

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Tózsér Zétény Bsc
Programtervező informatikus
QGNLD2

Miskolc, 2022

1. Feladat

a.) Hozza létre a következő mappa szerkezetet!

```
C:\gyak>md neptunkod
C:\gyak>md neptunkod\bokor
C:\gyak>md neptunkod\bokor\banan
C:\gyak>md neptunkod\bokor\mogyoró
C:\gyak>md neptunkod\bokor\barack
C:\gyak>md neptunkod\fa
C:\gyak>md neptunkod\fa\korte
C:\gyak>md neptunkod\land
C:\gyak>md neptunkod\land\szeder
C:\gyak>md neptunkod\land\kokusz
```

b.) Készítsen másolatot:

a *neptunkod/land/szeder* katalógusról a *neptunkod/fa* katalógusba a
neptunkod/bokor/banan katalógusról a *neptunkod/fa* katalógusba

```
C:\Windows\System32\cmd.exe
C:\gyak\neptunkod>xcopy bokor fa /T/E
C:\gyak\neptunkod>xcopy land fa /T/E
C:\gyak\neptunkod>rmdir fa\barack
C:\gyak\neptunkod>rmdir fa\kokusz
C:\gyak\neptunkod>rmdir fa\mogyoró
```

c.) Végezze el a következő áthelyezéseket:

a *neptunkod/bokor/barack* katalógust helyezze át a *neptunkod/fa* katalógusba a
neptunkod/land/kokusz katalógust helyezze át a *neptunkod/fa* katalógusba

```
C:\Windows\System32\cmd.exe
C:\gyak\neptunkod>move bokor\barack fa
1 dir(s) moved.
C:\gyak\neptunkod>move land\kokusz fa
1 dir(s) moved.
```

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

neptunkod/bokor/banan/leiras.txt

neptunkod/fa/felsorolas.txt

```
C:\Windows\System32\cmd.exe
C:\gyak\neptunkod>rmdir /s land
land, Are you sure (Y/N)? Y
C:\gyak\neptunkod>type nul > bokor\banan\leiras.txt
C:\gyak\neptunkod>type nul > fa\felsorolas.txt
```

e.) A *leiras.txt* szöveges állományba írjon 3 sort a barackról.

A *felsorolas* szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
C:\Windows\System32\cmd.exe
C:\gyak\neptunkod>echo finom > bokor\banan\leiras.txt
C:\gyak\neptunkod>echo ledus >> bokor\banan\leiras.txt
C:\gyak\neptunkod>echo erett >> bokor\banan\leiras.txt
C:\gyak\neptunkod>echo Barna Gergo > fa\felsorolas.txt
C:\gyak\neptunkod>echo Alma Aladar >> fa\felsorolas.txt
C:\gyak\neptunkod>echo Zeke Zebulon >> fa\felsorolas.txt
C:\gyak\neptunkod>echo Takacs Tamara >> fa\felsorolas.txt
C:\gyak\neptunkod>echo Csikos Csaba >> fa\felsorolas.txt
```

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

Directory of C:\gyak\neptunkod

2022. 02. 16.	20:22	<DIR>	.
2022. 02. 16.	20:22	<DIR>	..
2022. 02. 16.	20:19	<DIR>	bokor
2022. 02. 16.	20:23	<DIR>	fa
		0 File(s)	0 bytes

Directory of C:\gyak\neptunkod\bokor

2022. 02. 16.	20:19	<DIR>	.
2022. 02. 16.	20:19	<DIR>	..
2022. 02. 16.	20:23	<DIR>	banan
2022. 02. 16.	19:58	<DIR>	mogyoro
		0 File(s)	0 bytes

Directory of C:\gyak\neptunkod\bokor\banan

2022. 02. 16.	20:23	<DIR>	.
2022. 02. 16.	20:23	<DIR>	..
2022. 02. 16.	20:27		24 leiras.txt
		1 File(s)	24 bytes

Directory of C:\gyak\neptunkod\bokor\mogyoro

2022. 02. 16.	19:58	<DIR>	.
2022. 02. 16.	19:58	<DIR>	..
		0 File(s)	0 bytes

Directory of C:\gyak\neptunkod\fa

2022. 02. 16.	20:23	<DIR>	.
2022. 02. 16.	20:23	<DIR>	..
2022. 02. 16.	19:58	<DIR>	banan
2022. 02. 16.	19:58	<DIR>	barack
2022. 02. 16.	20:30		74 felsorolas.txt
2022. 02. 16.	19:59	<DIR>	kokusz
2022. 02. 16.	19:58	<DIR>	korte
2022. 02. 16.	19:59	<DIR>	szeder
		1 File(s)	74 bytes

Directory of C:\gyak\neptunkod\fa\banan

2022. 02. 16.	19:58	<DIR>	.
2022. 02. 16.	19:58	<DIR>	..
		0 File(s)	0 bytes

Directory of C:\gyak\neptunkod\fa\barack

2022. 02. 16.	19:58	<DIR>	.
2022. 02. 16.	19:58	<DIR>	..
		0 File(s)	0 bytes

Directory of C:\gyak\neptunkod\fa\kokusz

2022. 02. 16.	19:59	<DIR>	.
2022. 02. 16.	19:59	<DIR>	..
		0 File(s)	0 bytes

Directory of C:\gyak\neptunkod\fa\korte

2022. 02. 16.	19:58	<DIR>	.
2022. 02. 16.	19:58	<DIR>	..
		0 File(s)	0 bytes

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

