

# **Operációs rendszerek BSc**

2. gyak.

2022. 02. 16.

**Készítette:**

Takács Bálint Bsc

Programtervező informatikus

P2GNFT

**Miskolc, 2022**

1.

a.) Hozza létre a következő mappa szerkezetet!

```
Parancssor
VOL          Displays a disk volume label and serial number.
XCOPY        Copies files and directory trees.
WMIC         Displays WMI information inside interactive command shell.

For more information on tools see the command-line reference in the online help.

C:\Users\takacs\Bálint>cd C:\Users\takacs\Bálint\Desktop
C:\Users\takacs\Bálint\Desktop>mkdir P2GNFT
C:\Users\takacs\Bálint\Desktop>cd C:\Users\takacs\Bálint\Desktop\P2GNFT
C:\Users\takacs\Bálint\Desktop\P2GNFT>mkdir bokor
C:\Users\takacs\Bálint\Desktop\P2GNFT>mkdir fa
C:\Users\takacs\Bálint\Desktop\P2GNFT>mkdir land
C:\Users\takacs\Bálint\Desktop\P2GNFT>cd C:\Users\takacs\Bálint\Desktop\P2GNFT\bokor
C:\Users\takacs\Bálint\Desktop\P2GNFT\bokor>mkdir banan
C:\Users\takacs\Bálint\Desktop\P2GNFT\bokor>mkdir mogoró
C:\Users\takacs\Bálint\Desktop\P2GNFT\bokor>mkdir barack
C:\Users\takacs\Bálint\Desktop\P2GNFT\bokor>cd C:\Users\takacs\Bálint\Desktop\P2GNFT\fa
C:\Users\takacs\Bálint\Desktop\P2GNFT\fa>mkdir korte
C:\Users\takacs\Bálint\Desktop\P2GNFT\fa>cd C:\Users\takacs\Bálint\Desktop\P2GNFT\land
C:\Users\takacs\Bálint\Desktop\P2GNFT\land>mkdir szeder
C:\Users\takacs\Bálint\Desktop\P2GNFT\land>mkdir kokusz
C:\Users\takacs\Bálint\Desktop\P2GNFT\land>
```

b.) Készítsen másolatot!

```
C:\Users\takacs\Bálint\Desktop\P2GNFT\fa>xcopy "C:\Users\takacs\Bálint\Desktop\P2GNFT\land\szeder" "C:\Users\takacs\Bálint\Desktop\P2GNFT\fa" /T /E
C:\Users\takacs\Bálint\Desktop\P2GNFT\fa>xcopy "C:\Users\takacs\Bálint\Desktop\P2GNFT\bokor\banan" "C:\Users\takacs\Bálint\Desktop\P2GNFT\fa" /T /E
```

c.) Végezze el a következő áthelyezéseket!

```
C:\Users\takacs\Bálint\Desktop\P2GNFT\fa>cd C:\Users\takacs\Bálint\Desktop\P2GNFT
C:\Users\takacs\Bálint\Desktop\P2GNFT>move bokor\barack fa
1 dir(s) moved.
C:\Users\takacs\Bálint\Desktop\P2GNFT>move land\kokusz fa
1 dir(s) moved.
```

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

```
C:\Users\takacs\Bálint\Desktop\P2GNFT>rmdir land\szeder
C:\Users\takacs\Bálint\Desktop\P2GNFT>rmdir land
'rmdir land' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\takacs\Bálint\Desktop\P2GNFT>rmdir land
```

```
C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\banan>type nul>leiras.txt
C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\banan>cd C:\Users\Takács Bálint\Desktop\P2GNFT\fa
C:\Users\Takács Bálint\Desktop\P2GNFT\fa>type nul>felsorolas.txt
```

