

Operációs rendszerek BSc

2.Gyak.

2022. 02. 15.

Készítette: Nagy Bence
Neptunkód: WH8L7E

Miskolc, 2022

1.feladat:

a.) Hozza létre a következő mappa szerkezetet!

neptunkod

|

|- bokor

 |- banan

 |- mogyoro

 |- barack

|

|- fa

 |- korte

|

|-land

|- szeder

|- kokusz

megoldás:

```
C:\Users\Acer>cd wh817e

C:\Users\Acer\wh817e>tree
Folder PATH listing
Volume serial number is D481-D28A
C: .
|_ bokor
|   |_ banan
|   |_ barack
|   |_ mogyoro
|_ fa
|   |_ korte
|_ land
|   |_ kokusz
|   |_ szeder

C:\Users\Acer\wh817e>
```

b) Készítsen másolatot:

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

megoldás:

```
C:\Users\Acer>xcopy C:\Users\Acer\wh817e\bokor\>banan C:\Users\Acer\wh817e\fa /e
C:\Users\Acer>xcopy C:\Users\Acer\wh817e\land\>szeder C:\Users\Acer\wh817e\fa /e
```

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

megoldás:

```
C:\Users\Acer\wh817e>move C:\Users\Acer\wh817e\land\kokusz C:\Users\Acer\wh817e\fa
1 dir(s) moved.

C:\Users\Acer\wh817e>tree
Folder PATH listing
Volume serial number is D481-D28A
C:..
|---bokor
|   |---banan
|   |---mogyoro
|---fa
|   |---barack
|   |---kokusz
|   |---korte
|   |---szeder
|---land
|   |---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

megoldás:

```
C:\Users\Acer\wh817e>rmdir/s C:\Users\Acer\wh817e\land
C:\Users\Acer\wh817e\land, Are you sure (Y/N)? y
```

```
C:\Users\Acer>echo >"C:\Users\Acer\wh817e\bokor\banan\leiras.txt"

C:\Users\Acer>echo >"C:\Users\Acer\wh817e\fa\felsorolas.txt"
```

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

A felsorolás szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
C:\Users\Acer>echo A barack finom. >"C:\Users\Acer\wh817e\bokor\banan\leiras.txt"
C:\Users\Acer>echo A barack sarga >>"C:\Users\Acer\wh817e\bokor\banan\leiras.txt"
C:\Users\Acer>echo A barack magjába cian van. >>"C:\Users\Acer\wh817e\bokor\banan\leiras.txt"
C:\Users\Acer>echo Beviz Elek,Futy Imre,Mikorka Kalman,Mike Oxlong,Siska David >"C:\Users\Acer\wh817e\fa\felsorolas.txt"
```

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

megoldás:

```
C:\Users\Acer\wh817e>dir \s
Volume in drive C has no label.
Volume Serial Number is D481-D28A

Directory of C:\

File Not Found

C:\Users\Acer\wh817e>dir /s
Volume in drive C has no label.
Volume Serial Number is D481-D28A

Directory of C:\Users\Acer\wh817e

2022. 02. 15. 15:30 <DIR>      .
2022. 02. 15. 15:30 <DIR>      ..
2022. 02. 15. 19:43 <DIR>      bokor
2022. 02. 15. 19:44 <DIR>      fa
0 File(s)          0 byte(s)

Directory of C:\Users\Acer\wh817e\bokor

2022. 02. 15. 19:43 <DIR>      .
2022. 02. 15. 19:43 <DIR>      ..
2022. 02. 15. 19:43 <DIR>      banan
2022. 02. 15. 14:31 <DIR>      mogyoro
0 File(s)          0 bytes

Directory of C:\Users\Acer\wh817e\bokor\banan

2022. 02. 15. 19:43 <DIR>      .
2022. 02. 15. 19:43 <DIR>      ..
2022. 02. 15. 19:52      64 leiras.txt
1 File(s)          64 bytes

Directory of C:\Users\Acer\wh817e\bokor\mogyoro

2022. 02. 15. 14:31 <DIR>      .
2022. 02. 15. 14:31 <DIR>      ..
0 File(s)          0 bytes

Directory of C:\Users\Acer\wh817e\fa

2022. 02. 15. 19:44 <DIR>      .
```

```
Directory of C:\Users\Acer\wh817e\fa

2022. 02. 15. 19:44 <DIR>      .
2022. 02. 15. 19:44 <DIR>      ..
2022. 02. 15. 18:48 <DIR>      banan
2022. 02. 15. 19:56      62 felsorolas.txt
2022. 02. 15. 14:33 <DIR>      kokusz
2022. 02. 15. 14:32 <DIR>      korte
2022. 02. 15. 14:33 <DIR>      szeder
1 File(s)          62 bytes

Directory of C:\Users\Acer\wh817e\fa\banan

2022. 02. 15. 18:48 <DIR>      .
2022. 02. 15. 18:48 <DIR>      ..
0 File(s)          0 bytes

Directory of C:\Users\Acer\wh817e\fa\kokusz

2022. 02. 15. 14:33 <DIR>      .
2022. 02. 15. 14:33 <DIR>      ..
0 File(s)          0 bytes

Directory of C:\Users\Acer\wh817e\fa\korte

2022. 02. 15. 14:32 <DIR>      .
2022. 02. 15. 14:32 <DIR>      ..
0 File(s)          0 bytes

Directory of C:\Users\Acer\wh817e\fa\szeder

2022. 02. 15. 14:33 <DIR>      .
2022. 02. 15. 14:33 <DIR>      ..
0 File(s)          0 bytes

Total Files Listed:
    2 File(s)          126 bytes
   26 Dir(s)  79 146 090 496 bytes free

C:\Users\Acer\wh817e>
```