```
C:\Windows\System32\cmd.exe

C:\gyak\neptunkod>dir ?e* /s
Volume in drive C has no label.
Volume Serial Number is 963F-37EB

Directory of C:\gyak\neptunkod\bokor\banan

2022. 02. 16.  20:27                24 leiras.txt
                1 File(s)                24 bytes

Directory of C:\gyak\neptunkod\fa

2022. 02. 16.  20:30                74 felsorolas.txt
                1 File(s)                74 bytes

Total Files Listed:
                2 File(s)                98 bytes
                0 Dir(s)  11 176 267 776 bytes free
```

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

```
C:\gyak\neptunkod>icacls felsorolas.txt /grant everyone:(R)
```

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

```
Total Files Listed:
                2 File(s)                98 bytes
                29 Dir(s)  10 975 338 496 bytes free
```

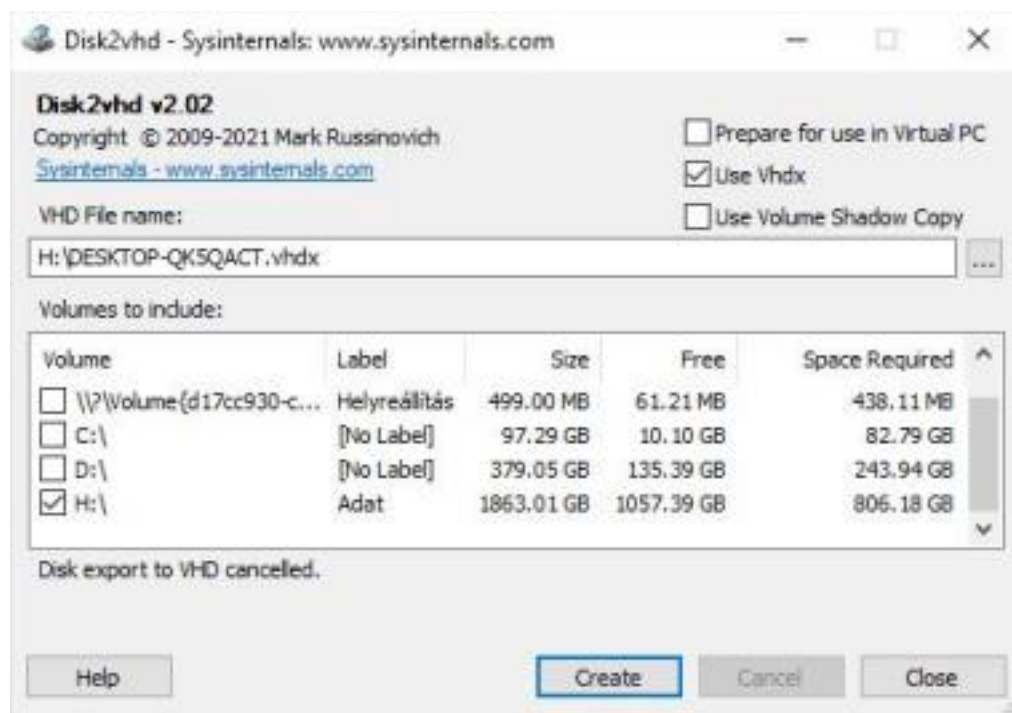
j.) Rendezze ABC-szerint a *felsorolas.txt* file tartalmát.

