Operációs Rendszerek BSc

3. gyak.

2021. 02. 24.

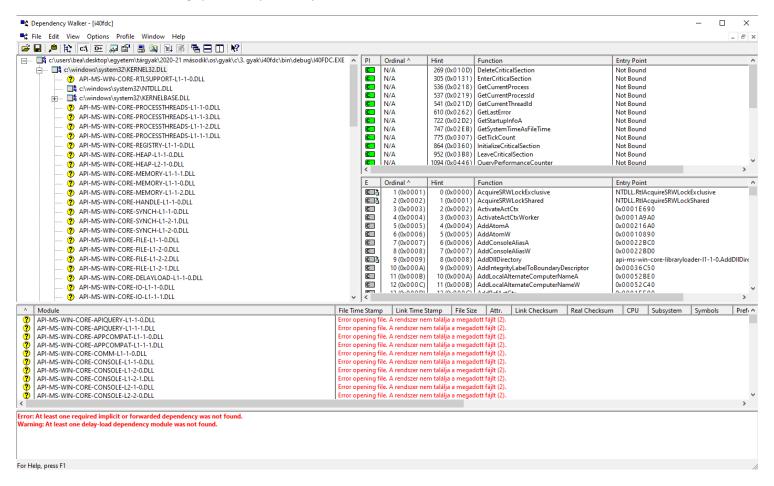
Készítette:

Nyíri Beáta Programtervező Informatikus I40FDC

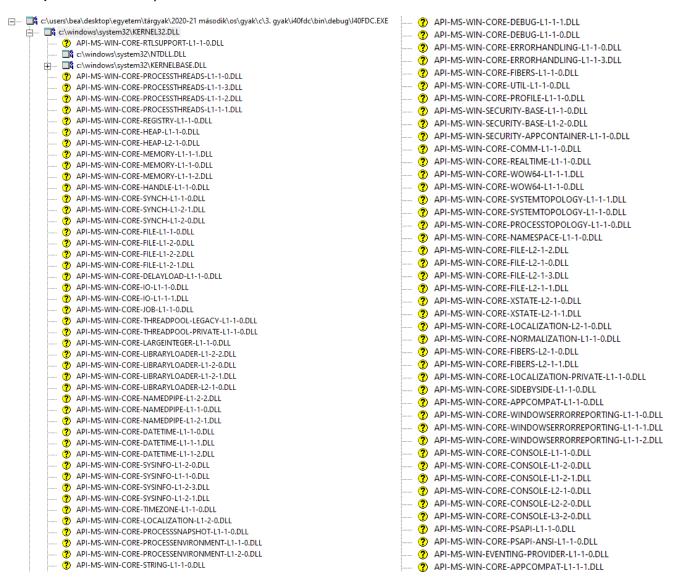
Miskolc, 2021

4. Dependency Walker

Az i40fdc.exe megnyitva a Dependency Walkerben:



a.) Az i40fdc.exe milyen hívásokat használ a kernel32.dll-ből:



b.) Milyen függőségei vannak a kernel32.dll-nek?

Az NTDLL.DLL függősége a kernel32.dll-nek:

्रीडाई c:\windows\system32\NTDLL.DLL

Forwarded module. This module is a dependency because the parent module has forwarded one of its functions to this module.

c.) Mi az NTDLL.DLL szerepe? Importálja a Windows Native API-t.

Exportált függvényei:

E	Ordinal ^	Hint	Function	Entry Point	^
0#	8 (0x0008)	N/A	N/A	0x0007D5E0	
C	9 (0x0009)	0 (0x0000)	A_SHAFinal	0x0000C4D0	
C	10 (0x000A)	1 (0x0001)	A_SHAInit	0x0000C600	
C	11 (0x000B)	2 (0x0002)	A_SHAUpdate	0x0000C640	
C	12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000DFA10	
C	13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage	0x0006C7A0	
C	14 (0x000E)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation	0x000DFA40	
C	15 (0x000F)	6 (0x0006)	AlpcGetCompletionListMessageAttributes	0x000DFA60	
C	16 (0x0010)	7 (0x0007)	AlpcGetHeaderSize	0x0006F020	
C	17 (0x0011)	8 (0x0008)	AlpcGetMessageAttribute	0x0006EFE0	
C	18 (0x0012)		AlpcGetMessageFromCompletionList	0x00031DF0	
C	19 (0x0013)	10 (0x000A)	AlpcGetOutstandingCompletionListMessageCount	0x00085740	
C	20 (0x0014)	11 (0x000B)	AlpcInitializeMessageAttribute	0x0006EF80	
C	21 (0x0015)	12 (0x000C)	AlpcMaxAllowedMessageLength	0x00084260	
C	22 (0x0016)	13 (0x000D)	AlpcRegisterCompletionList	0x000855B0	
C	23 (0x0017)		AlpcRegisterCompletionListWorkerThread	0x0006FEB0	
C	24 (0x0018)	15 (0x000F)	AlpcRundownCompletionList	0x00085700	
C	25 (0x0019)	16 (0x0010)	AlpcUnregisterCompletionList	0x00085720	
C	26 (0x001A)	17 (0x0011)	AlpcUnregisterCompletionListWorkerThread	0x0006FE50	
C	27 (0x001B)	18 (0x0012)	ApiSetQueryApiSetPresence	0x000754B0	
C	28 (0x001C)		ApiSetQueryApiSetPresenceEx	0x000D5710	
C	29 (0x001D)	20 (0x0014)	CsrAllocateCaptureBuffer	0x0004C260	
TC	30 (0x001E)	21 (0x0015)	CsrAllocateMessagePointer	0x0004C220	
C	31 (0x001F)	22 (0x0016)	CsrCaptureMessageBuffer	0x0004C330	
C	32 (0x0020)	23 (0x0017)	CsrCaptureMessageMultiUnicodeStringsInPlace	0x0004C060	
C	33 (0x0021)	24 (0x0018)	CsrCaptureMessageString	0x0004C170	
C	34 (0x0022)	25 (0x0019)	CsrCaptureTimeout	0x000CBED0	
1 °	35 (0x0023)	26 (0x001A)	CsrClientCallServer	0x0004BFF0	~