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

```
C:\Users\Acer\wh817e>dir /S /P "C:\Users\Acer\wh817e\fa\felsorolas.txt"
Directory of C:\Users\Acer\wh817e\fa

2022. 02. 15.  19:56                62 felsorolas.txt
                  1 File(s)                62 bytes

    Total Files Listed:
          1 File(s)                62 bytes
          0 Dir(s)  79 147 540 480 bytes free
```

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

```
C:\Users\Acer>attrib +r "C:\Users\Acer\wh817e\fa\felsorolas.txt"
```

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

```
C:\Users\Acer>dir /s C:\Users\Acer\wh817e
Directory of C:\Users\Acer\wh817e

2022. 02. 15.  15:30    <DIR>      .
2022. 02. 15.  15:30    <DIR>      ..
2022. 02. 15.  19:43    <DIR>      bokor
2022. 02. 15.  19:44    <DIR>      fa

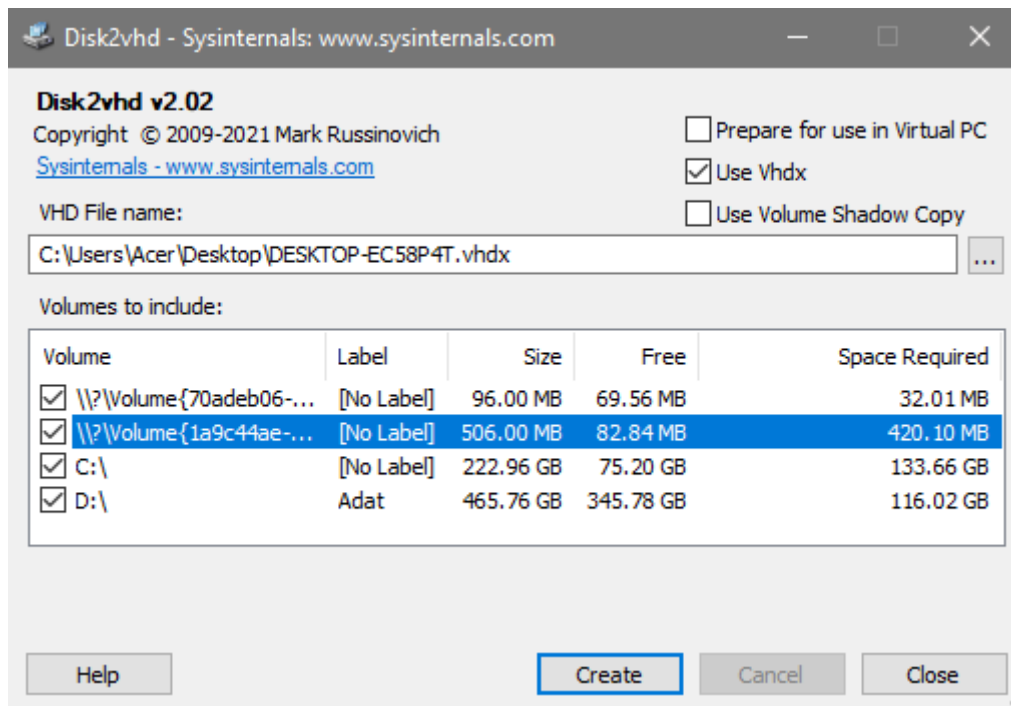
    Total Files Listed:
          2 File(s)                131 bytes
```

