Malware Samples

<https://bazaar.abuse.ch/browse/>

Reference Classifiers

<https://github.com/pratikpv/malware_detect2/tree/d46667608aa24c810b3c44e10d981f90c6a296e7/models>

<https://github.com/DasariJayanth/Malware-Detection-in-PE-files-using-Machine-Learning/blob/master/Final%20Evaluation/FER.pdf>

PE Header parsing

Pefile library use - <https://axcheron.github.io/pe-format-manipulation-with-pefile/>

PE header parsing - <https://cobweb.cs.uga.edu/~liao/PE_Final_Report.pdf>

PE header structure - <https://tech-zealots.com/malware-analysis/pe-portable-executable-structure-malware-analysis-part-2/>

DOS header variables - <https://0xrick.github.io/win-internals/pe3/>

<https://stixproject.github.io/data-model/1.2/WinExecutableFileObj/DOSHeaderType/>

NT header variables - <https://0xrick.github.io/win-internals/pe4/>

PE Section and Directory variables - <https://0xrick.github.io/win-internals/pe5/>

Directory types:

#define IMAGE\_DIRECTORY\_ENTRY\_EXPORT 0 // Export Directory

#define IMAGE\_DIRECTORY\_ENTRY\_IMPORT 1 // Import Directory

#define IMAGE\_DIRECTORY\_ENTRY\_RESOURCE 2 // Resource Directory

#define IMAGE\_DIRECTORY\_ENTRY\_EXCEPTION 3 // Exception Directory

#define IMAGE\_DIRECTORY\_ENTRY\_SECURITY 4 // Security Directory

#define IMAGE\_DIRECTORY\_ENTRY\_BASERELOC 5 // Base Relocation Table

#define IMAGE\_DIRECTORY\_ENTRY\_DEBUG 6 // Debug Directory

// IMAGE\_DIRECTORY\_ENTRY\_COPYRIGHT 7 // (X86 usage)

#define IMAGE\_DIRECTORY\_ENTRY\_ARCHITECTURE 7 // Architecture Specific Data

#define IMAGE\_DIRECTORY\_ENTRY\_GLOBALPTR 8 // RVA of GP

#define IMAGE\_DIRECTORY\_ENTRY\_TLS 9 // TLS Directory

#define IMAGE\_DIRECTORY\_ENTRY\_LOAD\_CONFIG 10 // Load Configuration Directory

#define IMAGE\_DIRECTORY\_ENTRY\_BOUND\_IMPORT 11 // Bound Import Directory in headers

#define IMAGE\_DIRECTORY\_ENTRY\_IAT 12 // Import Address Table

#define IMAGE\_DIRECTORY\_ENTRY\_DELAY\_IMPORT 13 // Delay Load Import Descriptors

#define IMAGE\_DIRECTORY\_ENTRY\_COM\_DESCRIPTOR 14 // COM Runtime descriptor

#define IMAGE\_DIRECOTRY\_ENTRY\_RESERVED 15 // Reserved Directory

Section types:

|  |  |  |
| --- | --- | --- |
| .bss | Uninitialized data (free format) | IMAGE\_SCN\_CNT\_UNINITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE |
| .cormeta | CLR metadata that indicates that the object file contains managed code | IMAGE\_SCN\_LNK\_INFO |
| .data | Initialized data (free format) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE |
| .debug$F | Generated FPO debug information (object only, x86 architecture only, and now obsolete) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_DISCARDABLE |
| .debug$P | Precompiled debug types (object only) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_DISCARDABLE |
| .debug$S | Debug symbols (object only) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_DISCARDABLE |
| .debug$T | Debug types (object only) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_DISCARDABLE |
| .drective | Linker options | IMAGE\_SCN\_LNK\_INFO |
| .edata | Export tables | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ |
| .idata | Import tables | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE |
| .idlsym | Includes registered SEH (image only) to support IDL attributes. For information, see "IDL Attributes" in [References](https://learn.microsoft.com/en-us/windows/win32/debug/pe-format#references) at the end of this topic. | IMAGE\_SCN\_LNK\_INFO |
| .pdata | Exception information | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ |
| .rdata | Read-only initialized data | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ |
| .reloc | Image relocations | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_DISCARDABLE |
| .rsrc | Resource directory | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ |
| .sbss | GP-relative uninitialized data (free format) | IMAGE\_SCN\_CNT\_UNINITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE | IMAGE \_SCN\_GPREL The IMAGE\_SCN\_GPREL flag should be set for IA64 architectures only; this flag is not valid for other architectures. The IMAGE\_SCN\_GPREL flag is for object files only; when this section type appears in an image file, the IMAGE\_SCN\_GPREL flag must not be set. |
| .sdata | GP-relative initialized data (free format) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE | IMAGE \_SCN\_GPREL The IMAGE\_SCN\_GPREL flag should be set for IA64 architectures only; this flag is not valid for other architectures. The IMAGE\_SCN\_GPREL flag is for object files only; when this section type appears in an image file, the IMAGE\_SCN\_GPREL flag must not be set. |
| .srdata | GP-relative read-only data (free format) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE \_SCN\_GPREL The IMAGE\_SCN\_GPREL flag should be set for IA64 architectures only; this flag is not valid for other architectures. The IMAGE\_SCN\_GPREL flag is for object files only; when this section type appears in an image file, the IMAGE\_SCN\_GPREL flag must not be set. |
| .sxdata | Registered exception handler data (free format and x86/object only) | IMAGE\_SCN\_LNK\_INFO Contains the symbol index of each of the exception handlers being referred to by the code in that object file. The symbol can be for an UNDEF symbol or one that is defined in that module. |
| .text | Executable code (free format) | IMAGE\_SCN\_CNT\_CODE | IMAGE\_SCN\_MEM\_EXECUTE | IIMAGE\_SCN\_MEM\_READ |
| .tls | Thread-local storage (object only) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE |
| .tls$ | Thread-local storage (object only) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE |
| .vsdata | GP-relative initialized data (free format and for ARM, SH4, and Thumb architectures only) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ | IMAGE\_SCN\_MEM\_WRITE |
| .xdata | Exception information (free format) | IMAGE\_SCN\_CNT\_INITIALIZED\_DATA | IMAGE\_SCN\_MEM\_READ |