

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Sziráczki Soma

Bsc

Programtervező

informatikus

BK6QE8

Miskolc, 2022

1.feladat

a) Hozza létre a következő mappa szerkezetet!

Megvalósítás:

```
c:\>tree BK6QE8
Folder PATH listing
Volume serial number is 0000006F 543B:62AB
C:\BK6QE8
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
├── land
│   ├── kokusz
│   └── szeder
```

b) Készítsen másolatot:

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

Megvalósítás:

```
c:\BK6QE8>tree fa
Folder PATH listing
Volume serial number is 00000021 543B:62AB
C:\BK6QE8\FA
├── banan
├── korte
└── szeder
```

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

Megvalósítás:

```

c:\BK6QE8>move C:\BK6QE8\bokor\barack C:\BK6QE8\fa
1 dir(s) moved.

c:\BK6QE8>move C:\BK6QE8\land\kokusz C:\BK6QE8\fa
1 dir(s) moved.

c:\BK6QE8>tree fa
Folder PATH listing
Volume serial number is 000000A7 543B:62AB
C:\BK6QE8\FA
|
|___banan
|___barack
|___kokusz
|___korte
|___szeder

```

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

- neptunkod/bokor/banan/ leiras.txt
- neptunkod/tree/felsorolas.txt

Megvalósítás:

```

c:\BK6QE8>rmdir /s land
land, Are you sure (Y/N)? y

c:\BK6QE8>cd c:\

c:\>tree BK6QE8
Folder PATH listing
Volume serial number is 00000030 543B:62AB
C:\BK6QE8
|
|___bokor
|   |___banan
|   |___mogyoro
|___fa
|   |___banan
|   |___barack
|   |___kokusz
|   |___korte
|   |___szeder

```

```

c:\>cd C:\BK6QE8\bokor\banan
C:\BK6QE8\bokor\banan>type nul > leiras.txt
C:\BK6QE8\bokor\banan>cd C:\BK6QE8\fa
C:\BK6QE8\fa>type nul > felsorolas.txt
C:\BK6QE8\fa>cd c:\

c:\>tree BK6QE8 /f
Folder PATH listing
Volume serial number is 00000096 543B:62AB
C:\BK6QE8
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   └── mogyoro
└── fa
    ├── felsorolas.txt
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

```

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

Megvalósítás:

```

C:\BK6QE8\bokor\banan>echo A barack ledus gyumolcs. >leiras.txt
C:\BK6QE8\bokor\banan>echo Nepszeru fajtai peldaul az oszibarack es a kajszibarack. >> leiras.txt
C:\BK6QE8\bokor\banan>echo A fa akar 8m magasra is megnohet. >> leiras.txt
C:\BK6QE8\bokor\banan>sort leiras.txt
A fa akar 8m magasra is megnohet.
A barack ledus gyumolcs.
Nepszeru fajtai peldaul az oszibarack es a kajszibarack.

```

```

C:\BK6QE8\fa>echo CsonkaPatrik, HajduAdrian, SzaboAlen, OnodiBence, BerkiViktor >felsorolas.txt
C:\BK6QE8\fa>sort felsorolas.txt
CsonkaPatrik, HajduAdrian, SzaboAlen, OnodiBence, BerkiViktor

```

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

Megvalósítás:

```

C:\>tree BK6QE8 /f
Folder PATH listing
Volume serial number is 00000053 543B:62AB
C:\BK6QE8
|
+-- bokor
|   |
|   +-- banan
|       leiras.txt
|   |
|   +-- mogyoro
|
+-- fa
    felsorolas.txt
    |
    +-- banan
    +-- barack
    +-- kokusz
    +-- korte
    +-- szeder

```

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

Megvalósítás:

```

C:\BK6QE8>dir /s *e*
Volume in drive C has no label.
Volume Serial Number is 543B-62AB

Directory of C:\BK6QE8\bokor\banan

2022. 02. 20.  20:42                123 leiras.txt
                1 File(s)              123 bytes

Directory of C:\BK6QE8\fa

2022. 02. 20.  20:49                64 felsorolas.txt
2022. 02. 20.  18:47    <DIR>         korte
2022. 02. 20.  18:47    <DIR>         szeder
                1 File(s)              64 bytes