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

```
C:\Users\Takács Bálint\Desktop\P2GNFT\fa>cd C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\banan
C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\banan>echo "A banán a trópusokon elterjedt és termesztett egzotikus, lágy szárú, bár gyakran fatermetű növények n
emzetsége a banánfélék (Musaceae) róluk elnevezett családjában. A világ legmagasabb egzotikus, lágy szárú növénye. " > leiras.txt
C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\banan>cd C:\Users\Takács Bálint\Desktop\P2GNFT\fa
C:\Users\Takács Bálint\Desktop\P2GNFT\fa>echo "Alma, Meggy, Dió, Cseresznye, Szilva" > felsorolas.txt
```

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

```
C:\Users\Takács Bálint\Desktop\P2GNFT\fa>cd C:\Users\Takács Bálint\Desktop\P2GNFT
C:\Users\Takács Bálint\Desktop\P2GNFT>tree
Folder PATH listing
Volume serial number is FEC5-2BD9
C:
├── bokor
│   ├── banan
│   └── mogyoro
└── fa
    ├── barack
    ├── kokusz
    └── korte
```

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

```
C:\Users\Takács Bálint\Desktop\P2GNFT>dir ?e*.txt /s /p
Volume in drive C has no label.
Volume Serial Number is FEC5-2BD9

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\banan
2022. 02. 16. 13:21                219 leiras.txt
                  1 File(s)          219 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\fa
2022. 02. 16. 13:23                41 felsorolas.txt
                  1 File(s)          41 bytes

Total Files Listed:
                2 File(s)          260 bytes
                0 Dir(s)  66 666 946 560 bytes free
```

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

```
C:\Users\Takács Bálint\Desktop\P2GNFT>cd fa  
C:\Users\Takács Bálint\Desktop\P2GNFT\fa> attrib -h felsorolas.txt  
C:\Users\Takács Bálint\Desktop\P2GNFT\fa>
```

