

Operációs rendszerek BSc

3.gyak.

2021. 02. 24.

Készítette:

Juhász Marcell Tibor
Bsc

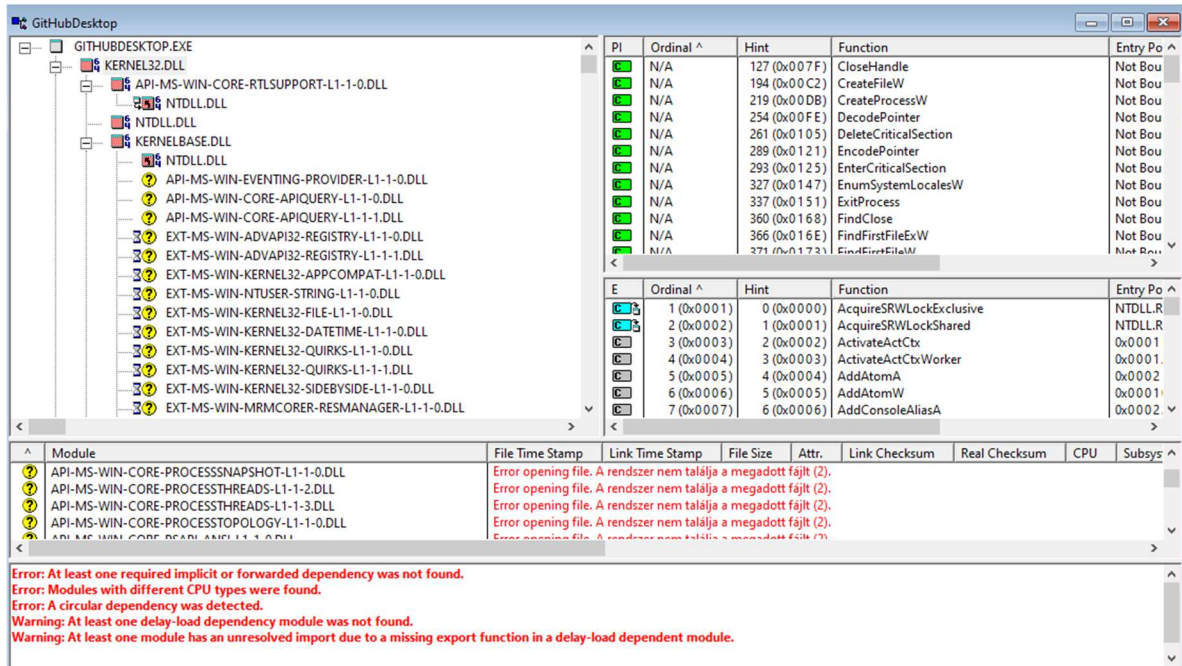
Programtervező
informatikus

O9V4M0

Miskolc, 2021

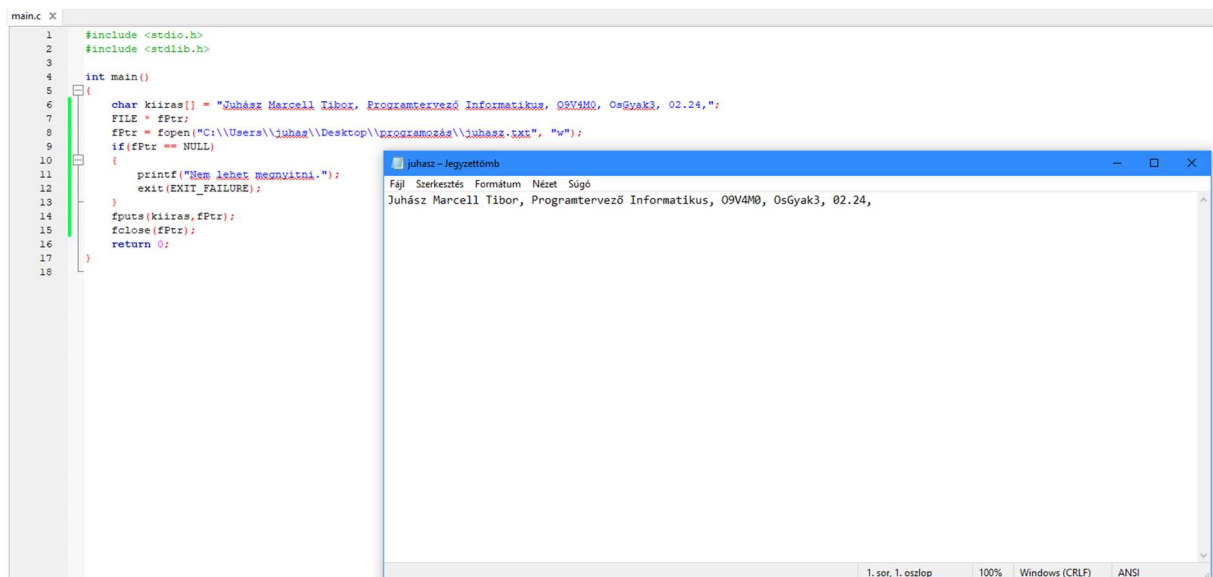
4.Feladat: Dependency Walker vizsgálata

A GitHub vizsgálatokor felfedeztem hogy milyen sok funkciója van a fájlok fölött.



