XBE File Format, Document V 0.9

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

"IMPORTANT!!! READ THIS FIRST: This document is for educational purpose only. In no event author of this document will be liable for any damage arising out of the use of any information on this document. You assume total legal responsibility and risk for use of any information on this document. If you don't agree on these terms you must stop reading and discard this document immediately.

terminated

IDs are

These

Title name - Unicode String Title alternate title id (1) ' by 0.

Certificate Structure, size=1D0h
Description
Size of certificate
Time date stamp

Type DWORD DWORD

Offset

	DWORD DWOR	er Structu			
BYTE[26] Digital Number Add-4528h - Represents string XBEH BOWRED Digital Number Add-4528h - Represents string XBEH BYTE[26] Digital Signature 1 am not very sure, but seems Ad DWO	PYPE TYPE		/ -	-/	-//-
DWORD Major Number 4845/288h = Represents structured DwoRD	DWORD		94		e title
BYTE[256] Digital Signature - I am not very sure, but seems A0 Dimon	104 DWORD 008 DWORD 009 DWORD 000 DWORD 000 DWORD 010 DWORD 011 DWORD 012 DWORD 013 DWORD 014 DWORD 015 Char* 016 Char* 017 Char* 018 DWORD 018 DW	Magic Number 48454258	36		
11ke a message digest of the image headers encrypted A4 Dumo	04 DWORD 08 DWORD 10 DWORD 14 DWORD 18 POINTER 10 DWORD 18 POINTER 20 POINTER 21 DWORD 22 POINTER 23 DWORD 33 DWORD 34 DWORD 34 DWORD 34 DWORD 40 DWORD 41 DWORD 42 DWORD 44 DWORD 46 POINTER 60 DWORD 64 POINTER 60 DWORD 60 DWORD 61 POINTER 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 DWORD 64 POINTER 66 POINTER 66 POINTER 67 POINTER 68 POINTER 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 65 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 60 D	Digital Signature - I	AO		Game region
DWORD Dword	04 DWORD 08 DWORD 110 DWORD 114 DWORD 118 POINTER 12 DWORD 120 POINTER 120 POINTER 121 DWORD 130 DWORD 131 DWORD 131 DWORD 132 DWORD 134 DWORD 134 DWORD 135 DWORD 136 POINTER 14 DWORD 150 POINTER 150 Char* 150 Char* 150 Char* 150 DWORD 151 DWORD 152 DWORD 153 DWORD 154 DWORD 155 DWORD 155 DWORD 156 DWORD 157 DWORD 158 DWORD 158 DWORD 159 DWORD 150 DWORD		A4		Game ratings
DWORD Dword	0.04 DWORD 0.05 DWORD 0.05 DWORD 1.10 DWORD 1.14 DWORD 1.18 POINTER 1.20 DWORD 2.0 DWORD 2.24 DWORD 2.34 DWORD 2.34 DWORD 2.34 DWORD 2.35 DWORD 2.36 DWORD 2.40 DWORD 2.50 Char* 2.60 DWORD 2.60 DWORD 2.70 POINTER 2.80 DWORD 2.90 DWO		A8		Disk number
DWORD Size of finage headers DWORD Size of finage headers DWORD Size of finage headers DWORD Size of finage header (Usually 178h) DWORD Size of finage header (Usually 178h) DWORD Size of finage header (See Certificate structure) DWORD Line date stamp DWORD Line date stamp DWORD Sections Section SPT	08 DWORD 0C DWORD 110 DWORD 118 POINTER 120 DWORD 220 POINTER 224 DWORD 230 DWORD 330 DWORD 330 DWORD 34 DWORD 34 DWORD 44 DWORD 45 DWORD 46 DWORD 47 CAR* 56 CAR* 56 CAR* 57 CAR* 56 CONTER 56 CONTER 57 CONTER 60 DWORD 64 POINTER 60 DWORD 64 POINTER 65 CONTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 69 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 DWORD 67 POINTER 68 POINTER 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 POINT		AC		Version
