Incident Report 13068: Intro: Wireshark

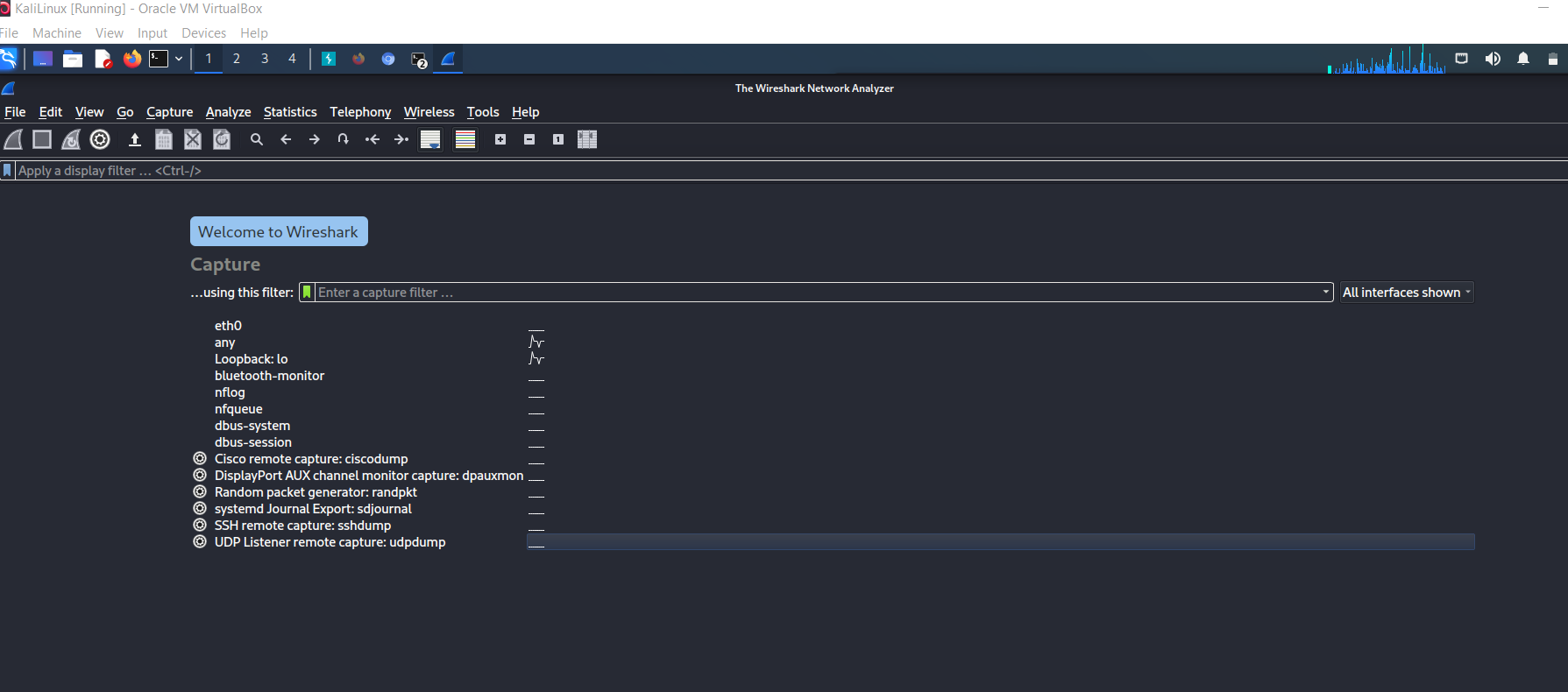
Date: 5-24-2022 (DS)

# Executive Summary:

I learned a few tips on how to navigate in Wireshark including:

* malware-traffic-analysis.net (malicious traffic lab/tutorials)
* Analyzing Pcap files
* Endpoints - apply IPs as a filter
* Protocol Hierarchy Stats - you can filter by things like http only or kerberos.
* Following TCP streams allows you to get a built message (like OS and type of device)
* mac address lookup (or wireshark OUI lookup) will tell you the device information.
* Be careful of opening possible malicious executables or portable executables (PE files)
* File/Export Objects may show as one file but actually be another
* You can download these and send them to virustotal.com to be scanned for malicious files.
* Once you find the infected machine you can take the hash and search for it anywhere else

**Results**

****

**Application Details:**

Application was installed successfully.

**Attack Narrative:**

No attack or defensive incidents yet. (Preparation)

**Conclusion:**

I learned a lot about Wireshark and how much of a very good tool it is to use for a forensic analyst in cybersecurity. I still feel like I have a lot to learn with just what to look for but I hope that the experience with these next stories will make it easier.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_