XBE File Format, Document V 0.9

by Robin Hood / Digital Sherwood Inc. (c) 2001

Image Header Structure, size=178h		
Offset	**Type**	**Description**
0	DWORD	Magic Number 48454258h - Represents string XBEH
4	BYTE[256]	Digital Signature - I am not very sure, but seems like a message digest of the image headers encrypted with RSA 1024 bit private key
104	DWORD	base address for XBE image (Usually 10000h)
108	DWORD	size of headers
10C	DWORD	size of image
110	DWORD	size of image header (Usually 178h)
114	DWORD	time date stamp
118	POINTER	certificate address (See Certificate structure)
11C	DWORD	number of sections
120	POINTER	section headers address
124	DWORD	initialization flags bit 0 - Mount utility drive bit 1 - Format utility drive bit 2 - Limit development kit runtime memory to 64MB bit 3 - Don't setup hard disk
128	POINTER	entry point address XOR PUBKEY[80h] XOR PUBKEY[90h]
12C	POINTER	thread local storage directory address
130	DWORD	size of stack commit (PE copy)
134	DWORD	size of heap reserve (PE copy)
138	DWORD	size of heap commit (PE copy)
13C	POINTER	original base address (PE copy)
140	DWORD	original size of image (PE copy)
144	DWORD	original checksum (PE copy)
148	DWORD	original time date stamp (PE copy)
14C	char*	debug path name address
150	char*	debug file name address
154	BSTR*	debug Unicode file name address
158	POINTER	kernel image thunk address XOR PUBKEY[84h] XOR PUBKEY[88h]
15C	POINTER	non-kernel import directory address
160	DWORD	number of library versions
164	POINTER	library versions address
168	POINTER	kernel library version address
16C	POINTER	XAPI library version address
170	POINTER	logo bitmap address
174	DWORD	logo bitmap size
Comments: Entry point and kernel thunk addresses are XORed with two DWORDs taken from RSA1 public key. These are the values taken from imagebld.exe: PUBKEY[80h] = 1B103FE6h, PUBKEY[90h] = 8F95A2ADh PUBKEY[84h] = 14A34FA8h, PUBKEY[88h] = FB12BEFAh		

Certificate Structure, size=1D0h		
Offset	**Type**	**Description**
0	DWORD	Size of certificate
4	DWORD	Time date stamp
8	DWORD	Title id
0C	WCHAR[40]	Title name - Unicode String
5C		Title alternate title id (1) These IDs are terminated by 0.
60		Title alternate title id (2)
-//-	-//-	-//-
94		Title alternate title id (16)
9C	DWORD	Allowed media types
A0	DWORD	Game region
A4	DWORD	Game ratings
A8	DWORD	Disk number
AC	DWORD	Version
B0	BYTE[16]	LAN Key
C0	BYTE[16]	Signature Key
D0	BYTE[16]	Title alternate Signature Key (1)
E0	BYTE[16]	Title alternate Signature Key (2)
-//-	-//-	-//-
1C0	BYTE[16]	Title alternate Signature Key (16)

Section Header Structure - size 38h		
Offset	**Type**	**Description**
0	DWORD	Flags Bit 0 - Writeable Bit 1 - Preload Bit 2 - Executable Bit 3 - Inserted file Bit 4 - Head page read-only Bit 5 - Tail page read-only
4	DWORD	Virtual address
8	DWORD	Virtual size
C	DWORD	File pointer to raw data
10	DWORD	Size of raw data
14	BYTE[8]	Section Name (Zero terminated string)
1C	DWORD	Head shared page reference count address
20	DWORD	Tail shared page reference count address
24 - 37	???	Unknown
…	…	…

Thread Local Storage Directory Structure, size=18h		
Offset	**Type**	**Description**
0	POINTER	raw data start address
4	POINTER	raw data end address
8	POINTER	TLS index address
C	POINTER	TLS callbacks address
10	DWORD	size of zero fill
14	DWORD	Characteristics

Library Version Structure, size=10h		
Offset	**Type**	**Description**
0	BYTE[8]	Library Name
8	WORD	Major Version
A	WORD	Middle Version
C	WORD	Minor Version
E	WORD	Flags Bits: ZZZ????? D??????? ZZZ=0 unapproved ZZZ=1 possibly approved ZZZ=2 approved D = Debug version of library Versions Below 1.0.3911 are always unapproved.
…	…	…