DWORD Size of image DWORD Size of image DWORD Size of image DWORD Size of image DWORD Size of heap reserve (PE copy) DWORD DWORD Size of heap reserve (PE copy) DWORD DWORD Size of heap reserve (PE copy) DWORD DWORD DWORD Size of heap reserve (PE copy) DWORD DWORD Size of heap reserve (PE copy) DWORD DWORD DWORD Size of heap reserve (PE copy) Size of h	0C DWORD 14 DWORD 1.0 DWORD 1.18 POINTER 1.2 DWORD 2.0 POINTER 2.4 DWORD 2.0 POINTER 2.5 POINTER 2.6 POINTER 3.4 DWORD 3.4 DWORD 3.4 DWORD 4.4 DWORD 4.4 DWORD 4.5 Char* 5.6 Char* 5.6 Char* 5.6 POINTER 6.6 POINTER 6.6 POINTER 6.6 POINTER 6.7 POINTER 6.7 POINTER 6.8 POINTER 6.9 POINTER 6.1 POINTER 6.1 POINTER 6.2 POINTER 6.3 POINTER 6.4 POINTER 6.5 POINTER 6.6 POINTER 6.7 POINTER 6.7 POINTER 6.7 POINTER 6.7 POINTER 6.8 POINTER 6.9 POINTER 6.0 DWORD 6.1 POINTER 6.1 POINTER 6.2 POINTER 6.3 POINTER 6.4 POINTER 6.5 POINTER 6.6 POINTER 6.7 POINTER 6.7 POINTER 6.7 POINTER 6.7 POINTER 6.8 POINTER 6.9 POINTER 6.9 POINTER 6.0 DWORD 6.0 DWO	size of headers	B0		LAN Key
DWORDD Line date stamp DWORDD Line date station Ligar	110 DWORD 1.14 DWORD 1.18 POINTER 1.1C DWORD 2.0 POINTER 2.2 POINTER 2.2 POINTER 3.3 DWORD 3.3 DWORD 3.4 DWORD 3.4 DWORD 4.4 DWORD 4.4 DWORD 4.5 Char* 5.0 Char* 5.0 Char* 5.0 Char* 6.4 BSTR* 5.1 BSTR* 5.2 POINTER 6.4 POINTER 6.5 POINTER 6.6 POINTER 6.7 POINTER 6.8 POINTER 6.9 POINTER 6.1 POINTER 6.2 POINTER 6.3 POINTER 6.4 POINTER 6.5 POINTER 6.6 POINTER 6.7 POINTER 6.7 POINTER 6.7 POINTER 6.7 POINTER 6.8 POINTER 6.9 POINTER 6.0 DWORD 6.0 DWO	size of image	00		Signature Key
DOUNTED Line date at statempoon DOUNTED	14 DWORD 118 POINTER 11C DWORD 20 POINTER 22 POINTER 32 DWORD 33 DWORD 33 DWORD 34 DWORD 36 POINTER 40 DWORD 44 DWORD 40 DWORD 50 Char* 50 Char* 51 DWORD 60 DWORD 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 DWORD 62 Char* 63 POINTER 66 DWORD 66 DWORD 67 POINTER 66 DWORD 67 POINTER 68 POINTER 68 POINTER 68 POINTER 60 DWORD		D0		alternate Signature Key
POINTER Certificate address (See Certificate structure)	18 POINTER 10 DWORD 24 DWORD 28 POINTER 28 POINTER 30 DWORD 34 DWORD 34 DWORD 36 POINTER 40 DWORD 48 DWORD 48 DWORD 48 DWORD 40 DWORD 40 DWORD 40 DWORD 40 DWORD 40 DWORD 41 DWORD 42 DWORD 44 DWORD 46 DWORD 46 DWORD 46 POINTER 47 CAR* 56 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 64 POINTER 67 POINTER 68 POINTER 69 POINTER 60 DWORD 60 DWORD 60 DWORD 61 POINTER 61 POINTER 62 POINTER 63 POINTER 66 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 66 POINTER 67 POINTER 68	time date stamp	E0		alternate Signature Key
DWORD	11C DWORD 2.0 POINTER 2.4 DWORD 2.2 POINTER 2.2 POINTER 2.0 DWORD 3.4 DWORD 3.8 DWORD 4.0 DWORD 4.4 DWORD 4.4 DWORD 4.4 DWORD 5.5 POINTER 5.6 Char* 5.6 Char* 5.6 POINTER 6.0 DWORD 6.1 POINTER 6.0 DWORD 6.1 POINTER 6.1 POINTER 6.2 POINTER 6.3 POINTER 6.4 POINTER 6.5 POINTER 6.6 POINTER 6.7 POINTER 6.8 POINTER 6.9 DWORD 6.9 POINTER 6.0 DWORD 6.0 DW)	/-	_	
