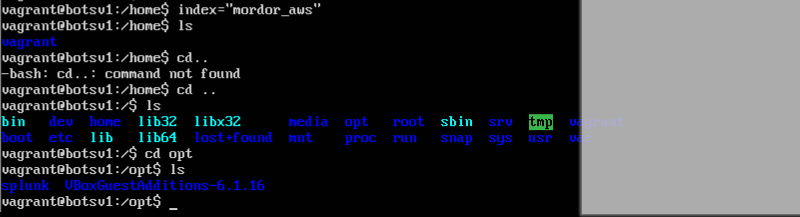
Hélio Ferreira 02/06/2024

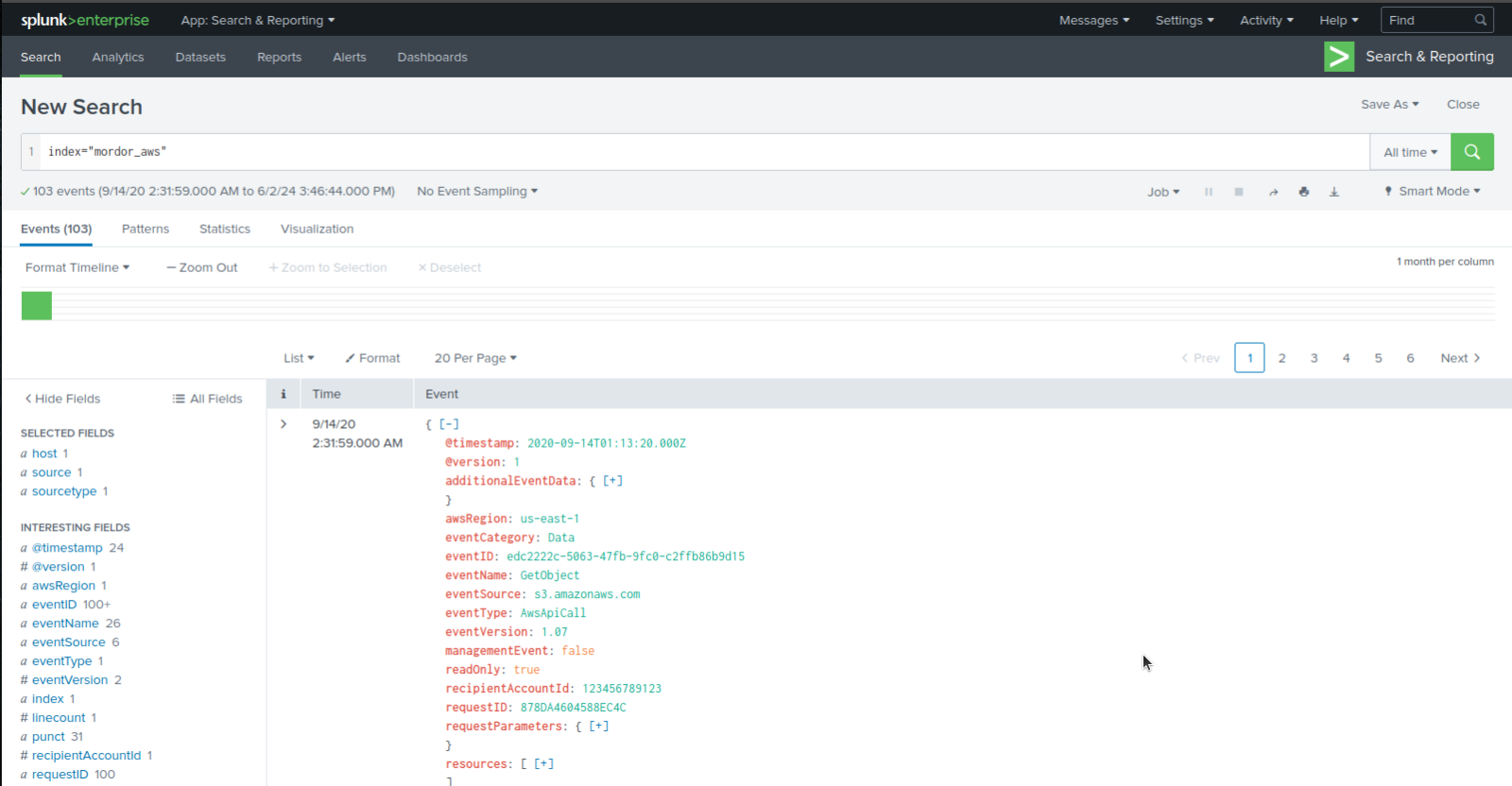
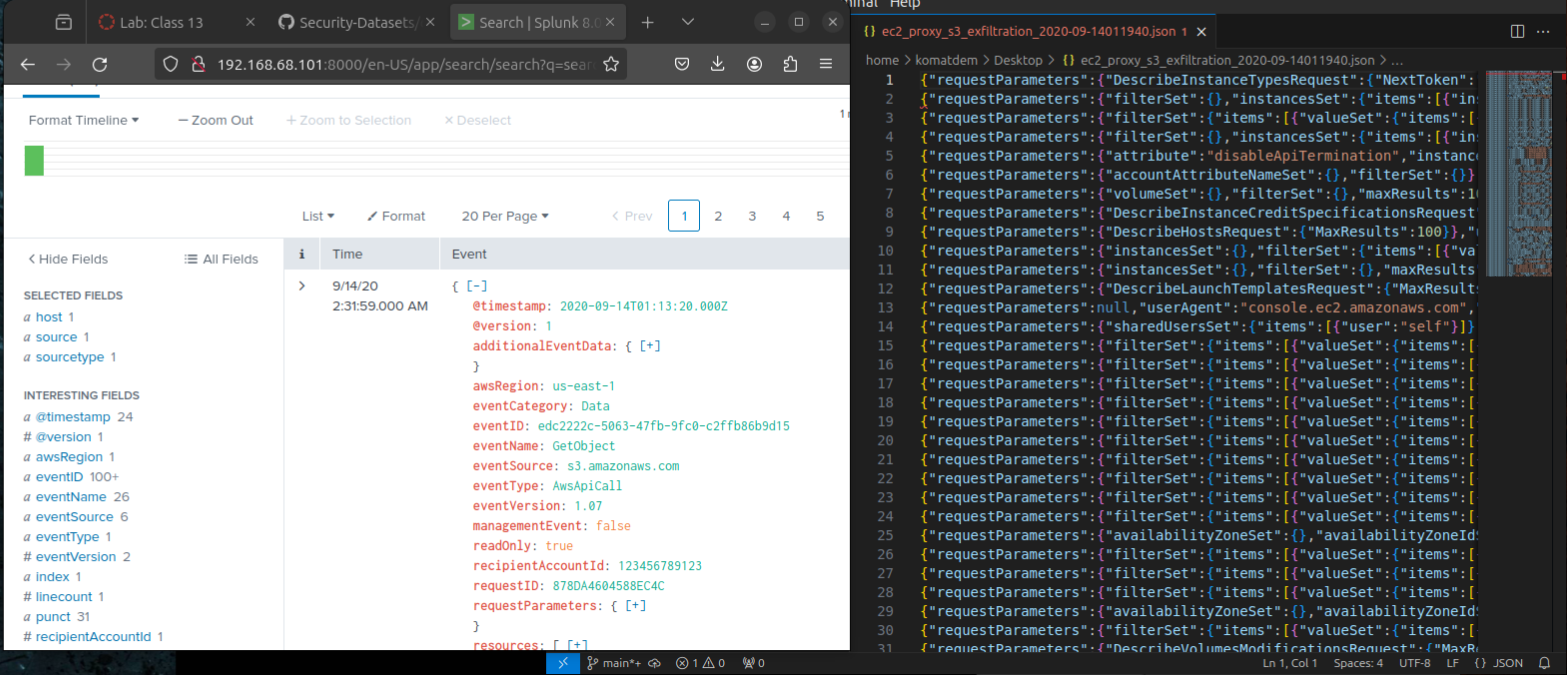
