Damien Claeyman
Camille Beaugendre
Hugo Cordier

Bigdata

Détection des Malwares

Partie 1 : Analyses du dataset & choix du modèle

Cette partie se trouve dans le notebook : « Analyse – Bigdata_Malware.ipynb »

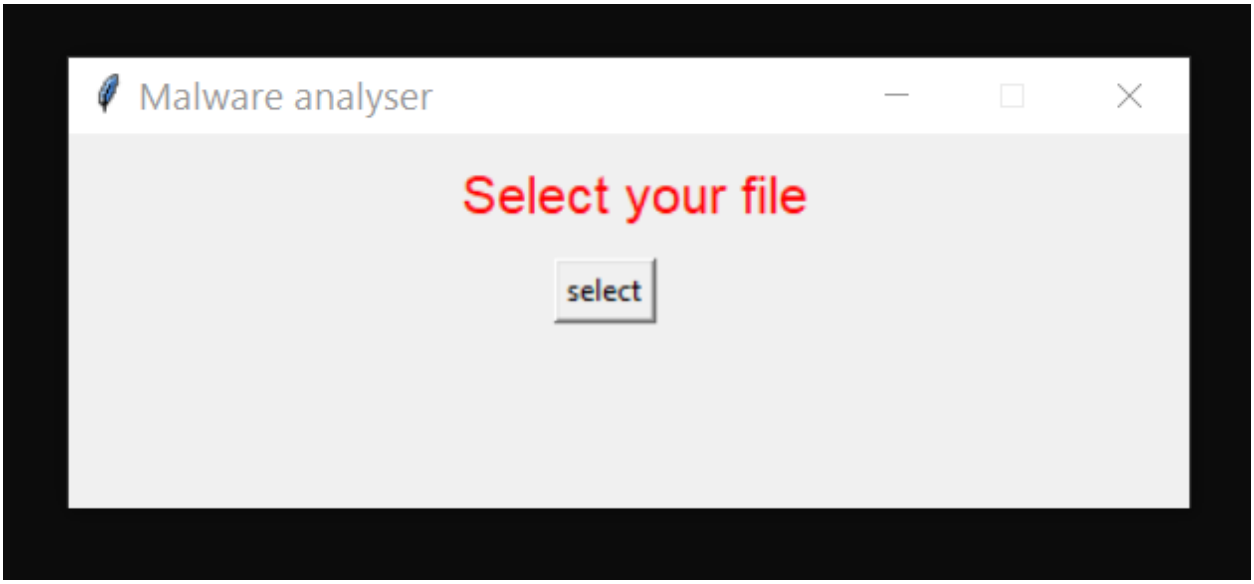
Partie 2 : Création d'un parser

Pour cette partie nous avons créé un parser avec la Bibliothèque pefile afin de récupérer les mêmes informations que celles que nous avons gardées de notre dataset. Il a fallu également créer des algorithmes pour calculer l'entropie du fichier.

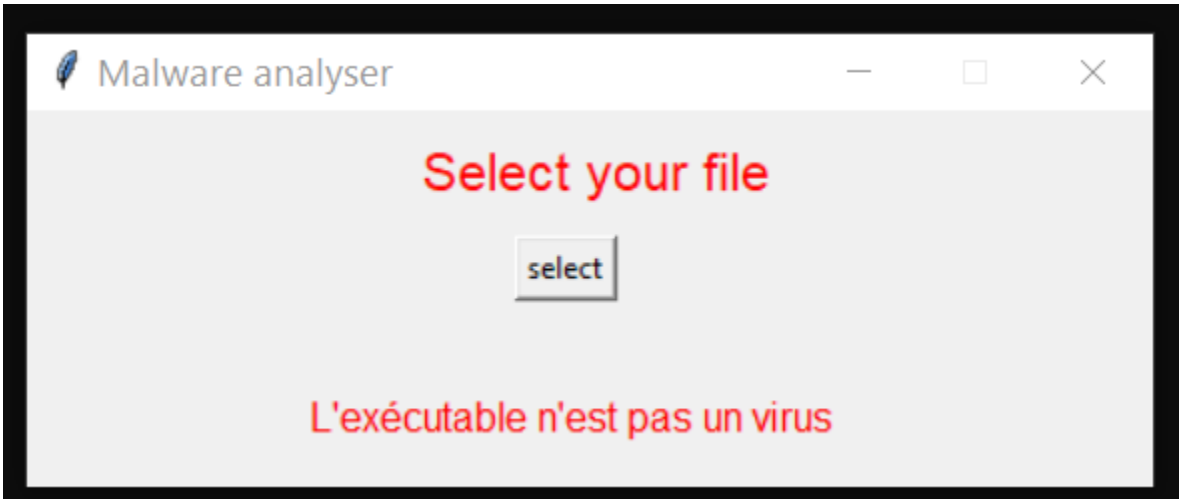
```
def open_file():
    file = askopenfilename()
    if file is not None:
        data = {}
        #Récupération des données du fichier
        pe = pefile.PE(file)
        data['Subsystem'] = pe.OPTIONAL_HEADER.Subsystem
        data['MajorSubsystemVersion'] = pe.OPTIONAL_HEADER.MajorSubsystemVersion
        data['SizeOfOptionalHeader'] = pe.FILE_HEADER.SizeOfOptionalHeader
        data['DllCharacteristics'] = pe.OPTIONAL_HEADER.DllCharacteristics


        resources= get_resources(pe)
        if len(resources)> 0:
            entropy = list(map(lambda x:x[0], resources))
            data['ResourcesMinEntropy'] = min(entropy)
            data['ResourcesMaxEntropy'] = max(entropy)
        else:
            data['ResourcesMinEntropy'] = 0
            data['ResourcesMaxEntropy'] = 0


    entropy = list(map(lambda x:x.get_entropy(), pe.sections))
    data['SectionsMeanEntropy'] = sum(entropy)/float(len(entropy))
    data['SectionsMaxEntropy'] = max(entropy)
```