```
C:\gyak\neptunkod>sort fa\felsorolas.txt
Alma Aladar
Barna Gergo
Csikos Csaba
Takacs Tamara
Zeke Zebulon
```

2. Feladat

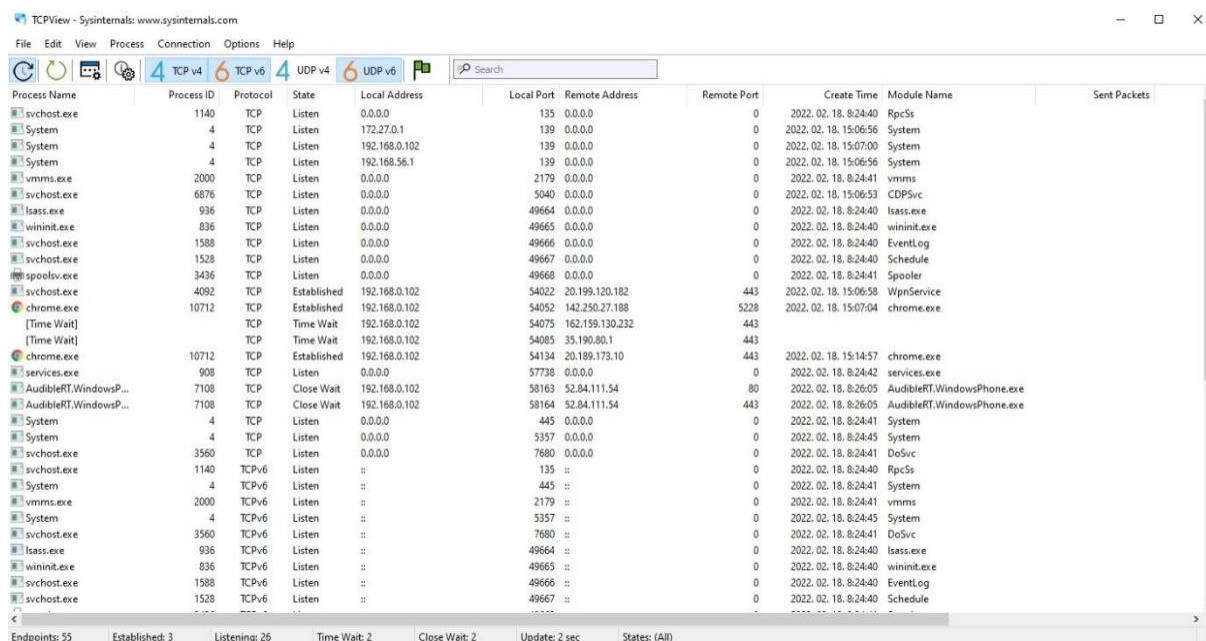
a) File and Disk Utilities (Disk2vhd)

A Disk2vhd fizikai merevlemezekből virtuális merevlemezeket hoz létre, virtuális számítógépekhez való használatra. Minden kijelölt lemezen létrehoz egy vhd-t. Megfelelő virtuális géppel lehet használni a vhd-kat.



b) Networking Utilities (TCPView)

A TCPView felsorolja az összes TCP és UDP végpontot. Felbontja az IP címeket a tartománynév verziójukra.



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

Megmutatja a jelenleg aktív folyamatok listáját, beleértve a saját fiókjaik nevét. Leíró módban a felső ablakban kiválasztott folyamat leírói jelennek meg; DLL módban látni fogja a folyamat által betöltött DLL-eket és memória leképezett fájlokat.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	188 K	40 536 K	88		
Registry		11 460 K	94 752 K	156		
System Idle Process	96.73	60 K	8 K	0		
System	0.12	200 K	144 K	4		
Interrupts	0.12	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 088 K	1 072 K	584		
Memory Compression		776 K	119 236 K	2468		
csrss.exe		1 836 K	4 580 K	748		
wininit.exe		1 412 K	6 196 K	836		
services.exe		5 916 K	10 312 K	908		
svchost.exe		11 980 K	28 496 K	700	Windows-szolgáltatások gaz...	Microsoft Corporation
SettingSyncHost.exe		5 228 K	5 908 K	648	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperience...		77 356 K	73 032 K	8280		
RuntimeBroker.exe		6 696 K	24 328 K	8512	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		7 196 K	27 488 K	9104	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	83 720 K	43 152 K	10088		Microsoft Corporation
RuntimeBroker.exe		3 236 K	20 108 K	7672	Runtime Broker	Microsoft Corporation
TextInputHost.exe		62 576 K	46 276 K	9872		Microsoft Corporation
AudibleRT.WindowsP...	Susp...	72 368 K	21 416 K	7108	AudibleRT.WindowsPhone	
RuntimeBroker.exe		12 292 K	23 300 K	4784	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		13 924 K	33 716 K	5560	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		2 132 K	9 484 K	5852	User OOBEBroker	Microsoft Corporation
dllhost.exe		3 340 K	11 504 K	9080	COM Surrogate	Microsoft Corporation
ShellExperienceHost...		73 900 K	87 716 K	5832	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		8 244 K	27 016 K	9404	Runtime Broker	Microsoft Corporation
YourPhoneServer.exe	< 0.01	66 680 K	76 156 K	3412		
LockApp.exe	Susp...	64 220 K	58 056 K	2664	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		9 244 K	33 076 K	10336	Runtime Broker	Microsoft Corporation
WmiPriv SE.exe		2 932 K	9 500 K	10976		

CPU Usage: 2.25% Commit Charge: 46.50% Processes: 168 Physical Usage: 35.43%

A folyamatfigyelő egy fejlett, valós idejű megfigyelési eszköz. Több korábbi program funkcióit örökölte és fejlesztette.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time Process Name PID Operation Path Result Detail

