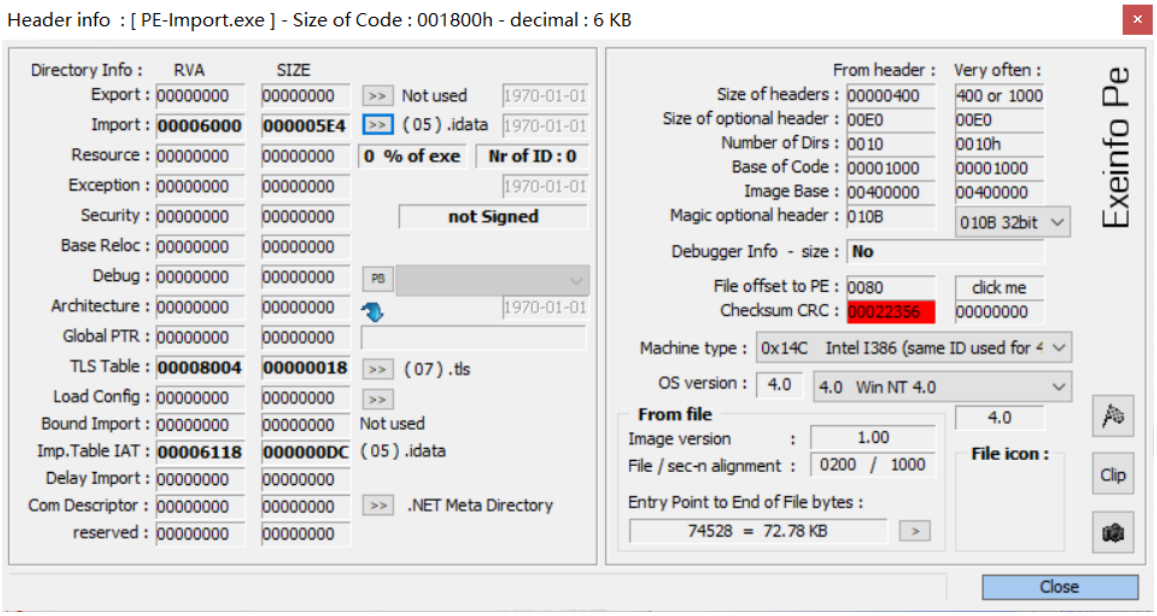
HW2-1

Step2:

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



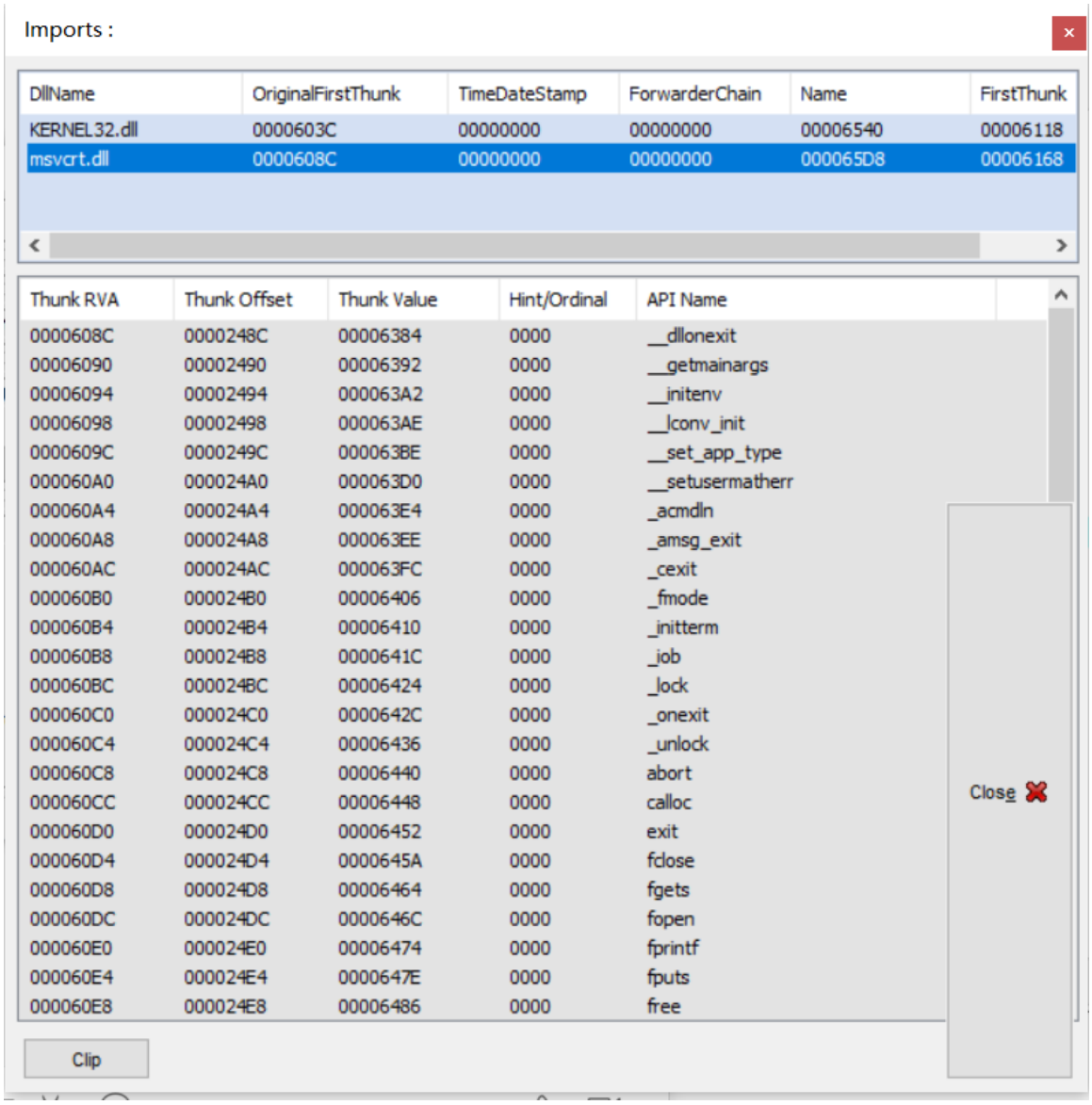
Imports :