```

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

Megvalósítás:

```

C:\BK6QE8>cd fa

C:\BK6QE8\fa>attrib
A                  C:\BK6QE8\fa\felsorolas.txt

C:\BK6QE8\fa>attrib +r felsorolas.txt

C:\BK6QE8\fa>attrib
A      R          C:\BK6QE8\fa\felsorolas.txt

```

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

Megvalósítás:

```
C:\BK6QE8>dir /S
Volume in drive C has no label.
Volume Serial Number is 543B-62AB

Directory of C:\BK6QE8

2022. 02. 20.  19:51    <DIR>        .
2022. 02. 20.  19:51    <DIR>        ..
2022. 02. 20.  19:47    <DIR>        bokor
2022. 02. 20.  19:57    <DIR>        fa
                0 File(s)                0 bytes

Directory of C:\BK6QE8\bokor

2022. 02. 20.  19:47    <DIR>        .
2022. 02. 20.  19:47    <DIR>        ..
2022. 02. 20.  19:56    <DIR>        banan
2022. 02. 20.  18:46    <DIR>        mogyoro
                0 File(s)                0 bytes

Directory of C:\BK6QE8\bokor\banan

2022. 02. 20.  19:56    <DIR>        .
2022. 02. 20.  19:56    <DIR>        ..
2022. 02. 20.  20:42    <FILE>        123 leiras.txt
                1 File(s)                123 bytes

Directory of C:\BK6QE8\bokor\mogyoro

2022. 02. 20.  18:46    <DIR>        .
2022. 02. 20.  18:46    <DIR>        ..
                0 File(s)                0 bytes

Directory of C:\BK6QE8\fa

2022. 02. 20.  19:57    <DIR>        .
2022. 02. 20.  19:57    <DIR>        ..
2022. 02. 20.  18:46    <DIR>        banan
2022. 02. 20.  18:46    <DIR>        barack
2022. 02. 20.  20:49    <FILE>        64 felsorolas.txt
2022. 02. 20.  18:47    <DIR>        kokusz
2022. 02. 20.  18:47    <DIR>        korte
2022. 02. 20.  18:47    <DIR>        szeder
                1 File(s)                64 bytes
```

```

Directory of C:\BK6QE8\fa\banan
2022. 02. 20. 18:46 <DIR> .
2022. 02. 20. 18:46 <DIR> ..
0 File(s) 0 bytes

Directory of C:\BK6QE8\fa\barack
2022. 02. 20. 18:46 <DIR> .
2022. 02. 20. 18:46 <DIR> ..
0 File(s) 0 bytes

Directory of C:\BK6QE8\fa\kokusz
2022. 02. 20. 18:47 <DIR> .
2022. 02. 20. 18:47 <DIR> ..
0 File(s) 0 bytes

Directory of C:\BK6QE8\fa\korte
2022. 02. 20. 18:47 <DIR> .
2022. 02. 20. 18:47 <DIR> ..
0 File(s) 0 bytes

Directory of C:\BK6QE8\fa\szeder
2022. 02. 20. 18:47 <DIR> .
2022. 02. 20. 18:47 <DIR> ..
0 File(s) 0 bytes

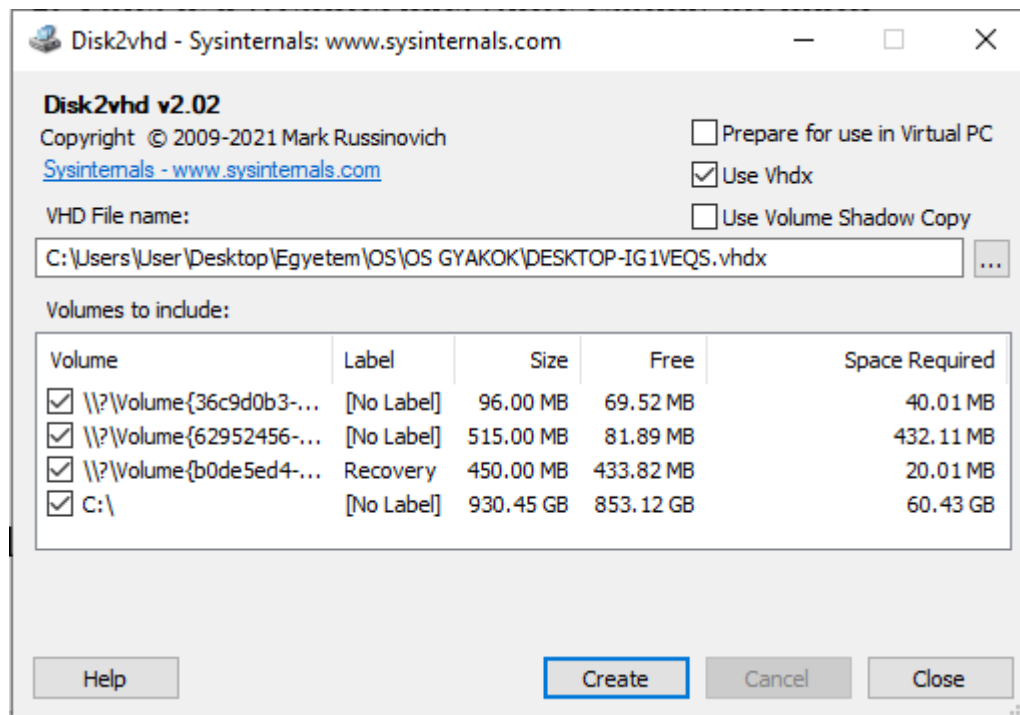
Total Files Listed:
2 File(s) 187 bytes
29 Dir(s) 915 661 778 944 bytes free