20:52:...	lsass.exe	936	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 607 168, ...
20:52:...	NVDisplay.Cont...	2876	ReadFile	C:\Windows\System32\DriverStore\File...	SUCCESS	Offset: 7 168 000, ...
20:52:...	NVDisplay.Cont...	2876	Thread Exit		SUCCESS	Thread ID: 11700, ...
20:52:...	Explorer.EXE	6848	ReadFile	C:\Program Files\Classic Shell\ClassicSt...	SUCCESS	Offset: 1 683 968, ...
20:52:...	lsass.exe	936	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 590 784, ...
20:52:...	lsass.exe	936	Thread Create		SUCCESS	Thread ID: 8180
20:52:...	NVDisplay.Cont...	2876	ReadFile	C:\Windows\System32\DriverStore\File...	SUCCESS	Offset: 8 807 936, ...
20:52:...	MsMpEng.exe	4072	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15 175 680, ...
20:52:...	Explorer.EXE	6848	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 212 480, Le...
20:52:...	lsass.exe	936	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 505 280, ...
20:52:...	Explorer.EXE	6848	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 193 536, Le...
20:52:...	NVDisplay.Cont...	2876	ReadFile	C:\Windows\System32\DriverStore\File...	SUCCESS	Offset: 7 110 656, ...
20:52:...	Explorer.EXE	6848	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
20:52:...	Explorer.EXE	6848	RegCloseKey	HKCU	SUCCESS	
20:52:...	NVDisplay.Cont...	2876	ReadFile	C:\Windows\System32\DriverStore\File...	SUCCESS	Offset: 7 806 976, ...
20:52:...	Explorer.EXE	6848	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
20:52:...	Explorer.EXE	6848	RegCloseKey	HKCU	SUCCESS	
20:52:...	Explorer.EXE	6848	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
20:52:...	Explorer.EXE	6848	RegCloseKey	HKCU	SUCCESS	
20:52:...	Explorer.EXE	6848	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
20:52:...	Explorer.EXE	6848	RegCloseKey	HKCU	SUCCESS	

Showing 103 319 of 364 002 events (28%) Backed by virtual memory

Az Autoruns megmutatja, hogy mely programok vannak rendszerindításkor futásra állítva. Egyszerűen csak futtassa az Autoruns-t, hogy lássa a jelenleg auto-indításra állított programokat.

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

Known DLLs				
WinLogon				
Winsock Providers				
Print Monitors				
LSA Providers				
Network Providers				
WMI				
Office				
Everything				
Logon				
Explorer				
Internet Explorer				
Scheduled Tasks				
Services				
Drivers				
Codecs				
Boot Execute				
Image Hijacks				
Appinit				
Description				
Publisher				
Image Path				
Timestamp				
Autostart Entry				
Logon				
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
GalaxyClient				
OneDrive				
Classic Start Menu				
cmd.exe				
Google Chrome				
Microsoft Edge				
Java Update Scheduler				
XboxStat				

d) Security Utilities (LogonSession)

Az összes aktív logon session-t megjeleníti. Több opcióval lehet futtatni, például „-c”-vel CSV-ként írja ki a kimenetet.