POINTER section headers address DNORD initialization flags bit 0 - Mount utility drive 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 runtime memory to 64MB bit 3 - Don't setup hard disk runtime memory to 64MB bit 2 - Limit development kit runtime memory to 64MB bit 2 - Limit development kit runtime memory to 64MB bit 2 - Limit development kit runtime memory to 64MB bit 2 - Limit development kit runtime memory to 64MB bit 2 - Limit development kit runtime memory to 64MB bit 3 - Don't setup hard disk groupy) DNORD size of heap reserve (Fe copy) DNORD size of heap reserve (Fe copy) DNORD size of lange (Fe copy) DNORD criginal the copy) DNORD criginal time date stamp (Fe copy) DNORD criginal time datess are xore pubresy (84h) xore DNORD criginal time datess are xored with two DNORDs taken DNORD number of library version address DNORD criginal cheeves are xored with two DNORDs taken DNORD criginal cheeves are xored with two DNORDs taken M RAA1 public key. DNORD criginal cheeves by DNORDS taken EXT 8 - POINTER DNORD criginal cheeves are xored with two DNORDs taken M RAA1 public key.	24 DWORD 24 DWORD 28 POINTER 20 POINTER 30 DWORD 31 DWORD 31 DWORD 32 DWORD 40 DWORD 40 DWORD 40 DWORD 41 DWORD 41 DWORD 42 DWORD 42 DWORD 43 DWORD 44 DWORD 46 Char* 50 Char* 50 Char* 50 Char* 60 DWORD	number of sections	1C		
DWORD initialization flags DWORD Dit 0 - Mount utility drive	28 POINTER 20 DWORD 30 DWORD 33 DWORD 33 DWORD 33 DWORD 34 DWORD 34 DWORD 44 DWORD 44 DWORD 44 DWORD 44 DWORD 45 Char* 50 Char* 50 Char* 51 Char* 60 DWORD 64 BSTR* 51 CHAR* 60 CHAR* 60 CHAR* 61 CHAR* 62 CHAR* 63 CHAR* 64 DWORD 64 DWORD 64 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 67 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 60 DWORD 64 POINTER 67 POINTER 68 POINTER 60 DWORD 64 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 60 DWORD 64 POINTER 68 POINTER 6	section headers address			
Dit 0 - Mount utility drive	28 POINTER 20 POINTER 34 DWORD 34 DWORD 33 DWORD 34 DWORD 40 DWORD 44 DWORD 44 DWORD 46 Char* 50 Char* 51 Char* 52 Char* 60 Char* 64 POINTER 66 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 64 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 64 POINTER 60 DWORD 64 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 60 DWORD 60 DWORD 61 DWORD 62 POINTER 63 POINTER 66 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 60 DWORD 60 DWORD 61 DWORD 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 67 POINTER 68	initialization flags			
Dit 1 - Format utility drive Dit 2 - Limit development kite Dit 3 - Don't setup hard disk Don't setup hard local storage directory address DWORD Size of heap commit (PE copy) DWORD Size of heap commit (PE copy) DWORD DWORD Size of heap commit (PE copy) DWORD Original base address (PE copy) DWORD Original time date stamp (PE copy) DWORD Original time date stamp datess DWORD DWORD Original time datess are XORed with two DWORDs taken DWORD Original time datess are the values taken from imagebld.exe: DWORD DWORD Original stamp size DWORD Original stamp size DWORD Original time dates taken from imagebld.exe: DWORD Original time dates taken from imagebld.exe: DWORD DWORD Original time dates are the values taken from imagebld.exe: DWORD Original time dates DWORD Original timed dates DWORD Original timed dates DWORD Original timed dates DWORD Orig	28 POINTER 20 POINTER 31 DWORD 314 DWORD 318 DWORD 318 DWORD 319 DWORD 310 D	0	4		