```

2. Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.
<https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite> A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

a) File and Disk Utilities (Disk2vhd):

Megvalósítás:

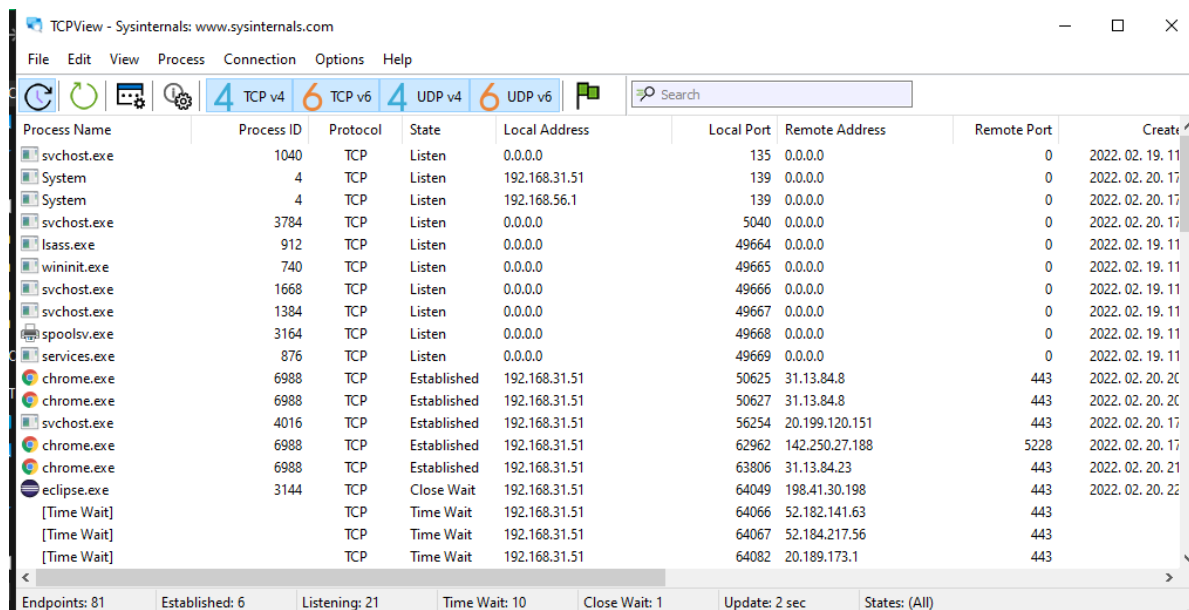


A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-verzióit (Virtuális merevlemez – A Microsoft virtuálisgép-lemezformátuma) a Microsoft Virtual PC-n vagy Microsoft Hyper-V virtuális gépeken való használatra. A disk2vhd online felületen is futtatható. A Disk2vhd felhasználói felületén felsorolja a rendszeren lévő partíciókat.

Minden olyan lemezhez létrehoz egy VHD-t, amelyen a kiválasztott kötetek találhatóak. Megőrzi a lemez particionálási adatait, de csak a kiválasztott lemezen lévő kötetek adattartalmait másolja. Így például csak a rendszerköteteket rögzítheti, és kizárhatja az adatköteteket. A futtatás a kijelölt lemezek másolatát eredményezi VHD-ra.

b) Networking Utilities (TCPView)

Megvalósítás:



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create
svchost.exe	1040	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.19.11
System	4	TCP	Listen	192.168.31.51	139	0.0.0.0	0	2022.02.20.17
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.20.17
svchost.exe	3784	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.20.17
lsass.exe	912	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.19.11
wininit.exe	740	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.19.11
svchost.exe	1668	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.19.11
svchost.exe	1384	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.19.11
spoolsv.exe	3164	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.19.11
services.exe	876	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2022.02.19.11
chrome.exe	6988	TCP	Established	192.168.31.51	50625	31.13.84.8	443	2022.02.20.20
chrome.exe	6988	TCP	Established	192.168.31.51	50627	31.13.84.8	443	2022.02.20.20
svchost.exe	4016	TCP	Established	192.168.31.51	56254	20.199.120.151	443	2022.02.20.17
chrome.exe	6988	TCP	Established	192.168.31.51	62962	142.250.27.188	5228	2022.02.20.17
chrome.exe	6988	TCP	Established	192.168.31.51	63806	31.13.84.23	443	2022.02.20.21
eclipse.exe	3144	TCP	Close Wait	192.168.31.51	64049	198.41.30.198	443	2022.02.20.22
[Time Wait]		TCP	Time Wait	192.168.31.51	64066	52.182.141.63	443	
[Time Wait]		TCP	Time Wait	192.168.31.51	64067	52.184.217.56	443	
[Time Wait]		TCP	Time Wait	192.168.31.51	64082	20.189.173.1	443	

Endpoints: 81 Established: 6 Listening: 21 Time Wait: 10 Close Wait: 1 Update: 2 sec States: (All)

A TCPView egy Windows program, amely részletes listában mutatja be a rendszer összes TCP- és UDP-végpontját, beleértve a helyi és távoli címeket, valamint a TCP-kapcsolatok állapotát.

A TCPView indítani fogja az összes aktív TCP- és UDP-végpont felsorolását, és feloldja az összes IP-címet a tartománynév-verziójukra.

