le cnam

SEC 102 - TP06
Comprendre l'outil d'analyse

Date	Version	Description	Auteurs
02/04/2023	1	Retranscription collective des informations présentées en cours	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

Sommaire

1. Description du logiciel CFF Explorer

CFF Explorer est un logiciel gratuit et open-source**.**

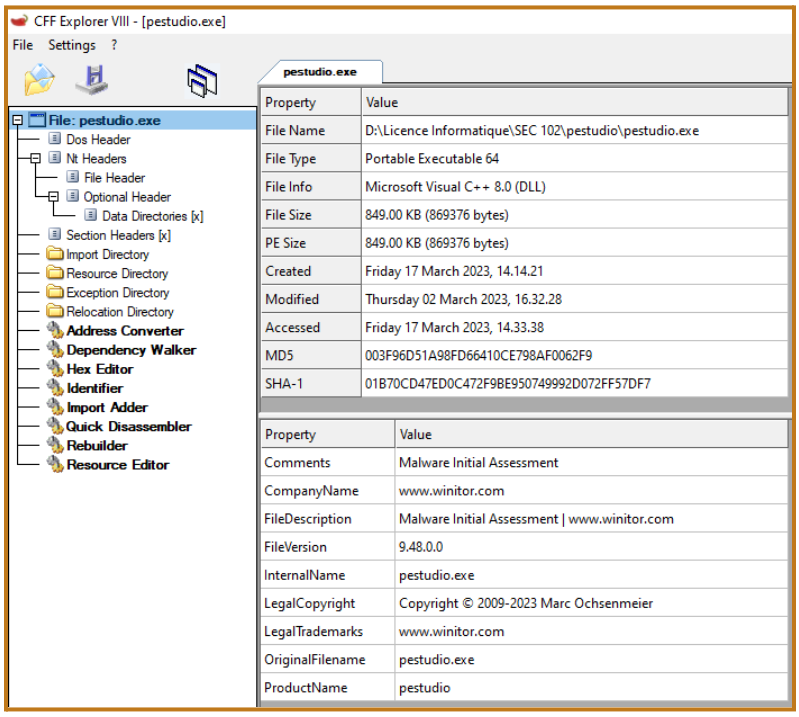
Il est utilisé pour l'analyse de fichiers binaires.

En particulier les fichiers exécutables (fichiers .exe) et les bibliothèques de liens dynamiques (fichiers .dll).

Il permet de visualiser et de modifier la structure interne de ces fichiers :

