

Operációs rendszerek BSc

1. Gyak.

2022. 02. 08.

Készítette:

Gerőcs Gergő Bsc
Mérnökinformatika
FEU2E5

Miskolc, 2022

1. feladat

a.) Hozza létre a következő mappa szerkezetet!

```
C:\>cd feu2e5

C:\feu2e5>tree feu2e5
Folder PATH listing
Volume serial number is 06F1-06EF
C:\FEU2E5\FEU2E5
Invalid path - \FEU2E5\FEU2E5
No subfolders exist

C:\feu2e5>cd..

C:\>tree feu2e5
Folder PATH listing
Volume serial number is 00000056 06F1:06EF
C:\FEU2E5
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
├── land
│   ├── kokusz
│   └── szeder
└──
```

b.) Készítsen másolatot:

```
C:\>tree feu2e5
Folder PATH listing
Volume serial number is 0000006A 06F1:06EF
C:\FEU2E5
|
|---bokor
|   |
|   |---banan
|   |---barack
|   |---mogyoro
|
|---fa
|   |
|   |---barack
|   |---korte
|   |---szeder
|
|---land
|   |
|   |---kokusz
|   |---szeder
|
C:\>
```

c.) Végezze el a következő áthelyezéseket:

```
C:\>tree feu2e5
Folder PATH listing
Volume serial number is 00000097 06F1:06EF
C:\FEU2E5
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── land
    └── szeder

C:\>
```

d.) Törölje a neptunkod/land katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:

```
Volume Serial Number is 06F1-06EF

Directory of C:\feu2e5\bokor

2022. 02. 16. 08:59 <DIR>      .
2022. 02. 16. 08:59 <DIR>      ..
2022. 02. 16. 09:01 <DIR>      banan
2022. 02. 16. 08:18 <DIR>      mogyoro
                0 File(s)        0 bytes
                4 Dir(s)  20 920 987 648 bytes free

C:\feu2e5\bokor>cd banan

C:\feu2e5\bokor\banan>dir
Volume in drive C has no label.
Volume Serial Number is 06F1-06EF

Directory of C:\feu2e5\bokor\banan

2022. 02. 16. 09:01 <DIR>      .
2022. 02. 16. 09:01 <DIR>      ..
2022. 02. 16. 09:01          0 leiras.txt
                1 File(s)        0 bytes
                2 Dir(s)  20 920 983 552 bytes free

C:\feu2e5\bokor\banan>cd....

C:\feu2e5\bokor\banan>cd..

C:\feu2e5\bokor>cd..

C:\feu2e5>cd fa

C:\feu2e5\fa>dir
Volume in drive C has no label.
Volume Serial Number is 06F1-06EF

Directory of C:\feu2e5\fa

2022. 02. 16. 09:01 <DIR>      .
2022. 02. 16. 09:01 <DIR>      ..
2022. 02. 16. 08:19 <DIR>      barack
2022. 02. 16. 09:01          0 felsorolas.txt
2022. 02. 16. 08:19 <DIR>      kokusz
2022. 02. 16. 08:18 <DIR>      korte
2022. 02. 16. 08:19 <DIR>      szeder
                1 File(s)        0 bytes
                6 Dir(s)  20 920 614 912 bytes free
```

e.) A leiras.txt szöveges állományba írjon 3 sort a barackról. A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét

```
C:\feu2e5\fa>ECHO DOBAI >felsorolas.txt  
C:\feu2e5\fa>ECHO DOBAI >felsorolas.txt  
C:\feu2e5\fa>ECHO DOBAI >felsorolas.txt  
C:\feu2e5\fa>ECHO DOBAI >felsorolas.txt  
C:\feu2e5\fa>ECHO DOBAI >felsorolas.txt  
C:\feu2e5\fa>_
```

```
C:\feu2e5\bokor\banan>ECHO A barack okos >leiras.txt  
C:\feu2e5\bokor\banan>ECHO A barack szép >>leiras.txt  
C:\feu2e5\bokor\banan>ECHO A barack finom mert tomival mos >>leiras.txt  
C:\feu2e5\bokor\banan>
```

