## **Activity File: Analyzing HTTP Data**

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

* Your manager has provided you with a capture of web traffic from Sally Stealer. They would like you to analyze the traffic to determine if Sally Stealer is a spy for your rival company, WidgetCorp.
* Your manager has tasked you with analyzing the web traffic to determine what websites and webpages Sally has accessed. You must also interrogate the logs to see if Sally is sending any communications to WidgetCorp.
* <https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/UCI-VIRT-CYBER-PT-03-2022-U-LOL/-/tree/main/08-Networking-Fundamentals/2/Resources>

### **Instructions**

1. Use Wireshark to open the packet capture you were provided.
2. Determine what websites Sally Stealer visited.
   * http.request.method==”Get”
   * *Hint: Inspect the HTTP packet details to find the websites visited.*
3. Determine which PHP pages were visited on the websites.  
   * Filter using
     1. http && frame contains "php HTTP"
4. Determine if Sally Stealer sent any communications.
   * http.request.method==”POST”
   * *Hint: Look for POST requests.*
5. Based on the above findings, summarize whether you believe Sally has malicious intent.