**SYNOPSIS**

The objective of the project is **“EMBEDDED REVERSE ENGINEERING OF WIPER MALWARE”.** It is the process of analysing and understanding destructive wiper malware specifically designed to target embedded systems.

The tool used in the project is ghidra to detect the wiper malware and the operating system is **KALI LINUX 5.14.0.**

The existing system is Malware reverse engineering and dissection is to find out how a malware works and malware capabilities. The proposed system Embedded reverse engineering of wiper malwareinvolves a comprehensive and systematic approach to analyze, understand, and defend against destructive wiper malware specifically designed to target embedded systems.

This project consists of five modules:

**Module 1 ­- Initial Setup and Environment Configuration:** Set up the necessary hardware and software environment for malware analysis, such as a controlled isolated environment.

**Module 2 - Malware Sample Collection and Preparation:** Obtain a clean copy of the wiper malware sample for analysis.

**Module 3 - Static Analysis**: Use Ghidra to load the malware binary and perform static analysis.

**Module 4** - **Dynamic Analysis:** Execute the malware in a controlled environment to observe its behavior and interactions with the system.

**Module 5** - **Behavioral Analysis:** Analyze the dynamic analysis logs and captured network traffic by the malware that lead to data destruction or system compromise.