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

```
C:\Users\Acer\wh817e\fa>sort /r C:\Users\Acer\wh817e\fa\felsorolas.txt
Siska David,
Mikorka Kalman,
Mike Oxlorg,
Futy Imre,
Beviz Elek
```

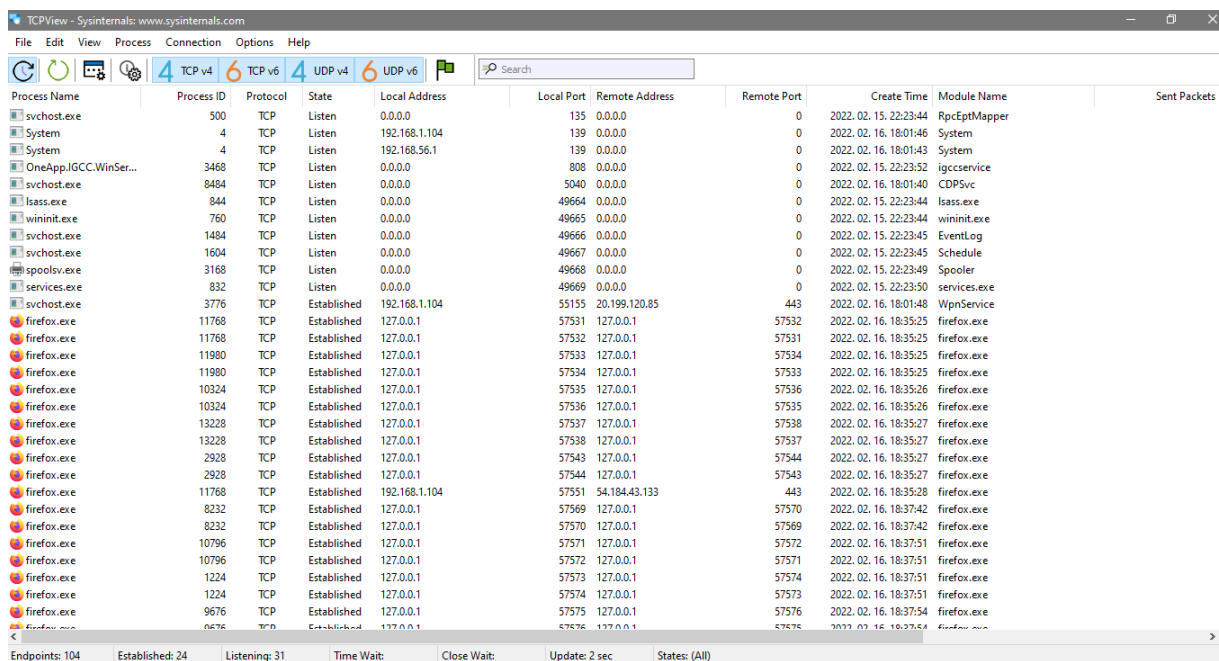
2.feladat:

a) File and Disk Utilities (Disk2vhd)



A **Disk2vhd** felsorolja a rendszerben jelenlévő köteteket. Ekkor .vhd fájlokat készít a lemezekről, amelyen a kiválasztott kötetek tartózkodnak. Ez megőrzi a partíciókat, csak átmásolja az adatokat.

b) Networking Utilities (TCPView)



A **TCPView** megmutatja a rendszer összes TCP- és UDP-végpontjának részletes listáját, beleértve a helyi és távoli címeket és a TCP-kapcsolatok állapotát.

A **Process Explorer** információkat jelenít meg arról, hogy mely leírók és DLL-ek folyamatai nyitottak vagy betöltöttek.

