

# MsPaint PE Header

Import Directory and  
IAT (Import Address Table) Structure

# Analysis of mspaint.exe PE Header

C:\Program Files (x86)\Windows Kits\10\Include\10.0.18362.0\um\winnt.h

C:\Windows\System32\mspaint.exe

# winnt.h

# PE Header of mspaint.exe (Optional Header Tab)

```
18281 typedef IMAGE_THUNK_DATA64 IMAGE_THUNK_DATA;  
18282 typedef PIMAGE_THUNK_DATA64 PIMAGE_THUNK_DATA;  
18283 #define IMAGE_SNAP_BY_ORDINAL(Ordinal) IMAGE_SNAP_BY_ORDINAL64(Ordinal)  
18284 typedef IMAGE_TLS_DIRECTORY64 IMAGE_TLS_DIRECTORY;  
18285 typedef PIMAGE_TLS_DIRECTORY64 PIMAGE_TLS_DIRECTORY;  
18286 #else  
18287 #define IMAGE_ORDINAL_FLAG IMAGE_ORDINAL_FLAG32  
18288 #define IMAGE_ORDINAL(Ordinal) IMAGE_ORDINAL32(Ordinal)  
18289 typedef IMAGE_THUNK_DATA32 IMAGE_THUNK_DATA;  
18290 typedef PIMAGE_THUNK_DATA32 PIMAGE_THUNK_DATA;  
18291 #define IMAGE_SNAP_BY_ORDINAL(Ordinal) IMAGE_SNAP_BY_ORDINAL32(Ordinal)  
18292 typedef IMAGE_TLS_DIRECTORY32 IMAGE_TLS_DIRECTORY;  
18293 typedef PIMAGE_TLS_DIRECTORY32 PIMAGE_TLS_DIRECTORY;  
18294 #endif  
18295  
18296 //@[comment("MVI tracked")]  
18297 typedef struct IMAGE_IMPORT_DESCRIPTOR {  
18298     union {  
18299         DWORD Characteristics; // 0 for terminating null  
18300         DWORD OriginalFirstThunk; // RVA to original unbound IAT  
18301     } DUMMYUNIONNAME;  
18302     DWORD TimeDateStamp; // 0 if not bound,  
18303     // -1 if bound, and real  
18304     // in IMAGE_DIRECTORY_ENTRY_IMPORT  
18305     // 0.W. date/time stamp o  
18306  
18307     DWORD ForwarderChain; // -1 if no forwarders  
18308     DWORD Name;  
18309     DWORD FirstThunk; // RVA to IAT (if bound to IAT)  
18310 } IMAGE_IMPORT_DESCRIPTOR;  
18311 typedef IMAGE_IMPORT_DESCRIPTOR UNALIGNED *PIMAGE_IMPORT_DESCRIPTOR;  
18312  
18313 //  
18314 // New format import descriptors pointed to by DataDirectory[ IMAGE_D  
18315 //
```

PE-bear v0.5.0 [C:/Users/pc/Desktop/maldev2/02-mspaint iat/mspaint.exe]

File Settings Compare Info

mspaint.exe

- DOS Header
- DOS stub
- NT Headers
- Signature
- File Header
- Optional Header
- Section Headers
- Sections
  - .text EP = 224B8
  - .rdata
  - .data
  - .pdata
  - .rsrc
  - .reloc

Offset	Name	Value	Value
13C	Size of Headers	600	
140	Checksum	66B77B	
144	Subsystem	2	Windows GUI
146	DLL Characteristics	8140	
		40	DLL can move
		100	Image is NX compatible
		8000	TerminalServer aware
148	Size of Stack Reserve	80000	
150	Size of Stack Commit	2000	
158	Size of Heap Reserve	100000	
160	Size of Heap Commit	1000	
168	Loader Flags	0	
16C	Number of RVAs and Sizes	10	
	Data Directory	Address	Size
70	Export Directory	0	0
	Import Directory	B005C	168
180	Resource Directory	D7000	57E098
188	Exception Directory	D3000	B8B0
190	Security Directory	0	0
198	Base Relocation Table	65E000	28A0
1A0	Debug Directory	96AF4	38
1A8	Architecture Specific Data	0	0
1B0	RVA of GlobalPtr	0	0
1B8	TLS Directory	0	0
1C0	Load Configuration Directory	0	0
1C8	Bound Import Directory in headers	2E0	170
1D0	Import Address Table	97000	2060

# winnt.h

# PE Header of mspaint.exe (Imports Tab)

The image shows two windows side-by-side. The left window is Notepad++ displaying the file `winnt.h`. The right window is PE-bear v0.5.0 displaying the PE Header of `mspaint.exe`, specifically the Imports Tab.

