

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

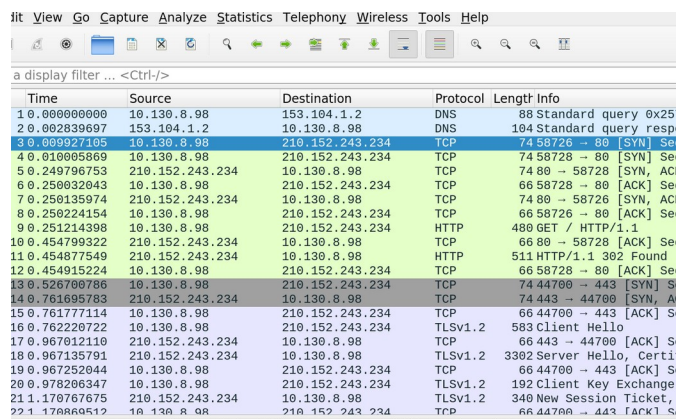
Upon analyzing the data, there were four different types of protocols that were being used over the network to communicate with U of Tokyo and Digikey. The protocols used are listed below along with a brief explanation and an image of the Wireshark output.

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.

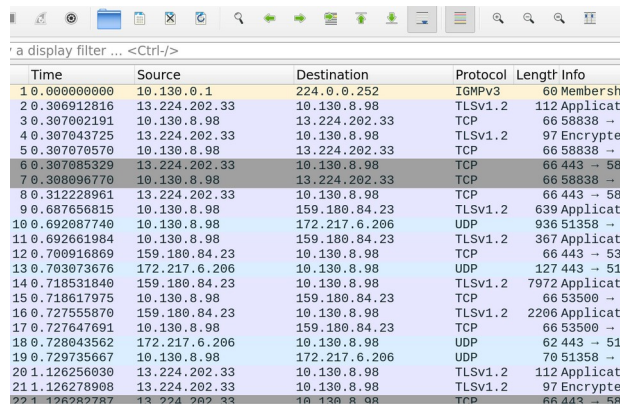
HTTP – Hypertext Transfer Protocol. HTTP is used on the internet as a way to define messages and requests to web servers.

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



Time	Source	Destination	Protocol	Length	Info
10.0000000000	10.130.8.98	153.104.1.2	DNS	88	Standard query 0x25
20.002839697	153.104.1.2	10.130.8.98	DNS	104	Standard query resp
30.009927195	10.130.8.98	210.152.243.234	TCP	74	58728 → 80 [SYN] Seq
40.010005869	10.130.8.98	210.152.243.234	TCP	74	58728 → 80 [SYN] Seq
50.249796753	210.152.243.234	10.130.8.98	TCP	74	80 → 58728 [SYN, AC
60.250032043	10.130.8.98	210.152.243.234	TCP	66	58728 → 80 [ACK] Seq
70.250135974	210.152.243.234	10.130.8.98	TCP	74	80 → 58726 [SYN, AC
80.250224154	10.130.8.98	210.152.243.234	TCP	66	58726 → 80 [ACK] Seq
90.251214398	10.130.8.98	210.152.243.234	HTTP	480	GET / HTTP/1.1
100.454799322	210.152.243.234	10.130.8.98	TCP	66	80 → 58728 [ACK] Seq
110.454877549	210.152.243.234	10.130.8.98	HTTP	511	HTTP/1.1 302 Found
120.454915224	10.130.8.98	210.152.243.234	TCP	66	58728 → 80 [ACK] Seq
130.526700786	10.130.8.98	210.152.243.234	TCP	74	44700 → 443 [SYN] S
140.761695783	210.152.243.234	10.130.8.98	TCP	74	443 → 44700 [SYN, A
150.761777114	10.130.8.98	210.152.243.234	TCP	66	44700 → 443 [ACK] S
160.762220722	10.130.8.98	210.152.243.234	TLSv1.2	583	Client Hello
170.967012110	210.152.243.234	10.130.8.98	TCP	66	443 → 44700 [ACK] S
180.967135791	210.152.243.234	10.130.8.98	TLSv1.2	3302	Server Hello, Certi
190.967252044	10.130.8.98	210.152.243.234	TCP	66	44700 → 443 [ACK] S
200.978206347	10.130.8.98	210.152.243.234	TLSv1.2	192	Client Key Exchange
210.170767675	210.152.243.234	10.130.8.98	TLSv1.2	340	New Session Ticket,
220.170860512	10.130.8.98	210.152.243.234	TCP	66	44700 → 443 [ACK] S