Process Explorer - Sysinternals www.sysinternals.com [DES-TOP-EC58P4T-Acer]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		10 940 K	66 632 K	100		
System Idle Process	58.33	60 K	8 K	0		
System	0.75	200 K	3 716 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 600 K	1 560 K	436		
csrss.exe		128 K	1 224 K	2376		
csrss.exe		1 928 K	6 084 K	660		
wininit.exe		1 544 K	7 452 K	760		
services.exe	1.13	5 768 K	10 872 K	832		
svchost.exe	< 0.01	14 320 K	35 228 K	976	Windows-szolgáltatások gazd...	Microsoft Corporation
WmPrvSE.exe		8 672 K	17 168 K	5776		
dlhost.exe		3 156 K	10 968 K	8708		
MoUsCoreWorker.exe	< 0.01	19 800 K	38 024 K	9584		
StartMenuExperience...		27 096 K	78 740 K	7908		
RuntimeBroker.exe		6 000 K	25 920 K	7456	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	128 032 K	207 452 K	3608	Search application	Microsoft Corporation
RuntimeBroker.exe		7 516 K	29 816 K	4900	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	32 532 K	67 112 K	8588		Microsoft Corporation
SettingSyncHost.exe		6 288 K	7 304 K	6656	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		3 652 K	18 392 K	5960	Runtime Broker	Microsoft Corporation
GCC.exe	Susp...	21 140 K	66 240 K	6196	IGCC	Intel Corporation
RuntimeBroker.exe		3 536 K	22 036 K	7424	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	19 688 K	69 240 K	9708	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		4 316 K	25 194 K	9648	Runtime Broker	Microsoft Corporation
VideoUI.exe	Susp...	20 492 K	2 804 K	13284		
RuntimeBroker.exe		3 720 K	21 728 K	12484	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		1 448 K	7 672 K	7488	Runtime Broker	Microsoft Corporation
TextInputHost.exe		13 828 K	53 496 K	7324		Microsoft Corporation
UserOOBEBroker.exe		1 988 K	9 592 K	12756	User OOBEBroker	Microsoft Corporation
LockApp.exe	Susp...	15 148 K	57 780 K	7212	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		9 700 K	36 784 K	8848	Runtime Broker	Microsoft Corporation
dlhost.exe		3 244 K	12 388 K	11848	COM Surrogate	Microsoft Corporation
ApplicationFrameHost.exe		8 172 K	30 432 K	4604	Application Frame Host	Microsoft Corporation
Microsoft.Photos.exe	Susp...	50 436 K	105 256 K	6884		
RuntimeBroker.exe		10 536 K	33 940 K	2352	Runtime Broker	Microsoft Corporation
svchost.exe	< 0.01	9 048 K	16 600 K	500	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe	< 0.01	2 944 K	8 720 K	1028	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		2 588 K	10 532 K	1264	Windows-szolgáltatások gazd...	Microsoft Corporation

CPU Usage: 42.52% Commit Charge: 28.69% Processes: 177 Physical Usage: 31.70%

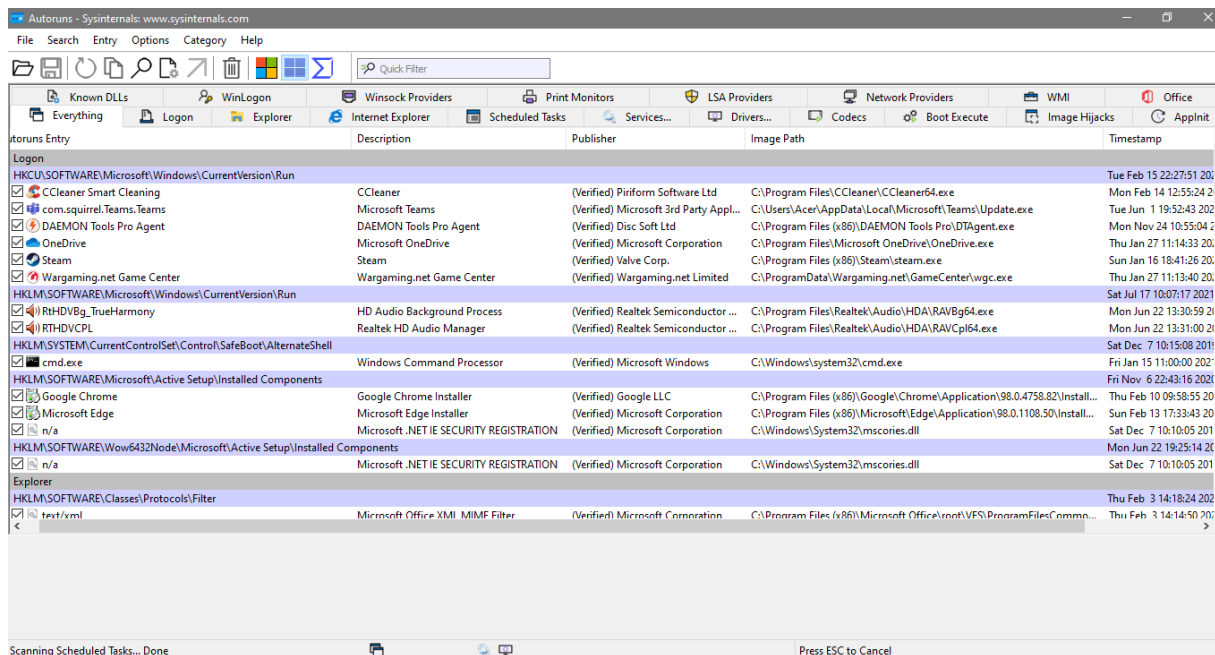
A **Process Monitor** egy valós idejű fájlrendszert, rendszerleíró adatbázist és folyamat/szál tevékenységet mutat.

