Operációs rendszerek BSc

2. Gyak.

2022. 02. 20.

Készítette:
Szabó Larion Bsc
BGI
NWS74Y

Miskolc, 2022

1. feladat

a, mkdir parancsal létrehoztam a mappákat

```
C:\>cd C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>$ mkdir bokor
'$' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>mkdir bokor

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>mkdir fa

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>mkdir land

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>cd bokor

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor>mkdir banan

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor>mkdir mogyoro

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor>mkdir barack

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor>cd -
The system cannot find the path specified.

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor>cd.

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor>cd..

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>cd fa

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>mkdir korte

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>cd..

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>cd land

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\land>mkdir szeder

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\land>mkdir kokusz

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\land>cd..
```

b, Átmásoltam a két mappát az xcopy /t paranccsal

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>xcopy /t C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\land\
szeder C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>xcopy /t C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor
 C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\
```

c, a move paranccsal áthelyeztem a következő mappákat

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>move C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\bar
ack C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa
        1 dir(s) moved.

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>move C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\land\koku
sz C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa
        1 dir(s) moved.
```

D, Az rmdir parancsar töröltem a land mappát az alábbi módon és létrehoztam az alábbi fájlokat a type nul > paranccsal a következő .txt állományokat

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>rmdir C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\land\sze
der

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>rmdir C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\land

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>type nul C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor
\banan\Leiras.txt
The system cannot find the file specified.
Error occurred while processing: C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan\Leiras.txt.

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>type nul > C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bok
or\banan\Leiras.txt

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>type nul > C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\
Felsorolas.txt
```

E, Az átirányítás operátor > és az echo segítségével írtam a txt fileokba a szövegeket

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan>cd C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216
\bokor\banan

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan>echo "Eheto" > Leiras.txt

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan>echo "Ledus" >> Leiras.txt

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan>echo "Finom" >> Leiras.txt

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan>cd C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216
\fa

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>echo "Dávid, Péter, Tamás, Szilvi, Anna" > Leiras.txt

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>echo "Dávid, Péter, Tamás, Szilvi, Anna" > Felsorolas.txt

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>echo "David, Peter, Tamas, Szilvi, Anna" > Felsorolas.txt

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>
```

F, TREE paranccsal kilistáztam a mappa tartalmát

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>tree C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216
Folder PATH listing
Volume serial number is 00000064 CECF:546E
C:\USERS\LARION\DOCUMENTS\REPO\NWS74YOSGYAK\NWS74Y_0216
├───bokor
│   ├───banan
│   └───mogyoro
└───fa
    ├───banan
    ├───barack
    ├───kokusz
    ├───korte
    └───szeder

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>
```

G, Az e-vel kezdődő karakterek listázása.

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa>cd..

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>dir /s "?e*"
 Volume in drive C has no label.
 Volume Serial Number is CECF-546E

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan

02/23/2022  10:45 AM                30 Leiras.txt
               1 File(s)             30 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa

02/23/2022  10:47 AM                38 Felsorolas.txt
               1 File(s)             38 bytes

     Total Files Listed:
               2 File(s)             68 bytes
               0 Dir(s)   9,196,531,712 bytes free

C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>
```

H, Az icacls parancsal jogosultságot adtam a file olvasására

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>icacls C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\Fels
orolas.txt
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\Felsorolas.txt NT AUTHORITY\SYSTEM:(I)(F)
                                                                         BUILTIN\Rendszergazdák:(I)(F)
                                                                         Larion-PC\Larion:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

I, A dir paranccsal kiírattam a mappa méretét

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>dir /s C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216
 Volume in drive C has no label.
 Volume Serial Number is CECF-546E

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216

02/23/2022  10:16 AM    <DIR>          .
02/23/2022  10:16 AM    <DIR>          ..
02/23/2022  10:12 AM    <DIR>          bokor
02/23/2022  10:46 AM    <DIR>          fa
               0 File(s)              0 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor

02/23/2022  10:12 AM    <DIR>          .
02/23/2022  10:12 AM    <DIR>          ..
02/23/2022  10:19 AM    <DIR>          banan
02/23/2022  09:20 AM    <DIR>          mogyoro
               0 File(s)              0 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\banan

