Standard Operating Procedure (SOP) to monitor network traffic between Windows workstation and Windows server

Objective:

This SOP provides information for monitoring the traffic that travels on the Corporate Home Network for administrator use on Windows Server.

Scope:

This SOP applies to IT administrators, Network administrators, and Help Desk Staff.

Procedure

Determine if Wireshark is downloaded

- Wireshark is a network protocol analyzer that captures network traffic
- Make sure Wireshark is downloaded and installed using the command “where wireshark.exe”

Installing Wireshark

- If Wireshark is not installed, go to the official Wireshark website’s download page with the provided link: https://www.wireshark.org/download.html
- Click on Windows x64 Installer to download

Open Wireshark

- Open Wireshark by doing either of the following
    - Go to File Explorer and clicking on Wireshark
    - Enter the command C:\Program Files\Wireshark and then wireshark.exe

Monitor network traffic

- In Wireshark, select the network adapter that currently has network traffic occurring in real time
- Halt the capture and review the captured packets

Document

- Provide detailed documentation of any important or unusual information that may be displayed by Wireshark
- Maintain that information for new employees to go over