```

Administrator: C:\Windows\System32\cmd.exe
C:\Users\user\Downloads\logonSessions (1)>logonsessions64.exe

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name:      WORKGROUP\DESKTOP-QK5QACT$
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            S-1-5-18
    Logon time:     2022. 02. 18. 8:24:40
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000dd89:
    User name:
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            (none)
    Logon time:     2022. 02. 18. 8:24:40
    Logon server:
    DNS Domain:
    UPN:

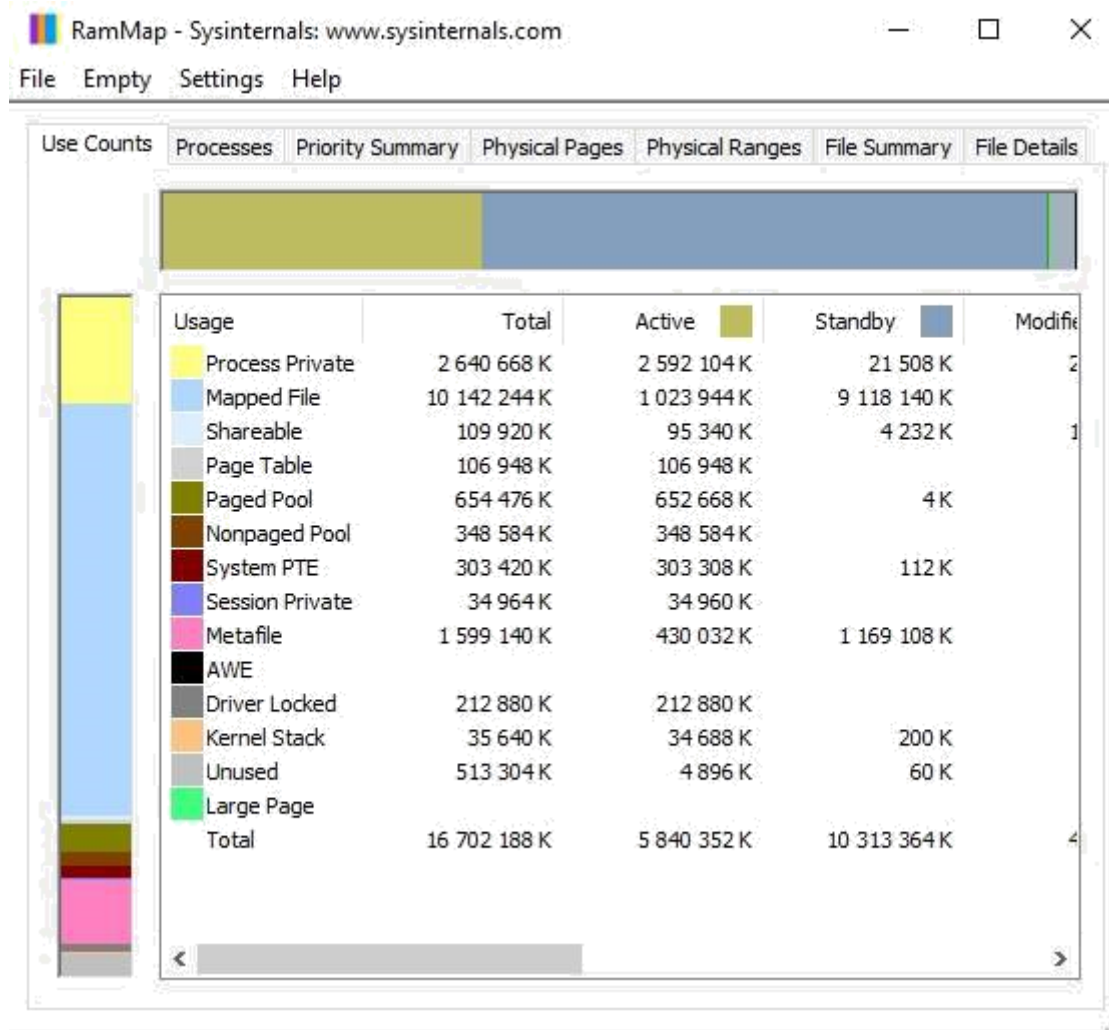
[2] Logon session 00000000:0000e5ad:
    User name:      Font Driver Host\UMFD-0
    Auth package:   Negotiate
    Logon type:     Interactive
    Session:        0
    Sid:            S-1-5-96-0-0
    Logon time:     2022. 02. 18. 8:24:40
    Logon server:
    DNS Domain:
    UPN:

```

e) Information Utilities (RAMMap)

A RAMMap egy fizikai memóriahasználat-elemzési segédprogram.

Több módon mutatja be a használati adatokat. Például típus és lapozási lista szerint, vagy fizikai memóriacím szerint.



3. Feladat

A Dependency Walker egy hierarchikus fa diagramot készít egy Windows modul összes függő modulról. Általános vizsgálatra és hibakeresésre is használható.

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

Windows Core memória kezelő hívásokat használ.

Dependency Walker - [neptunkod.exe]

File Edit View Options Profile Window Help

Kernel32.dll

PI	Ordinal	Hint	Function	Entry Point
N/A		269 (0x010D)	DeleteCriticalSection	Not Bound
N/A		305 (0x0131)	EnterCriticalSection	Not Bound
N/A		536 (0x0218)	GetCurrentProcess	Not Bound