02/23/2022  10:19 AM    <DIR>          .
02/23/2022  10:19 AM    <DIR>          ..
02/23/2022  10:45 AM                30 Leiras.txt
               1 File(s)             30 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\bokor\mogyoro

02/23/2022  09:20 AM    <DIR>          .
02/23/2022  09:20 AM    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa

02/23/2022  10:46 AM    <DIR>          .
02/23/2022  10:46 AM    <DIR>          ..
02/23/2022  10:01 AM    <DIR>          banan
02/23/2022  09:20 AM    <DIR>          barack
02/23/2022  10:47 AM                38 Felsorolas.txt
02/23/2022  09:22 AM    <DIR>          kokusz
02/23/2022  09:21 AM    <DIR>          korte
02/23/2022  09:56 AM    <DIR>          szeder
               1 File(s)             38 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\banan

02/23/2022  10:01 AM    <DIR>          .
02/23/2022  10:01 AM    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\barack

02/23/2022  09:20 AM    <DIR>          .
02/23/2022  09:20 AM    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\kokusz

02/23/2022  09:22 AM    <DIR>          .
02/23/2022  09:22 AM    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\korte

02/23/2022  09:21 AM    <DIR>          .
02/23/2022  09:21 AM    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\szeder

02/23/2022  09:56 AM    <DIR>          .
02/23/2022  09:56 AM    <DIR>          ..
               0 File(s)              0 bytes

     Total Files Listed:
               2 File(s)             68 bytes
              29 Dir(s)   9,197,420,544 bytes free
```

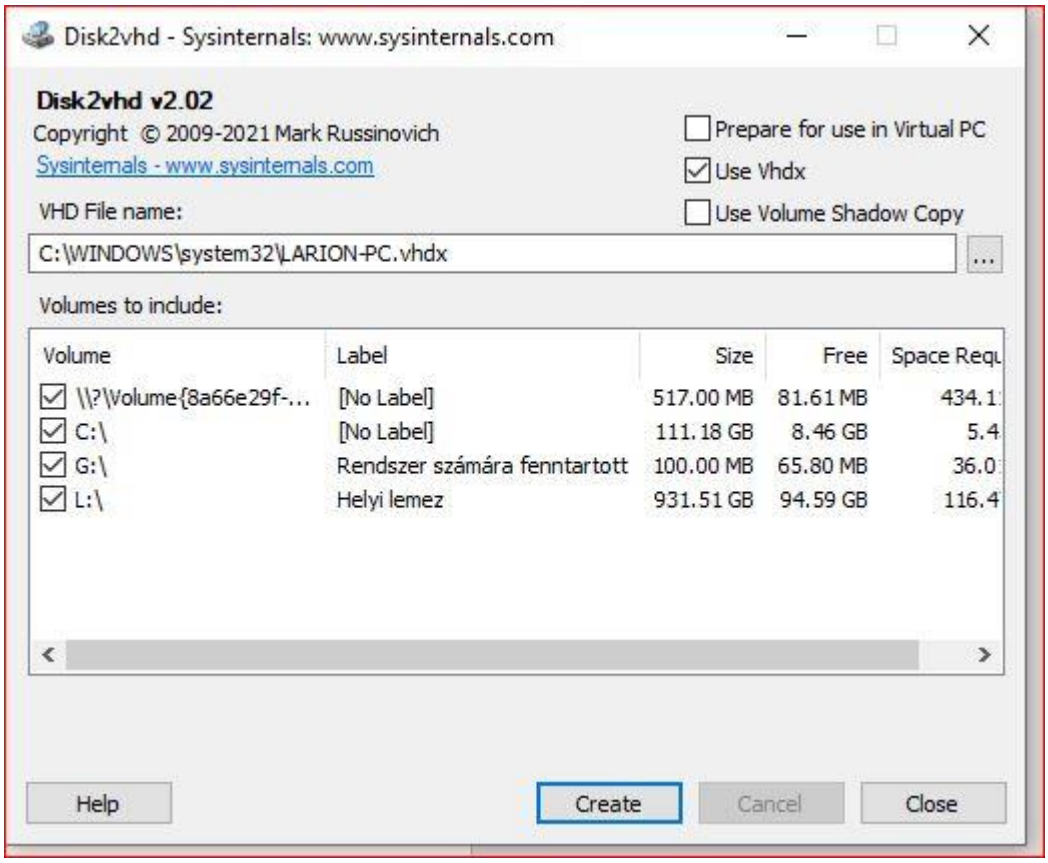
J, A sort paranccsal rendeztem a file tartalmát