Partie 3 : Création d'un IHM

Voilà l'interface d'accueil de l'IHM.



Lorsqu'il affiche un résultat.

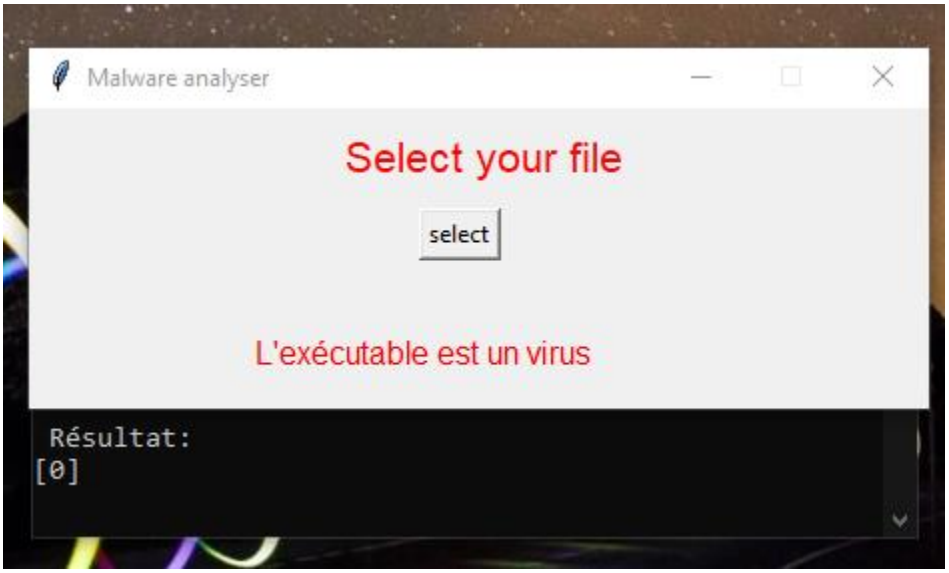


Démonstration :

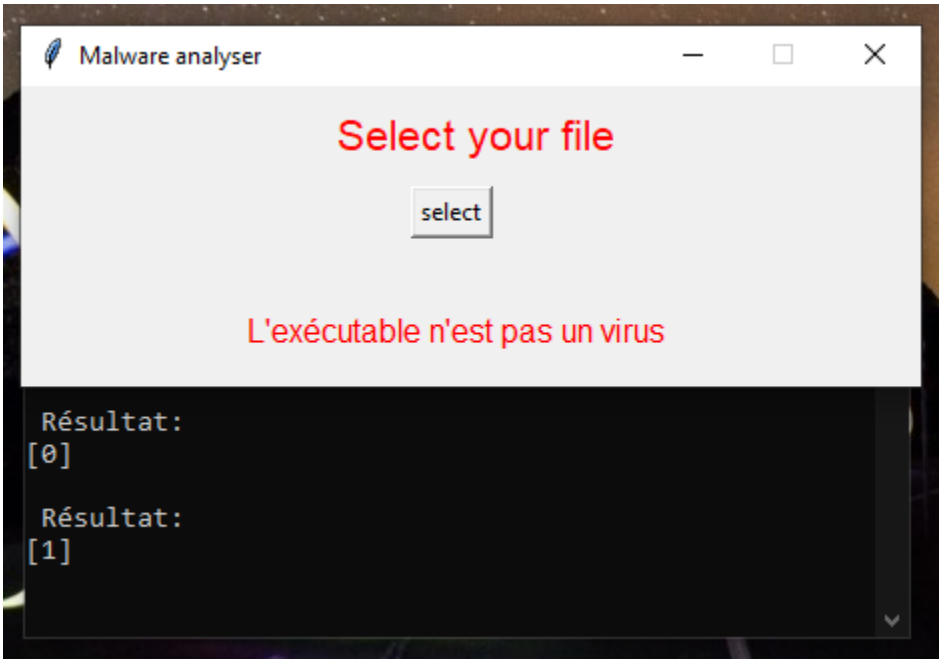
Nous avons fait la démonstration sur une VM Windows 10 avec l'antivirus désactiver pour ne pas que Windows Defender supprime le virus.

Voilà nos deux fichiers, internet explorer et un virus récupéré sur Root-me.org :

En sélectionnant l'exécutable virus il le l'évalue bien :



De même pour internet explorer :



Vous pouvez retrouver le programme sous le nom de : « MalwareDetection.py », il faudra également installer pefile si vous ne l'avez pas.