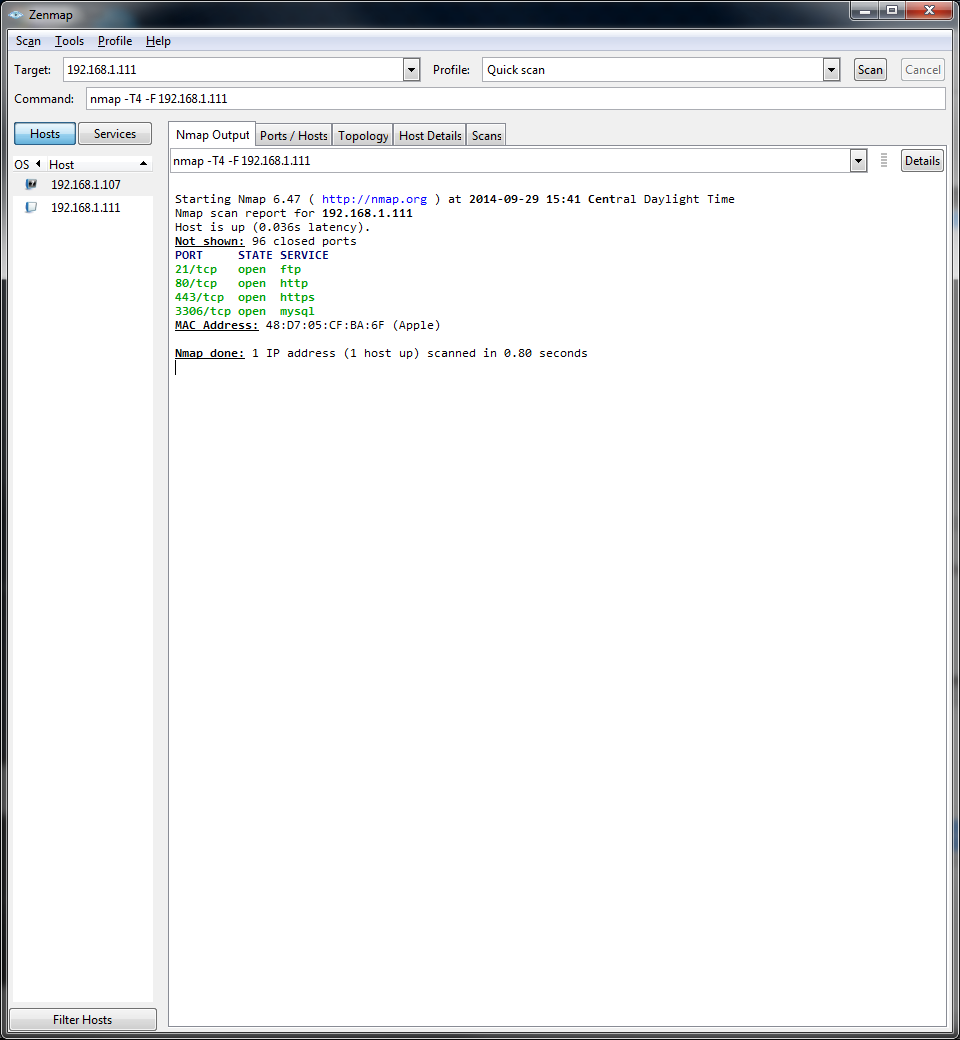


Figure 18. Quick Scan of Macbook Air.

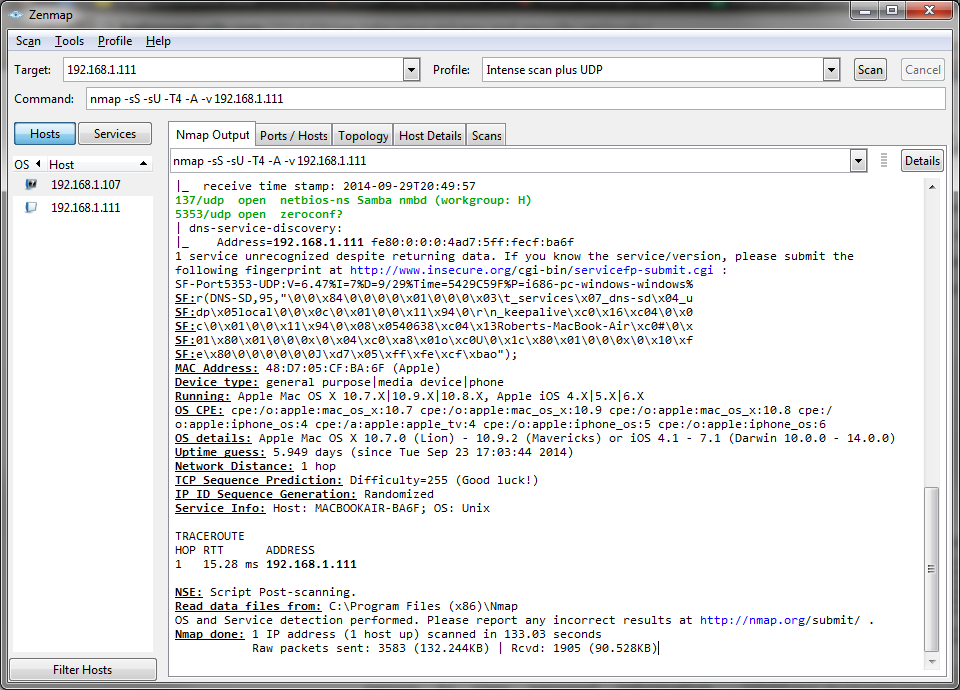


Figure 19. Intense scan plus UDP in Zenmap.