```
C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216>sort C:\Users\Larion\Documents\repo\NWS74YOsGyak\NWS74Y_0216\fa\Felsor
olas.txt
Anna
David
Peter
Szilvi
Tamas
```

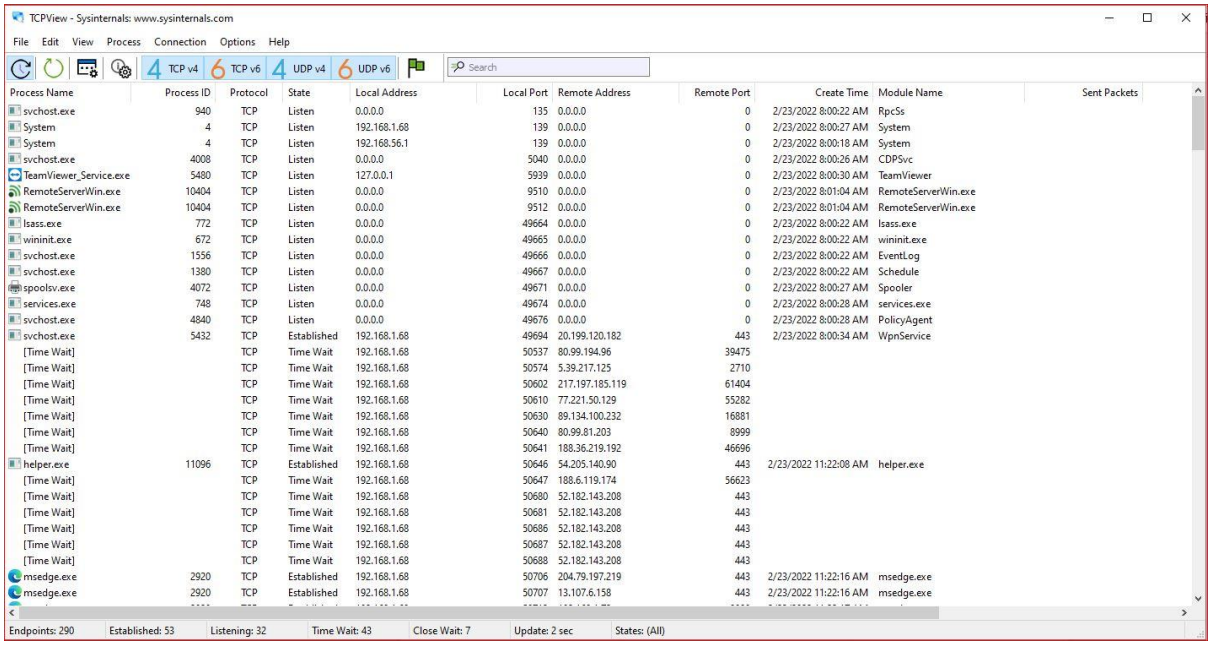
2. feladat

a, A **Disk2vhd** egy segédprogram, amely VHD (Virtual Hard Disk - a Microsoft Virtual Machine lemez formátum) változata - Microsoft Virtual PC vagy Microsoft Hyper-V virtuális gépekkel (VM) futtatható. A Volume Snapshot Service (VSS) képességgel már rendelkező Windows XP köteteiről készített pillanatképet konvertálja a Windows későbbi változataival is használható lemezképpé.

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



B, 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 Windows Server 2008, Vista és XP rendszeren a TCPView a végpont tulajdonában található folyamat nevét is jelenti. A TCPView a Netstat program egy informatívabb és kényelmesebben bemutatott részkészletét biztosítja.

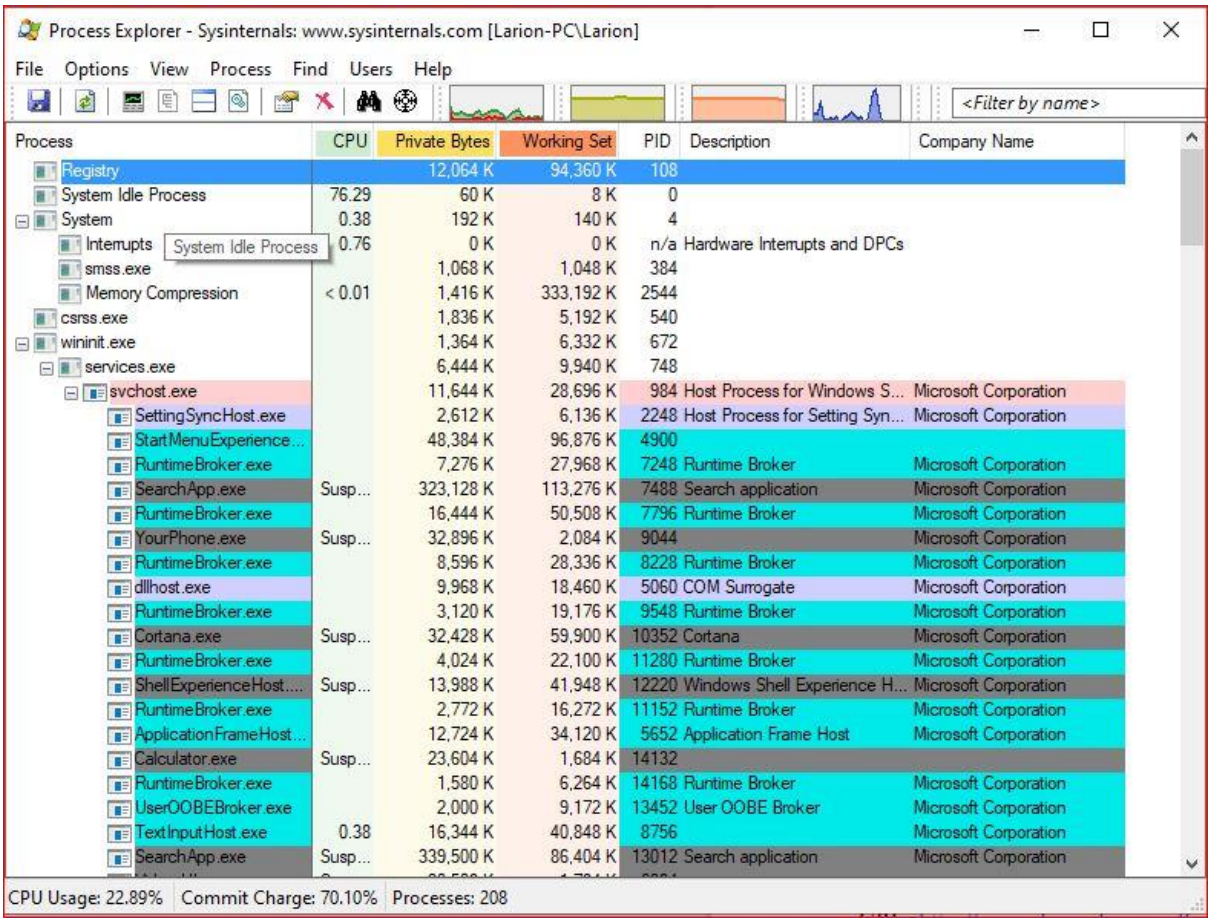


Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	940	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2/23/2022 8:00:22 AM	RpcSs	
