

# TP 6 Guillaume Sanchez

## CFF Explorer

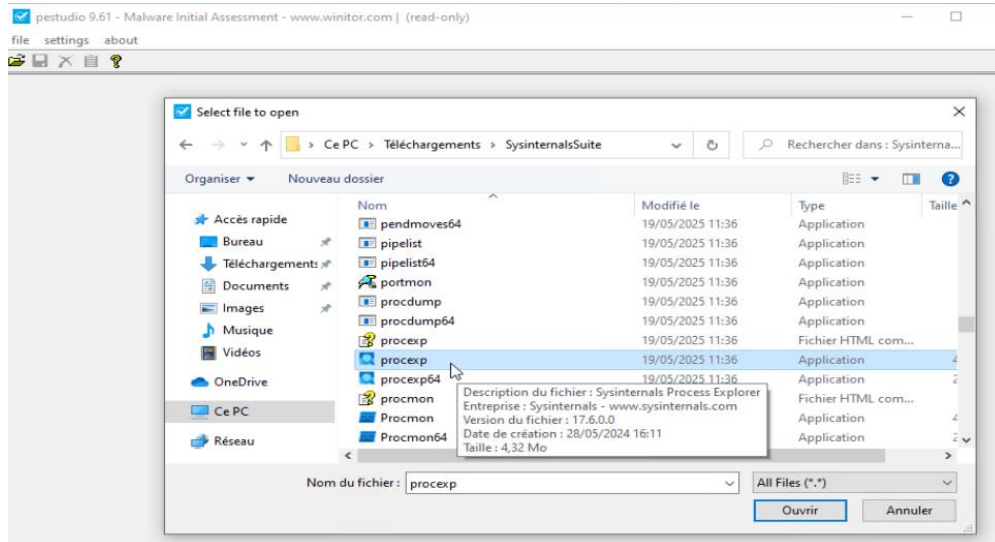
CFF Explorer est souvent utilisé par les développeurs, les chercheurs en sécurité, et les analystes de logiciels malveillants pour comprendre le fonctionnement interne des programmes Windows. Il permet de visualiser et de modifier les en-têtes des fichiers PE et de voir les différentes sections d'un fichier PE, comme le code, les données, les ressources. CFF Explorer permet de modifier directement le contenu des fichiers exécutables. Il offre des capacités de désassemblage basiques pour examiner le code assembleur contenu dans les fichiers exécutables.

## PE Studio

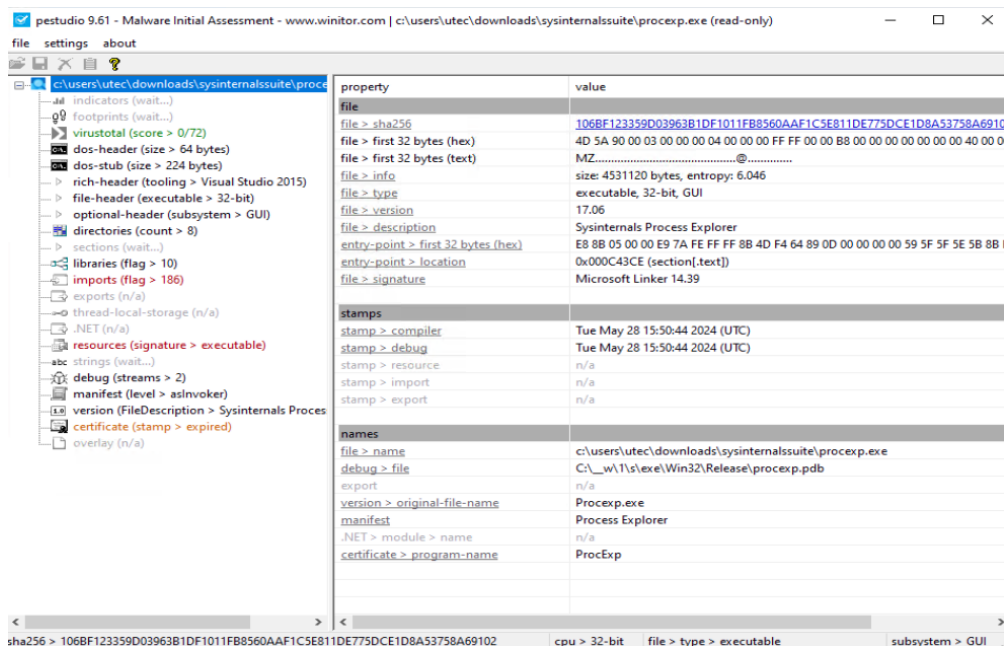
PE Studio est un outil d'analyse de fichiers exécutables au format PE, utilisé principalement pour l'analyse statique des logiciels Windows. Il est souvent utilisé par les développeurs, les chercheurs en sécurité, et les analystes de logiciels malveillants pour examiner les propriétés et le contenu des fichiers exécutables, des bibliothèques de liens dynamiques (DLL), et d'autres fichiers binaires. PE Studio permet de visualiser les en-têtes des fichiers PE, fournissant des informations sur la structure et les propriétés du fichier. Il permet de voir les différentes sections d'un fichier PE, comme le code, les données, les ressources. Il prend en charge les signatures numériques, permettant de vérifier l'authenticité et l'intégrité des fichiers exécutables.

# Tuto utilisation de PE Studio

1. Pour commencer, lancé PE Studio.
2. En suite cliquer sur “file” > “open file”, et sélectionné le fichier à analyser :



3. Maintenant vous allez pouvoir parcourir tout le contenu du PE :



De là vous allez, pouvoir récupérer toutes les informations utiles comme les sections, les signatures, la date de compilation etc.