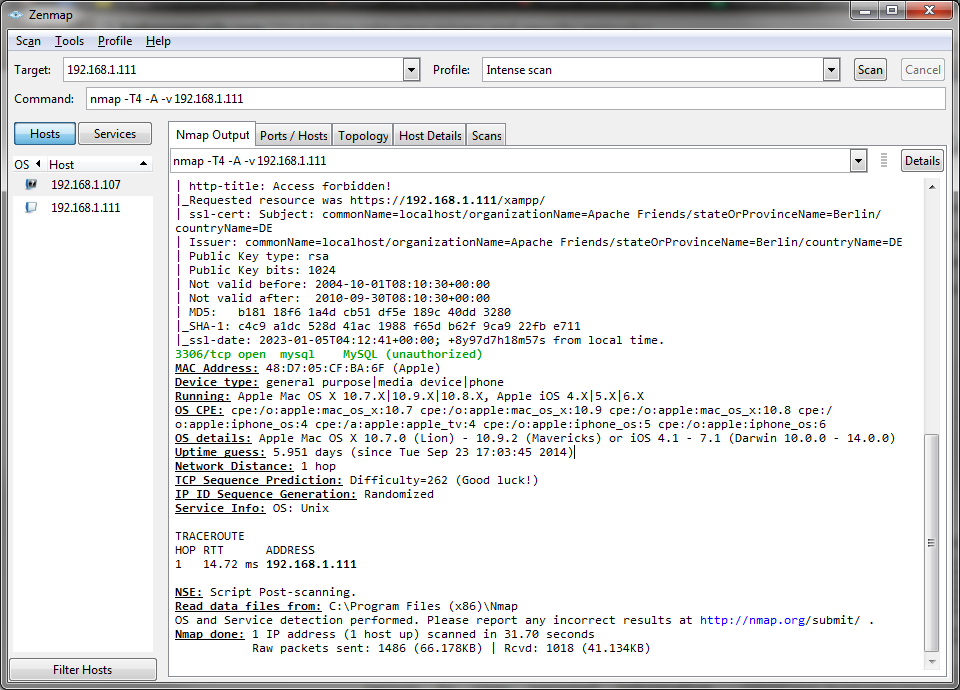


Figure 20. Intense scan.

