# Diploma Project
## Academic Year 2023 / 2024

***Project code:*** 202304

***Project Title (English):***

Implementing a Sandbox Environment for Malware Analysis

***Project Title (Arabic):***

تنفيذ بيئة Sandbox لتحليل البرامج الضارة

***Project Advisor:***
Name: Dr. Ibrahim Gomaa
email: igomaa@nti.sci.eg

***Project Objectives:***

Malware analysis is the process of understanding the behavior and purpose of files, applications, or suspicious executables. Effective analysis allows for uncovering hidden indicators of compromise (IOCs), triage of incidents, improving threat alerts and detection, and provide additional context into the latest exploits and defense evasion techniques. This project's goal is to enhance overall comprehension and provide exposure to malware infection techniques and popular tools used by professionals to aid in malware analysis.

***Project Outcomes:***

After completing this project, the studies will be familiar with:

- Learning the basics of malware infection tactics and common indicators of compromise (IOCs).
- Learning the foundations of static and dynamic malware analysis techniques.
- Understanding Malware Behavior.
- Identifying Malware Family.
- Assessing attack impact.
- Investigating samples of malware.