f.) Listázza a neptunkod mappa tartalmát úgy, hogy megjelenjen az almappák tartalma is.

```
C:\>tree feu2e5 /f
Folder PATH listing
Volume serial number is 000000D6 06F1:06EF
C:\FEU2E5
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   └── mogyoro
├── fa
│   ├── felsorolas.txt
│   ├── leiras.txt
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
C:\>
```

g.) Térjen vissza a gyökérmappába és keresse meg az összes olyan file-t, amelyek nevének második betűje e

```
C:\feu2e5>dir ?e* /s
Volume in drive C has no label.
Volume Serial Number is 06F1-06EF

Directory of C:\feu2e5\bokor\banan

2022. 02. 16. 09:15                66 leiras.txt
                1 File(s)                66 bytes

Directory of C:\feu2e5\fa

2022. 02. 16. 09:11                8 felsorolas.txt
2022. 02. 16. 09:13               34 leiras.txt
                2 File(s)                42 bytes

Total Files Listed:
                3 File(s)                108 bytes
                0 Dir(s) 20 907 741 184 bytes free

C:\feu2e5>_
```


h.) Tegye mindenki számára olvashatóvá a felsorolas.txt file-t

```
C:\feu2e5\fa>icacls felsorolas.txt /grant mindenki:(R)
processed file: felsorolas.txt
Successfully processed 1 files; Failed processing 0 files
C:\feu2e5\fa>_
```

