**Incident Report:** CH-15054-Intro-Wireshark

**Date:** 10-18-2022

**Executive Summary:**

As a means of an introduction to the Live Project, the goal of this reserve story was to familiarize myself with Wireshark and how it can be used when working as a cyber security professional.

**Methodology:**

To complete this task successfully, I took the following actions, in order:

1. Watched the YouTube tutorial - Simply Cyber’s “SOC Analyst Skills - Wireshark Malicious Traffic Analysis”
2. Followed along with the tutorial to access the additional resources referenced in the video:
   1. Malware-traffic-analysis.net
   2. Macvendorlookup.com
   3. Wireshark OUI lookup
   4. Virustotal.com
3. Downloaded and installed Wireshark on my device

**Findings/Solutions:**

Through this tutorial, I learned about the basic features of Wireshark, a network analysis tool used by SOC analysts and Blue Team/Security Ops in their forensic analysis of captured network traffic. Using the malware-traffic-analysis.net exercise “OK Boomer,” the video instructor walked me through the ways in which Wireshark can be used to glean specific information about the endpoints and traffic into and out of a specific network and its sources. Some of the analysis tools reviewed in this tutorial were:

* DNS queries
* Filtering specific endpoint addresses to analyze traffic through certain ports
* Web traffic statistics, such as protocol hierarchy and distribution and following TCP streams
* MAC address information
* User account log-ins for specific locations (i.e. cNameString)
* Identifying downloaded executables via IP contains “This program” searches
  + Using virustotal.com to determine whether or not the file (or web address) contains malware
* Locating infected points of entry on a network by tracking where malicious packages were sent
  + Adding any identified malware to block lists

**Conclusions:**

Wireshark is a necessary tool for any tier 2-level SOC analyst work and can be used as a resource when completing cyber security defensive tasks. Malware-traffic-analysis.net is an incredibly helpful resource to use to practice using Wireshark and hone one’s cyber security skills, as it provides relevant, real-world exercises and tutorials that will help improve on-the-job training. I will be using this resource to enhance my own job application as an entry level cyber security professional.