

HW2-1

Step2:

Here is the content in the import table of PE-import.exe, including KERNELL32.dll and msvcrt.dll

Header info : [PE-Import.exe] - Size of Code : 001800h - decimal : 6 KB

Directory Info :	RVA	SIZE		
Export :	00000000	00000000	>> Not used	1970-01-01
Import :	00006000	000005E4	>>> (05) .idata	1970-01-01
Resource :	00000000	00000000	0 % of exe	Nr of ID : 0
Exception :	00000000	00000000		1970-01-01
Security :	00000000	00000000	not Signed	
Base Reloc :	00000000	00000000		
Debug :	00000000	00000000	PD	
Architecture :	00000000	00000000		1970-01-01
Global PTR :	00000000	00000000		
TLS Table :	00008004	00000018	>>> (07) .tls	
Load Config :	00000000	00000000	>>	
Bound Import :	00000000	00000000	Not used	
Imp. Table IAT :	00006118	000000DC	(05) .idata	
Delay Import :	00000000	00000000		
Com Descriptor :	00000000	00000000	>>> .NET Meta Directory	
reserved :	00000000	00000000		

From header :	Very often :
Size of headers :	00000400 400 or 1000
Size of optional header :	00E0 00E0
Number of Dirs :	0010 0010h
Base of Code :	00001000 00001000
Image Base :	00400000 00400000
Magic optional header :	010B 010B 32bit
Debugger Info - size :	No
File offset to PE :	0080 click me
Checksum CRC :	00022356 00000000
Machine type :	0x14C Intel I386 (same ID used for 4)
OS version :	4.0 4.0 Win NT 4.0

From file

Image version : 1.00

File / sec-n alignment : 0200 / 1000

Entry Point to End of File bytes : 74528 = 72.78 KB

File icon :

Close

Imports :



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	0000603C	00000000	00000000	00006540	00006118
msvcrt.dll	0000608C	00000000	00000000	000065D8	00006168

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
0000603C	0000243C	000061F4	0000	DeleteCriticalSection
00006040	00002440	0000620C	0000	EnterCriticalSection
00006044	00002444	00006224	0000	GetCurrentProcess
00006048	00002448	00006238	0000	GetCurrentProcessId
0000604C	0000244C	0000624E	0000	GetCurrentThreadId
00006050	00002450	00006264	0000	GetLastError
00006054	00002454	00006274	0000	GetStartupInfoA
00006058	00002458	00006286	0000	GetSystemTimeAsFileTime
0000605C	0000245C	000062A0	0000	GetTickCount
00006060	00002460	000062B0	0000	InitializeCriticalSection
00006064	00002464	000062CC	0000	LeaveCriticalSection
00006068	00002468	000062E4	0000	QueryPerformanceCounter
0000606C	0000246C	000062FE	0000	SetUnhandledExceptionFilter
00006070	00002470	0000631C	0000	Sleep
00006074	00002474	00006324	0000	TerminateProcess
00006078	00002478	00006338	0000	TlsGetValue
0000607C	0000247C	00006346	0000	UnhandledExceptionFilter
00006080	00002480	00006362	0000	VirtualProtect
00006084	00002484	00006374	0000	VirtualQuery

Close

Clip

Imports :

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	0000603C	00000000	00000000	00006540	00006118
msvcrt.dll	0000608C	00000000	00000000	000065D8	00006168

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
0000608C	0000248C	00006384	0000	__dllonexit
00006090	00002490	00006392	0000	__getmainargs
00006094	00002494	000063A2	0000	__initenv
00006098	00002498	000063AE	0000	__lconv_init
0000609C	0000249C	000063BE	0000	__set_app_type
000060A0	000024A0	000063D0	0000	__setusermatherr
000060A4	000024A4	000063E4	0000	_acmdln
000060A8	000024A8	000063EE	0000	_amsg_exit
000060AC	000024AC	000063FC	0000	_cexit
000060B0	000024B0	00006406	0000	_fmode
000060B4	000024B4	00006410	0000	_initterm
000060B8	000024B8	0000641C	0000	_job
000060BC	000024BC	00006424	0000	_lock
000060C0	000024C0	0000642C	0000	_onexit
000060C4	000024C4	00006436	0000	_unlock
000060C8	000024C8	00006440	0000	abort
000060CC	000024CC	00006448	0000	calloc
000060D0	000024D0	00006452	0000	exit
000060D4	000024D4	0000645A	0000	fclose
000060D8	000024D8	00006464	0000	fgets
000060DC	000024DC	0000646C	0000	fopen
000060E0	000024E0	00006474	0000	fprintf
000060E4	000024E4	0000647E	0000	fputs
000060E8	000024E8	00006486	0000	free

Clip

Close X

Step3.2

Content in the import tables for the packed PE-Import.exe. As we can see from the content below. The KERNEL.dll and msvcrt.dll has decreased after packing.