System	4	TCP	Listen	192.168.1.68	139	0.0.0.0	0	2/23/2022 8:00:27 AM	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2/23/2022 8:00:18 AM	System	
svchost.exe	4008	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2/23/2022 8:00:26 AM	CDPSvc	
TeamViewer_Service.exe	5480	TCP	Listen	127.0.0.1	5939	0.0.0.0	0	2/23/2022 8:00:30 AM	TeamViewer	
RemoteServerWin.exe	10404	TCP	Listen	0.0.0.0	9510	0.0.0.0	0	2/23/2022 8:01:04 AM	RemoteServerWin.exe	
RemoteServerWin.exe	10404	TCP	Listen	0.0.0.0	9512	0.0.0.0	0	2/23/2022 8:01:04 AM	RemoteServerWin.exe	
lsass.exe	772	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2/23/2022 8:00:22 AM	lsass.exe	
wininit.exe	672	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2/23/2022 8:00:22 AM	wininit.exe	
svchost.exe	1556	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2/23/2022 8:00:22 AM	EventLog	
svchost.exe	1380	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2/23/2022 8:00:22 AM	Schedule	
spoolsv.exe	4072	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	2/23/2022 8:00:27 AM	Spooler	
services.exe	748	TCP	Listen	0.0.0.0	49674	0.0.0.0	0	2/23/2022 8:00:28 AM	services.exe	