- en-têtes
- chaînes de caractères
- signatures numériques

2. Interface CFF avec l'exécutable PE Studio exécuté

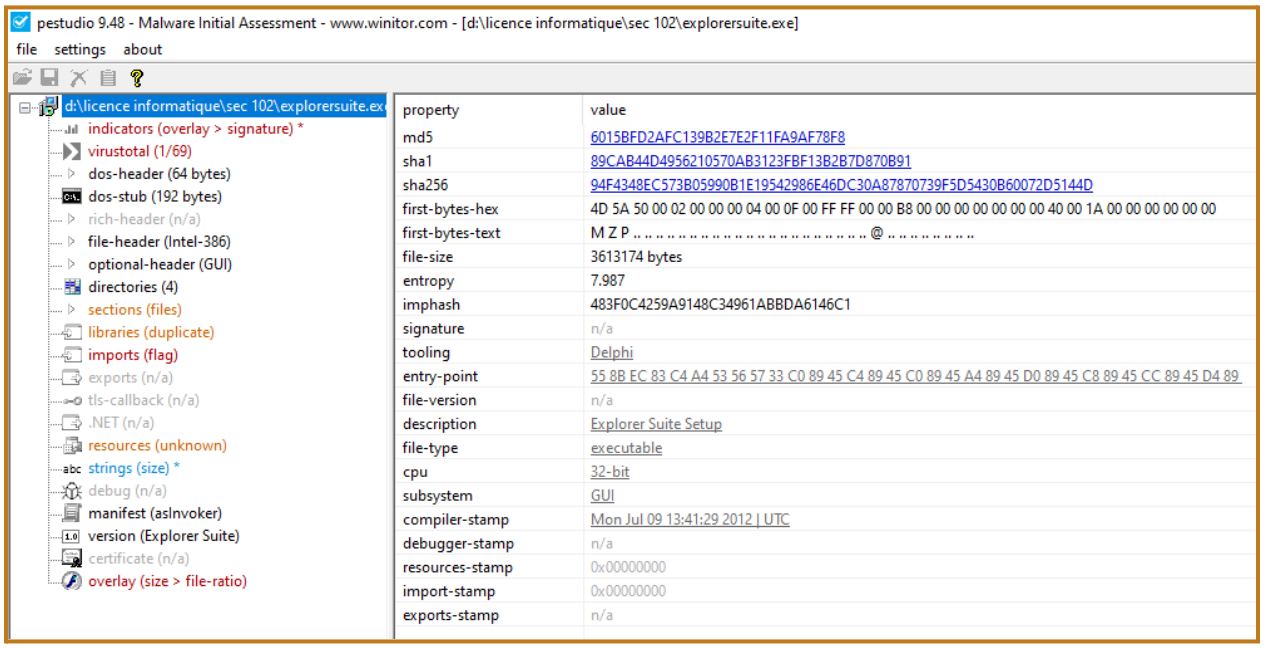


3. Description du logiciel PE Studio

PE Studio est un outil pour les développeurs Windows et les professionnels de la sécurité permettant d'analyser et de comprendre les fichiers exécutables Windows, ainsi que pour détecter les menaces de sécurité potentielles.

Tout comme CFF Explorer, PE Studio n’est pas compatible avec des systèmes d’exploitations autres que Windows.

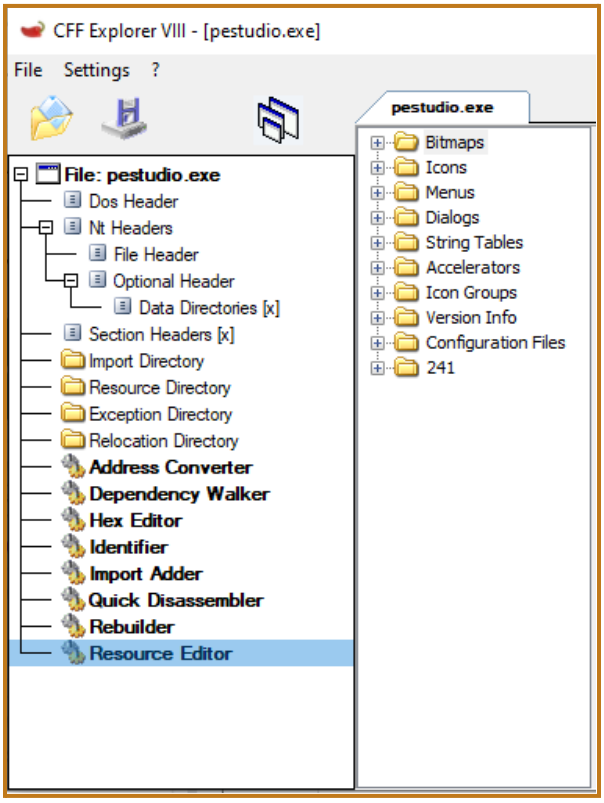
4. Interface PE Studio avec l'exécutable CFF Explorer exécuté

