RESEARCH PROPOSAL

Cyber forensics analysis is the procedure to find crucial evidence with respect to a crime from a digital media. Malware forensics and Network security plays a crucial role in the current scenario where malware attacks are a common problem. A malicious software which can be commonly termed as a malware would cause interruption to a computer operation and may collect necessary information or illegally access private systems. A malware may either take the form of a script, code, spyware and many other kinds of malicious programs. Reverse engineering principles are applied in this domain to analyse malware. It is the comprehensive process of breaking software to figure out how it works.

The volume of new malware variants is increasing rapidly, with many using advanced evasion techniques like obfuscation, encryption, and polymorphism. Static analysis which involves analysing malware without executing it is a scalable and resource-efficient method widely used in malware triage. However, traditional static methods struggle against heavily obfuscated code and cannot always capture the behavioural intent of malware.

This research proposes an advanced and resource friendly malware forensics analysis procedure which uses the principles of static analysis to figure out the exact purpose of an executable file. Portable executable format can be explored with higher accuracy using the proposed method. This research aims to enhance static malware analysis using machine learning, code semantics extraction, and graph-based representations to improve classification, detection, and clustering of malware variants without execution dependency.