## **Activity File: Analyzing TCP Traffic**

In this activity, you will continue to play the role of a security analyst at Acme Corp.

* CompuCom, a software company, has hired Acme Corp to do a security assessment of its network.
* CompuCom has requested that you analyze a new employee's TCP traffic to determine what they're working on during their first week.

### **Instructions**

1. Open the packet capture provided and filter out for TCP activity.  
   * New Employee TCP Packet Capture
2. Find all the TCP handshakes for establishing a connection.
   * SYN request
     1. tcp.flags.syn ==1 && tcp.flags.ack == 0
   * SYN/ACK request
     1. tcp.flags.syn ==1 && tcp.flags.ack == 1
   * ACK request
     1. tcp.flags.syn == 0 && tcp.flags.ack == 1
   * FIN request
     1. tcp.flags.syn == 0 && tcp.flags.ack == 1 && tcp.flags.fin == 0
3. Find any TCP terminations.
   * tcp.flags.fin==1
4. Use your findings to determine what the employee is doing during their first week of work.
   * View > Name Resolution > Resolve Network Address
     1. Travelocity.com
     2. Trivago.com
     3. cruises.com
   * *Hint: Try to determine what websites are being visited.*
   * *Hint: If the IPs aren't being resolved within Wireshark, use the following website to lookup the domains that the IPs are connected to:*<https://securitytrails.com/domain/example.com/dns>