# 9.3 Lab: Analyze a DDoS Attack

**Candidate:** COMPTIA COMPTIA ()
**Time Spent:** 00:51

**Score: 0%**

## Task Summary

## Lab Questions

✕ Filter for SYN and ACK packets

✕ *Q1*: Which sign indicates this is a distributed denial-of-service (DDoS) attack?

Your answer:

Correct answer: There are multiple source addresses for the SYN packets with the destination address 198.28.1.1.

## Explanation

Complete this lab as follows:

1. Use Wireshark to capture packets and filter for packets with the SYN flag set.
   a. From the Favorites bar, select **Wireshark**.
   b. Under Capture, select **enp2s0**.
   c. From the menu, select the **blue fin** to begin the capture.
   d. In the *Apply a display filter* field, type **tcp.flags.syn==1 and tcp.flags.ack==0** and press **Enter** to filter the Wireshark display to show packets with only the SYN flag.

      Notice that there is a flood of SYN packets being sent to 198.28.1.1 (www.corpnet.xyz).

2. Use a filter to display only packets that have the SYN flag and the ACK flag set.
   a. In the *Apply a display filter* field, change the ending of the **tcp.flags.ack** portion from a **0** to a **1** and press **Enter** to filter the Wireshark display to only those packets with both the SYN flag and ACK flag.

      You should notice that there are far fewer SYN-ACK packets than SYN packets. The server is so busy that it can't respond to all of the packets.

   b. Select the **red square** to stop the capture.
3. Use a filter only to display packets that contain the ACK flag and answer the question.
   a. In the *Apply a display filter* field, change the ending of the **tcp.flags.syn** portion from a **1** to a **0** and press **Enter** to filter the Wireshark display to packets with only the ACK flag.

      You should see ACK packets, but none of them are being sent to 198.28.1.1 (www.corpnet.xyz). In a SYN attack, the ACK packets are never sent so that it ties

up the half-open connections on the server.

b. In the top right, select **Questions**.
c. Answer the question.