***TOC PROJECT***

**Topic** **Name :** Static Malware Analysis

<https://github.com/dhruvchandel/static_malware_analysis/>

**Introduction :**

* Executables are the programs packed into a executable package as one whole package for he purpose of Installation on the host device.
* Many a times these come from an untrusted source and it is unknown whether if they are genuine executables or are tampered with or are themselves some sort of malware.
* Static Malware Analysis is a technique where malware can be analysed without actually running it.

**Objective :**

* Main objective of our program is to implement a popular method of static analysis , find strings of that particular executable, analyse strings(**using REGEX**) obtained to find some indicative information about the particular executable without actually running it.

**Future Work:**

* In many cases, sophisticated Malware authors use packers to pack their executable to hide useful information that can be used to retrieve useful indicative information about the executable.
* As a future work we can implement steps to find if an executable is packed and has tried to hide some information about itsel
* We can Further expand the work to Mac and Linux executables.
* Functions identification of a particular DLL.