svchost.exe	4840	TCP	Listen	0.0.0.0	49676	0.0.0.0	0	2/23/2022 8:00:28 AM	PolicyAgent	
svchost.exe	5432	TCP	Established	192.168.1.68	49694	20.199.120.182	443	2/23/2022 8:00:34 AM	WpnService	
[Time Wait]		TCP	Time Wait	192.168.1.68	50537	80.99.194.96	39475			
[Time Wait]		TCP	Time Wait	192.168.1.68	50574	5.39.217.125	2710			
[Time Wait]		TCP	Time Wait	192.168.1.68	50602	217.197.185.119	61404			
[Time Wait]		TCP	Time Wait	192.168.1.68	50610	77.221.50.129	55282			
[Time Wait]		TCP	Time Wait	192.168.1.68	50630	89.134.100.232	16881			
[Time Wait]		TCP	Time Wait	192.168.1.68	50640	80.99.81.203	8999			
[Time Wait]		TCP	Time Wait	192.168.1.68	50641	188.36.219.192	46696			
helper.exe	11096	TCP	Established	192.168.1.68	50646	54.205.140.90	443	2/23/2022 11:22:08 AM	helper.exe	
[Time Wait]		TCP	Time Wait	192.168.1.68	50647	188.6.119.174	56623			
[Time Wait]		TCP	Time Wait	192.168.1.68	50680	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50681	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50686	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50687	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50688	52.182.143.208	443			