The screenshot displays the Process Monitor application window. The top menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. Below the menu is a toolbar with icons for file operations, filtering, and viewing. The main pane shows a list of system events. The columns are: Time, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show only those from Explorer.exe. The status bar at the bottom indicates that 99,633 of 378,832 events are shown (26%) and that the data is backed by virtual memory.

Time	Process Name	PID	Operation	Path	Result	Detail
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
18:58...	Explorer EXE	10852	RegOpenKey	HKCR\Applications\Procom64.exe	NAME NOT FOUND	Desired Access: R...
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:58...	Explorer EXE	10852	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
18:58...	Explorer EXE	10852	RegOpenKey	HKCR\Applications\Procom64.exe	NAME NOT FOUND	Desired Access: R...
18:58...	ctfmon.exe	11028	ReadFile	C:\Windows\System32\TextInputFrame...	SUCCESS	Offset: 900 608, Le...
18:58...	Explorer EXE	10852	CreateFile	C:\Users\Acer\Desktop\Procom64.exe	SUCCESS	Desired Access: R...
18:58...	Explorer EXE	10852	QueryBasicInfo	C:\Users\Acer\Desktop\Procom64.exe	SUCCESS	CreationTime: 202...
18:58...	Explorer EXE	10852	CloseFile	C:\Users\Acer\Desktop\Procom64.exe	SUCCESS	
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
18:58...	ctfmon.exe	11028	RegOpenKey	HKCU	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: R...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DW...
18:58...	ctfmon.exe	11028	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:58...	ctfmon.exe	11028	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
18:58...	ctfmon.exe	11028	RegOpenKey	HKCU	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: R...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
18:58...	Explorer EXE	10852	QueryStandardI...	C:\Users\Acer\AppData\Local\Microso...	SUCCESS	AllocationSize: 32 ...
18:58...	Explorer EXE	10852	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 212 480, Le...
18:58...	ctfmon.exe	11028	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
18:58...	ctfmon.exe	11028	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: Handle Tag...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
18:58...	ctfmon.exe	11028	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144

Showing 99 633 of 378 832 events (26%) Backed by virtual memory

Az **autoruns** megmutatja, milyen programok vannak beállítva a rendszerindítás vagy bejelentkezés során, valamint a különféle beépített Windows-alkalmazások (például Internet Explorer, Explorer és média) indításakor.



d) Security Utilities (LogonSession)