i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a neptunkod mappa az al-mappáival együtt.

```
2022. 02. 16. 09:01 <DIR> .
2022. 02. 16. 09:01 <DIR> ..
2022. 02. 16. 09:15      66 leiras.txt
                1 File(s)      66 bytes

Directory of C:\feu2e5\bokor\mogyor

2022. 02. 16. 08:18 <DIR> .
2022. 02. 16. 08:18 <DIR> ..
                0 File(s)      0 bytes

Directory of C:\feu2e5\fa

2022. 02. 16. 09:21 <DIR> .
2022. 02. 16. 09:21 <DIR> ..
2022. 02. 16. 08:19 <DIR> barack
2022. 02. 16. 09:11      8 felsorolas.txt
2022. 02. 16. 08:19 <DIR> kokusz
2022. 02. 16. 08:18 <DIR> korte
2022. 02. 16. 08:19 <DIR> szeder
                1 File(s)      8 bytes

Directory of C:\feu2e5\fa\barack

2022. 02. 16. 08:19 <DIR> .
2022. 02. 16. 08:19 <DIR> ..
                0 File(s)      0 bytes

Directory of C:\feu2e5\fa\kokusz

2022. 02. 16. 08:19 <DIR> .
2022. 02. 16. 08:19 <DIR> ..
                0 File(s)      0 bytes

Directory of C:\feu2e5\fa\korte

2022. 02. 16. 08:18 <DIR> .
2022. 02. 16. 08:18 <DIR> ..
                0 File(s)      0 bytes

Directory of C:\feu2e5\fa\szeder

2022. 02. 16. 08:19 <DIR> .
2022. 02. 16. 08:19 <DIR> ..
                0 File(s)      0 bytes

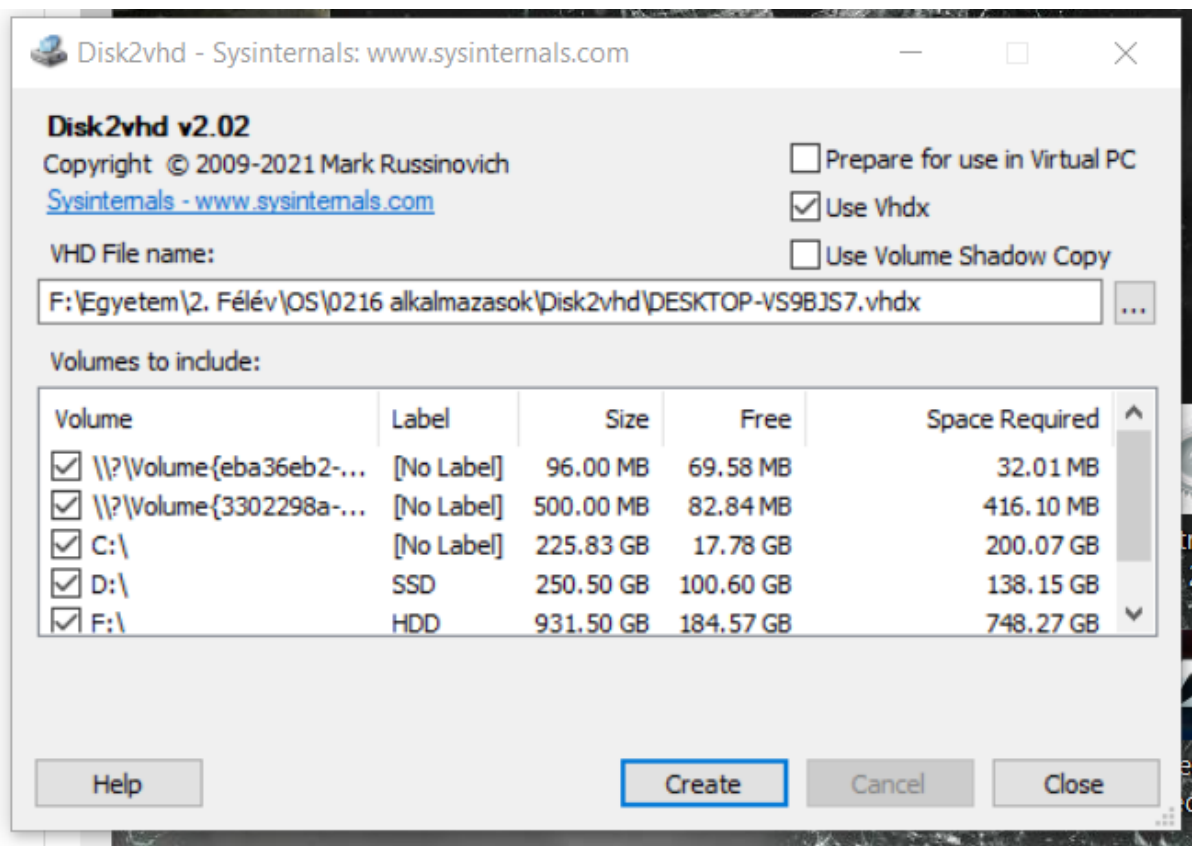
Total Files Listed:
      2 File(s)      74 bytes
     26 Dir(s)  20 905 259 008 bytes free
```

j.) Rendezze ABC-szerint a felsorolas.txt file tartalmát.

```
C:\feu2e5>sort C:\feu2e5\fa\felsorolas.txt
Attila
DOBAI
Eniko
Peter
Zseniko
```