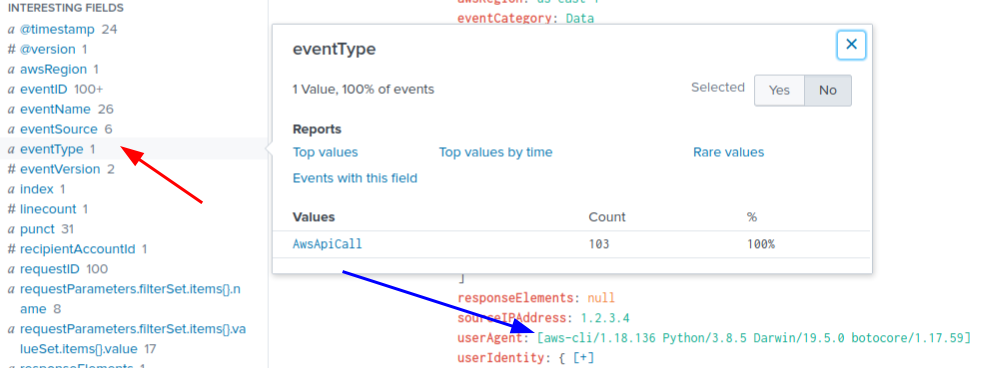
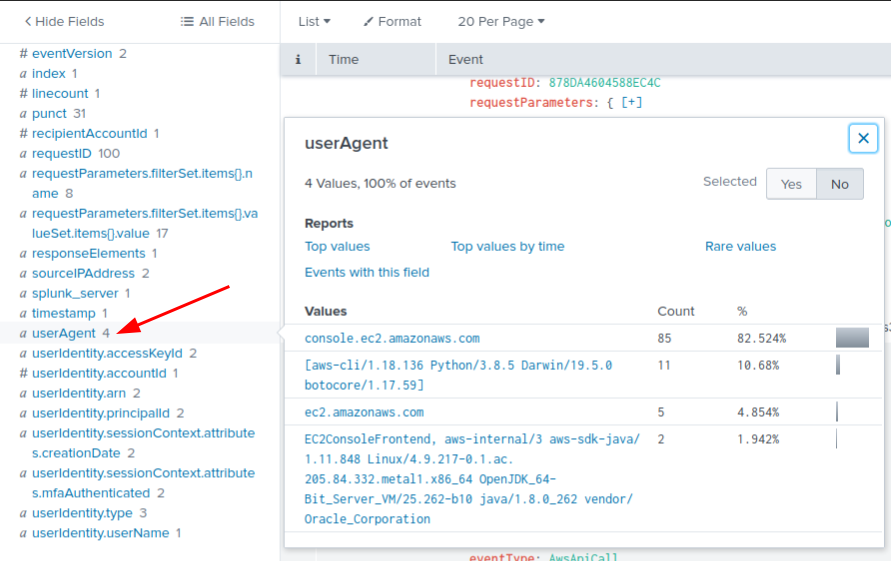
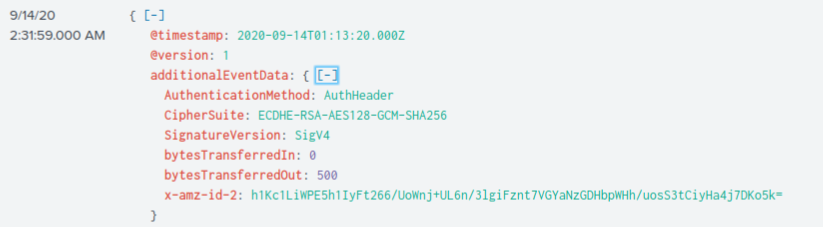
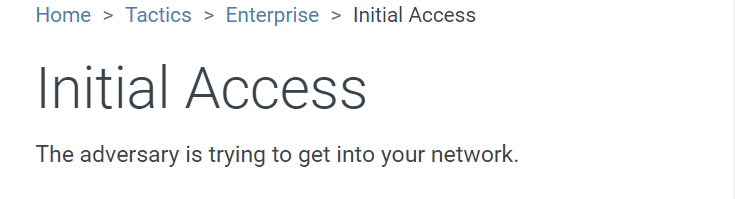