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

```
C:\Users\Takács Bálint\Desktop\P2GNFT>dir /s
Volume in drive C has no label.
Volume Serial Number is FEC5-2BD9

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT

2022. 02. 16. 13:11 <DIR>      .
2022. 02. 16. 13:11 <DIR>      ..
2022. 02. 16. 13:05 <DIR>      bokor
2022. 02. 16. 13:19 <DIR>      fa
                0 File(s)      0 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\bokor

2022. 02. 16. 13:05 <DIR>      .
2022. 02. 16. 13:05 <DIR>      ..
2022. 02. 16. 13:17 <DIR>      banan
2022. 02. 16. 12:29 <DIR>      mogyoro
                0 File(s)      0 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\banan

2022. 02. 16. 13:17 <DIR>      .
2022. 02. 16. 13:17 <DIR>      ..
2022. 02. 16. 13:21      219 leiras.txt
                1 File(s)      219 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\bokor\mogyoro

2022. 02. 16. 12:29 <DIR>      .
2022. 02. 16. 12:29 <DIR>      ..
                0 File(s)      0 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\fa

2022. 02. 16. 13:19 <DIR>      .
2022. 02. 16. 13:19 <DIR>      ..
2022. 02. 16. 12:29 <DIR>      barack
2022. 02. 16. 13:23      41 felsorolas.txt
2022. 02. 16. 12:31 <DIR>      kokusz
2022. 02. 16. 12:29 <DIR>      korte
                1 File(s)      41 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\fa\barack

2022. 02. 16. 12:29 <DIR>      .
2022. 02. 16. 12:29 <DIR>      ..
                0 File(s)      0 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\fa\kokusz

2022. 02. 16. 12:31 <DIR>      .
2022. 02. 16. 12:31 <DIR>      ..
                0 File(s)      0 bytes

Directory of C:\Users\Takács Bálint\Desktop\P2GNFT\fa\korte

2022. 02. 16. 12:29 <DIR>      .
2022. 02. 16. 12:29 <DIR>      ..
                0 File(s)      0 bytes

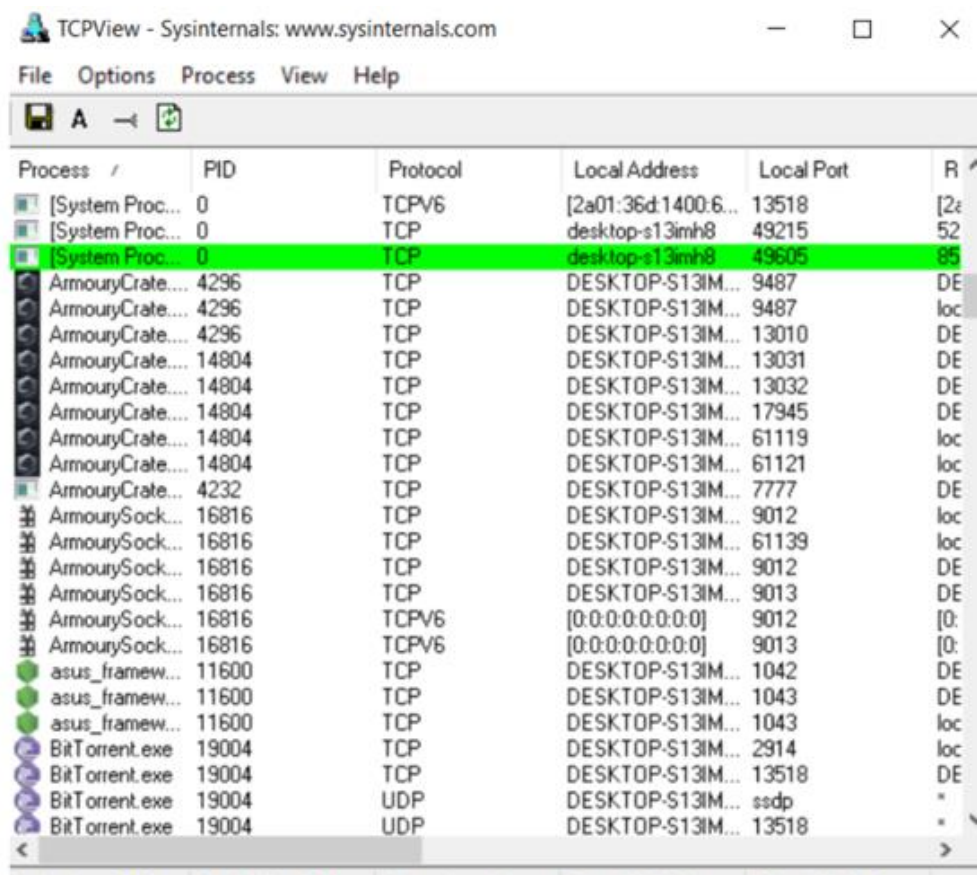
Total Files Listed:
        2 File(s)      260 bytes
       23 Dir(s)  66 408 759 296 bytes free
```

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

```
C:\Users\Takács Bálint\Desktop\P2GNFT>cd fa  
  
C:\Users\Takács Bálint\Desktop\P2GNFT\fa>sort felsorolas.txt  
"Alma, Meggy, Dió, Cseresznye, Szilva"
```

2. A felsorolt eszközök közül minden eszköz esetén töltse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét - majd mentse el a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

TCPView:



The screenshot shows the TCPView application window from Sysinternals. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. The main window displays a table of network connections. The table has columns for 'Process /', 'PID', 'Protocol', 'Local Address', 'Local Port', and 'R'. The third row is highlighted in green, showing a connection for '[System Proc...]' with PID 0, using TCP protocol, local address 'desktop-s13imh8', local port 49605, and state '85'. Below this, several 'ArmouryCrate...' processes are listed with various TCP connections to 'DESKTOP-S13IM...'. At the bottom, 'BitTorrent.exe' is shown with multiple connections, including one to 'ssdp'.

