**Static Detection of Malicious PE Files**

Static analysis provides thorough analysis of source code of portable executable (PE) files without executing them, allowing early-stage detection of malicious programs. Detecting the malicious file before it executes is highly effective to minimize the risk of malware contaminating the system. Static analysis can be used to extract many features from the parsed PE file such as: section names, order of the sections, entropy of sections, imported DLL’s, suspicious strings, usage of specific functions, code sections snippets, etc.

Stages:

1. Acquire datasets - <https://www.kaggle.com/>
2. Extract features of the exe file
3. Train & build models of machine learning