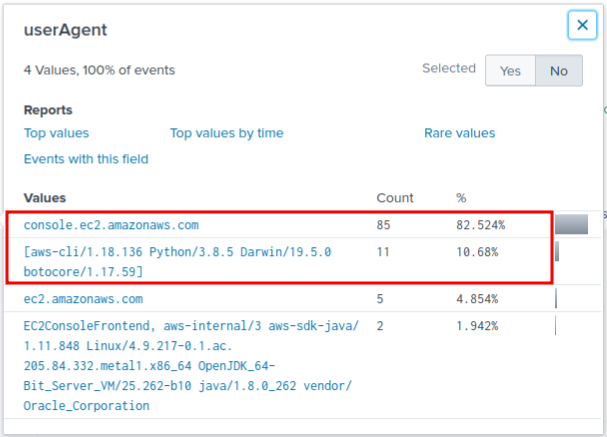
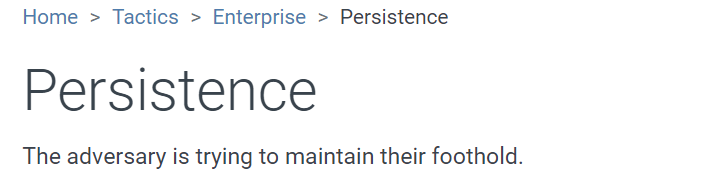
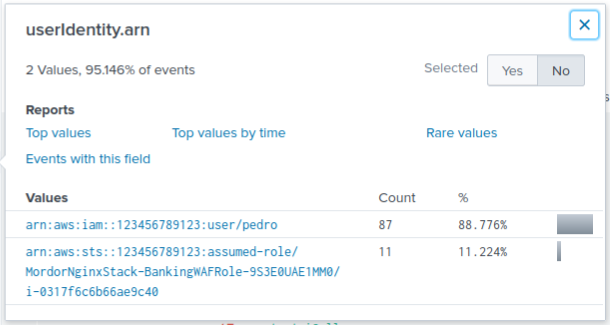
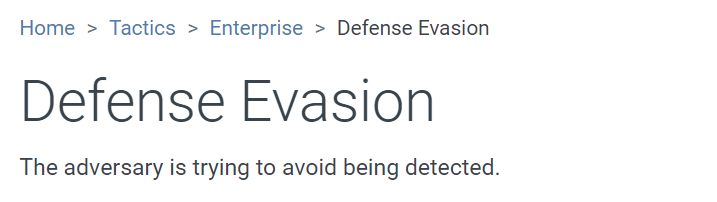
