Network Monitoring SOP (Wireshark):

Purpose:

Process to implement Wireshark to monitor network activity to identify nefarious activity or employee misuse.

Scope:

Wireshark will be utilized to monitor all network activity within the organization's infrastructure.

Responsibilities:

Information Technology (IT) department has sole responsibility for monitoring the organizations network. IT Department is required to conduct real-time monitoring of traffic based on an established network baseline.

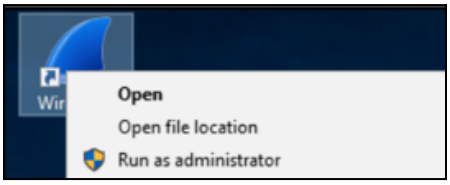
Prerequisites:

Wireshark - world's most popular network protocol analyzer

Wireshark should be run as an administrator for full functionality.

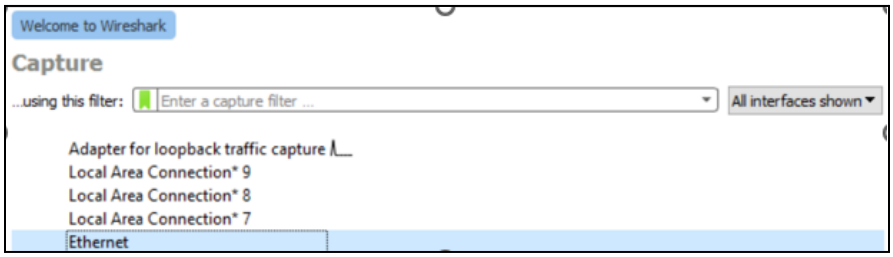
Procedure:

- **1. Download, Install, and Launch Wireshark**
    - Download Wireshark from the official website wireshark.org (Wireshark)
        - Ensure you select the correct install file for your Operating System (OS)
        - Select all defaults during installation wizard
    - Launch Wireshark as an administrator
        - Right click on icon > Select Run as administrator



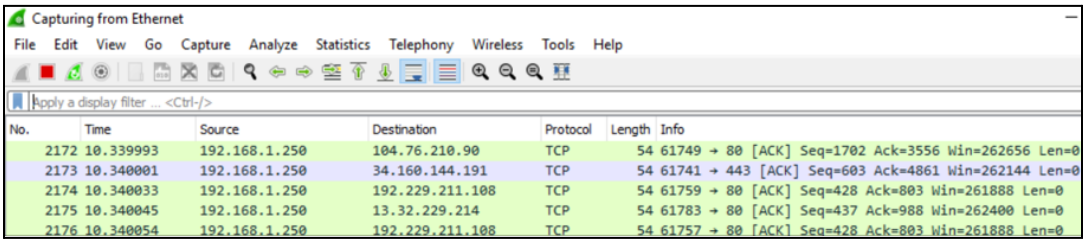
- **2. Select a Network Interface**

    - After launch available network interfaces are displayed
        - Left click twice on the network interface you would like to monitor



- **3. Capture Network Traffic**

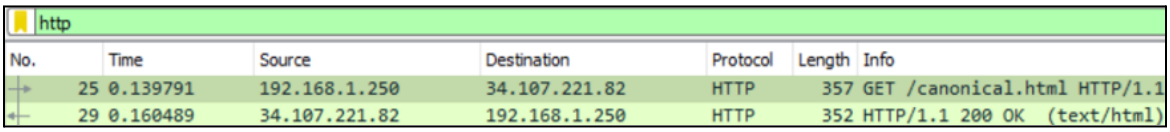
    - After selecting the appropriate network interface packet capture initiates



    - Capture remains active until red square STOP button is selected

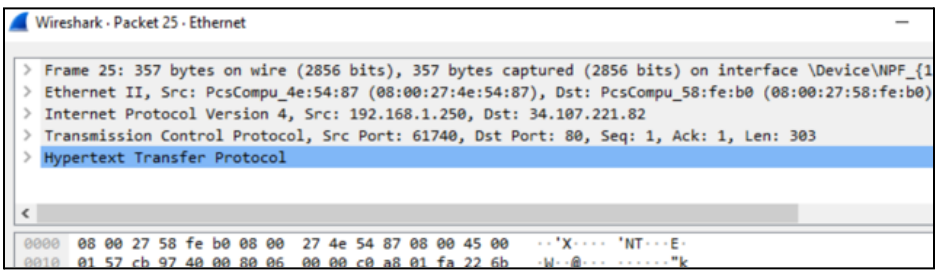
- **4. Apply Display Filters**

    - Filters can be applied to look at specific traffic to include specific protocols
        - Below Wireshark's filtering is used to only observe HTTP traffic



- **5. Analyze Network Traffic**

    - To analyze a specific packet left click twice on the packet to select it



- Once selected several headings can be expanded to observe additional details
    - In the example below the HTTP heading is expanded which provides us more detailed information on the HTTP GET request packet

- **6. Stop & Save Captured Traffic**

    - Left click on the red square STOP button to halt the capture
        - To save capture left click File > Save As… > Name .pcap file and select Save

References:

- So, You Want to Write an SOP?
- 37 Best Standard Operating Procedure (SOP) Templates
- How to Use Wireshark to Capture, Filter and Inspect Packets
- What Is a Network Interface?
- Display Filters
- PCAP: Packet Capture, what it is & what you need to know

Definitions:

- **Network Interface** - interconnection between a computer and a private or public network
- **Display Filters** - for general packet filtering while viewing
- **Pcap** – application programming interface (API) that captures live network packet data

Revision History:

4/4/2022 -- "Network Monitoring SOP" created by Rob Gregor