5.Feladat: C Program vizsgálata

Készítettem egy alapszintű programot, ami csinált egy txt fájlt.



a.) O9V4M0.exe vizsgálata

A nepunkod.exe vizsgálatakor ezt találtam, szerintem ezek azt mutatják, hogy milyen processzeket hoz létre. Ezt a zöld részben látom

[illegible]

b.) O9V4M0.exe vizsgálata

A függőségek főként biztonsági hívásokat csinál a tűzfalon belül a hozzáféréseknek.

Dependency Walker - [O9V4M0]

File Edit View Options Profile Window Help

O9V4M0.EXE

- KERNEL32.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- NTDLL.DLL
- KERNELBASE.DLL
- NTDLL.DLL
- API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
- API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
- API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
- EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
- EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
- EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
- EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
- EXT-MS-WIN-MRMCMORER-RESMANAGER-L1-1-0.DLL
- EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
- EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
- EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL
- EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-NTMARTA-L1-1-0.DLL
- EXT-MS-WIN-SECURITY-CAPAUTHZ-L1-1-1.DLL
- EXT-MS-WIN-SECURITY-ENCRIPTEDFILE-L1-1-0.DLL
- EXT-MS-WIN-SECURITY-EFSWRT-L1-1-0.DLL
- API-MS-WIN-SECURITY-SDDL-L1-1-0.DLL
- EXT-MS-ONECORE-APPMODEL-STATEREPOSITORY-CACHE-L1-1-0.DLL
- EXT-MS-WIN-APPMODEL-DAXCORE-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-ERRORHANDLING-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-REGISTRY-L1-1-0.DLL
- EXT-MS-WIN-KERNELBASE-PROCESSTHREAD-L1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-NPUSERNAME-L1-1-0.DLL
- EXT-MS-WIN-APPXDEPLOYMENTCLIENT-APPXDEPLOY-L1-1-0.DLL
- EXT-MS-ONECORE-APPMODEL-STATEREPOSITORY-INTERNAL-L1-1-0.DLL
- EXT-MS-WIN-APPXDEPLOYMENTCLIENT-APPXDEPLOYONEC-L1-1-0.DLL

PI	Ordinal ^	Hint	Function	Entr
6	N/A	269 (0x010D)	DeleteCriticalSection	Not
6	N/A	305 (0x0131)	EnterCriticalSection	Not
6	N/A	536 (0x0218)	GetCurrentProcess	Not
6	N/A	537 (0x0219)	GetCurrentProcessId	Not
6	N/A	541 (0x021D)	GetCurrentThreadId	Not
6	N/A	610 (0x0262)	GetLastError	Not
6	N/A	722 (0x02D2)	GetStartupInfoA	Not
6	N/A	747 (0x02EB)	GetSystemTimeAsFileTime	Not
6	N/A	775 (0x0307)	GetTickCount	Not
6	N/A	864 (0x0360)	InitializeCriticalSection	Not
6	N/A	952 (0x03B8)	LeaveCriticalSection	Not
6	N/A	1094 (0x0446)	QueryPerformanceCounter	Not
6	N/A	1180 (0x049C)	RtlAddFunctionTable	Not
6	N/A	1181 (0x049D)	RtlCaptureContext	Not
6	N/A	1188 (0x04A4)	RtlLookupFunctionEntry	Not
6	N/A	1195 (0x04AB)	RtlVirtualUnwind	Not
6	N/A	1347 (0x0543)	SetUnhandledExceptionFilter	Not
6	N/A	1361 (0x0551)	Sleep	Not
6	N/A	1376 (0x0560)	TerminateProcess	Not
6	N/A	1396 (0x0574)	TlsGetValue	Not
6	N/A	1410 (0x0582)	UnhandledExceptionFilter	Not
6	N/A	1444 (0x05A4)	VirtualProtect	Not
6	N/A	1446 (0x05A6)	VirtualQuery	Not

E	Ordinal ^	Hint	Function	Ent
1	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTI
2	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTI
3	3 (0x0003)	2 (0x0002)	ActivateActCtx	0xC
4	4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0xC
5	5 (0x0005)	4 (0x0004)	AddAtomA	0xC
6	6 (0x0006)	5 (0x0005)	AddAtomW	0xC
7	7 (0x0007)	6 (0x0006)	AddConsoleAliasA	0xC
8	8 (0x0008)	7 (0x0007)	AddConsoleAliasW	0xC
9	9 (0x0009)	8 (0x0008)	AddDllDirectory	api
10	10 (0x000A)	9 (0x0009)	AddInterlockedShelToBoundDescriptor	0xC

c.) O9V4M0.exe vizsgálata

Ntdll.dll-t a Microsoft készítette az operációs rendszer fejlesztéséhez. Az exportált függvények hozzáférést kapnak a kernelhez.