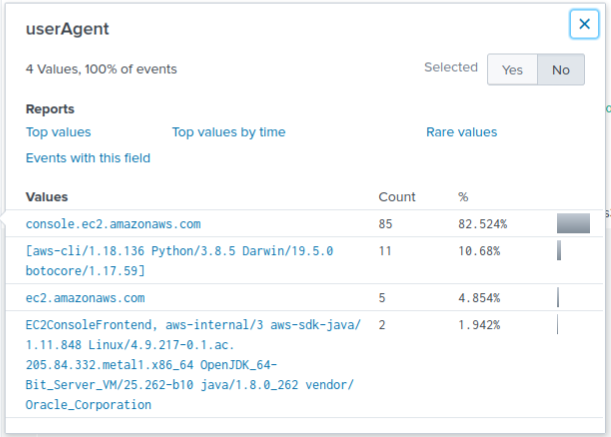
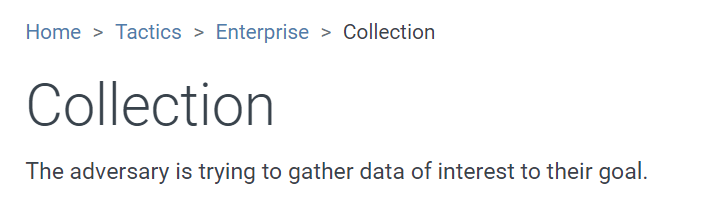
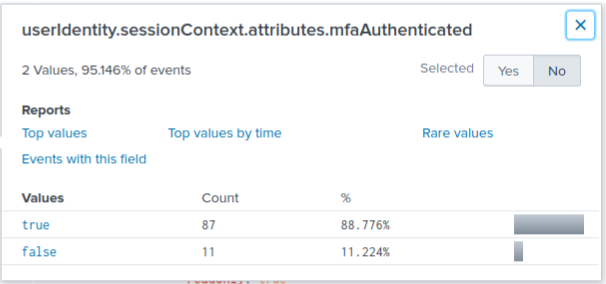
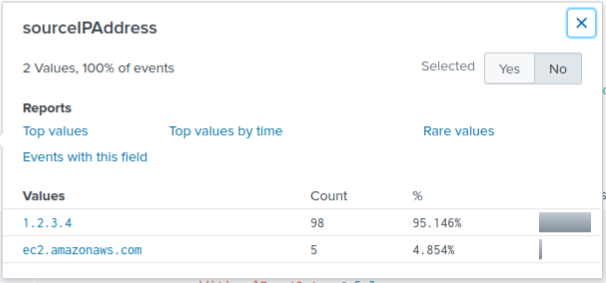
