**INCIDENT REPORT: TS-1894-Intro: Wireshark**

**Date: 06/11/2024**

**Executive summary:**

The objective of this User Story is to get familiar with basic operations in Wireshark.

**Methodology:**

Per the User Story instructions, I visited the Malware-Traffic-Analysis.net site, and downloaded the MTA-2019-files-contains-malware.zip file. I was able to make the necessary file extractions and was able to get a copy of the 2019-11-12-traffic-analysis-exercise.pcap. file and open it with Wireshark. I then followed along on the assigned YouTube link with Charlie Auger of Simply Cyber: <https://www.youtube.com/watch?v=M8yoYmiL7rA>.

**Findings/Solutions:**

The video demonstrated some captured traffic that was prepared by Malware-Traffic-Analysis.net, which contained malicious code. This included some exercises such as identifying the Operating System used in the traffic (Chrome), and the manufacturer information through the MAC Address (Motorola/Lenovo).

Wireshark was able to filter the huge volume of captured data down to a specific IPV4 address, and the contents of the traffic between the client and server could be analyzed in detail. I visited Wireshark’s site directly, and glanced through their own tutorial documentation, which was quite thorough. It made note that Wireshark is designed to examine network packets, but won’t alter or inject testing payloads into the packets for vulnerability testing.

Charlie Auger mentioned that this program is essential to a Cyber Security Professional, and the process followed in the demonstration was applicable to a “Level 2” SOC Analyst. He briefly mentioned that a common task for entry-level SOC Analysts is to contact end-users and gather information about phishing incidents.

Included below (on the next page) is the required screenshot of the exercise file open in Wireshark:

