Assignment: Network Activity Attack
By: Shihab Islam

Section 1: Identify the type of attack that may have caused this network interruption
One possible explanation for the website's connection timeout error message is due to a Denial of Service (DOS) attack. The logs reported from Wireshark report the network is overloaded with SYN packet requests. This is a type of DOS attack usually known as SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction
Normally when visitors visit the website the connection occurs using a TCP protocol. It is defined in three steps. 1. A SYN packet is sent from the source to the destination, requesting to connect. 2. The destination sends back a SYN/ACK packet to agree to the connection from the source. Then it will attempt to reserve resources for the connection. 3. The source then sends a ACK packet back and agrees to the connection. In this case the SYN flood attack sends a huge amount of SYN packets into the server network and overloads the ports to agree to a connection. As a result TCP connection can not be possible and no resources exist in the connection for it. Any new visitor will be timed out with an error message with every new legitime SYN packet.