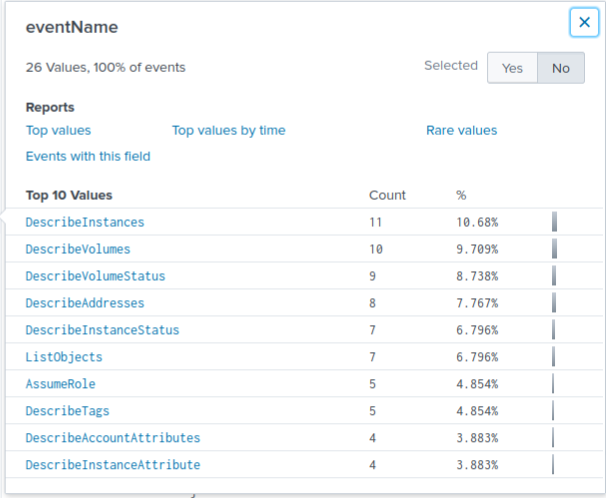
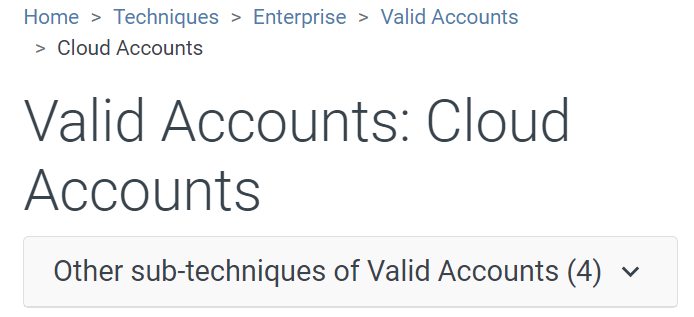
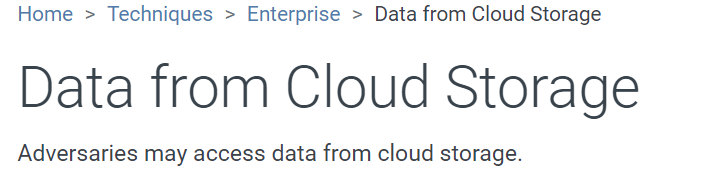
# **Lab: Reconstructing a Cloud Attack Using Log Data**