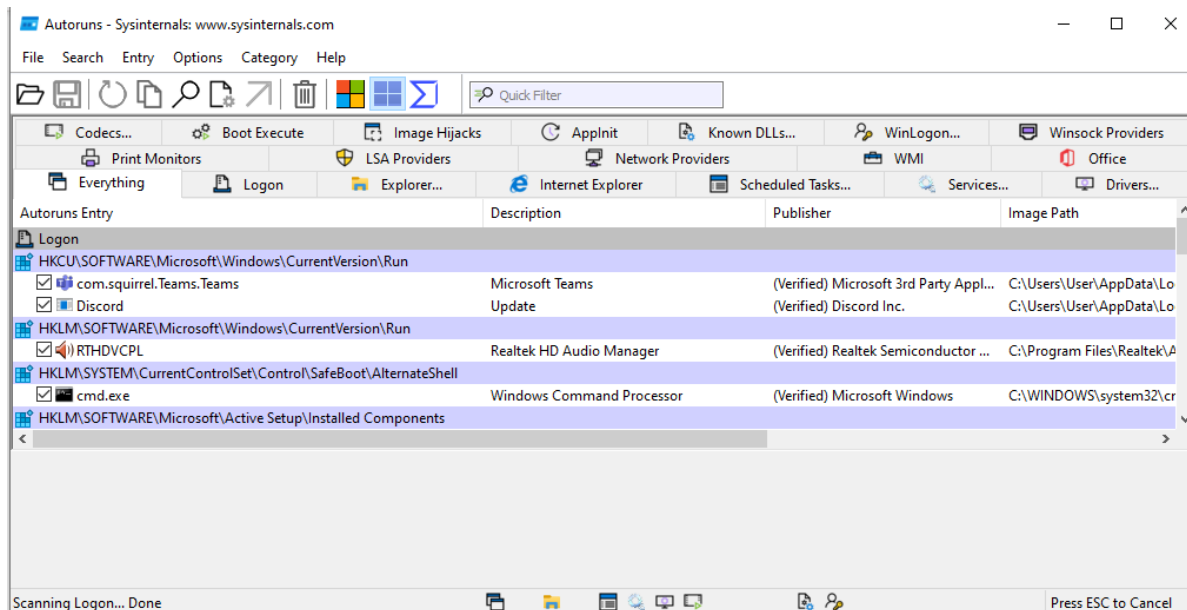
A TCPView elindításakor az összes aktív TCP- és UDP-végpontot felsorolja, majd jellemzi Processz névvel, Processz ID-vel, protokollal, állapottal, IP-címmel, távoli címmel, kezdeti időponttal, modul névvel. Másodpercenként frissül.

Azok a végpontok, amelyek állapotát egyik frissítésről a másikkra változtatják, sárga színnel jelölik, törölteket pirossal, új végpontokat zölddel.

A futtatás során láthatóvá válik az operációs rendszeren futó összes processz adata.

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

Megvalósítás:



Ez a segédprogram, amely a legátfogóbb ismeretekkel rendelkezik az indítási figyelők automatikus indítási helyéről, megmutatja, milyen programok futtatására van konfigurálva a rendszerindítás vagy a bejelentkezés során, és mikor indít el különböző beépített Windows-alkalmazásokat.

A program futtatásakor megmutatja, hogy a rendszer indítása során milyen alkalmazások indulnak el automatikusan, továbbá az automatikus indítási konfigurációhoz elérhető rendszerleíró adatbázis és fájlrendszer helyek teljes listáját.

d,Security Utilities (LogonSession)

Megvalósítás:

Felsorolja a jelenleg aktív bejelentkezési munkameneteket, és ha megadja a -p beállítást, az egyes munkamenetekben futó folyamatokat.