Lab 1 Report



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.130.0.1	224.0.0.252	IGMPv3	60	Membersh
2	0.306912816	13.224.202.33	10.130.8.98	TLSv1.2	112	Applicat
3	0.307002191	10.130.8.98	13.224.202.33	TCP	66	58838 →
4	0.307043725	13.224.202.33	10.130.8.98	TLSv1.2	97	Encrypte
5	0.307079570	10.130.8.98	13.224.202.33	TCP	66	58838 →
6	0.307085329	13.224.202.33	10.130.8.98	TCP	66	443 → 58
7	0.308096770	10.130.8.98	13.224.202.33	TCP	66	58838 →
8	0.312228961	13.224.202.33	10.130.8.98	TCP	66	443 → 58
9	0.687656815	10.130.8.98	159.180.84.23	TLSv1.2	639	Applicat
10	0.692087740	10.130.8.98	172.217.6.206	UDP	936	51358 →
11	0.692661984	10.130.8.98	159.180.84.23	TLSv1.2	367	Applicat
12	0.700916869	159.180.84.23	10.130.8.98	TCP	66	443 → 53
13	0.703073676	172.217.6.206	10.130.8.98	UDP	127	443 → 51
14	0.718531840	159.180.84.23	10.130.8.98	TLSv1.2	7972	Applicat
15	0.718617975	10.130.8.98	159.180.84.23	TCP	66	53500 →
16	0.727555870	159.180.84.23	10.130.8.98	TLSv1.2	2206	Applicat
17	0.727647691	10.130.8.98	159.180.84.23	TCP	66	53500 →
18	0.728043562	172.217.6.206	10.130.8.98	UDP	62	443 → 51
19	0.729735667	10.130.8.98	172.217.6.206	UDP	70	51358 →
20	1.126256030	13.224.202.33	10.130.8.98	TLSv1.2	112	Applicat
21	1.126278998	13.224.202.33	10.130.8.98	TLSv1.2	97	Encrypte

[3] <https://www.cloudflare.com/learning/dns/what-is-dns/>

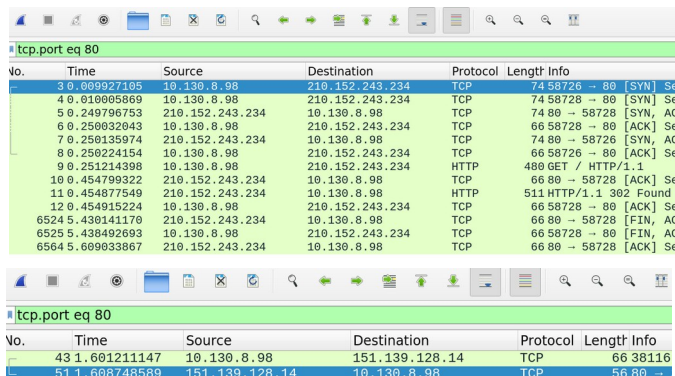
[4] <https://searchnetworking.techtarget.com/definition/TCP>

[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.



No.	Time	Source	Destination	Protocol	Length	Info
3	0.009927185	10.130.8.98	210.152.243.234	TCP	74	58728 → 80 [SYN] Seq
4	0.010005869	10.130.8.98	210.152.243.234	TCP	74	58728 → 80 [SYN] Seq
5	0.249796753	210.152.243.234	10.130.8.98	TCP	74	80 → 58728 [SYN, ACK]
6	0.250032043	10.130.8.98	210.152.243.234	TCP	66	58728 → 80 [ACK] Seq
7	0.250135974	210.152.243.234	10.130.8.98	TCP	74	80 → 58728 [SYN, ACK]
8	0.250224154	10.130.8.98	210.152.243.234	TCP	66	58728 → 80 [ACK] Seq
9	0.251214398	10.130.8.98	210.152.243.234	HTTP	480	GET / HTTP/1.1
10	0.454799322	210.152.243.234	10.130.8.98	TCP	66	80 → 58728 [ACK] Seq
11	0.454877549	210.152.243.234	10.130.8.98	HTTP	511	HTTP/1.1 302 Found
12	0.454915224	10.130.8.98	210.152.243.234	TCP	66	58728 → 80 [ACK] Seq
6524	5.430141170	210.152.243.234	10.130.8.98	TCP	66	80 → 58728 [FIN, ACK]
6525	5.430492693	10.130.8.98	210.152.243.234	TCP	66	58728 → 80 [FIN, ACK]
6564	5.609333867	210.152.243.234	10.130.8.98	TCP	66	80 → 58728 [ACK] Seq

No.	Time	Source	Destination	Protocol	Length	Info
43	1.601211147	10.130.8.98	151.139.128.14	TCP	66	38116 →
51	1.608748589	151.139.128.14	10.130.8.98	TCP	56	80 →

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/>