

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Hajdu Adrián

Progterv. Inf.

UY5E1L

Miskolc, 2022

1. feladat – Command prompt

a, Hozza létre a következő mappa szerkezetet...

Leírás:

Elkészítettem a gyökérbe a kért faszerkezetet a “mkdir” illetve az “md” parancsok segítségével.

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Adri bácsi>cd \

C:\>mkdir UYSEIL

C:\>cd UYSEIL

C:\UYSEIL>md bokor fa land

C:\UYSEIL>cd bokor

C:\UYSEIL\bokor>md bananogyoro barack

C:\UYSEIL\bokor>cd..

C:\UYSEIL>cd fa

C:\UYSEIL\fa>mkdir korte

C:\UYSEIL\fa>cd..

C:\UYSEIL>cd land

C:\UYSEIL\land>md szederkokusz

C:\UYSEIL\land>cd \

C:\>tree UYSEIL
Folder PATH listing
Volume serial number is 0000007D D4A5:52A7
C:\UYSEIL
|-- bokor
|   |-- banan
|   |-- barack
|   |--ogyoro
|   |-- fa
|       |-- korte
|-- land
|   |-- kokusz
|   |-- szeder
-->
```

b, Készítsen másolatot

Leírás:

A másolást az “Xcopy” parancs segítségével végeztem el, amelyhez segítségül készítettem egy szöveges állományt, amelyet a masolas.txt néven mentettem el. Az állományban megtalálhatóak azok az elemek, amelyeket a másolás során nem szeretnék lemásolni. Ez azért szükséges, mert a felhasznált /E kapcsoló minden almappát másolt volna, nem csak azt az egyet, amire szükség van.

```
C:\>cd UYSEIL

C:\UYSEIL>echo kokusz > masolas.txt

C:\UYSEIL>xcopy land fa /E /T /Exclude:masolas.txt

C:\UYSEIL>tree
Folder PATH listing
Volume serial number is D4A5-52A7
C:
|-- bokor
|   |-- banan
|   |-- barack
|   |--ogyoro
|   |-- fa
|       |-- korte
|       |-- szeder
|-- land
|   |-- kokusz
|   |-- szeder
-->
```

```

C:\UY5E1L>tree
Folder PATH listing
Volume serial number is D4A5-52A7
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── korte
│   └── szeder
├── land
├── kokusz
└── szeder

C:\UY5E1L>echo barack > masolas.txt
C:\UY5E1L>echo mogyoro >> masolas.txt
C:\UY5E1L>xcopy bokor fa /E /T /Exclude:masolas.txt

C:\UY5E1L>tree
Folder PATH listing
Volume serial number is D4A5-52A7
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── banan
│   ├── korte
│   └── szeder
├── land
├── kokusz
└── szeder

C:\UY5E1L>del masolas.txt

```

c, Végezze el az áthelyezéseket

Leírás:

Az áthelyezéseket a “move” paranccsal végeztem el, amely képes áthelyezni egy mappát/fájlt egy másik mappába.

```

Command Prompt
└── szeder

C:\>move C:\UY5E1L\bokor\barack C:\UY5E1L\fa
1 dir(s) moved.

C:\>move C:\UY5E1L\land\kokusz C:\UY5E1L\fa
1 dir(s) moved.

C:\>tree \UY5E1L
Folder PATH listing
Volume serial number is 00000056 D4A5:52A7
C:\UY5E1L
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
├── land
└── szeder

C:\>

```

d, Törölje az UY5E1L/land katalógust...

Leírás:

Töröltem a neptunkod/land katalógust a mappa teljes tartalmával együtt. Ehhez az “rmdir” parancsot használtam. Alapvetően a parancs csak olyan mappákat képes törölni, amelyek üresek. Ezért a /S kapcsolót vettem segítségül a feladathoz, amely ráerőlteti a parancsot az elvégzésre akkor is, ha a mappának tartalma van.

```
C:\UY5E1L>tree
Folder PATH listing
Volume serial number is D4A5-52A7
C:.
|-- bokor
|   |-- banan
|   |-- mogyoro
|-- fa
|   |-- banan
|   |-- barack
|   |-- kokusz
|   |-- korte
|   |-- szeder
|-- land
|   |-- szeder
```

```
C:\UY5E1L>mkdir land /s
land, Are you sure (Y/N)? Y

C:\UY5E1L>tree
Folder PATH listing
Volume serial number is D4A5-52A7
C:.
|-- bokor
|   |-- banan
|   |-- mogyoro
|-- fa
|   |-- banan
|   |-- barack
|   |-- kokusz
|   |-- korte
|   |-- szeder
```

Ezután létrehoztam a kért szöveges állományokat a copy con “fájlnév” paranccsal.

```
Command Prompt

C:\UY5E1L>copy con bokor\banan\leiras.txt
^Z
    1 file(s) copied.

C:\UY5E1L>copy con fa\felsorolas.txt
^Z
    1 file(s) copied.