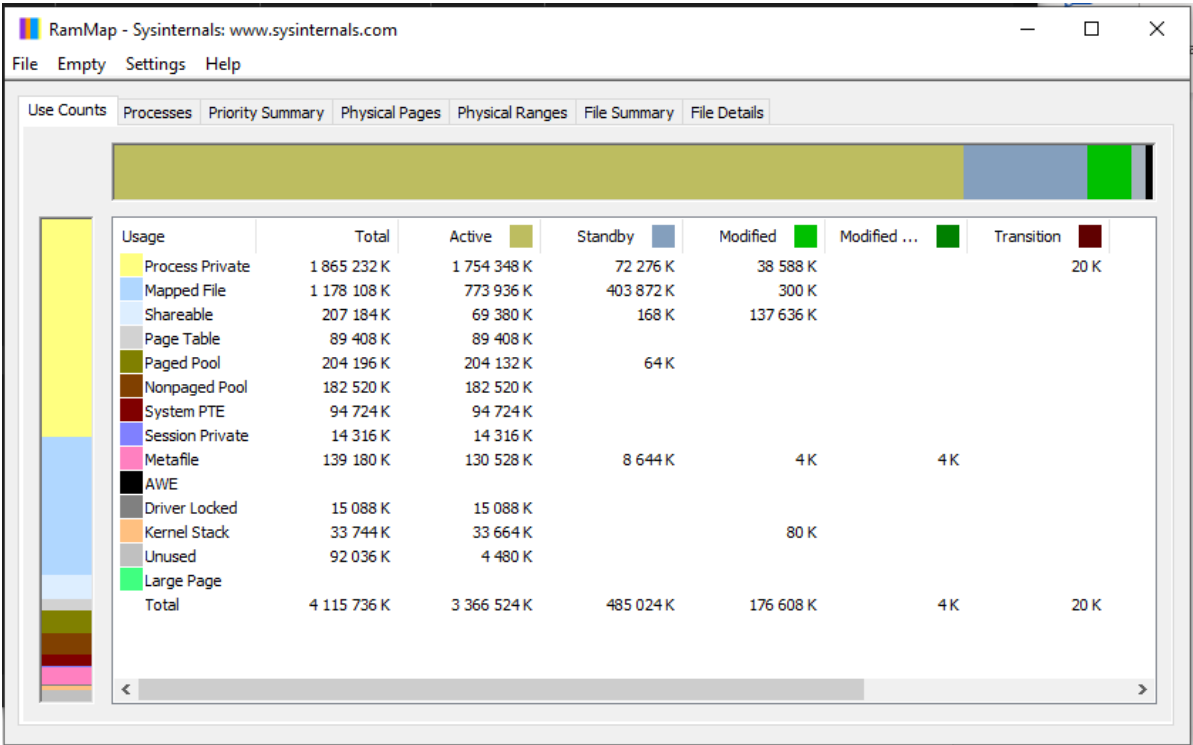
```
C:\Users\User\Desktop\Egyetem\OS\OS GYAKOK>logonsessions -p

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-IG1VEQS$
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            S-1-5-18
  Logon time:     2022. 02. 19. 11:47:29
  Logon server:
  DNS Domain:
  UPN:
    796: winlogon.exe
    912: lsass.exe
    568: svchost.exe
   1088: svchost.exe
   1328: svchost.exe
   1384: svchost.exe
   1508: svchost.exe
   1600: svchost.exe
```

e) Information Utilities (RAMMap)

Megvalósítás:



A RAMMap egy speciális fizikai memóriahasználat-elemzési
Különböző módokon mutatja be a használati adatokat.