Dit 2 - Limit development kit runtime memory to 64MB	28 POINTER 30 DWORD 34 DWORD 38 DWORD 38 DWORD 38 DWORD 40 DWORD 44 DWORD 44 DWORD 44 DWORD 45 Char* 50 Char* 50 Char* 56 Char* 56 POINTER 66 POINTER 66 POINTER 67 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 60 DWORD 60 DWORD 60 DWORD 61 POINTER 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 DWORD 66 DWORD 67 POINTER 67 POINTER 68 POINTER 68 POINTER 69 POINTER 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 60 DWORD 61 POINTER 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 66 POINTER 67 POINTER 67 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 60 DWORD 60 DWOR	\vdash			der structure
DINTER	28 POINTER 20 DWORD 34 DWORD 33 DWORD 33 DWORD 44 DWORD 44 DWORD 44 DWORD 44 DWORD 44 DWORD 44 DWORD 46 DWORD 64 BSTR* 54 BSTR* 54 BSTR* 56 Char* 56 Char* 60 Char* 71 Charter 60 Char* 60 Char* 72 Charter 74 DWORD 64 BOINTER 66 POINTER 66 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 68 POINTER 67 DWORD 64 POINTER 67 DWORD 64 DWORD 64 DWORD 65 POINTER 66 POINTER 67 DWORD 67 POINTER 68 POINTER 68 POINTER 68 POINTER 69 DWORD 60 DWORD 60 DWORD 60 DWORD 61 DWORD 61 DWORD 62 DWORD 63 DWORD 64 DWORD 65 DWORD 66 POINTER 66 POINTER 67 DWORD 67 DWORD 68 DWORD 68 DWORD 69 DWORD 69 DWORD 60 DWORD 60 DWORD 60 DWORD 61 DWORD 61 DWORD 61 DWORD 62 DWORD 63 DWORD 64 DWORD 65 DWORD 66 DWORD 66 DWORD 66 DWORD 67 DWORD 68 DWORD	2	5 c		Description
POINTER entry point address XOR PUBKEY[90h] POINTER thread local storage directory address DWORD Size of stack commit (PE copy) DWORD Size of heap reserve (PE copy) DWORD Size of heap commit (PE copy) DWORD Original size of image (PE copy) DWORD Original time date stamp (PE copy) SIZE of DWORD DWORD Original time date stamp (PE copy) SIZE of DWORD	22 POINTER 22 DONNER 23 DWORD 34 DWORD 33 DWORD 38 DWORD 40 DWORD 44 DWORD 44 DWORD 45 Char* 50 Char* 51 Char* 52 Char* 60 Char* 60 Char* 61 Char* 62 Char* 64 POINTER 65 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 68 POINTER 67 POINTER 68 POINTER 69 POINTER 70 POINTER 71 DWORD 74 DWORD 74 DWORD 74 DWORD 75 POINTER 76 POINTER 77 POINTER 78 POINTER 70 POINTER 70 POINTER 71 DWORD 71 DWORD 71 DWORD 72 POINTER 71 DWORD 73 POINTER 74 DWORD 75 POINTER 75 POINTER 76 POINTER 77 POINTER 77 POINTER 77 POINTER 78 PO	3 - Don't setup hard disk	>	DWORF	
POINTER thread local storage directory address DOINTER thread local storage directory address DOINTER size of heap reserve (PE copy)	2C POINTER 30 DWORD 34 DWORD 38 DWORD 38 DWORD 40 DWORD 41 DWORD 42 Char* 50 Char* 51 BSTR* 52 POINTER 54 BSTR* 55 POINTER 60 DWORD 64 POINTER 66 POINTER 67 POINTER 68 POINTER 68 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 67 POINTER 67 POINTER 68 POINTER 68 POINTER 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 67 POINTER 67 POINTER 68 POINTER 69 POINTER 60) -
