# Module 12: Cloud Forensics

# report

Lara Alofi

2110886

Y

Computer Hacking Forensic Investigator (CHFI)

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/c7a120d8-8164-400e-b3a9-a206a1710d4a>

Username on EC-Council System

1. 2110886@uj.edu.sa

**Lab 01:**

In this lab, i assume the role of a forensic investigator tasked with examining a compromised Amazon EC2 instance. The incident involves a file tampering attack on a file called Tender\_quote.txt. The lab guides you through the process of acquiring the affected Elastic Block Store (EBS) volume, taking it offline, creating a snapshot, and then converting that snapshot into a volume for further analysis.

The investigation starts with setting up two EC2 instances: a Production machine (suspected to be compromised) and a Forensic workstation. You will upload a file to the Production machine, simulate a file tampering attack using PuTTY, and then create a snapshot of the compromised instance. The snapshot is converted into an evidence volume, which is attached to the Forensic workstation. You will use forensic tools like FTK Imager to examine the contents and check the file's integrity by comparing hash values before and after tampering.

The lab teaches important skills such as forensic acquisition, hash comparison for file integrity, and using AWS for cloud-based investigations. The lab concludes with performing a file integrity check to confirm the attack, followed by properly terminating AWS resources to prevent unnecessary charges.

**Lab 02:**

In this lab, i play the role of a forensic investigator tasked with investigating a compromised Azure VM named *azure-ubuntu*. The investigation involves acquiring a snapshot of the VM's OS disk, copying it to a file share, and then analyzing it on a forensic workstation using tools like Autopsy and VirusTotal.

The lab begins with the creation of two resource groups in Microsoft Azure: *Production* and *chfi-investigation*. Next, you set up the compromised VM in the *Production* group and simulate a malicious file injection attack by transferring an infected file to the VM.

To acquire evidence, you take a snapshot of the OS disk, create a storage account and file share, and then copy the snapshot to the file share. You mount the file share to a forensic workstation running Windows Server 2022 and use Autopsy to analyze the contents of the snapshot, identifying the compromised file. The file is exported and analyzed on VirusTotal, revealing it as suspicious.

The lab teaches skills such as using Azure CLI for snapshot creation, managing Azure storage, and performing forensic analysis on cloud environments. The lab concludes with the unmounting of the file share and the deletion of all resources to prevent additional charges.

**Lab 03:**

In this lab, i assume the role of a forensic investigator tasked with investigating a compromised virtual machine (VM) in Google Cloud Platform (GCP). The investigation involves extracting sensitive data that has been uploaded as a password-protected file. The objective is to create a snapshot of the compromised VM, mount it to a forensic workstation, and crack the password of the extracted file for further analysis.

The lab begins with the creation of two VMs: *production-machine* (the compromised VM) and *forensic-workstation* (the machine used for analysis). You simulate a data exfiltration attack by uploading a password-protected file to the *production-machine*.

Next, you stop the *production-machine*, create a snapshot of its disk, and then attach the snapshot to the *forensic-workstation*. Once the snapshot is mounted, you use FTK Imager to view its contents and extract the uploaded file. The file is then analyzed using Passware Kit Forensic to crack its password and unlock its contents.

The lab teaches key skills such as using GCP to create and manage VM instances, taking snapshots, mounting disks, and performing forensic analysis of cloud-based data. The lab concludes with the deletion of all created resources to avoid unnecessary charges.