Bemutathatja például processzek vagy fájlok alapján.

A futtatás során a windows memóriakezelésébe nyerhetünk betekintést.

**3. Töltse le a következő programot: Dependency Walker URL:
<http://www.dependencywalker.com/> Feladata: a segédprogram
megvizsgálja milyen mappákra, és azon belül milyen
függvényekre hivatkozik egy elindított program. „**

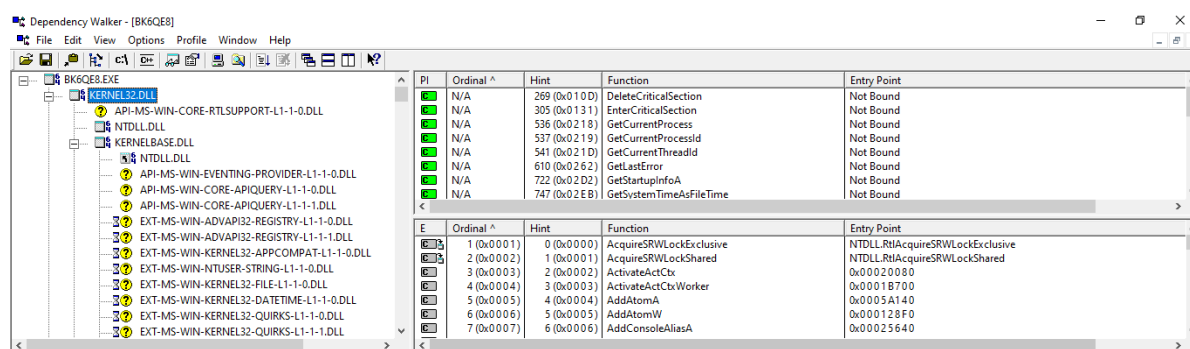
**Készítsen egy neptunkod.c nevű forráskódot, amely egy
vezeteknev.txt fájlt létrehoz, olvas, majd bezár. Tartalma: Név,
Szak, Neptunkod etc. Fordítsa le kódot a C fordító, majd tegye
futtathatóvá az állományt: neptunkod.exe A Dependency Walker
segítségével végezze el a következő feladatokat.**

