1. **Activity 10.1: Analyze a network capture file**

Follow the instructions for the lab found in your textbook. Submit a word document listing which source file you used and the answers. This is great practice for Wireshark!

## Source File: 2022-01-07 - TRAFFIC ANALYSIS EXERCISE – SPOONWATCH

A screenshot of a computer

Description automatically generated

* Write an incident report based on the pcap and the alerts.
* The incident report should contains 3 sections:
* **Executive Summary**: State in simple, direct terms what happened (when, who, what).
* **Details**: Details of the victim (hostname, IP address, MAC address, Windows user account name).
* **Indicators of Compromise (IOCs)**: IP addresses, domains and URLs associated with the infection.  SHA256 hashes if any malware binaries can be extracted from the pcap

Answers:

Executive summary:

On the 21st of March 2022, around 20:58 UTC, an infiltration of IcedID (Bokbot) malware followed by Cobalt Strike occurred on a Windows host utilized by Patrick Zimmerman.

The details are as follows:

Name of host: DESKTOP-5QS3D5D

MAC address: 00:60:52:b7:33:0f; IP address: 10.0.18.14

The user account name on Windows is patrick.zimmerman.

IP addresses and domains connected to IcedID (Bokbot):

Indicators of Compromise:

Port 80 of 188.166.154.118 is oceriesfornot.top. - GET port 443 at 157.245.142.66 - antnosience.com - Suncoastpinball.com - HTTPS traffic at 160.153.32.99 port 443. - HTTPS traffic at port 443, 157.245.142.66; - otectagain.top - HTTPS traffic on port 443, 91.193.16.181; - seaskysafe.com - HTTPS traffic on port 443 at 91.193.16.181 for dilimoretast.com - Traffic over HTTPS

Unusual behavior with file-sharing domains:

Filebin.net port 443 is used for HTTPS traffic.

HTTPS traffic on situla.bitbit.net port 443

IP addresses and domains connected to Cobalt Strike:

Port 757 - 23.227.198.203 - bupdater.com - Traffic over HTTPS