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

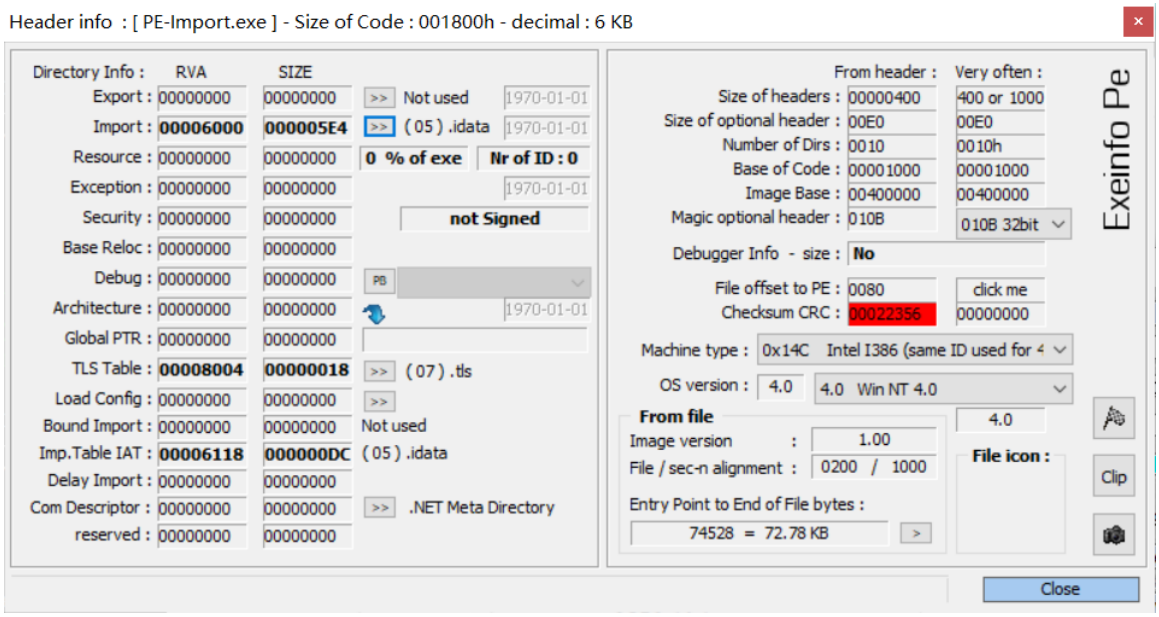
Close

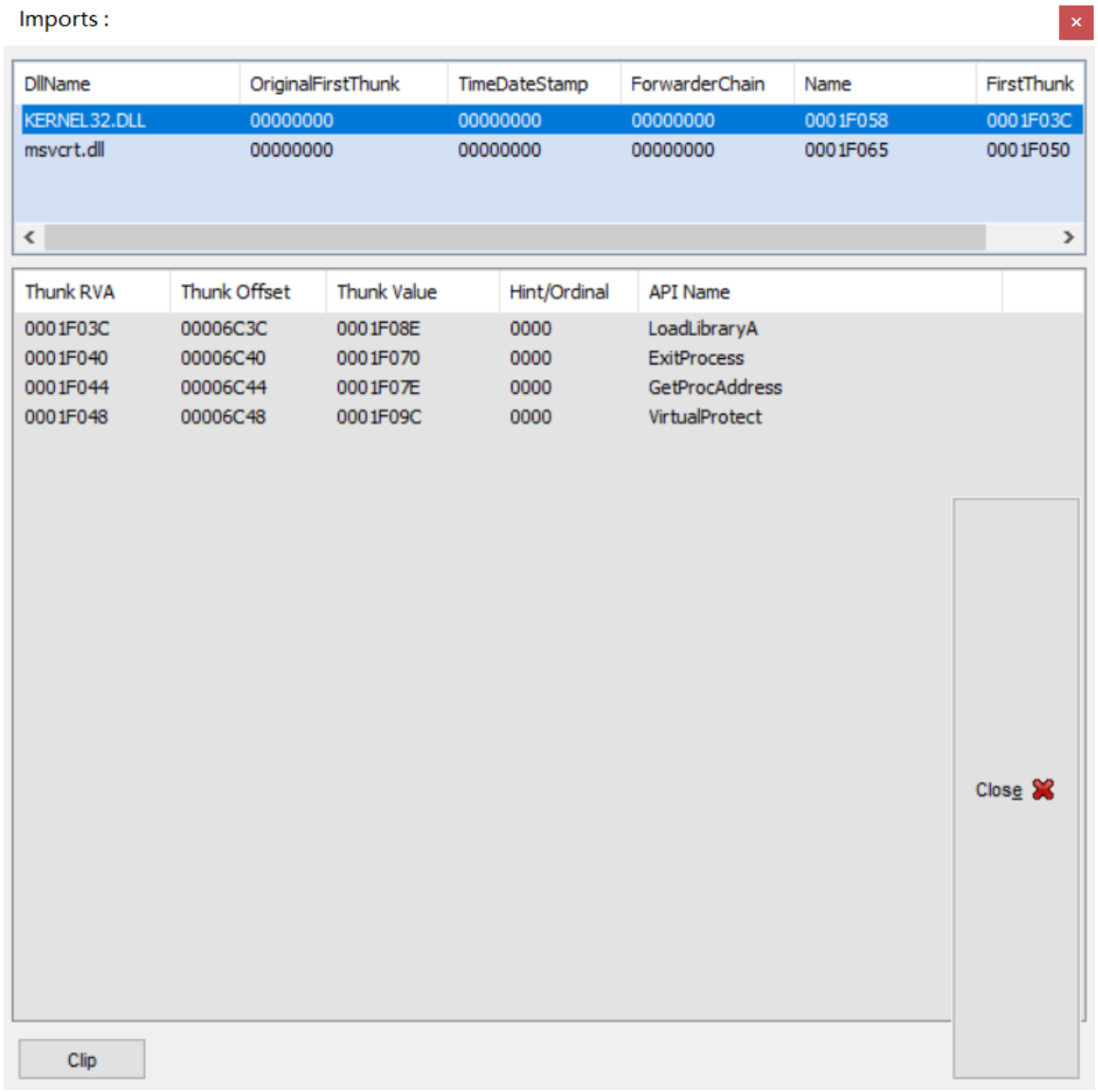
Clip

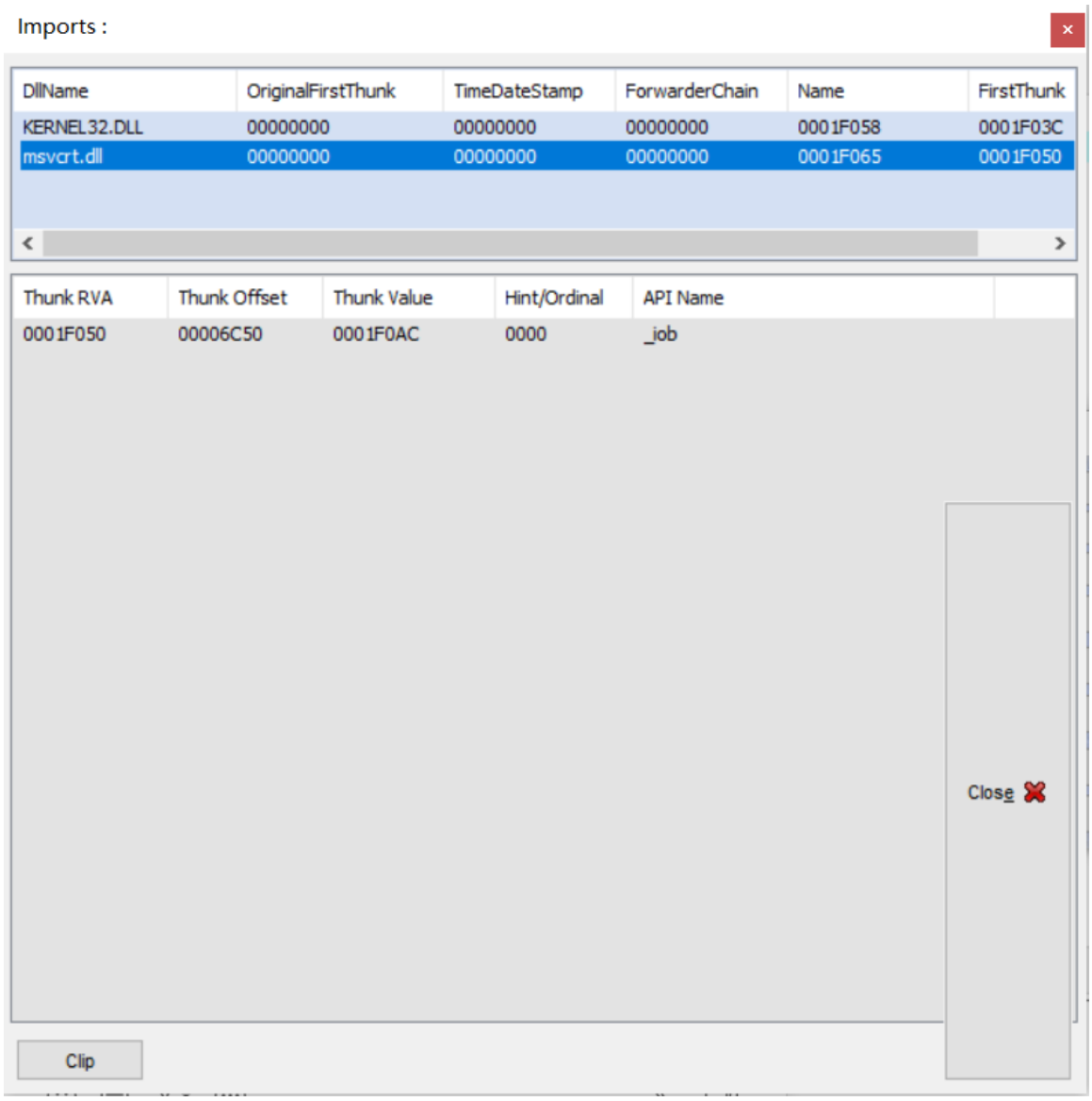


Step3.2

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

