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:

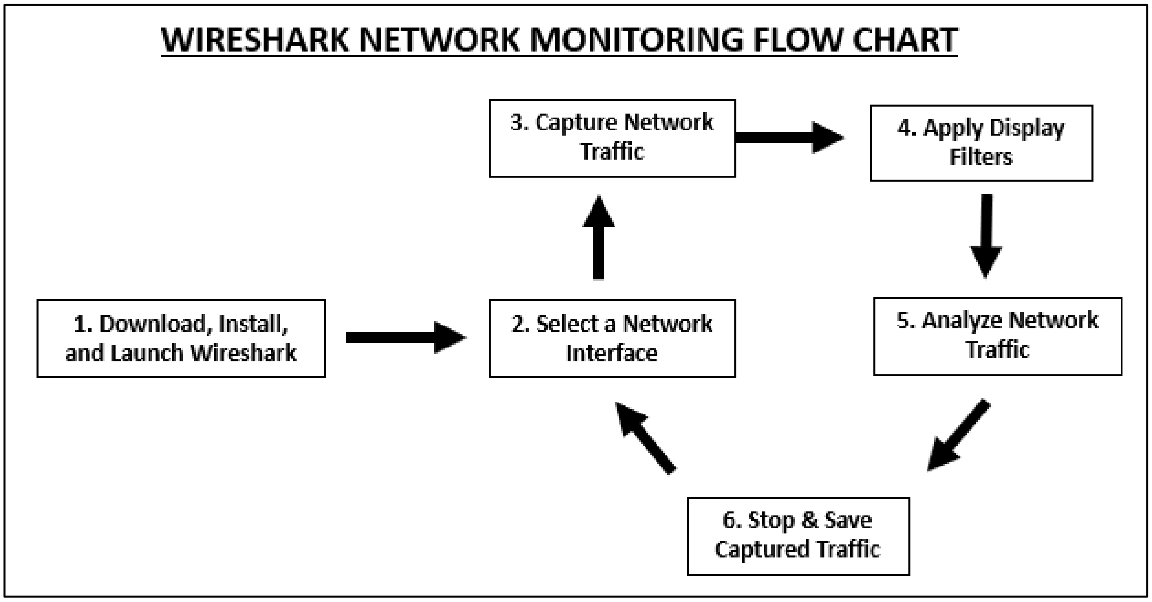
Information Technology (IT) department has sole responsibility for monitoring the organizations network. IT Department is required to conduct real-time monitoring of traffic based on an established network baseline.

Prerequisites:

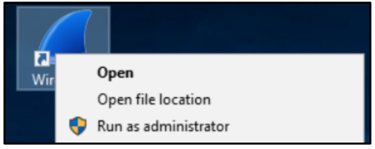
Wireshark - world's most popular network protocol analyzer

Wireshark should be run as an administrator for full functionality.

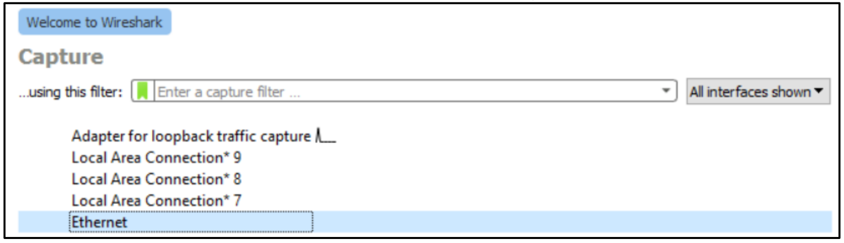
Procedure:


WIRESHARK NETWORK MONITORING FLOW CHART
1. Download, Install, and Launch Wireshark
2. Select a Network Interface
3. Capture Network Traffic
4. Apply Display Filters
5. Analyze Network Traffic
6. Stop & Save Captured Traffic

- **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

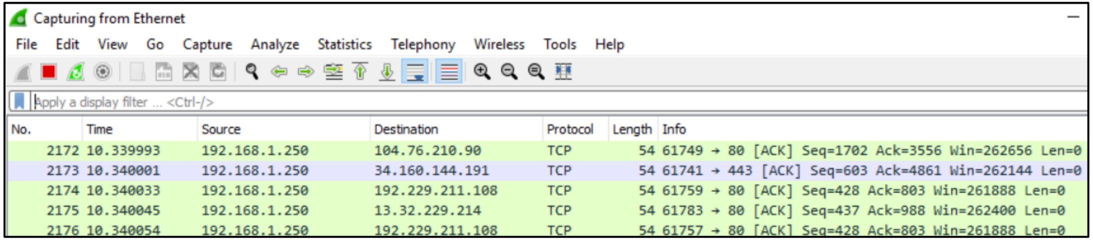


- **2. Select a Network Interface**
  - After launch available network interfaces are displayed
    - Left click twice on the network interface you would like to monitor



Adapter for loopback traffic capture
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Ethernet

