Malware Analysis

Malware stands for malicious software. *Software* refers to programs, documents, and files that you can save on a disk or :send over the network. Malware includes many types, such as

- **Virus is a piece of code (part of a program) that attaches itself to a program. It is designed to spread from one computer to another; moreover, it works by altering, overwriting, and deleting files once it infects a computer. The result ranges from the computer becoming slow to .unusable**
- **Trojan Horse is a program that shows one desirable function but hides a malicious function underneath. For example, a victim might download a video player from a shady website .that gives the attacker complete control over their system**
- **Ransomware is a malicious program that encrypts the user's files. Encryption makes the files unreadable without knowing the encryption password. The attacker offers the user the encryption password if the user is willing to pay a ".“ransom**

Malware analysis aims to learn about such malicious programs using various means:

1. **Static analysis works by inspecting the malicious program without running it. Usually, this requires solid knowledge of assembly language (processor's instruction set, i.e., computer's fundamental instructions).**
2. **Dynamic analysis works by running the malware in a controlled environment and monitoring its activities. It lets you observe how the malware behaves when running.**