### **Part 1: Staging**

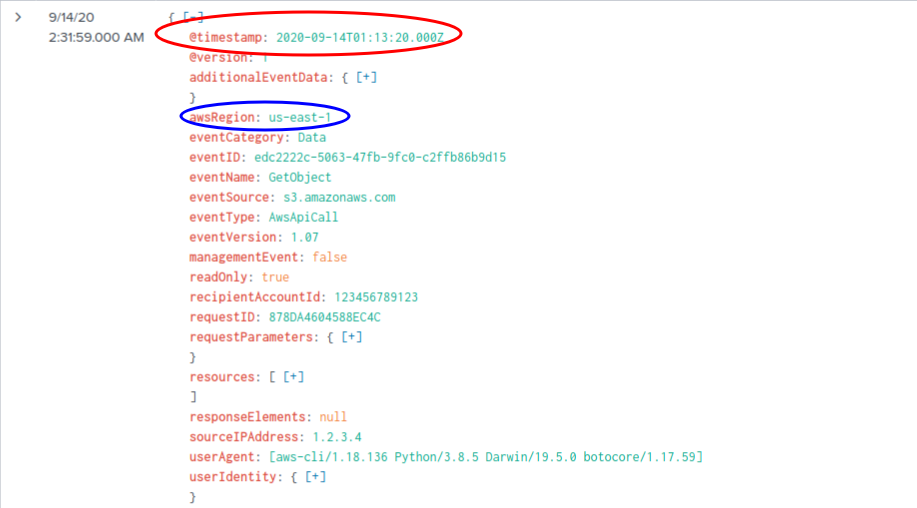
This lab uses the same OVA created during Class 11.

* The JSON file from GitHub AWS collection **ec2\_proxy\_s3\_exfiltration.zip** has already been loaded into Splunk
* Search **index="mordor\_aws"** in Splunk to complete the rest of the assignment

### **Part 2: Log Analysis**

* The data set you’ll be analyzing today is now imported into Splunk as the index name of mordor\_aws. Access the full index using **index="mordor\_aws"** and paste the first log you see into your submission.
* Open the JSON file in VS Code. Compare it to the same data set in Splunk. What do you observe?  
    
  I noticed that the JSON file opened on VSCode is almost illegible comparing to the one with Splunk. Splunk are prepared to deal with JSON file instead of VS Code.
* How is the attacker accessing the company’s AWS systems? Check the **userAgent** and **eventType** attributes.  
    
  Attacker is using a Python command line, most likely a script , running on Darwin OS and the event source is s3.amazonaws.com, wich means that is related to Amazon S3 attack on buckets or objects.  
    
  Event Type - AwsApiCall,so it shows us there was a GET requests for the data contained on Aws s3 services
* Find evidence that the following tactics were utilized, and paste the logs into your submission:
  + [TA0001](https://attack.mitre.org/tactics/TA0001)
  + [TA0003](https://attack.mitre.org/tactics/TA0003)
  + [TA0004](https://attack.mitre.org/tactics/TA0004)  
    
  + [TA0005](https://attack.mitre.org/tactics/TA0005)  
      
    
  + [TA0009](https://attack.mitre.org/tactics/TA0009)  
      
      
    
* Find evidence that the following techniques were utilized, and paste the logs into your submission (may overlap with previous findings in “tactics” section):
  + [T1078.004](https://attack.mitre.org/techniques/T1078/004)
  + [T1530](https://attack.mitre.org/techniques/T1530)  
      
    

### **Part 3: Reporting**

* Summarize in your own words how the attacker was able to exfiltrate data from the S3 bucket. Be sure to include:
  + When did the attack take place?
  + How was the attacker interacting with AWS?
  + Did you find any information about the attacker/attack origin?