Hope you're all doing well. This is a simple assignment that will help you understand malware and how they can be analyzed in a sandbox environment.

There are many tools out there that can analyze malware in controlled environments, and then shows you what the malware did on that environment and which resources it tried accessing. Here's a list of a few common and well known malware analysis tools online:

- https://www.joesandbox.com/ (you can see a list of previous results here https://www.joesandbox.com/analysispaged/0)

- Here's a malicious file analysis example from cuckoo (https://sandbox.pikker.ee/analysis/2061678/summary/)

- VMRay https://www.vmray.com/products/analyzer-malware-sandbox/#top

- AnyRun https://any.run/

However, most of these require subscriptions to get all their features. Luckily, there is a free online analysis tool you can all access by SITE (Saudi Information Technology Company).

What you need to do for this assignment is the following:

TASK 1:

- Download an executable file from any source you want, but it needs to be an executable file (.exe). Go to https://inspect.site.sa/ and analyze the executable there.

- Take screenshots and write about your findings.

TASK 2:

- Go to https://any.run/ , and click on Tracker or Reports from the top menu (as shown in class). Then choose any MALWARE that we previously analyzed. Read about their findings and look into the malware's network connections, requests, Threats, processes, the CPU usage, RAM usage, the ATT&CK matrix, etc.

- Take screenshots and write about your findings and explain how it was determined by the sandbox of Any Run that this file was malicious.