**Project Report: Masqueraded Files Detector**

**Introduction**

The Masqueraded Files Detector project goal is to identify masqueraded files within a specified folder. Masqueraded files are those whose file extensions do not match their actual file signatures. This tool was developed as a part of the [CIS 442 course (Fall 2023) at UMass Dartmouth](https://catalog.umassd.edu/preview_course_nopop.php?catoid=69&coid=233840).

**Methodology**

**Features:**

**File Identification**:

The program scans a user-specified folder, examining file signatures and extensions to determine if they match. If a discrepancy is found, the files are flagged as masqueraded files found.

**User Interaction:**

A simple command-line interface prompts the user to enter the path of the folder user want to scan. The program then displays the paths of any masqueraded files found.

**Implementation**:

**Language**:

The program is implemented in **Python**, utilizing file I/O operations and basic string matching.

**Signature and Extension Checks:**

Each file's signature (first 8 bytes) is compared with predefined signatures for common file types jpg, mp4, png, and pdf. If a mismatch is detected, the file is considered masqueraded.

**Results**

The Masqueraded Files Detector successfully identifies masqueraded files within the specified folder. During testing, the program correctly flagged files whose extensions did not align with their actual file signatures. The tool provides a means of detecting potential security risks related to file manipulation.

**Conclusion**

This project demonstrates a practical application of file signature analysis to identify masqueraded files. While the current implementation is functional, there is room for improvement, such as incorporating more file types and refining signature checks. The Masqueraded Files Detector serves as a valuable tool for users concerned about the integrity of their file systems.