A **logonsession** felsorolja az aktív bejelentkezési munkameneteket, és ha a -p kapcsoló segítségével az egyes munkamenetekben futó folyamatok is láthatók lesznek.

```
Administrator: Command Prompt

UPN:

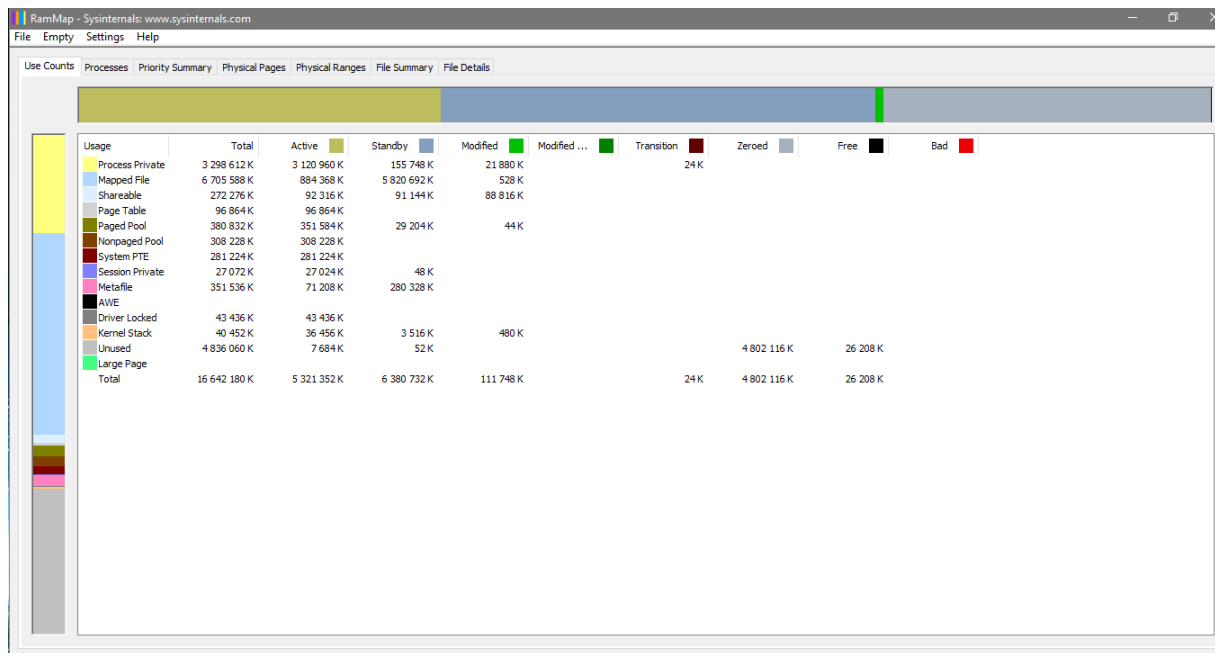
C:\>logonsessions -p

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

[0] Logon session 00000000:0000003e7:
User name: WORKGROUP\DESKTOP-MO4J1HK$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 5/14/2021 1:28:56 PM
Logon server:
DNS Domain:
UPN:
616: lsass.exe
768: svchost.exe
888: winlogon.exe
1056: svchost.exe
1268: svchost.exe
1276: svchost.exe
1308: svchost.exe
1416: svchost.exe
1440: svchost.exe
1980: svchost.exe
1988: svchost.exe
```

e) Information Utilities (RAMMap)

A **rammap** megmutatja, hogy a Windows pontosan hogyan rendel hozzá fizikai memóriát, mennyi fájladat van gyorsítótárban a RAM-ban, vagy mennyi RAM-ot használnak a kernel és az eszközillesztők.



3.feladat:

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!

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

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

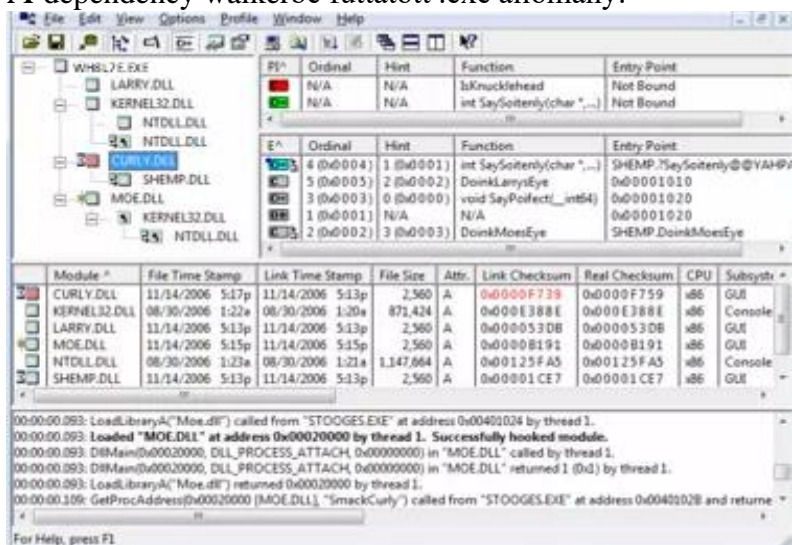
Mentés: Írja le a program szolgáltatásait és a futtatás eredményét a feladat számával a megadott jegyzőkönyvbe (képernyőkép is)

megoldás: A C kód, ami beolvassa a vezeteknev.txt állományt:

```
#include <stdio.h>
#include <stdlib.h>

int main()
{
    FILE *fp;
    fp=fopen("vezeteknev.txt", "r");
    char line[100];
    while(!feof(fp)){
        fgets(line, 100, fp);
        puts(line);
    }
    fclose(fp);
    return 0;
}
```

A dependency walkerbe futtatott .exe állomány:



A dependency walker egy futtatható fájl importált és exportált funkcióinak felsorolására szolgál.