Header info : [PE-Import.exe] - Size of Code : 001800h - decimal : 6 KB

Directory Info :

RVA	SIZE		
Export :	00000000	>> Not used	1970-01-01
Import :	00006000	>> (05) .idata	1970-01-01
Resource :	00000000	0 % of exe	Nr of ID : 0
Exception :	00000000		1970-01-01
Security :	00000000	not Signed	
Base Reloc :	00000000		
Debug :	00000000	PE	
Architecture :	00000000		1970-01-01
Global PTR :	00000000		
TLS Table :	00008004	>> (07) .tls	
Load Config :	00000000	>>	
Bound Import :	00000000	Not used	
Imp.Table IAT :	00006118	(05) .idata	
Delay Import :	00000000		
Com Descriptor :	00000000	>> .NET Meta Directory	
reserved :	00000000		

From header :

Size of headers :	00000400	400 or 1000
Size of optional header :	00E0	00E0
Number of Dirs :	0010	0010h
Base of Code :	00001000	00001000
Image Base :	00400000	00400000
Magic optional header :	010B	010B 32bit
Debugger Info - size :	No	
File offset to PE :	0080	click me
Checksum CRC :	00022356	00000000
Machine type :	0x14C Intel I386 (same ID used for 4	
OS version :	4.0	4.0 Win NT 4.0

From file

Image version :	1.00
File / sec-n alignment :	0200 / 1000
Entry Point to End of File bytes :	74528 = 72.78 KB

File icon :

Close

Exeinfo Pe

Imports :



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.DLL	00000000	00000000	00000000	0001F058	0001F03C
msvcrt.dll	00000000	00000000	00000000	0001F065	0001F050

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name	
0001F03C	00006C3C	0001F08E	0000	LoadLibraryA	
0001F040	00006C40	0001F070	0000	ExitProcess	
0001F044	00006C44	0001F07E	0000	GetProcAddress	
0001F048	00006C48	0001F09C	0000	VirtualProtect	

Close

Clip

Imports :

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.DLL	00000000	00000000	00000000	0001F058	0001F03C
msvcrt.dll	00000000	00000000	00000000	0001F065	0001F050

<

>

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
0001F050	00006C50	0001F0AC	0000	_job

Close ✕

Clip

Step 3.3

Content in the import table for the unpacked PE-Import.exe

Header info : [PE-Import.exe] - Size of Code : 001800h - decimal : 6 KB

Directory Info :

RVA	SIZE		
Export :	00000000	>> Not used	1970-01-01
Import :	00006000	>> (05) .idata	1970-01-01
Resource :	00000000	0 % of exe	Nr of ID : 0
Exception :	00000000		1970-01-01
Security :	00000000	not Signed	
Base Reloc :	00000000		
Debug :	00000000	PE	
Architecture :	00000000		1970-01-01
Global PTR :	00000000		
TLS Table :	00008004	>> (07) .tls	
Load Config :	00000000	>>	
Bound Import :	00000000	Not used	
Imp.Table IAT :	00006118	(05) .idata	
Delay Import :	00000000		
Com Descriptor :	00000000	>> .NET Meta Directory	
reserved :	00000000		

From header :

Size of headers :	00000400	400 or 1000
Size of optional header :	00E0	00E0
Number of Dirs :	0010	0010h
Base of Code :	00001000	00001000
Image Base :	00400000	00400000
Magic optional header :	010B	010B 32bit
Debugger Info - size :	No	
File offset to PE :	0080	click me
Checksum CRC :	00022356	00000000
Machine type :	0x14C Intel I386 (same ID used for 4	
OS version :	4.0	4.0 Win NT 4.0

From file

Image version :	1.00
File / sec-n alignment :	0200 / 1000
Entry Point to End of File bytes :	74528 = 72.78 KB

File icon :

Clip

Close

Exeinfo Pe

Imports :

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.DLL	00000000	00000000	00000000	00006540	00006118
msvcrt.dll	00000000	00000000	00000000	000065D8	00006168

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
00006168	00002568	00006384	0000	__dlopenexit
0000616C	0000256C	00006392	0000	__getmainargs
00006170	00002570	000063A2	0000	__initenv
00006174	00002574	000063AE	0000	__lconv_init
00006178	00002578	000063BE	0000	__set_app_type
0000617C	0000257C	000063D0	0000	__setusermatherr
00006180	00002580	000063E4	0000	_acmdln
00006184	00002584	000063EE	0000	_amsg_exit
00006188	00002588	000063FC	0000	_cexit
0000618C	0000258C	00006406	0000	_fmode
00006190	00002590	00006410	0000	_initterm
00006194	00002594	0000641C	0000	_job
00006198	00002598	00006424	0000	_lock
0000619C	0000259C	0000642C	0000	_onexit
000061A0	000025A0	00006436	0000	_unlock
000061A4	000025A4	00006440	0000	abort
000061A8	000025A8	00006448	0000	calloc
000061AC	000025AC	00006452	0000	exit
000061B0	000025B0	0000645A	0000	fclose
000061B4	000025B4	00006464	0000	fgets
000061B8	000025B8	0000646C	0000	fopen
000061BC	000025BC	00006474	0000	fprintf
000061C0	000025C0	0000647E	0000	fputs
000061C4	000025C4	00006486	0000	free

Clip

Close X

Step 4: use obfuscation to fool the anti-malware scanner(s)' s detection, which is to hide the underlying logic of the program so as to prevent the others from having any related knowledge of the code.