|  |  |  |
| --- | --- | --- |
| C:\Users\thg\Desktop\ICT Logo\ICT_4C.jpg | | |
| Week | Malware Analysis Tools and Techniques | Duration |
| 2 | Basic Dynamic Analysis Tutorial | 60 mins |

**Lesson Objectives**

* Understand concepts of Basic Dynamic Analysis

Submit your answers on MeL.

1. How do you run a malware in the form of DLL?

Use the command:

Rundll32.exe DLLname, Export arguments

1. Which tool would you use to monitor Registry? Procmon
2. What is the difference in purpose between Procmon & Process Explorer?

Procmon is able to track the time of an action/process is done and display as it happens which Process Explorer cannot

1. Which tool would you use to capture network packets?

Wireshark

1. What is mutex? Why is it important in the context of malware analysis?

Mutex is a mutually exclusive flag, malware use to check if the malware is installed or not. If will are able to find this flag in the system, we will be analysis that the host is infected.

1. What is the purpose of Windows Registry?

Windows Registry is a database that stores settings for the Windows OS and for applications that opt to use the registry.

1. What is the difference between a process and a thread?

A thread is component of a process (can have more than 1 thread in a process) which does not require to interact with the OS. A process is an instance of a program which require to interact with the OS.

1. What is the difference between an Application, Process, and Services?

An application is program that interact with the desktop.

A process is instance of a program which run simultaneously. For example, there will be a process for each tab you open on google chrome

A service is a process that run in the background and do not interact with the desktop.