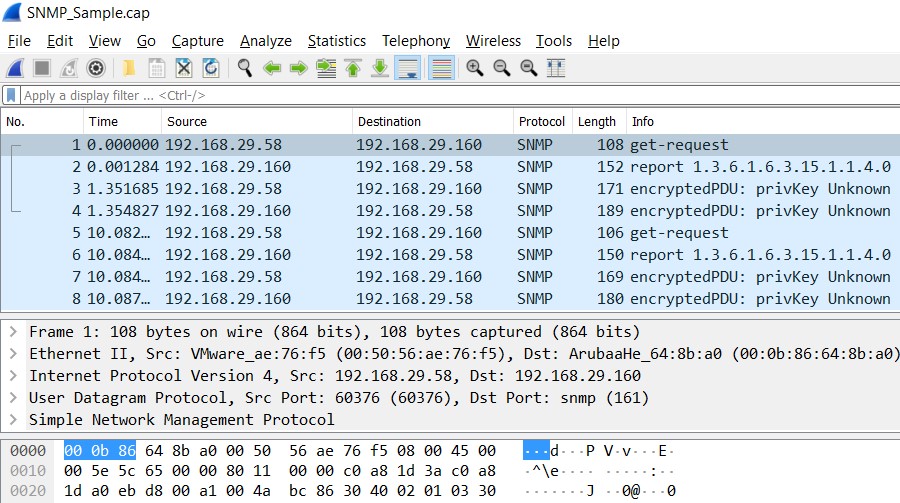
This lab involves analysis of two packet capture (pcap) files (SNMP\_Sample.cap and HTTP\_Sample.cap) using the Wireshark network analysis tool. The pcap files are available on Blackboard as attachments to the project assignment. Open each file in Wireshark and use it to determine answers to the questions below the underlined file name. To complete the assignment, **upload a Word (.docx) or Adobe (.pdf) file with answers to the numbered questions as your submission to this assignment in Blackboard**.

****

**SNMP\_Sample**

1. Examine the details in the first packet. What transport layer protocol is being used?

**UDP is being used**

1. What is the first packet’s destination port number? What is the significance, if any, of this port number?

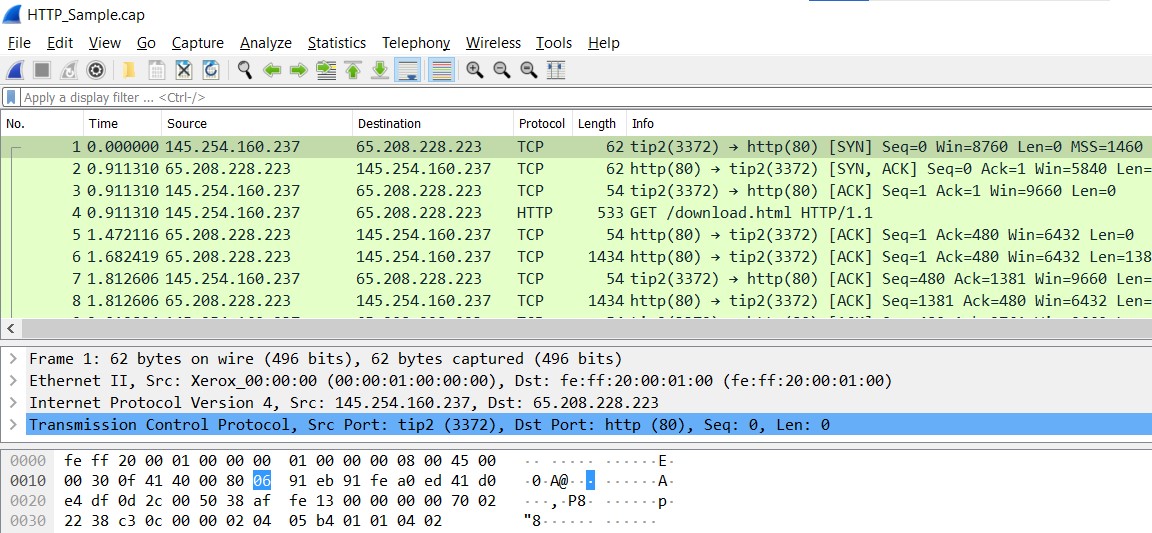
**Destination port number is 161. The significance is it is used by SNMP to send and receive requests and messages.**

1. What is the first packet’s source port number? What is the significance, if any, of this port number?

**The packet's source port number is 60376. The significance of this port number is that UDP will not think error checking is necessary therefore messages may arrive out of order, duplicated, or missing.**

1. Consider all 8 packets in this pcap file. Taken together, are they part of a connection-oriented message between two endpoints? Why or why not?

**Since they are using UDP protocol the message is not connection-oriented but connectionless. Connection-oriented uses TCP as its protocol.**



**HTTP\_Sample**

1. Examine the details in the first packet. What transport layer protocol is being used?

**The TCP protocol is being used**

1. What is the first packet’s destination port number? What is the significance, if any, of this port number?

**The destination port number is 80. The significance of port 80 is that it is the primarily used by the world wide web system. It is called the well-known port and every web browser automatically generates a port address of 80 for any web page you click on.**

1. What is the first packet’s source port number?

**The source port number is 3372**

1. Examine the first 3 packets. What transport layer flags are set and what does this sequence of packets represent in terms of a connection-oriented messaging session?

**The flags that are sent are an acknowledgement (packet 3) segment a synchronize segment (packet 1) or both (packet 2). The packets are establishing a connection to the receiver since the packet is sending a SYN segment and the acknowledgement segment is also sent by the sender when the receiver (usually a server) sends its own SYN segment. This is a called a three-way handshake.**