**winnt.h (Left Window):**

```
18278 #ifdef _WIN64
18279 #define IMAGE_ORDINAL_FLAG          IMAG
18280 #define IMAGE_ORDINAL(Ordinal)     IMAG
18281 typedef IMAGE_THUNK_DATA64        IMAG
18282 typedef PIMAGE_THUNK_DATA64      PIMA
18283 #define IMAGE_SNAP_BY_ORDINAL(Ordinal) IMAG
18284 typedef IMAGE_TLS_DIRECTORY64    IMAG
18285 typedef PIMAGE_TLS_DIRECTORY64  PIMA
18286 #else
18287 #define IMAGE_ORDINAL_FLAG          IMAG
18288 #define IMAGE_ORDINAL(Ordinal)     IMAG
18289 typedef IMAGE_THUNK_DATA32        IMAG
18290 typedef PIMAGE_THUNK_DATA32      PIMA
18291 #define IMAGE_SNAP_BY_ORDINAL(Ordinal) IMAG
18292 typedef IMAGE_TLS_DIRECTORY32    IMAG
18293 typedef PIMAGE_TLS_DIRECTORY32  PIMA
18294 #endif
18295
18296 //@[comment("MVI_tracked")]
18297 typedef struct _IMAGE_IMPORT_DESCRIPTOR {
18298     union {
18299         DWORD Characteristics;
18300         DWORD OriginalFirstThunk;
18301     } DUMMYUNIONNAME;
18302     DWORD TimeDateStamp;
18303
18304
18305
18306
18307     DWORD ForwarderChain;
18308     DWORD Name;
18309     DWORD FirstThunk;
18310 } IMAGE_IMPORT_DESCRIPTOR;
18311 typedef IMAGE_IMPORT_DESCRIPTOR UNALIGNED *P
18312
18313 //
18314 // New format import descriptors pointed to
18315 //
18316
18317 typedef struct _IMAGE_BOUND_IMPORT_DESCRIPTOR
```

**PE-bear v0.5.0 (Right Window):**

The PE Header of `mspaint.exe` is shown. The Imports Tab is selected, displaying a list of imported DLLs and functions. The first three entries are highlighted with red boxes and arrows pointing to the corresponding struct definition in `winnt.h`:

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
AF25C	ADVAPI32.dll	21	TRUE	B02A8	FFFFFFFF	FFFFFFFF	B0294	97000
AF270	KERNEL32.dll	91	TRUE	B0358	FFFFFFFF	FFFFFFFF	B0284	970B0
AF284	GDI32.dll	72	TRUE	B0638	FFFFFFFF	FFFFFFFF	B0278	97390

The bottom table shows the details for the `ADVAPI32.dll` import:

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
97000	EncryptFileW	-	B2308	7FF7FF71610	-	F9
97008	DecryptFileW	-	B2318	7FF7FF714E0	-	D8
97010	EventWrite	-	B2328	78E7E630	-	110
97018	EventRegister	-	B2336	78E8E4F0	-	10E
97020	EventUnregister	-	B2346	78E73110	-	10F
97028	RegOpenKeyExW	-	B2358	7FF7FF306F0	-	261
97030	RegCreateKeyEx...	-	B2368	7FF7FF2B520	-	239
97038	RegCloseKey	-	B237A	7FF7FF30710	-	230
97040	RegQueryValue...	-	B2388	7FF7FF2C2D0	-	26E
97048	RegSetValueExW	-	B239C	7FF7FF21ED0	-	27E
97050	GetNamedSecu...	-	B23AE	7FF7FF1F990	-	142
97058	SetNamedSecur...	-	B23C6	7FF7FF189A0	-	2B1

Thank you