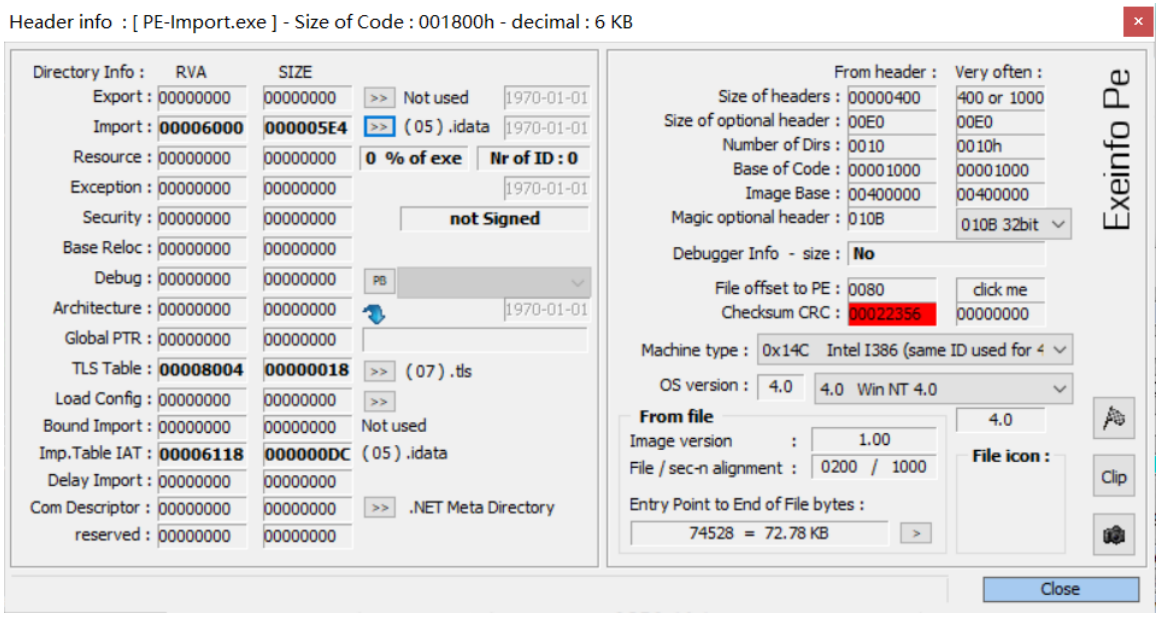

Header info : [PE-Import.exe] - Size of Code : 001800h - decimal : 6 KB
Directory Info : RVA SIZE
Export : 00000000 00000000 >> Not used 1970-01-01
Import : 00006000 000005E4 >> (05) .idata 1970-01-01
Resource : 00000000 00000000 0 % of exe Nr of ID : 0
Exception : 00000000 00000000 1970-01-01
Security : 00000000 00000000 not Signed
Base Reloc : 00000000 00000000
Debug : 00000000 00000000 PB
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
4.0
File icon :
Exeinfo Pe
Clip
Close