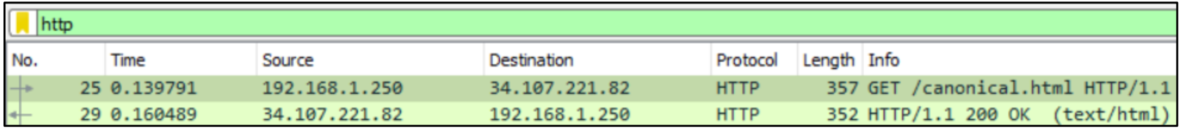
- **3. Capture Network Traffic**
  - After selecting the appropriate network interface packet capture initiates



No.	Time	Source	Destination	Protocol	Length	Info
2172	10.339993	192.168.1.250	104.76.210.90	TCP	54	61749 → 80 [ACK] Seq=1702 Ack=3556 Win=262656 Len=0
2173	10.340001	192.168.1.250	34.160.144.191	TCP	54	61741 → 443 [ACK] Seq=603 Ack=4861 Win=262144 Len=0
2174	10.340033	192.168.1.250	192.229.211.108	TCP	54	61759 → 80 [ACK] Seq=428 Ack=803 Win=261888 Len=0
2175	10.340045	192.168.1.250	13.32.229.214	TCP	54	61783 → 80 [ACK] Seq=437 Ack=988 Win=262400 Len=0
2176	10.340054	192.168.1.250	192.229.211.108	TCP	54	61757 → 80 [ACK] Seq=428 Ack=803 Win=261888 Len=0

  - Capture remains active until red square STOP button is selected

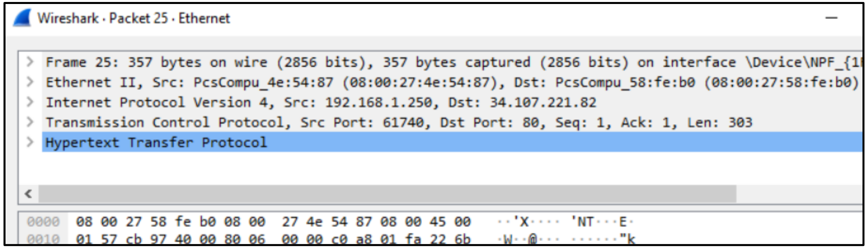
- **4. Apply Display Filters**
  - Filters can be applied to look at specific traffic to include specific protocols
  - Below Wireshark's filtering is used to only observe HTTP traffic



http

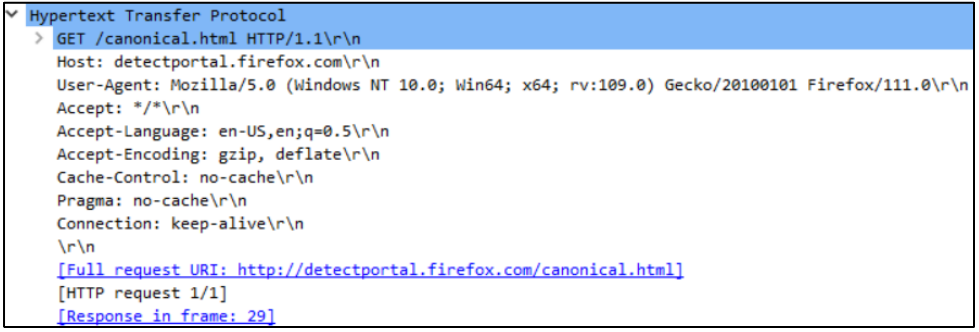
No.	Time	Source	Destination	Protocol	Length	Info
25	0.139791	192.168.1.250	34.107.221.82	HTTP	357	GET /canonical.html HTTP/1.1
29	0.160489	34.107.221.82	192.168.1.250	HTTP	352	HTTP/1.1 200 OK (text/html)

- **5. Analyze Network Traffic**
  - To analyze a specific packet left click twice on the packet to select it



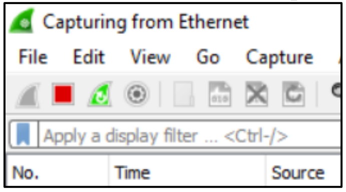
```
> Frame 25: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF_{1
> Ethernet II, Src: PcsCompu_4e:54:87 (08:00:27:4e:54:87), Dst: PcsCompu_58:fe:b0 (08:00:27:58:fe:b0)
> Internet Protocol Version 4, Src: 192.168.1.250, Dst: 34.107.221.82
> Transmission Control Protocol, Src Port: 61740, Dst Port: 80, Seq: 1, Ack: 1, Len: 303
> Hypertext Transfer Protocol

0000  08 00 27 58 fe b0 08 00  27 4e 54 87 08 00 45 00   ··'X···· 'NT···E·
0010  01 57 cb 97 40 00 80 06  00 00 c0 a8 01 fa 22 6b   ·W··@··· ······"k
```

  - 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



```
v Hypertext Transfer Protocol
  > GET /canonical.html HTTP/1.1\r\n
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Cache-Control: no-cache\r\n
    Pragma: no-cache\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://detectportal.firefox.com/canonical.html]
    [HTTP request 1/1]
    [Response in frame: 29]
```

- **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