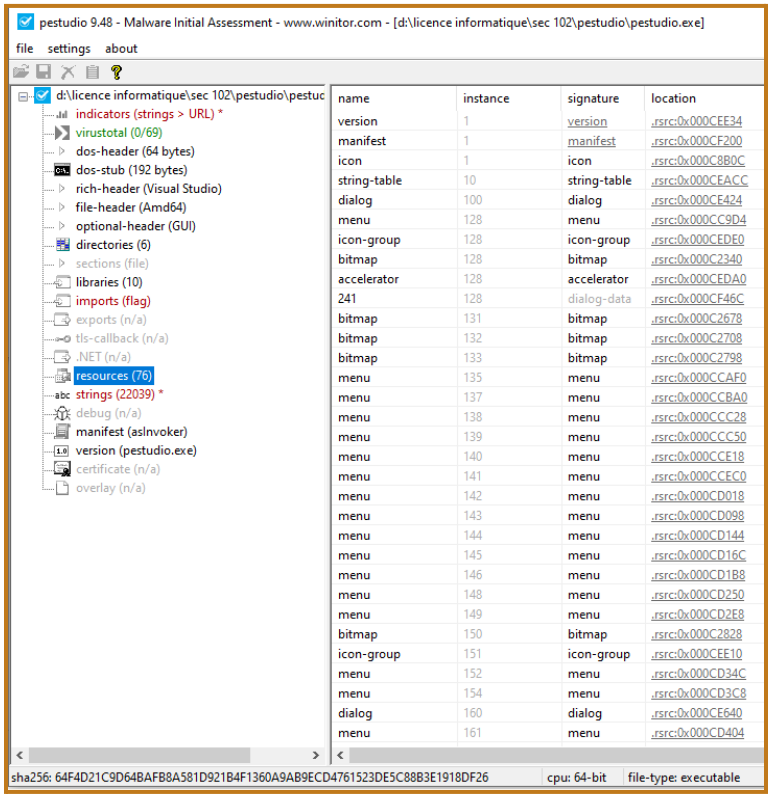


5. Comparaison des deux logiciels

Caractéristique	CFF Explorer	PEStudio
Avantages	- Gratuit	- Interface utilisateur conviviale
	- Possibilité de modifier des fichiers binaires	- Possibilité de rechercher et d'identifier les indicateurs de compromission
	- Possibilité d'afficher des informations détaillées sur les fichiers binaires	- Prise en charge des fichiers exécutables Windows et Android
	- Possibilité de vérifier les signatures numériques de fichiers binaires	- Capacité à effectuer des analyses en profondeur des fichiers binaires
Inconvénients	- Interface utilisateur moins conviviale	- Licence payante pour les fonctionnalités avancées
	- Peu de fonctionnalités d'analyse avancées	- Fonctionnalités limitées dans la version gratuite
	- N'inclut pas de fonctionnalités pour la désassemblage ou la décompilation	- Ne prend pas en charge les fichiers binaires pour les systèmes d'exploitation autres que Windows et Android

6. Comparaison de l’interface des deux logiciels





7. Conclusion

Pour conclure, ces deux outils sont utiles pour les développeurs, les chercheurs en sécurité et les analystes de logiciels pour comprendre la structure interne des fichiers exécutables, identifier les dépendances, les vulnérabilités et les comportements malveillants éventuels.

Cependant, il est important de noter que ces outils peuvent également être utilisés à des fins malveillantes. Il est donc crucial de les utiliser de manière éthique et responsable, en respectant la vie privée des utilisateurs et en évitant de violer les lois et les réglementations en vigueur.

8. Glossaire

CFF Explorer : Un logiciel gratuit et open-source utilisé pour l'analyse de fichiers binaires, en particulier les fichiers exécutables (fichiers .exe) et les bibliothèques de liens dynamiques (fichiers .dll). Il permet de visualiser et de modifier la structure interne de ces fichiers.

PE Studio : Un outil pour les développeurs Windows et les professionnels de la sécurité permettant d'analyser et de comprendre les fichiers exécutables Windows, ainsi que pour détecter les menaces de sécurité potentielles.

Fichier binaire : Un fichier informatique qui contient des données en forme de code binaire.

Bibliothèque de liens dynamiques (DLL) : Un fichier binaire qui contient du code exécutable et des données qui peuvent être utilisées simultanément par plusieurs programmes.

Fichier exécutable (EXE) : Un fichier binaire qui contient du code exécutable qui peut être directement exécuté par un système d'exploitation.

En-tête : Une partie d'un fichier binaire qui contient des informations sur sa structure et son format.

Chaîne de caractères : Une séquence de caractères qui représente du texte dans un fichier informatique.

Signature numérique : Une technique de cryptographie utilisée pour vérifier l'authenticité et l'intégrité d'un fichier informatique.

Système d'exploitation : Un logiciel qui permet de gérer les ressources matérielles et logicielles d'un ordinateur, ainsi que de fournir une interface utilisateur pour les programmes.