DWORD	30 DWORD 34 DWORD 38 DWORD 3C POINTER 40 DWORD 44 DWORD 4C char* 50 char* 50 char* 54 BSTR* 54 BSTR* 56 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 67 POINTER 68 POINTER 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 DWORD 67 POINTER 67 POINTER 68 POINTER 69 POINTER 60 DWORD 60	directory			 (
DWORD size of heap reserve (PE copy) 2	34 DWORD 38 DWORD 38 DWORD 40 DWORD 44 DWORD 44 DWORD 46 Char* 50 Char* 51 Char* 52 Char* 54 BSTR* 54 BSTR* 56 Char* 57 Chary 60 DWORD 60 DWORD 61 POINTER 62 POINTER 62 POINTER 63 POINTER 64 POINTER 67 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 67 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 60 DWORD 64 POINTER 67 DWORD 67 DWORD 68 POINTER 69 POINTER 60 DWORD 60 POINTER 60 POINTER 60 POINTER 60 POINTER 60 POINTER 60 POINTER 61 POINTER 62 POINTER 63 POINTER 64 POINTER 66 POINTER 67 POINTER 67 POINTER 68 POINTER 69 POINTER 60 POINTER 60 POINTER 60 POINTER 60 POINTER 61 POINTER 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 66 POINTER 67 POINTER 67 POINTER 68 POINTER 68 POINTER 68 POINTER 69 POINTER 60 POINTER				ا ا م 4
DWORD	38 DWORD 3C POINTER 40 DWORD 48 DWORD 48 DWORD 48 DWORD 49 Char* 50 Char* 50 Char* 54 BSTR* 58 POINTER 60 DWORD 64 POINTER 60 DWORD 64 POINTER 67 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 74 DWORD ONMENTER 70 POINTER 71 DWORD ONMENTER 72 DWORD ONMENTER 73 DWORD ONMENTER 74 DWORD ONMENTER 75 POINTER 76 DWORD ONMENTER 77 DWORD ONMENTER 78 DWORD ONMENTER 78 DWORD ONMENTER 79 DWORD ONMENTER 70 POINTER 70 POINTER 71 DWORD ONMENTER 72 DWORD ONMENTER 74 DWORD ONMENTER 75 DWORD ONMENTER 76 DWORD ONMENTER 77 DWORD ONMENTER 78 DWORD ONMENTER				4 7
POINTER Original base address (PE copy) 4 DWO DWORD Original checksum (PE copy) C DWO DWORD Original checksum (PE copy) C DWO DWORD Original checksum (PE copy) 10 DWO DWORD Original time date stamp (PE copy) 14 BYT Char* debug path name address DWORD DWO DOINTER debug file name address DWORD DWO DOINTER kernel image thunk address XOR PUBKEY[84h] XOR DWO POINTER Non-kernel import directory address DWORD DWO DOINTER Non-kernel import directory address DWORD DWO DOINTER APPHILIPARY Version address DWORD DWO POINTER Library version address DWORD DWO POINTER Library version address DWORD DWO POINTER Logo bitmap address DWORD DWO POINTER Logo bitmap address DWORD DWO POINTER Logo bitmap datess are XORed with two DWORDs taken DWO Seare the values taken from imagebid.exer: DWORD DWO Seare the values taken from imagebid.exer: DWORD DWO SEARE RENEROR DWORD DWORD DWO LARREW RAN LARAFRÁB, PUBKEY[84h] = FB103EBFAh	3C POINTER 40 DWORD 48 DWORD 48 DWORD 4C Char* 50 Char* 54 BSTR* 58 POINTER 60 DWORD 64 POINTER 60 DWORD 64 POINTER 67 POINTER 68 POINTER 67 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 67 POINTER 68 POINTER 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 63 POINTER 64 POINTER 65 POINTER 66 POINTER 67 POINTER 74 DWORD 67 DWORD 68 POINTER 76 DWORD 69 DWORD 60 DWORD 60 DWORD 60 DWORD 60 DWORD 61 POINTER 62 POINTER 70 DWORD 64 POINTER 71 DWORD 65 POINTER 72 DWORD 66 POINTER 73 DWORD 67 DWORD 68 POINTER 74 DWORD 69 DWORD 75 POINTER 76 DWORD 77 POINTER 77 PWORD 78 DWORD 78 DWORD				רו ו