Process /	PID	Protocol	Local Address	Local Port	R
[System Proc...]	0	TCPV6	[2a01:36d:1400:6...	13518	[2e
[System Proc...]	0	TCP	desktop-s13imh8	49215	52
[System Proc...]	0	TCP	desktop-s13imh8	49605	85
ArmouryCrate...	4296	TCP	DESKTOP-S13IM...	9487	DE
ArmouryCrate...	4296	TCP	DESKTOP-S13IM...	9487	loc
ArmouryCrate...	4296	TCP	DESKTOP-S13IM...	13010	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	13031	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	13032	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	17945	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	61119	loc
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	61121	loc
ArmouryCrate...	4232	TCP	DESKTOP-S13IM...	7777	DE
ArmourySock...	16816	TCP	DESKTOP-S13IM...	9012	loc
ArmourySock...	16816	TCP	DESKTOP-S13IM...	61139	loc
ArmourySock...	16816	TCP	DESKTOP-S13IM...	9012	DE
ArmourySock...	16816	TCP	DESKTOP-S13IM...	9013	DE
ArmourySock...	16816	TCPV6	[0:0:0:0:0:0:0:0]	9012	[0:
ArmourySock...	16816	TCPV6	[0:0:0:0:0:0:0:0]	9013	[0:
asus_framew...	11600	TCP	DESKTOP-S13IM...	1042	DE
asus_framew...	11600	TCP	DESKTOP-S13IM...	1043	DE
asus_framew...	11600	TCP	DESKTOP-S13IM...	1043	loc
BitTorrent.exe	19004	TCP	DESKTOP-S13IM...	2914	loc
BitTorrent.exe	19004	TCP	DESKTOP-S13IM...	13518	DE
BitTorrent.exe	19004	UDP	DESKTOP-S13IM...	ssdp	*
BitTorrent.exe	19004	UDP	DESKTOP-S13IM...	13518	*

A TCP View segédprogramon keresztül a számítógépen jelenleg futó hálózati aktivitásokat láthatom.

Process Explorer:

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-S13IMH8\Takács Bálint]