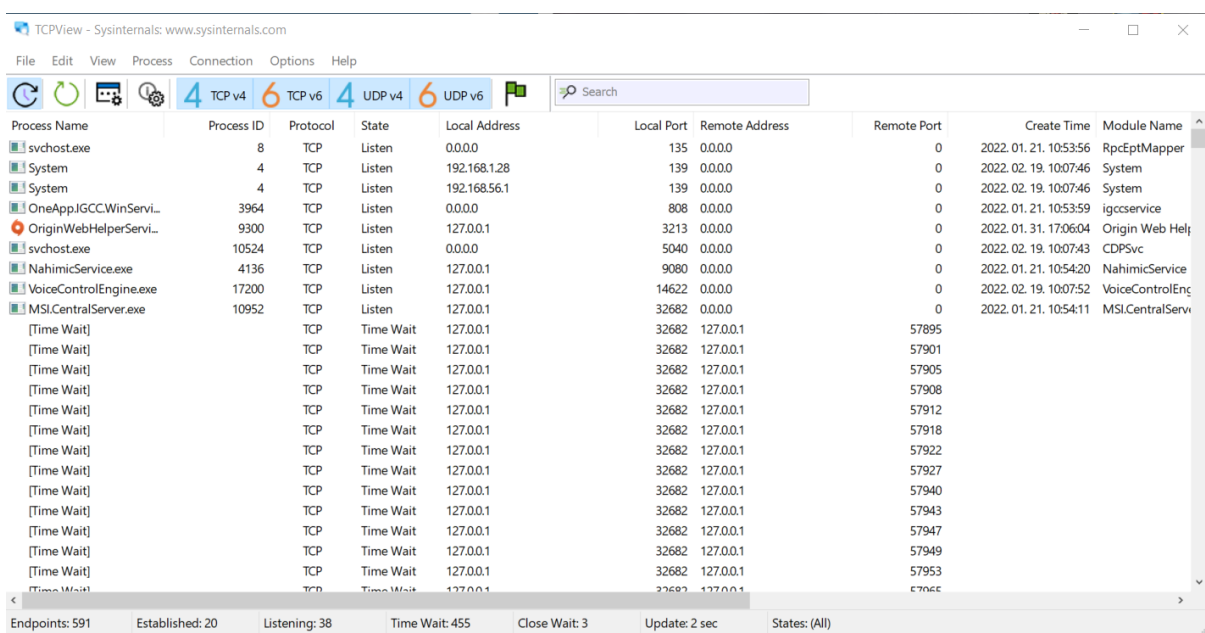
2).feladat

a) File and Disk Utilities (Disk2vhd)



A program egy virtuális másolatot készít a kijelölt lemezeiről.

b) Networking Utilities (TCPView)



The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Edit', 'View', 'Process', 'Connection', 'Options', and 'Help'. The toolbar has icons for refreshing, pausing, and other functions, along with filters for '4 TCP v4', '6 TCP v6', '4 UDP v4', and '6 UDP v6'. A search bar is present. The main table displays network connections with columns: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, and Module Name. The table lists various system and application processes, including svchost.exe, System, OneApp.JGCC.WinServi..., OriginWebHelperServi..., NahimicService.exe, VoiceControlEngine.exe, and MSI.CentralServer.exe. It shows multiple 'Time Wait' states for TCP connections. At the bottom, a status bar provides summary statistics: Endpoints: 591, Established: 20, Listening: 38, Time Wait: 455, Close Wait: 3, Update: 2 sec, and States: (All).

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	8	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.01.21.10:53:56	RpcEptMapper
System	4	TCP	Listen	192.168.1.28	139	0.0.0.0	0	2022.02.19.10:07:46	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.19.10:07:46	System
OneApp.JGCC.WinServi...	3964	TCP	Listen	0.0.0.0	808	0.0.0.0	0	2022.01.21.10:53:59	igccservice
OriginWebHelperServi...	9300	TCP	Listen	127.0.0.1	3213	0.0.0.0	0	2022.01.31.17:06:04	Origin Web Hel
svchost.exe	10524	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.19.10:07:43	CDPSvc
NahimicService.exe	4136	TCP	Listen	127.0.0.1	9080	0.0.0.0	0	2022.01.21.10:54:20	NahimicService
VoiceControlEngine.exe	17200	TCP	Listen	127.0.0.1	14622	0.0.0.0	0	2022.02.19.10:07:52	VoiceControlEng
MSI.CentralServer.exe	10952	TCP	Listen	127.0.0.1	32682	0.0.0.0	0	2022.01.21.10:54:11	MSI.CentralServ
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57895		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57901		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57905		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57908		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57912		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57918		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57922		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57927		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57940		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57943		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57947		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57949		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57953		
[Time Wait]		TCP	Time Wait	127.0.0.1	32682	127.0.0.1	57955		