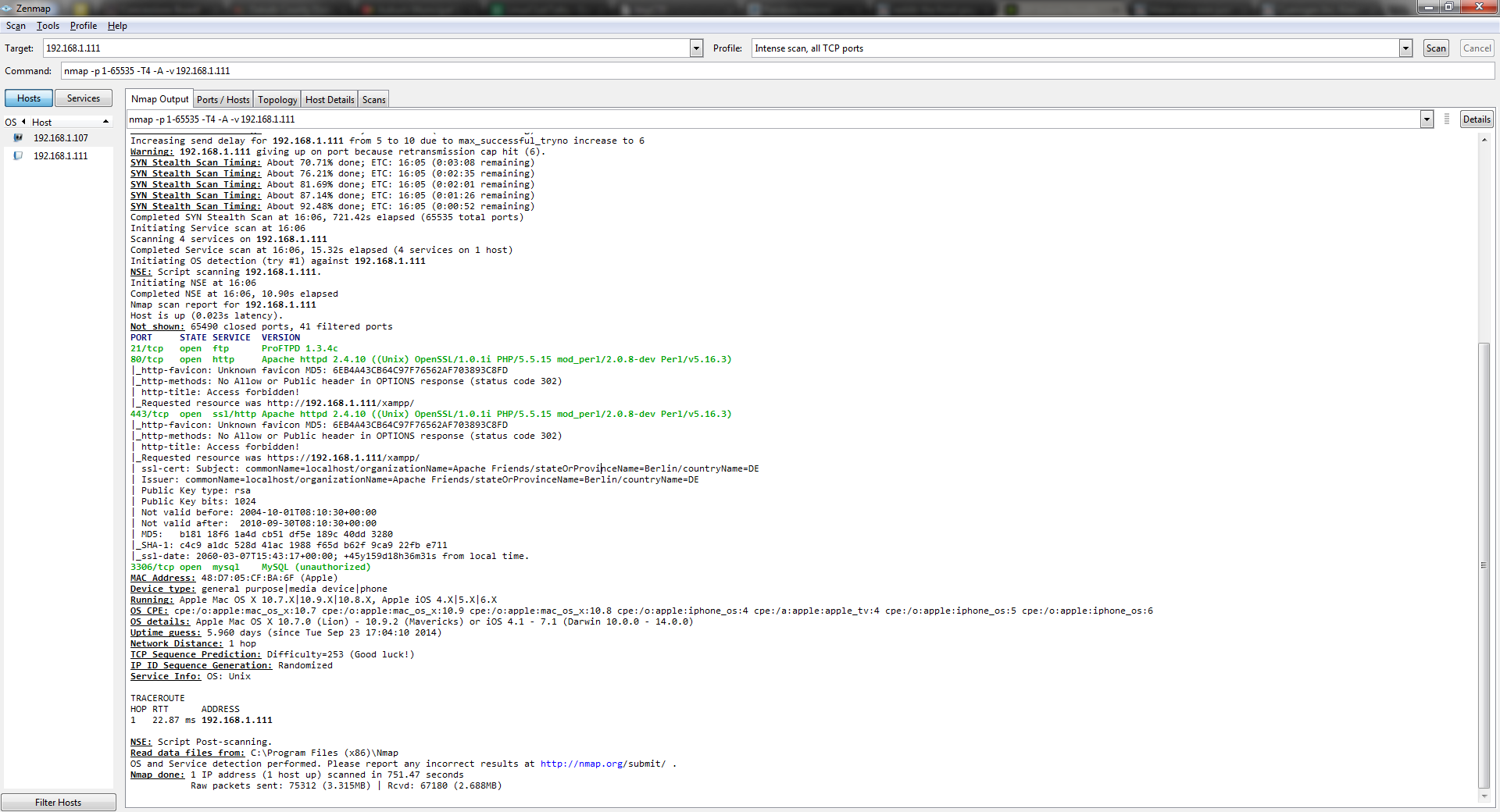


Figure 21. Intense scan with all TCP ports.

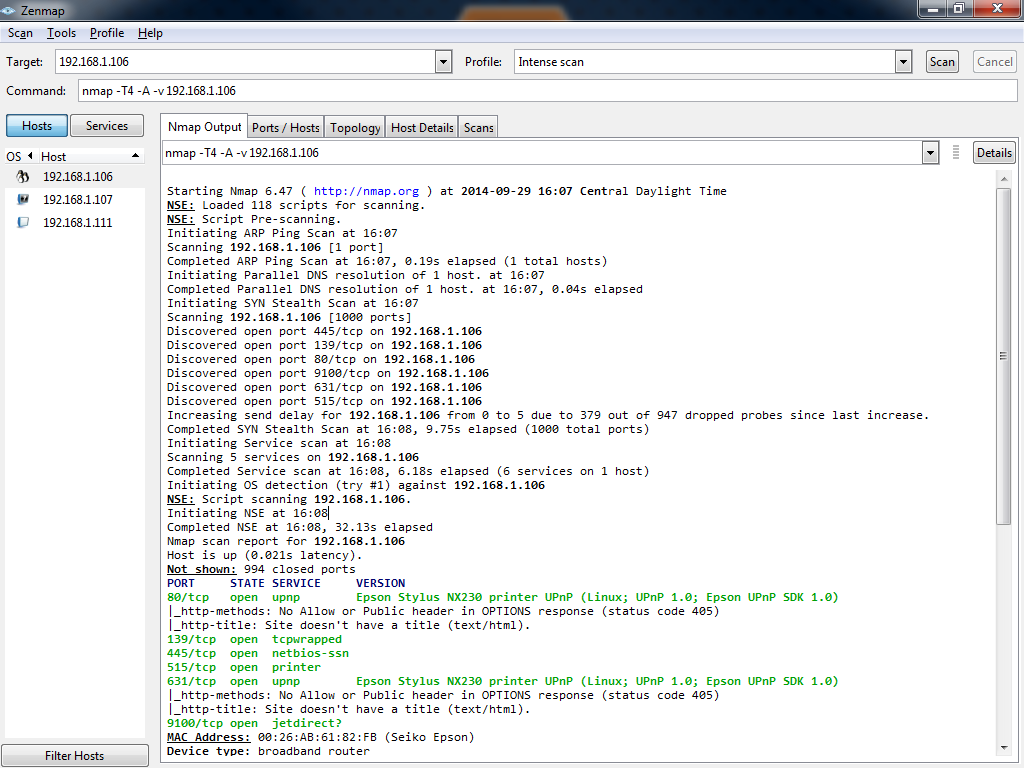


Figure 22. BONUS! I found an Epson printer on my router.

# Result

I completed both the Wireshark and the nmap sections of this lab with relative ease. This was my favorite lab, because it was the most applicable, and because we didn’t have to write any code! Nmap and Wireshark are useful penetration tools that I can use to make my roommates mad.

# Conclusion

This lab was a great introduction to two great network tools. Wireshark and Zenmap are both useful hacker tools, whether you wear a white, black, or grey hat. Hopefully I’ll have a job that is cool enough that I’ll get to use these programs regularly.

# References

* Dr. Wu’s included slides and lab materials
* <https://ask.wireshark.org/questions/4210/measuring-round-trip-time>
* https://www.youtube.com/watch?v=UUeIwzvrvoA