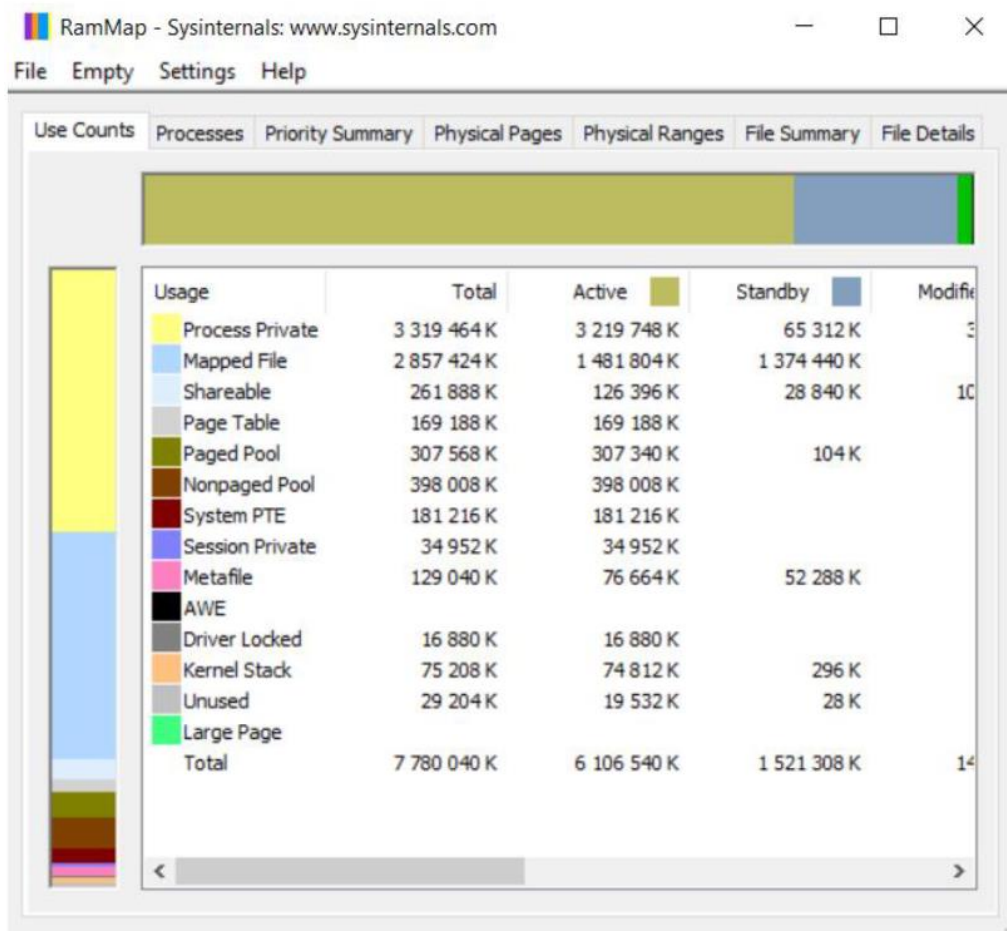
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		10 728 K	39 912 K	172		
System Idle Process	95.22	60 K	8 K	0		
System	0.49	208 K	6 524 K	4		
Interrupts	0.24	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 072 K	1 016 K	604		
Memory Compression	< 0.01	720 K	96 936 K	2900		
csrss.exe	< 0.01	2 148 K	5 632 K	1016		
wininit.exe		1 588 K	6 640 K	1556		
services.exe	0.02	6 160 K	10 528 K	1680		
svchost.exe	0.08	15 220 K	34 248 K	1812	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPvSE.exe		3 968 K	10 704 K	7456		
MoUsocoreWorker.exe		41 420 K	51 484 K	17592		
StartMenuExperienceHost.exe		29 916 K	68 908 K	8428		
RuntimeBroker.exe		6 436 K	26 516 K	10440	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	87 688 K	87 236 K	16748	Search application	Microsoft Corporation
RuntimeBroker.exe		5 824 K	24 240 K	5332	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	27 348 K	12 500 K	15692	YourPhone	Microsoft Corporation
SettingSyncHost.exe		5 936 K	10 932 K	3488	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	15 816 K	43 288 K	5228	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		4 720 K	21 860 K	17136	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		9 800 K	35 288 K	1144	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 740 K	14 824 K	13732	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	14 876 K	42 872 K	11992	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2 940 K	18 148 K	17956	Runtime Broker	Microsoft Corporation
Cortana.exe	Susp...	30 112 K	56 000 K	1004	Cortana	Microsoft Corporation
RuntimeBroker.exe		4 648 K	24 852 K	19648	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 144 K	10 348 K	10592	Runtime Broker	Microsoft Corporation
dilhost.exe		1 520 K	7 452 K	7004	COM Surrogate	Microsoft Corporation
SystemSettings.exe	Susp...	24 472 K	9 652 K	6672	Gépház	Microsoft Corporation
ApplicationFrameHost.exe	< 0.01	8 944 K	28 532 K	16820	Application Frame Host	Microsoft Corporation

CPU Usage: 4.78% Commit Charge: 52.93% Processes: 256 Physical Usage: 80.33%

A Process Explorerben láthatjuk, hogy jelenleg milyen műveletek futnak a számítógépen.

RamMap:



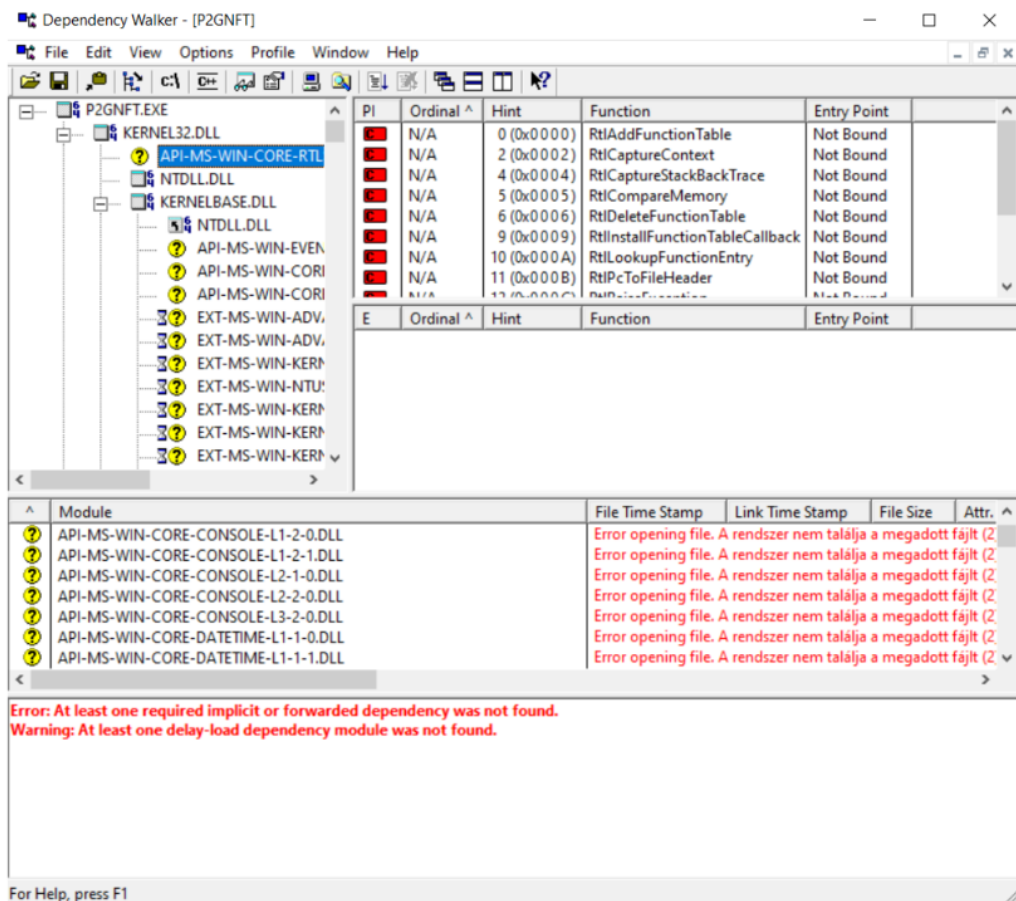
A RamMap –ban a számítógépben található memória felhasználását követhetjük nyomon.

**3.** Készítsen egy neptunkod.c nevű forráskódot, amely egy vezeteknev.txt fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc. Fordítsa le kódot a C fordító, majd tegye futtathatóvá az állományt: neptunkod.exe

A Dependency Walker segítségével végezze el a következő feladatokat.

- a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből





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

Dependency Walker - [P2GNFT]

File Edit View Options Profile Window Help

Kernel32.dll API-MS-WIN-CORE-RTL NTDLL.dll KERNELBASE.dll NTDLL.dll API-MS-WIN-EVEN API-MS-WIN-COR API-MS-WIN-COR API-MS-WIN-ADV API-MS-WIN-ADV API-MS-WIN-KER API-MS-WIN-KER API-MS-WIN-KER API-MS-WIN-KER API-MS-WIN-KER

PI	Ordinal ^	Hint	Function
N/A		20 (0x0014)	CsrAllocateCaptureBuffer
N/A		21 (0x0015)	CsrAllocateMessagePointer
N/A		23 (0x0017)	CsrCaptureMessageMultiUnicodeStringsInPlace
N/A		24 (0x0018)	CsrCaptureMessageString
N/A		26 (0x001A)	CsrClientCallServer
N/A		28 (0x001C)	CsrFreeCaptureBuffer
N/A		32 (0x0020)	CsrVerifyRegion

E	Ordinal ^	Hint	Function
N/A			N/A
8 (0x0008)		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

Module	File Time Stamp	Link Time Stamp	File Size	Attr.
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)
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL				Error opening file. A rendszer nem találja a megadott fájlt (2)
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL				Error opening file. A rendszer nem találja a megadott fájlt (2)
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL				Error opening file. A rendszer nem találja a megadott fájlt (2)
API-MS-WIN-CORE-DATETIME-L1-1-1.DLL				Error opening file. A rendszer nem találja a megadott fájlt (2)

Error: At least one required implicit or forwarded dependency was not found.  
Warning: At least one delay-load dependency module was not found.

For Help, press F1