Parser pentru fișiere executabile Windows - Portable Executable Files (MZ-PE)

Să se scrie un program care să parseze un executabil Windows în format MZ-PE, și să afișeze diverse informații utile din structura și conținutul acestuia.

Aplicația primește cel puțin un argument pozițional (obligatoriu) din linia de comandă, path-ul fișierului MZ-PE pe care să îl parseze. În plus puteți introduce alte argumente opționale.

Pentru accesul la conținutul fișierului se vor folosi obiecte de tip File Mapping din Win32 API.

Se va folosi un stil de programare defensiv pentru a mări robustețea aplicației în fața acțiunilor impredictibile ale utilizatorilor și a interacțiunii incorecte dintre componentele programului.

Programul trebuie să afișeze următoarele informații:

<table>
<tr>
<td rowspan="3">1. Informații din header-ele de fișier:
File Header:
• Machine
• NumberOfSections
• Characteristics

Optional Header:
• AddressOfEntryPoint
• ImageBase
• SectionAlignment
• FileAlignment
• Subsystem
• NumberOfRvaAndSizes</td>
<td>2. Informații din header-ele de secțiuni:
• Name
• Address
• Size</td>
</tr>
<tr>
<td>3. Lista funcțiilor exportate, dacă există.
• Name
• Ordinal
• Address</td>
</tr>
<tr>
<td>4. Lista funcțiilor importate, per modul.
• Name</td>
</tr>
</table>

Reguli generale de afișare a informațiilor:

- Adresele se afișează în baza 16 - RVA (Relative Virtual Address) și FA (File Alignment)
- Flag-urile și Enumerările se afișează în baza 16 și cu nume textual - pentru cele mai relevante
- Alte valori numberice se afișează în baza 10.

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.

Observații

- NU se vor folosi funcții Win32 API pentru parsarea fișierului, precum ImageNtHeader, ImageRvaToVa, etc. Funcții echivalente pot fi implementate, dacă este nevoie.
- Pentru verificarea informațiilor afișate, se pot compara valorile cu cele furnizate de tool-ul gratuit CFF Explorer (http://www.ntcore.com/exsuite.php).