N/A		537 (0x0219)	GetCurrentProcessId	Not Bound
N/A		541 (0x021D)	GetCurrentThreadId	Not Bound
N/A		610 (0x0262)	GetLastError	Not Bound
N/A		722 (0x02D2)	GetStartupInfoA	Not Bound
N/A		747 (0x02EB)	GetSystemTimeAsFileTime	Not Bound

E	Ordinal	Hint	Function	Entry Point
1 (0x0001)	0 (0x0000)		AcquireSRWLockExclusive	NTDLL.RtlAcquireSi
2 (0x0002)	1 (0x0001)		AcquireSRWLockShared	NTDLL.RtlAcquireSi
3 (0x0003)	2 (0x0002)		ActivateActCtx	0x00020080
4 (0x0004)	3 (0x0003)		ActivateActCtxWorker	0x0001B700
5 (0x0005)	4 (0x0004)		AddAtomA	0x0005A140
6 (0x0006)	5 (0x0005)		AddAtomW	0x000128F0
7 (0x0007)	6 (0x0006)		AddConsoleAliasA	0x00025640

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum
ACTIVEDS.DLL	2021/01/17 20:07	2037/08/17 15:05	274 432	A	0x00052A6C	0x00052A6C
ADSLDPC.DLL	2021/06/11 7:09	2102/03/08 5:59	258 560	A	0x0004D816	0x0004D816
ADVAPI32.DLL	2019/12/07 10:08	2016/07/16 12:22	151 552	A	0x00033A66	0x00033A66
AEPIC.DLL	2021/09/17 18:42	1970/10/25 11:49	598 344	A	0x00095815	0x00095815
API-MS-WIN-CORE-LIBRARYLOADER-L1-1-0.DLL	2019/03/18 18:50	2022/12/28 9:34	12 736	A	0x00006056	0x00006056
API-MS-WIN-CRT-CONVERT-L1-1-0.DLL	2019/03/18 18:50	2054/10/31 18:01	15 816	A	0x00013587	0x00013587
API-MS-WIN-CRT-ENVIRONMENT-L1-1-0.DLL	2019/03/18 18:50	2100/12/14 6:45	12 232	A	0x00007F10	0x00007F10
API-MS-WIN-CRT-FILESYSTEM-L1-1-0.DLL	2019/03/18 18:50	2034/02/06 6:26	13 768	A	0x000128EA	0x000128EA
API-MS-WIN-CRT-HEAP-L1-1-0.DLL	2019/03/18 18:50	2091/07/08 14:26	12 744	A	0x0001284A	0x0001284A

Error: At least one required implicit or forwarded dependency was not found.