Endpoints: 591 Established: 20 Listening: 38 Time Wait: 455 Close Wait: 3 Update: 2 sec States: (All)

Egy program, amely megmutatja a rendszer összes TCP és UDP végpontjának részletes listáját, beleértve a helyi és távoli címeket és a TCP kapcsolatok állapotát.

c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)

The screenshot displays a Windows desktop with three utility windows open:

- AutoRuns - Sysinternals:** Shows a list of programs that start automatically with Windows. The 'Logon' tab is selected, showing entries like 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and 'Adobe Acrobat Synchronizer'.
- Process Explorer - Sysinternals:** Displays a list of running processes. The 'Process' tab is selected, showing columns for CPU, Private Bytes, Working Set, PID, Description, and Company Name. Processes like 'svchost.exe', 'smss.exe', and 'csrss.exe' are visible.
- Process Monitor - Sysinternals:** Shows a log of system events. The 'Process Name' column is selected, showing events for 'svchost.exe' and 'smss.exe'.

A Process Explorer a futó folyamatok monitorozása alkalmas míg a AutoRuns a rendszer indítással induló folyamatok jeleníti meg.

d) Security Utilities (LogonSession)

```
Administrator: PowerShell
UPN:

22] Logon session 00000000:0f45d7ad:
  User name: Window Manager\WM-9
  Auth package: Negotiate
  Logon type: Interactive
  Session: 9
  Sid: 5-1-5-98-0-9
  Logon time: 2022. 02. 16. 13:00:45
  Logon server:
  DNS Domain:
  UPN:

23] Logon session 00000000:0f45d7c5:
  User name: Window Manager\WM-9
  Auth package: Negotiate
  Logon type: Interactive
  Session: 9
  Sid: 5-1-5-98-0-9
  Logon time: 2022. 02. 16. 13:00:45
  Logon server:
  DNS Domain:
  UPN:

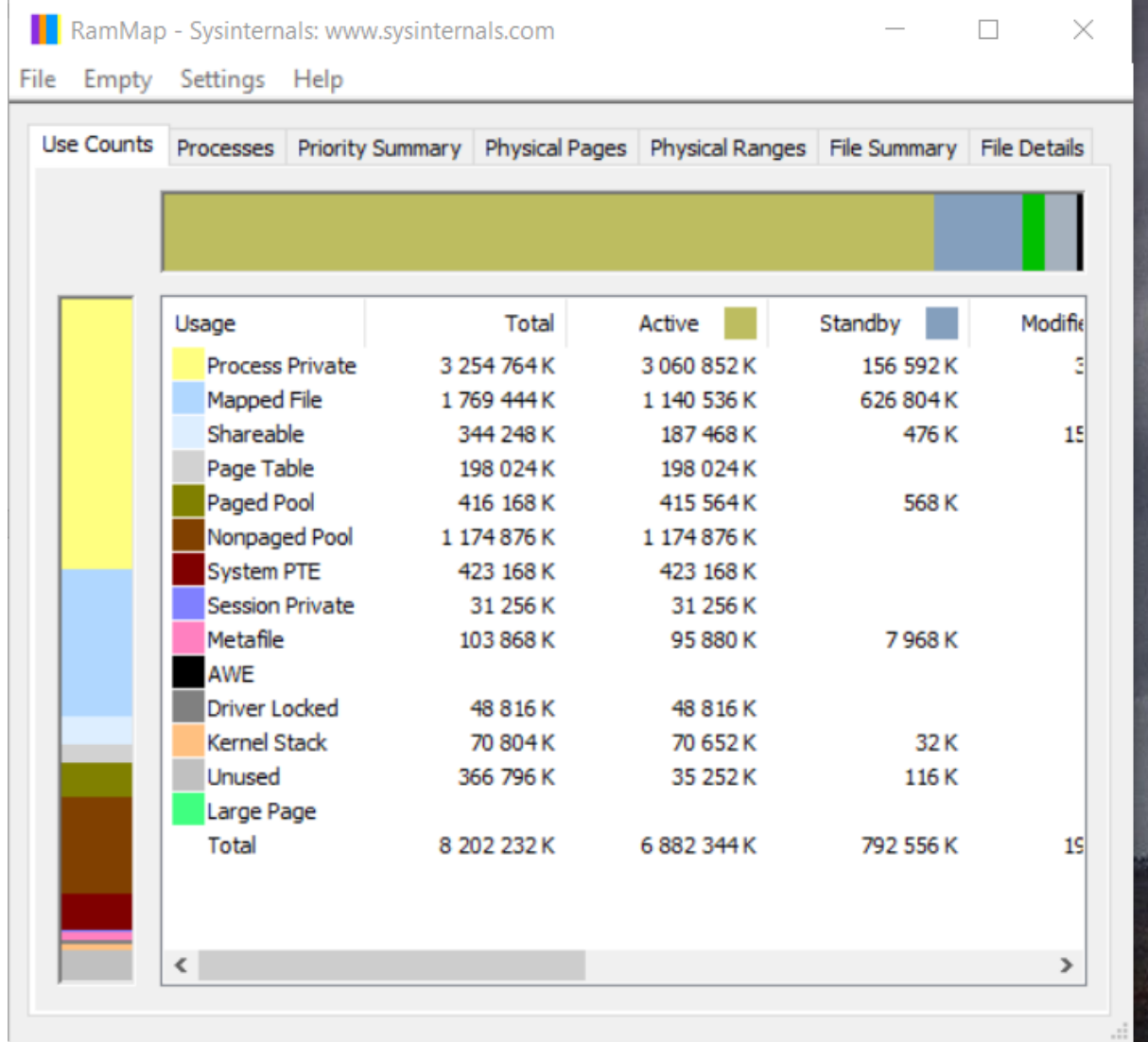
24] Logon session 00000000:0f49c600:
  User name: DESKTOP-OK08NMS\Acer
  Auth package: NTLM
  Logon type: Interactive
  Session: 9
  Sid: 5-1-5-21-1800262312-3136869809-3468689867-1001
  Logon time: 2022. 02. 16. 13:30:41
  Logon server: DESKTOP-OK08NMS
  DNS Domain:
  UPN:

25] Logon session 00000000:0f49c61f:
  User name: DESKTOP-OK08NMS\Acer
  Auth package: NTLM
  Logon type: Interactive
  Session: 9
  Sid: 5-1-5-21-1800262312-3136869809-3468689867-1001
  Logon time: 2022. 02. 16. 13:30:41
  Logon server: DESKTOP-OK08NMS
  DNS Domain:
  UPN:

C:\Users\Acer\Downloads\SysinternalsSuite>
```