Dependency Walker - [O9V4M0]

File Edit View Options Profile Window Help

O9V4M0.EXE

- KERNEL32.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
 - NTDLL.DLL
 - KERNELBASE.DLL
 - NTDLL.DLL**
 - API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
 - API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
 - API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
 - EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
 - EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
 - EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
 - EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
 - EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
 - EXT-MS-WIN-MRMCOER-RESMANAGER-L1-1-0.DLL
 - EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
 - EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
 - EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL
 - EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
 - EXT-MS-WIN-ADVAPI32-NTMARTA-L1-1-0.DLL
 - EXT-MS-WIN-SECURITY-CAPAUTHZ-L1-1-1.DLL
 - EXT-MS-WIN-FECLIENT-ENCRYPTEDFILE-L1-1-0.DLL
 - EXT-MS-WIN-SECURITY-EFSWRT-L1-1-0.DLL
 - API-MS-WIN-SECURITY-SDDL-L1-1-0.DLL
 - EXT-MS-ONECORE-APPMODEL-STATEREPOSITORY-CACHE-L1-1-0.DLL
 - EXT-MS-WIN-APPMODEL-DAXCORE-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-ERRORHANDLING-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-REGISTRY-L1-1-0.DLL
 - EXT-MS-WIN-KERNELBASE-PROCESSTHREAD-L1-1-0.DLL
 - EXT-MS-WIN-ADVAPI32-NPUSERNAME-L1-1-0.DLL
 - EXT-MS-WIN-APPXDEPLOYMENTCLIENT-APPXDEPLOY-L1-1-0.DLL
 - EXT-MS-ONECORE-APPMODEL-STATEREPOSITORY-INTERNAL-L1-1-0.DLL
 - EXT-MS-WIN-APPXDEPLOYMENTCLIENT-APPXDEPLOYONEC-L1-1-0.DLL

PI	Ordinal ^	Hint	Function
0#	8 (0x0008)	N/A	N/A
	N/A	20 (0x0014)	CsrAllocateCaptureBuffer
	N/A	21 (0x0015)	CsrAllocateMessagePointer
	N/A	22 (0x0016)	CsrCaptureMessageBuffer
	N/A	23 (0x0017)	CsrCaptureMessageMultiUnicodeStringsInPlace
	N/A	26 (0x001A)	CsrClientCallServer
	N/A	27 (0x001B)	CsrClientConnectToServer
	N/A	28 (0x001C)	CsrFreeCaptureBuffer
	N/A	29 (0x001D)	CsrGetProcessId
	N/A	34 (0x0022)	DbgPrint
	N/A	35 (0x0023)	DbgPrintEx
	N/A	40 (0x0028)	DbgUiConnectToDbg
	N/A	41 (0x0029)	DbgUiContinue
	N/A	42 (0x002A)	DbgUiConvertStateChangeStructure
	N/A	43 (0x002B)	DbgUiConvertStateChangeStructureEx
	N/A	44 (0x002C)	DbgUiDebugActiveProcess
	N/A	45 (0x002D)	DbgUiGetThreadDebugObject
	N/A	49 (0x0031)	DbgUiStopDebugging
	N/A	50 (0x0032)	DbgUiWaitStateChange
	N/A	52 (0x0034)	EtwCheckCoverage
	N/A	57 (0x0039)	EtwEventEnabled
	N/A	59 (0x003B)	EtwEventRegister
	N/A	61 (0x003D)	EtwEventUnregister
	N/A	62 (0x003E)	EtwEventWrite
	N/A	66 (0x0042)	EtwEventWriteNoRegistration
	N/A	69 (0x0045)	EtwEventWriteTransfer
	N/A	100 (0x0064)	LdrAccessResource
	N/A	101 (0x0065)	LdrAddDllDirectory
	N/A	102 (0x0066)	LdrAddDllData

E	Ordinal ^	Hint	Function
0#	8 (0x0008)	N/A	N/A
	9 (0x0009)	0 (0x0000)	A_SHAFinal
	10 (0x000A)	1 (0x0001)	A_SHAInit
	11 (0x000B)	2 (0x0002)	A_SHAUpdate
	12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount
	13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage
	14 (0x000E)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation
	15 (0x000F)	6 (0x0006)	AlpcGetCompletionListMessageAttributes
	16 (0x0010)	7 (0x0007)	AlpcGetHeaderSize
	17 (0x0011)	8 (0x0008)	AlpcGetMessageAttribute