

Rapport

Rapport sur l'Architecture et les Tests de l'Outil d'Analyse de Disque

Introduction

Ce rapport présente une analyse détaillée de l'architecture, des tests effectués, ainsi que des cas non supportés et des bugs connus de notre outil d'analyse de disque. L'outil est conçu pour extraire des informations à partir d'une image disque, en se concentrant sur les structures du système de fichiers et les fichiers de registre.

Argumentaire sur l'Architecture du Code

L'architecture du code est conçue de manière modulaire pour faciliter la maintenance et l'extension de l'outil. Voici une vue d'ensemble de ses principales composantes :

- **Subprocess Communication**: Le code utilise le module `subprocess` pour communiquer avec des commandes système telles que `mmls` et `fls`, afin d'extraire les métadonnées et les listes de fichiers de l'image disque.
- **Extraction de Données**: Des fonctions spécifiques sont définies pour extraire des données pertinentes à partir des sorties des commandes système. Ces données incluent les informations sur les partitions, les répertoires et les fichiers d'intérêt.
- **Récupération de Fichiers**: Une fois les données extraites, l'outil utilise les inode numbers pour récupérer les fichiers associés aux hive de registre et autres répertoires d'intérêt.

Répartition du Travail

La répartition du travail s'est faite comme suit :

- ****Partie 1 (Github + Discord) : Nathan**
- **Partie 2 (Bouts de codes) : Nathan + Christopher**
- **Partie 3 (Script principal) : Emilien**
- **Rendu : Emilien**

Séries de Tests Implémentés

Pour assurer la robustesse de l'outil, plusieurs séries de tests ont été implémentées. Ces tests couvrent divers cas de figure et sont conçus pour valider le bon fonctionnement de l'outil dans différentes situations. Voici quelques exemples de tests effectués :

- **Test de Lecture de l'Image Disque**: Vérifie que l'outil peut lire correctement l'image disque fournie.
- **Test de Communication avec les Commandes Système**: Vérifie que l'outil peut communiquer avec les commandes système et extraire les données correctement.
- **Test de Récupération de Fichiers**: Vérifie que l'outil peut récupérer les fichiers spécifiés à partir des inode numbers avec succès.

Cas Non Supportés

Bien que l'outil soit capable de traiter de nombreux cas de figure, certains cas spécifiques ne sont pas pris en charge. Parmi eux :

- **Chiffrement de Disque**: L'outil ne prend pas en charge les disques chiffrés.
- **Systèmes de Fichiers Non Pris en Charge**: Certains systèmes de fichiers exotiques peuvent ne pas être pris en charge par l'outil.

Bugs Connus et Solutions Envisagées

Malgré les tests effectués, quelques bugs ont été identifiés :

- **Problème de Récupération de Fichiers**: Dans certains cas, l'outil peut rencontrer des problèmes lors de la récupération de fichiers, en particulier pour les fichiers corrompus ou endommagés. Une solution envisagée est d'implémenter une vérification de l'intégrité des fichiers récupérés.
- **Incohérences dans les Données Extraies**: Il peut y avoir des incohérences dans les données extraites, notamment en raison de variations dans les formats de sortie des commandes système. Une solution possible est d'ajuster les expressions régulières utilisées pour l'extraction des données.

Conclusion

En conclusion, cet outil d'analyse de disque offre une architecture modulaire, une série de tests solide et une prise en charge pour de nombreux cas de figure. Cependant, des

améliorations sont toujours possibles pour renforcer la robustesse et la fiabilité de l'outil dans divers scénarios d'utilisation.