PROIECT 3 CERC C, MARTIE 2018

Să se scrie un program care să parseze un executabil Windows în format PE32 (Portable Executable 32bit) și să afișeze diverse informații utile din structura și conținutul acestuia.

Primește un parametru obligatoriu din linia de comandă: path-ul fișierului pe care să îl parseze.

Pentru citirea conținutului fișierului se vor folosi obiecte de tip File Mapping din Win32 API.

Se va folosi un stil de codare defensiv pentru a evita terminarea cu eroare a programului (crash).

Programul trebuie să afișeze informațiile in urmatorul format:

File Header:

-Machine:<valoare>

-NumberOfSections:<valoare>

-Characteristics:<valoare>

Optional Header:

-AddressOfEntryPoint:<FileAddress>

-ImageBase:<valoare>

-SectionAlignment:<valoare>

-FileAlignment:<valoare>

-Subsystem:<valoare>

-NumberOfRvaAndSizes:<valoare>

Sections:

<Name1>,<FileAddress1>,<Size1>

...

<NameN>,<FileAddressN>,<SizeN>

Exports:

<Name1>,<Ordinal1>,<FileAddress1>

...

<NameN>,<OrdinalN>,<FileAddressN>

Imports:

<DllName1>,<Name1>

<DllName1>,<Name2>

...

<DllNameN>,<Name1>

<DllNameN>,<Name2>

*In cazul in care nu exista sectiuni, functii importate sau functii exportate, campurile “Sections:”, “Exports:” si “Imports:” vor fi afisate, dar nu vor avea intrari.

**In cazul in care exista exporturi fara nume <NameX> va ramane gol. Mai exact, dacă un export nu are nume, în output, câmpul cu numele lui va fi gol, dar ii se va completa ordinalul și adresa.

***In cazul in care exista functii importate dupa ordinal, formatul pentru import va fi <DllNameX>,<OrdinalX>

**** Daca un RVA nu este translatabil catre un File Address valid, se va afisa textul ***undef***

Reguli generale de afișare a informațiilor:

ImageBase - Afisata valoare de VA in Baza 16

Adrese - File Address in Baza 16.

Toate valorile numerice - Baza 16.

Structuri folosite:

IMAGE_DOS_HEADER

IMAGE_NT_HEADERS

IMAGE_FILE_HEADER

IMAGE_OPTIONAL_HEADER

IMAGE_SECTION_HEADER

IMAGE_DATA_DIRECTORY

IMAGE_EXPORT_DIRECTORY

IMAGE_IMPORT_DESCRIPTOR

etc

!!! NU se vor folosi funcții Win32 API pentru parsarea fișierului, precum ImageNtHeader, ImageRvaToVa, etc. Funcții echivalente pot fi implementate, dacă este nevoie.

Pentru a verifica informațiile afișate, se pot compara cu tool-ul gratuit CFF Explorer (http://www.ntcore.com/exsuite.php).