**Incident Report: KG-19104-Intro:-Wireshark  
Date:** 09-16-2024

### **Executive Summary**

In this task, I familiarized myself with Wireshark by analyzing a PCAP file from a traffic analysis exercise called "Okay-Boomer." The objective was to understand how to use Wireshark for identifying network traffic details, answering questions related to device operating systems, MAC addresses, and traffic activities from the captured network packets.

### **Methodology**

I followed these steps to complete the analysis:

1. **Downloaded the PCAP File:**I accessed the PCAP file from the provided link, extracted it on my Kali Linux VM, and opened it in Wireshark for detailed analysis.
2. **Performed the Traffic Analysis Exercise:**I reviewed the PCAP file, focusing on the following questions to gain insights into the network traffic:
   * Identified operating systems and devices for IP addresses such as 10.11.11[.]94, 10.11.11[.]121, and others.
   * Determined the manufacturer/vendor based on MAC addresses, such as for 10.11.11[.]145.
   * Investigated Windows hosts, identifying user account names, versions, and activities.
   * Analyzed traffic to discover the IP that downloaded a Windows executable, the URL of the file, and its SHA256 hash.
   * Checked the VirusTotal detection rate for the executable file and tracked public IP connections made by the Windows host after downloading the file.
3. **Used Wireshark Filters:**Throughout the exercise, I utilized Wireshark’s filtering options to narrow down the relevant traffic and analyze the details of the captured packets, making it easier to answer each of the provided questions.

### **Findings/Solutions**

This exercise provided valuable hands-on experience in using Wireshark to analyze malicious network traffic. The ability to identify operating systems, file hashes, and suspicious connections highlights the importance of packet analysis in detecting and responding to network threats. This knowledge will be useful in future tasks involving malware detection and network forensics.

**Project Description**

The purpose of this story is to get you familiarized working with the software, Wireshark.

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. In the live project, you will be using Wireshark for PCAP file analysis which contains network traffic from a machine. PCAP files are creating from applications, like Wireshark, that contain TCP/IP and UDP network packets. In theory, it's a table of contents of incoming and outgoing traffic from your computer.

Here is a video that goes in depth on using Wireshark to analyze a PCAP file that has some malicious content inside of it. This will be very close to what the Defensive stories will be asking later on in the live project. You will need to follow step-by-step with the instructor on the video to get a hands on feel with achieving the end result.

**Wireshark**:

<https://www.wireshark.org/>

**Video**:

<https://www.youtube.com/watch?v=M8yoYmiL7rA>

**PCAP FILE**:

<https://www.malware-traffic-analysis.net/archived/index.html>

* Click MTA-2019-files-contains-malware.zip to download the zip that contains the PCAP for the tutorial above.
  + Make sure that you've downloaded this into your Kali Linux VM. Do not download this outside of your VM.
* Once downloaded you'll need to extract the contents and a new zip should appear: 2019.zip.
* Extract 2019.zip and a folder named "2019" will appear. Open this folder.
* Open folder 11, then folder 12.
* Inside folder 12 will be the zip for the PCAP file you need for the tutorial: 2019-11-12-traffic-analysis-exercise.pcap.zip
* Extract this final zip to gain access to 2019-11-12-traffic-analysis-exercise.pcap. Open this file with Wireshark.

Once you have completed the video, go ahead and write a brief incident report on what you learned and how you can use that information as a Cyber Security professional. Include a screenshot of the tutorial PCAP open in Wireshark.