This lab is designed for the student to use a standard tool used by the network administrator for forensics work.

**Part 1: Open Wireshark and file**

Open Wireshark on your VM and navigate to the location the Wireshark Trace files are located. Open the sec-nmap-intensescan.pcapng file.

**Part 2: Apply the appropriate filters and answer the following.**

1. Apply a filter for ICMP. Analyzing the results of the filter, what would this indicate?

A lot of Echo (ping) requests are being made and it’s getting no response back from the destination. The IP address seems unreachable.

1. What is the source of the scan of line 2821?

192.168.1.76

1. What the target of line 114?

128.241.194.25

1. Conduct a filter on HTTP packets. On line 2267, what Web server technology was used?

Microsoft-IIS/6.0\r\n

1. In the general analysis of the HTTP traffic, are there any indicators of reconnaissance tools? If so what tool?

On the info tab, Line 4392 and Line 4803 have the (application/ x-www-form-URL encoded)

1. In line 3142, what can be learned about the HTTP traffic?

There was a GET request made for the test file /robots.txt from the source IP 192.168.1.76 to the Destination IP 128.241.194.25. There is a warning alert that indicates an unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.

1. In line 3142, what does the URL (Uniform Resource Locator) indicate?

Since port 443 is always open for HTTP. Something else could be listening on the same port.

1. With all filters cleared and using the Tools Menu, determine if any credentials were used, what protocol used them and what lines were they used on?  
     
   FTP Protocol. Line 3540 and Line 4748.
2. Are there any Firewall ACL rules found? Copy and paste results below this line.

Graphical user interface, text, application

Description automatically generated