DWORD Original size of image (PE copy) 0	40 DWORD 44 DWORD 47 DWORD 47 Char* 50 Char* 50 Char* 54 BSTR* 58 POINTER 60 DWORD 64 POINTER 66 POINTER 67 POINTER 68 POINTER 67 POINTER 70 POINTER 71 POINTER 71 POINTER 72 POINTER 73 POINTER 74 DWORD 75 DWORD 76 POINTER 77 POINTER 78 DWORD 78 DWORD 79 DWORD 70 POINTER 70 POINTER 71 DWORD 72 DWORD 74 DWORD 75 DWORD 76 DWORD 77 DWORD 77 DWORD 78 DWO		4	DWORD	address
DWORD Original checksum (PE copy) DWORD Original checksum (PE copy) 10 DWORD DWORD Original time date stamp (PE copy) 14 DWORD DWORD Original time date stamp (PE copy) 14 DWORD 14 DWORD 15 DWORD 16 DWORD 17 DWORD	44 DWORD 48 DWORD 47	original size of image (PE copy)	∞	DWORD	1
DWORD	48 DWORD 4C char* 50 char* 54 BSTR* 54 BSTR* 55 POINTER 60 DWORD 64 POINTER 68 POINTER 68 POINTER 67 POINTER 70 POINTER 71 DWORD 74 DWORD 74 DWORD 71 DWORD 72 DWORD 74 DWORD 74 DWORD 75 DWORD 76 DWORD 77 DWORD 77 DWORD 78 DWORD	original checksum (PE copy)	U	DWORD	File pointer to raw data
14 BYT	4C char* 50 char* 54 BSTR* 58 POINTER 55 POINTER 60 DWORD 64 POINTER 68 POINTER 68 POINTER 67 POINTER 74 DWORD 70 POINTER 71 DWORD 71 DWORD 72 DWORD 73 DWORD 74 DWORD 74 DWORD 75 DWORD 76 DWORD 77 DWORD 77 DWORD 78 DWOR	original time date stamp (PE copy)	10		Size of raw data
10 10 10 10 10 10 10 10	50 char* 54 BSTR* 58 POINTER 56 POINTER 60 DWORD 64 POINTER 68 POINTER 6C POINTER 71 DWORD 70 POINTER 71 DWORD 71 DWORD 72 POINTER 73 POINTER 74 DWORD 75 POINTER 76 POINTER 77 POINTER 77 POINTER 78 POINTER 78 POINTER 79 POINTER 70 POINTER 71 PWORD 70 POINTER 71 PWORD 71 PWORD 72 PWORD 73 PWORD 74 PWORD 75 PWORD 76 PWORD 76 PWORD 76 PWORD 77 PW	debug path name address	14		Section Name (Zero terminated string)
BSTR* debug Unicode file name address 20 DWO	54 BSTR*	debug file name address	10		Head shared page reference count address
POINTER Kernel image thunk address XOR PUBKEY[84h] XOR PUBKEY[84h] XOR PUBKEY[84h] XOR PUBKEY[84h] XOR PUBKEY[84h] XOR PUBKEY[84h] POINTER Non-kernel import directory address	FOUNTER FOU	debug Unicode file name address	20		Tail shared page reference count address
PUBLEXY (88h) POINTER non-kernel import directory address DWORD number of library versions address POINTER library version address POINTER kernel library version address POINTER APPI library version address POINTER A	5C POINTER 60 DWORD 64 POINTER 68 POINTER 6C POINTER 70 POINTER 71 DWORD ONMENTS: ntry point and k iron RSAI public iron RSAI public hese are the val:	kernel image thunk address XOR PUBKEY[84h] XOR	24	ı	Unknown
POINTER non-kernel import directory address DMORD number of library versions POINTER kernel library version address POINTER kernel library version address POINTER XAPI library version address POINTER API library version address POINTER Logo bitmap size NORD logo bitmap size Nents: Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA1 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA1 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA2 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key. Typo point and kernel thunk addresses are XORed with two DWORDs taken N SA3 public key.	55C POINTER 66 DWORD 64 POINTER 68 POINTER 6C POINTER 77 POINTER 74 DWORD comments: Antry point and ke from RSAI public from RSAI public hese are the val	PUBKEY[88h]	3.7		