A program jegyzi a felhasználók bejelentkezését.

e) Information Utilities (RAMMap)



A program feladata a memória felhasználás monitorozása.

3.feladat

a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!

Dependency Walker - [neptunkod.exe]

File Edit View Options Profile Window Help

Kernel32.dll

PI	Ordinal	Hint	Function	Entry Point
N/A	215 (0x00D7)		DeleteCriticalSection	Not Bound
N/A	243 (0x00F3)		EnterCriticalSection	Not Bound
N/A	360 (0x0168)		FreeLibrary	Not Bound
N/A	456 (0x01C8)		GetCurrentProcess	Not Bound
N/A	457 (0x01C9)		GetCurrentProcessId	Not Bound
N/A	461 (0x01CD)		GetCurrentThreadId	Not Bound
N/A	519 (0x0207)		GetLastError	Not Bound
N/A	537 (0x0219)		GetModuleHandleA	Not Bound
N/A	585 (0x0249)		GetProcAddress	Not Bound
N/A	616 (0x0268)		GetStartupInfoA	Not Bound

Ordinal	Hint	Function	Entry Point
1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
3 (0x0003)	2 (0x0002)	ActivateActCtx	0x00020080
4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x00018700
5 (0x0005)	4 (0x0004)	AddAtomA	0x00059170
6 (0x0006)	5 (0x0005)	AddAtomW	0x000128F0
7 (0x0007)	6 (0x0006)	AddConsoleAliasA	0x00025640
8 (0x0008)	7 (0x0007)	AddConsoleAliasW	0x00025650
9 (0x0009)	8 (0x0008)	AddDllDirectory	api-ms-win-core-libraryloader-l1-1-0.AddDllDirectory
10 (0x000A)	9 (0x0009)	AddIntegrityLabelToBoundaryDescriptor	0x0003BD10

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											

Error: At least one required implicit or forwarded dependency was not found.
Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.

For Help, press F1

Írjon ide a kereséshez

1001
2022. 02. 19.

b.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról!

Dependency Walker - [Fouze5.exe]

File Edit View Options Profile Window Help

FEUZE5.EXE

- KERNEL32.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- NTDLL.DLL**
- KERNELBASE.DLL
- API-MS-WIN-CORE-PROCESSTHEADS-L1-1-0.DLL
- API-MS-WIN-CORE-PROCESSTHEADS-L1-1-2.DLL
- API-MS-WIN-CORE-PROCESSTHEADS-L1-1-1.DLL
- API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
- API-MS-WIN-CORE-HEAP-L2-1-0.DLL
- API-MS-WIN-CORE-MEMORY-L1-1-1.DLL
- API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
- API-MS-WIN-CORE-MEMORY-L1-1-2.DLL
- API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
- API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
- API-MS-WIN-CORE-SYNCH-L1-2-1.DLL
- API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
- API-MS-WIN-CORE-FILE-L1-1-0.DLL

P/I	Ordinal ^	Hint	Function	Entry Point
N/A	20 (0x0014)		CsrAllocateCaptureBuffer	Not Bound
N/A	21 (0x0015)		CsrAllocateMessagePointer	Not Bound
N/A	23 (0x0017)		CsrCaptureMessageMultiUnicodeStringsInPlace	Not Bound
N/A	24 (0x0018)		CsrCaptureMessageString	Not Bound
N/A	26 (0x001A)		CsrClientCallServer	Not Bound
N/A	28 (0x001C)		CsrFreeCaptureBuffer	Not Bound
N/A	32 (0x0020)		CsrVerifyRegion	Not Bound
N/A	34 (0x0022)		DbgPrint	Not Bound
N/A	35 (0x0023)		DbgPrintEx	Not Bound
N/A	45 (0x002D)		DbgUiGetThreadDebugObject	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
N/A	8 (0x0008)		N/A	0x0007F120
0	9 (0x0009)		A_SHAFinal	0x00040230
1	10 (0x000A)		A_SHAInit	0x00041060
2	11 (0x000B)		A_SHAUpdate	0x000410A0
3	12 (0x000C)		AlpcAdjustCompletionListConcurrencyCount	0x000E0600
4	13 (0x000D)		AlpcFreeCompletionListMessage	0x00070630
5	14 (0x000E)		AlpcGetCompletionListLastMessageInformation	0x000E0630
6	15 (0x000F)		AlpcGetCompletionListMessageAttributes	0x000E0650
7	16 (0x0010)		AlpcGetHeaderSize	0x00070360
8	17 (0x0011)		AlpcGetMessageAttribute	0x00070320

Module	File Time Stamp	Link Time Stamp	File Size	Attr	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											

Error: At least one required implicit or forwarded dependency was not found.
Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.

For Help, press F1

Írjon ide a kereséshez

1054
2022. 02. 19.

Az ntdll.dli egy speciális, dinamikusan kapcsolódó könyvtár (Dinamically Linked Library). A Windows NT alapú operációs rendszerekben az ntdll.dll az user mód és a kernel mód közötti kommunikáció lebonyolításához.

A Dependency Walker nevű programmal meglehet nézni, hogy egy adott program futásának milyen függőségei vannak.