msedge.exe	2920	TCP	Established	192.168.1.68	50706	204.79.197.219	443	2/23/2022 11:22:16 AM	msedge.exe	
msedge.exe	2920	TCP	Established	192.168.1.68	50707	13.107.6.158	443	2/23/2022 11:22:16 AM	msedge.exe	

C, Process Explorer – kiváló szoftver a folyamatok monitorozásához és ellenőrzéséhez. A szoftver minőségi szempontból szervezett főablaka, ahol az összes folyamat megjelenik a létrehozott listán, és elosztja a színeket, hogy megkülönböztesse őket típusonként. A Process Explorer számos olyan műveletet kínál, amelyeket a kiválasztott folyamattal végezhet: teljes, szüneteltetheti, újraindíthatja, újraindíthatja, megváltoztathatja a prioritást, minimalizálhatja vagy maximalizálhatja, ellenőrizheti a VirusTotal-ot stb. A szoftver adatokat gyűjt CPU-ról, GPU-ról, RAM-ról, I / O-lemezt és hálózatot, és a grafikonon végrehajtott változtatásokat valós időben jeleníti meg. A Process Explorer lehetővé teszi egy adott folyamat részletes információinak megtekintését is.

Főbb jellemzői:

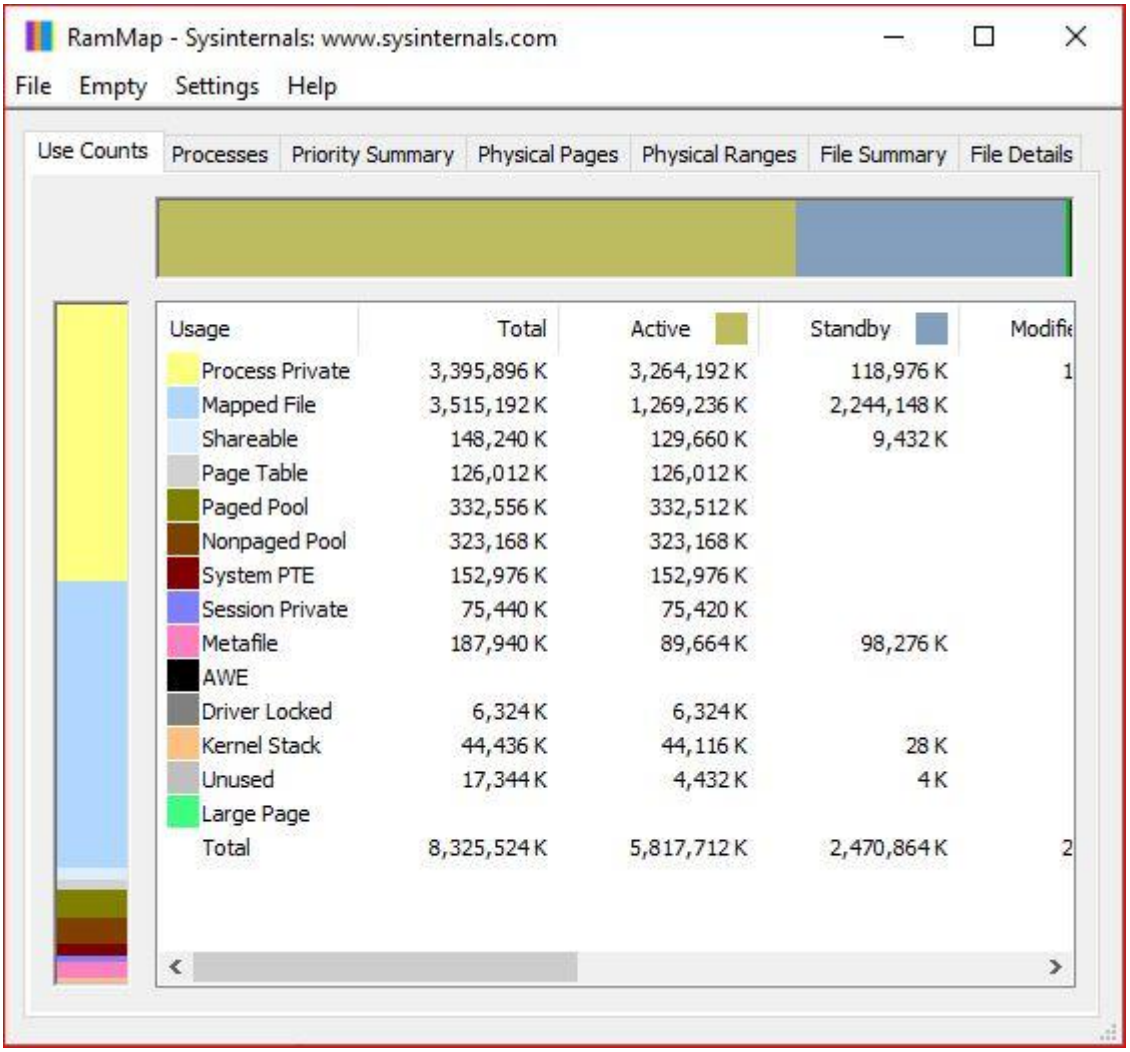
- Az aktív folyamatok felügyelete
- A folyamatok magatartáskezelése
