Lab 1 Report

Chris Auslander
ECE 4470 Computer Networks
28 January 2020

Summary

The purpose of this lab is to be able to analyze the data that is being sent to and from hosts over a computer network. We use Wireshark to observe the protocols and the data that has been sent based on a request to a specific URL. Once discovered, we can learn about the protocols used in the connection.

Key Words

Wireshark – A packet analyzer tool which tracks network data flowing in and out of the host device.

Protocol – A standard used by a network in order to interpret the data that is being provided.

1 Introduction

A computer network is made up of multiple autonomous computers which are able to pass data and communicate with each other. In order to understand one another, computer networks engineers have designed specific protocols to be able to transmit data and decode what information is being sent. When a connection is made between two computers, data is being sent both directions. The Wireshark tool allows a user to analyze this data and discover how the two machines are communicating.

The lab was broken up into two procedural steps. The first, was to run Wireshark and try to open the webpage, "http://u-tokyo.ac.jp" to see what information was being sent over the network. A list of protocols used was generated as well as a short list based on the filter of data when the tcp port equals 80. We then selected a webpage of our own to repeat the process. For this lab, I chose, "digikey.com," an electronic parts supplier.

This report is made up of sections that follow the general procedure of the lab and is listed as follows:

Section 2 – Understanding Protocols

Section 3 – Discussion and Conclusions

2 Understanding Protocols

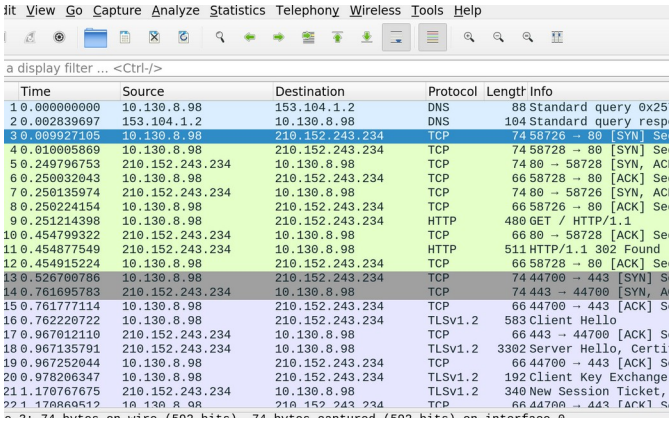
Upon analyzing the data, there were four different types of protocols that were being used over the network to communicate with U of Tokyo and Digikey. The protocols used are listed below along with a brief explanation and an image of the Wireshark output.

DNS – Domain Name System. The purpose of DNS is to be a lookup table for know ip addresses. When a URL is typed into a browser, the input is looked up in a DNS server and the resulting ip address is returned. From there, the host computer can use the ip to connect to the desired network.

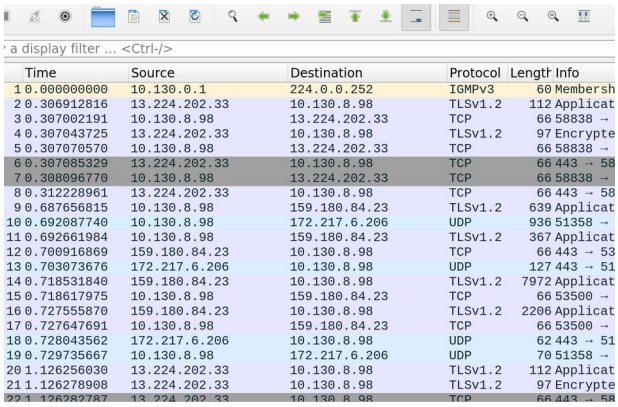
TCP – Transmission Control Protocol. The purpose of TCP is to have a standard way for computers to interpret the data that is being sent over a network.

HTTP – Hypertext Transfer Protocol. HTTP is used on the internet as a way to define messages and requests to web servers.

TLSv1.2 – Transport Layer Security. A protocol use for the security of transferring data over the internet. Encrypts data before travel over a network.



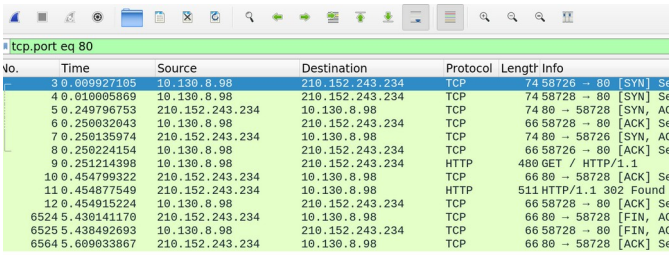
Lab 1 Report

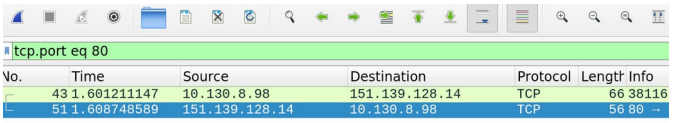


[3] https://www.cloudflare.com/learning/dns/what-is-dns/
[4] https://searchnetworking.techtarget.com/definition/TCP
[5] https://www.webopedia.com/TERM/H/HTTP.html
[6] https://wiki.openssl.org/index.php/SSL_and_TLS_Protocols

3 Discussion and Conclusion

An important feature of Wireshark is the ability to filter the data to a specific target. For this lab, we filtered to only see tcp data traveling over port 80. After contacting each server, we sampled the data with this filter and the following was returned.





By comparing the two images above, we can tell that the ip address of my laptop at the time of capture was 10.130.8.98, the ip of U Tokyo is 210.152.243.234, and the ip of Digikey is 151.139.128.14. When looking at the TCP calls, we can see that my laptop makes an initial request to each server, and then the server sends a response, completing the communication.

Protocols are essential for a fully functioning network. By scanning network traffic, we can see where information is being sent and by which type of protocol.

4 References

[1] http://u-tokyo.ac.jp
[2] https://www.digikey.com/