Error: A circular dependency was detected.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

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

Az NTDLL.DLL tartalmazza az NT kernel funkciókat. Exportálja a Native Windows API-t.

Dependency Walker - [neptunkod.exe]

File Edit View Options Profile Window Help

NEPTUNKOD.EXE

PI	Ordinal	Hint	Function	Entry Point
N/A		484 (0x01E4)	NtQueryInstallUILanguage	Not Bou
N/A		488 (0x01E8)	NtQueryLicenseValue	Not Bou
N/A		497 (0x01F1)	NtQuerySection	Not Bou
N/A		499 (0x01F3)	NtQuerySecurityObject	Not Bou
N/A		504 (0x01F8)	NtQuerySystemEnvironmentValueEx	Not Bou
N/A		505 (0x01F9)	NtQuerySystemInformation	Not Bou
N/A		509 (0x01FD)	NtQueryTimerResolution	Not Bou

E	Ordinal	Hint	Function	Entry Point
212 (0x00D4)	203 (0x00CB)		NtAddDriverEntry	0x0009
213 (0x00D5)	204 (0x00CC)		NtAdjustGroupsToken	0x0009
214 (0x00D6)	205 (0x00CD)		NtAdjustPrivilegesToken	0x0009
215 (0x00D7)	206 (0x00CE)		NtAdjustTokenClaimsAndDeviceGroups	0x0009
216 (0x00D8)	207 (0x00CF)		NtAlertResumeThread	0x0009
217 (0x00D9)	208 (0x00D0)		NtAlertThread	0x0009
218 (0x00DA)	209 (0x00D1)		NtAlertThreadByThreadId	0x0009

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum
CLDAPI.DLL	2021/10/16 9:28	2024/04/20 10:58	118 784	A	0x00020E09	0x00020E09
COMBASE.DLL	2021/11/13 19:20	2069/05/21 11:32	3 507 496	A	0x0035FAFA	0x0035FAFA
COMCTL32.DLL	2021/07/09 13:18	2003/01/03 17:27	702 792	A	0x000B6A20	0x000B6A20
COMCTI32.DLL	2021/07/09 13:18	2006/07/09 6:23	2 710 352	A	0x0029FA3C	0x0029FA3C

Error: At least one required implicit or forwarded dependency was not found.
Error: A circular dependency was detected.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1