## **Activity File: Ports**

In this exercise, you'll continue to play the role of a security analyst at Acme Corp.

* You will be analyzing several network requests captured from the potentially rogue employee, Sally Stealer.
* Your manager has tasked you with finding the source and destination port for each request, and determining the protocol for each destination port. You will use your findings to determine what kind of activities Sally Stealer may be conducting.
* Log File (secondlogfile):

<https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/UCI-VIRT-CYBER-PT-03-2022-U-LOL/-/tree/main/08-Networking-Fundamentals/2/Resources>

### **Instructions**

1. Open the log file provided to you, and note that each log record is distinguished with a title: Log Record 1, Log Record 2, etc.
2. Determine the source and destination port for each request.
   1. Log 1
      1. Source: 50152
      2. Dest: 80
   2. Log 2
      1. Source: 53367
      2. Dest: 443
   3. Log 3
      1. Source: 64836
      2. Dest: 21
3. Determine the protocol associated with each destination port.
   1. Grep 80 /etc/services
      1. HTTP world wide web
      2. Accessing unencrypted websites
   2. Grep 443 /etc/services
      1. HTTPS to access encrypted websits
   3. Grep 21 /etc/services
      1. FTP. to transfer files
4. Research each protocol and summarize what Sally Stealer might be doing based on your findings.