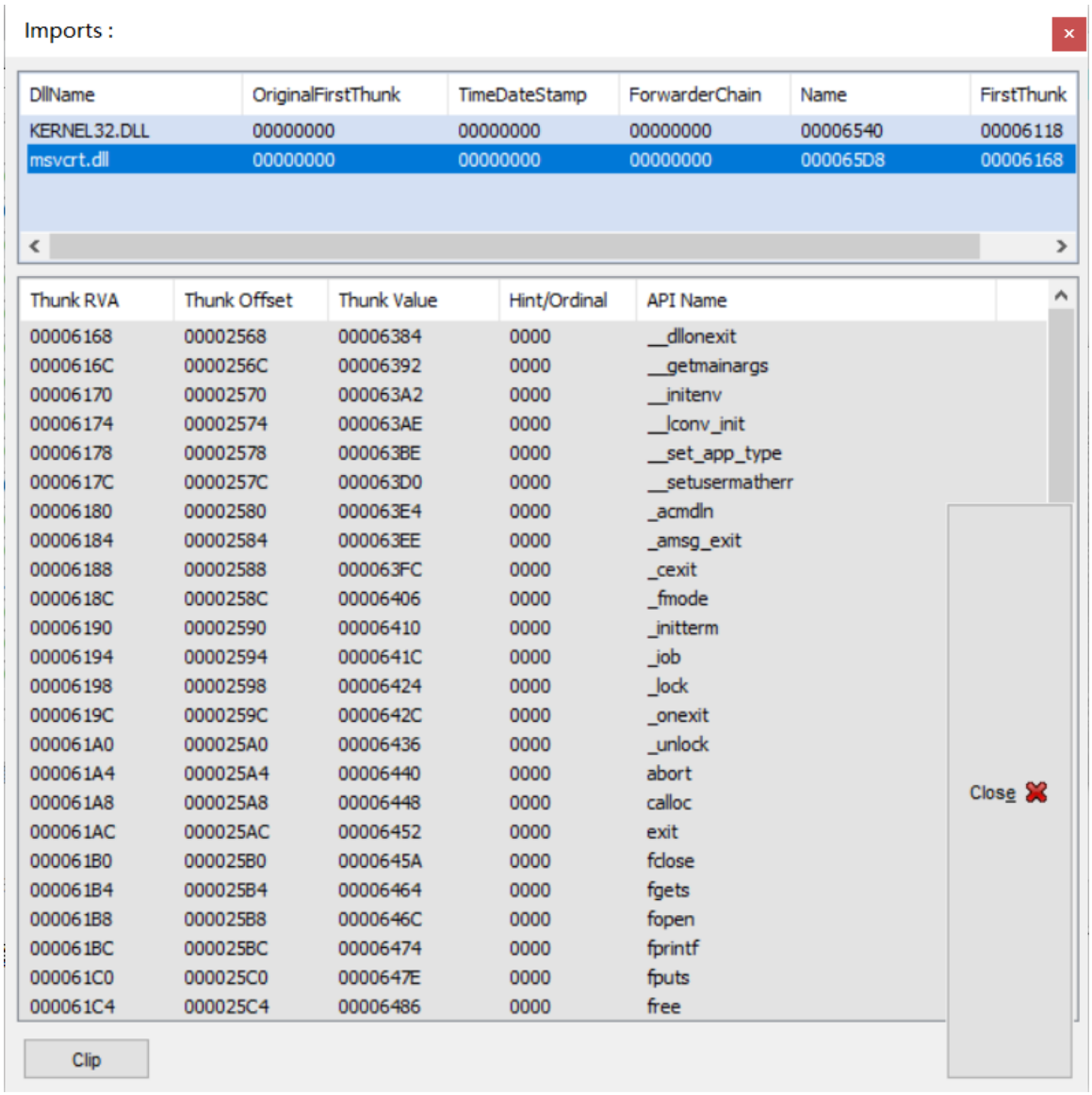

Imports :
DllName
OriginalFirstThunk
TimeDateStamp
ForwarderChain
Name
FirstThunk
KERNEL32.DLL
00000000
00000000
00000000
0001F058
0001F03C
msvcrt.dll
00000000
00000000
00000000
0001F065
0001F050
Thunk RVA
Thunk Offset
Thunk Value
Hint/Ordinal
API Name
0001F03C
00006C3C
0001F08E
0000
LoadLibraryA
0001F040
00006C40
0001F070
0000
ExitProcess
0001F044
00006C44
0001F07E
0000
GetProcAddress
0001F048
00006C48
0001F09C
0000
VirtualProtect
Close
Clip



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 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 PB
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
4.0
File icon :
Exeinfo Pe
Clip
Close



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.