**PROJECT DESCRIPTION/USER STORIES**

"As the use of cloud computing has been adopted very rapidly and provision of IaaS services as cloud providers offer more powerful resources with flexible offerings and models. Due to this rapid adoption opens new surface attacks to the organizations that attackers abuse with their malware to take advantage of these powerful resources and the valuable data that exist on them. Therefore, for organizations to well defend against malware attacks they need to have full visibility not only on their data centers but also on their resources hosted on the cloud and don't take their security for granted. For that purpose, malware detection on IaaS is important to implement to mitigate damage inflicted upon systems. This can only be obtained using cloud visibility and forensics."

**PROJECT GOAL**

"The main goal of this project is that it aims to provide the best approaches to achieve continuous monitoring of malware attacks on the cloud along with their phases (before, during, and after) and the limitations of today's available techniques suggesting needed developments. Logging and forensics techniques have always been the cornerstone of achieving continuous monitoring and detection of malware attacks on-premises, this project defines the best methods to bring loggings and forensics to the cloud and integrate them with on-premises visibility."

**RECOMMENDED APPROACH**

"The approach for this project shall be divided into two practical parts:

The First: when the malware attack happened, make cloud analysis for malware detection.

The Second: Forensics Analysis in the IaaS Cloud after the malware attack happens."

**RECOMMENDED TOOLS**

* AWS
* NIST Cybersecurity Framework/MITRE ATT&CK cloud framework
* Ubuntu/Linux
* Python
* SIEM Software/SIFT