Nyissa meg a neptunkod.exe fájlt!

```
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main()
5  {
6      FILE * fPointer;
7      fPointer = fopen("BK6QE8.txt","w");
8      fprintf(fPointer, "Sziraczki Soma, Programtervező Informatikus BSC, BK6QE8");
9      fclose(fPointer);
10     return 0;
11 }
12
```

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

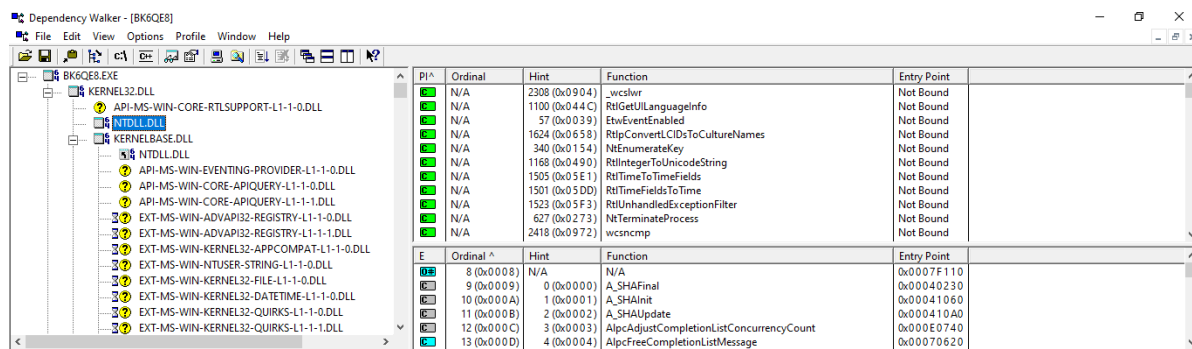
Megvalósítás:



a kernel32.dll-ből az API-MS-WIN-CORE-RTLSSUPPORT-L1-1-0.DLL hívást használja

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

Megvalósítás:



PI ^	Ordinal	Hint	Function	Entry Point
	N/A	2308 (0x0904)	_wcslwr	Not Bound
	N/A	1100 (0x044C)	RtlGetUILanguageInfo	Not Bound
	N/A	57 (0x0039)	EtwEventEnabled	Not Bound
	N/A	1624 (0x0658)	RtlpConvertLCIDsToCultureNames	Not Bound
	N/A	340 (0x0154)	NtEnumerateKey	Not Bound
	N/A	1168 (0x0490)	RtlIntegerToUnicodeString	Not Bound
	N/A	1505 (0x05E1)	RtlTimeToTimeFields	Not Bound
	N/A	1501 (0x05DD)	RtlTimeFieldsToTime	Not Bound
	N/A	1523 (0x05F3)	RtlUnhandledExceptionFilter	Not Bound
	N/A	627 (0x0273)	NtTerminateProcess	Not Bound
	N/A	2418 (0x0972)	wcsncmp	Not Bound
E	Ordinal ^	Hint	Function	Entry Point
	8 (0x0008)	N/A	N/A	0x0007F110
	9 (0x0009)	0 (0x0000)	A_SHAFinal	0x00040230
	10 (0x000A)	1 (0x0001)	A_SHAInit	0x00041060
	11 (0x000B)	2 (0x0002)	A_SHAUpdate	0x000410A0
	12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000E0740
	13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage	0x00070620

A fájl **ntdll.dll** NT kernel függvényeket tartalmaz.
Az ntdll.dll a system service dispatcherrel kommunikál.