DWORD number of library versions address POINTER library versions address POINTER library version address POINTER NAPI library version address POINTER NAPI library version address POINTER logo bitmap address POINTER logo bitmap address POINTER logo bitmap size POINTER	60 DWORD 64 POINTER 68 POINTER 70 POINTER 71 DWORD 71 DWORD 72 DOWNED 73 DWORD 74 DWORD 75 DW	non-kernel import directory address	:	:	
POINTER 11brary versions address POINTER 10go bitmap address POINTER POINTER 10go bitmap address POINTER POI	64 POINTER 68 POINTER 6C POINTER 70 POINTER 74 DWORD 74 DWORD 75 DWORD 76 DWORD 76 DWORD 77 D	number of library versions			
POINTER kernel library version address POINTER XAPI library version address POINTER APPLIATELY Version address POINTER LOGO bitmap address POINTER LOGO bitmap address DWORD LOGO bitmap address DWORD LOGO bitmap address Referred Logo bitmap address	68 POINTER 6C POINTER 74 DWORD Onments: ntry point and k iron RSA1 public hese are the val:	library versions address	4	Thre	d Local Storage Directory Structure. size=1
POINTER XAPI library version address 0 POINTER	70 POINTER 70 POINTER 74 DWORD Oorments: http://doi.org/10.1001/10.100	kernel library version address	į.	Ę	Degription
POINTER 10go bitmap address 4 POINTER	74 DWORD Ournents: Butry point and k rom RSA1 public these are the val:			-	rat data start address
WORD logo bitmap size In and kernel thunk addresses are XORed with two DWORDs taken public key. the values taken from imagebld.exe: 10 DWORD	74 DWORD Comments: Butry point and k From RSA1 public These are the val:	logo bitmap address	9	POTNIER	raw data and address
nt and kernel thunk addresses are XORed with two DWORDs taken 10 DWORD 14 DWORD 114 DWORD 115 LA34FR8h, PUBKEY[89h] = RF95A2ADh 114 DWORD	Comments: Intry point and karron RSA1 public These are the val	logo bitmap size	4 00	POTNTER	TI'S index address
aed with two DWORDs taken 10 DWORD 14 DWORD ADh	intry point and karrom RSA1 public Ihese are the val		U	POINTER	TLS callbacks address
ADh PADh	rom RSA1 public These are the val		10		size of zero fill
ADh	These are the val	key.	14		Characteristics
= FB12BEFAh	VIBKEY[80h] = 1B1	lues taken from imagebld.exe: 103FE6h. PUBKRY[90h] = 8F95A2ADh			
	OBKEY[84h] = 14A	34.748h, PUBKEY[88h] = FB12BEFAh	<u></u>		Library Version Structure, size=10h

Structure, size=18h							
Thread Local Storage Directory Structure, size=18h	Description	raw data start address	raw data end address	TLS index address	TLS callbacks address	size of zero fill	25,24,24,20
Thread		POINTER	POINTER	POINTER	POINTER	DWORD	ממטויים
	Offset Type	0	4	8	C	10	11

		Library Version Structure, Size=10h
Offset Type	Туре	Description
0	BYTE[8]	Library Name
8	WORD	Major Version
A	WORD	Middle Version
C	WORD	Minor Version
田	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.