- Egy adott folyamat részletes információinak megtekintése
- CPU, GPU, RAM, I / O adatok megjelenítése a grafikonokon



D, Ezt nem tudtam megcsinálni, nem tudtam feltelepíteni a szükséges programot a win 10-re.

E, A RAMMap megmutatja mennyi fájlt tárol a RAM memóriában, vagy mennyi RAM-ot használ a rendszermag és az eszközillesztők. Többféle módon jeleníti meg a használati információkat különböző lapokon:

- Használja a számlálást: a használati összefoglaló típus és keresési lista szerint
- Folyamatok: feldolgozó munka méretek
- Elsőbbségi összefoglaló: kiemelt készenléti listaméretek
- Fizikai oldalak: oldalankénti használat az összes fizikai memóriában
- Fizikai tartományok: fizikai memóriacímek
- Fájl összefoglalása: fájl adatok RAM-ban fájlonként
- A fájl részletei: egyéni fizikai oldalak fájlok szerint
- Használja a RAMMap-ot, hogy megértse, milyen módon kezeli a Windows a memóriát, elemzi az alkalmazás-memória használatát, vagy válaszol specifikus kérdéseket a RAM kiosztására.

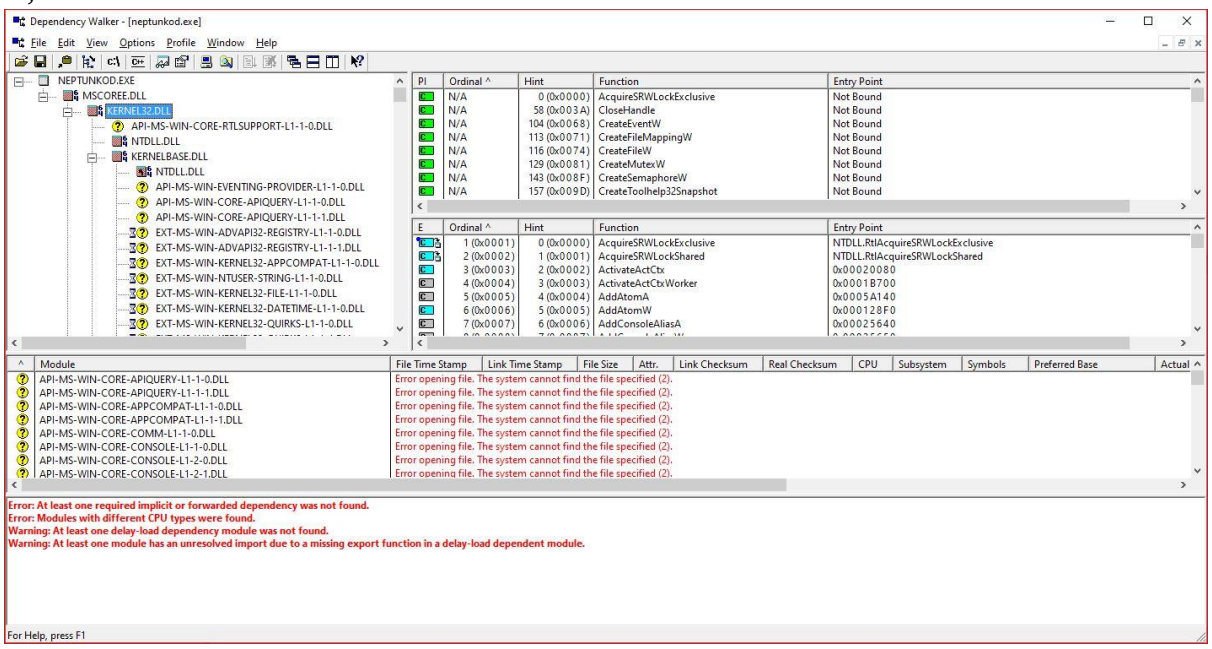


3. Feladat

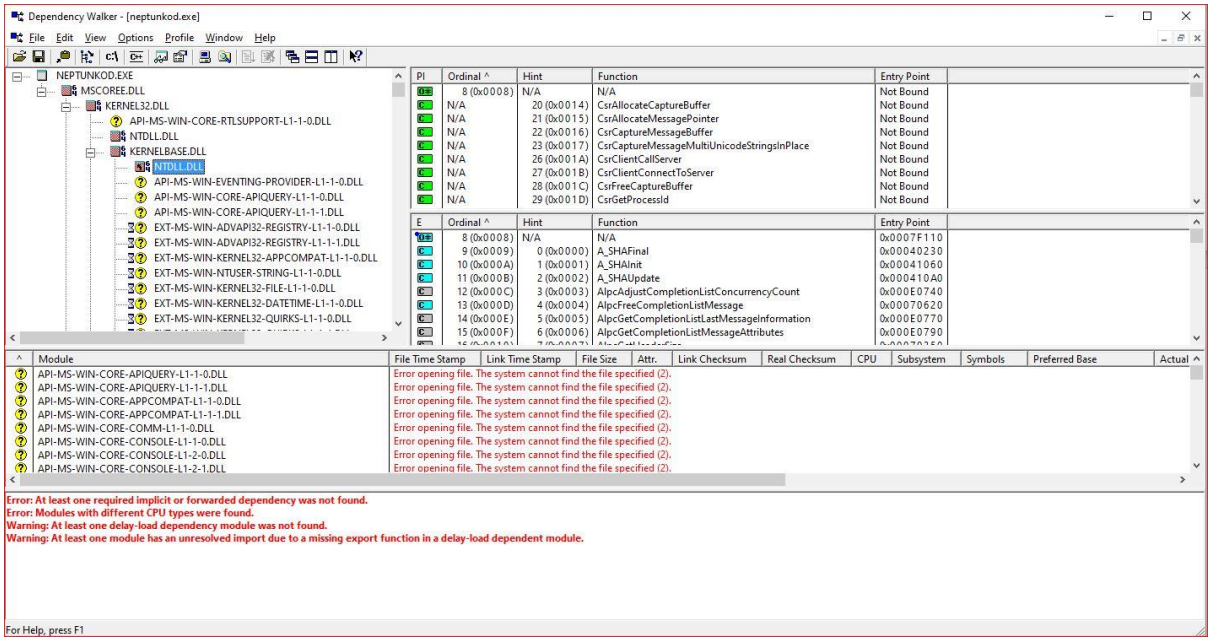
A program:

```
ConsoleApplication1                                   neptunkod.Program
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.IO;

namespace neptunkod
{
    0 references
    class Program
    {
        0 references
        static void Main(string[] args)
        {
            string fajlnev = @"l:\programok\asd\vezeteknev.txt";
            using (FileStream fs = File.Create(fajlnev));
            StreamWriter iras = new StreamWriter(fajlnev, false, Encoding.Default);
            iras.WriteLine("Szabó Larion, NWS74Y, BGI Gazdaságinformatikus");
            iras.Close();
            StreamReader olvas = new StreamReader(fajlnev, Encoding.Default);
            string szoveg;
            while(!olvas.EndOfStream)
            {
                szoveg = olvas.ReadLine();
            }
            Console.ReadLine();
            olvas.Close();

        }
    }
}
```

A,



B,



NTDLL.DLL (itt kezdődnek a user módú komponensek) Az NTDLL.DLL egy speciális, dinamikusan kapcsolódó (kölcsön)könyvtár (Dinamically Linked Library / Dinamikusan kapcsolódó [kölcsön]könyvtár. A kölcsönkönyvtár fogalmi magyarázata egy korábbi fejezetben már szerepelt.) A Windows NT alapú operációs rendszerekben az NTDLL.DLL használata megkerülhetetlen a user mód és a kernel mód közötti kommunikáció lebonyolításához. Az executive rétegben már tárgyalt objektumok közötti kapcsolattartás, az LPC (Local Procedure Call / Lokális eljáráshívás) az, amely a megfelelő függvényhívások segítségével teszi lehetővé ezt a kommunikációt is. A felhasználói objektumok csak az NTDLL.DLL igénybe vételével érhetik el az operációs rendszer kernel módban működő részét, illetve a hardvert.

Magát a kommunikációt az NTDLL.DLL néhány egyszerű lépésben hajtja végre.

1. lépés Az NTDLL.DLL-hez függvényhívás érkezik valamelyik felsőbb rétegből.

2. lépés Az NTDLL.DLL ellenőrzi a függvényhívás hívás paramétereit. (Normál esetben nincs szükség hibakezelésre.)

3. lépés Végre kell hajtani egy user mód – kernel mód váltást.

4. lépés Az NTDLL.DLL átadja a rendszerhívást a system service dispatcher-nek.

5. lépés Az operációs rendszer így már képes meghívni a kért funkciót realizáló kernel módú függvényét.

NTDLL.DLL tartalmilag az executive által kiajánlott függvényeknek megfelelő függvény csonkokból áll, melyek ugyanolyan a paraméterezésűek, mint az executive-ban lévő párjuk. Ezen kívül tartalmaz számos további függvény az alrendszerek támogatására. Ezek közül a két legfontosabb:

- dinamikus memória kezelés (Heap)
- Image Loader