C:\UY5E1L>
```

e, A leiras.txt szöveges állományba..

Leírás:

Ismét a copy con parancsot használtam a megoldáshoz, annak segítségével feltöltöttem a két szöveges állományt a kért tartalommal.

```
Command Prompt

C:\UY5E1L>copy con bokor\banan\leiras.txt
^Z
    1 file(s) copied.

C:\UY5E1L>copy con fa\felsorolas.txt
^Z
    1 file(s) copied.

C:\UY5E1L>copy con bokor\banan\leiras.txt
A barack fan terem.
Overwrite bokor\banan\leiras.txt? (Yes/No/All): yes
A barack legközelebbi rokona a mandula.
Az oszibarack faja a rozsafelek családjába tartozik.
^Z
    1 file(s) copied.

C:\UY5E1L>copy con fa\felsorolas.txt
Keresztes Iulia
Overwrite fa\felsorolas.txt? (Yes/No/All): yes
Kormos Balazs
Szabo Alen
Berki Viktor
David Rebeka
^Z
    1 file(s) copied.

C:\UY5E1L>
```

f, Listázza a UY5E1L mappa tartalmát..

Leírás:

A dir parancsot használva listáztam az UY5E1L mappa tartalmát. A /b és a /s kapcsolók szükségesek ahhoz, hogy a mappa tartalmát az almappákkal és a fileokkal együtt listázza ki a parancs.

```
Administrator: Command Prompt
C:\UVSEIL>dir /b /s
C:\UVSEIL\bokor
C:\UVSEIL\fa
C:\UVSEIL\bokor\banan
C:\UVSEIL\bokor\mogvoro
C:\UVSEIL\bokor\banan\leiras.txt
C:\UVSEIL\fa\banan
C:\UVSEIL\fa\barack
C:\UVSEIL\fa\felsorolas.txt
C:\UVSEIL\fa\kokusz
C:\UVSEIL\fa\korte
C:\UVSEIL\fa\szeder
C:\UVSEIL>
```

g, Keresse meg az összes olyan fájlt, aminek “e” a második betűje

Leírás: A kereséshez a dir parancsot használtam, ahol a /s kapcsolót arra használtam, hogy a fájlokat jelenítsem meg a listában. A kritérium megszabásához egy “?”-t használtam, ami azt eredményezi, hogy a keresett fájlok első betűje nem mérvadó. Ezután behelyeztem a második helyre az “e” betűt. Ezután pedig a wildcard(*) használatával megadtam azt, hogy a második karakter után már lényegtelen, hogy mi következik a fájl nevében.

```
Administrator: Command Prompt
C:\UVSEIL>cd..
C:\>dir ?e* /s

07/12/2019 17:25      20,344 ServiceMonikerSupport.dll
1 File(s)                20,344 bytes

Directory of C:\Windows\WinSxS\x86_wcf-m_svc_mon_sup_dll_31bf3856ad364e35_10.0.19200.110_none_756ba0685b6c3f32

21/03/2020 04:03      20,352 ServiceMonikerSupport.dll
1 File(s)                20,352 bytes

Directory of C:\Windows\WinSxS\x86_windows-defender-management-powershell_31bf3856ad364e35_10.0.19041.1_none_3d95cd0a88523a81

07/12/2019 17:25      13,569 Defender.psd1
1 File(s)                13,569 bytes

Directory of C:\Windows\WinSxS\x86_wpf-penimc_31bf3856ad364e35_10.0.19041.1_none_058384c7ebade92e

03/12/2019 13:04       71,032 PenIMC.dll
1 File(s)                71,032 bytes

Directory of C:\Windows\WinSxS\x86_wpf-penimc_31bf3856ad364e35_10.0.19200.250_none_7b137039149c1529

05/09/2020 03:19       71,032 PenIMC.dll
1 File(s)                71,032 bytes

Directory of C:\Windows\WinSxS\x86_wpf-reachframework_31bf3856ad364e35_10.0.19041.1_none_59fc9d300fb995a9

03/12/2019 13:04      532,480 ReachFramework.dll
1 File(s)                532,480 bytes

Directory of C:\Windows\WinSxS\x86_wpf-reachframework_31bf3856ad364e35_10.0.19200.250_none_cf8c888138a7c1a4

05/09/2020 02:54      536,576 ReachFramework.dll
1 File(s)                536,576 bytes

Directory of C:\Windows\WinSxS\x86_wpf-perfcnt_31bf3856ad364e35_10.0.19041.1_none_796f8f9ae78775e8

18/04/2019 17:47        844 PerfCounters.h
1 File(s)                844 bytes

Directory of C:\Windows\WinSxS\x86_wpf-perfcnt_ini_31bf3856ad364e35_10.0.19041.1_none_cd96d729e2516e04

18/04/2019 17:47       153,298 PerfCounters.ini
18/04/2019 17:47         31 PerfCounters_0.ini
2 File(s)                153,329 bytes

Total Files Listed:
56193 File(s) 31,194,844,094 bytes
5974 Dir(s)  112,851,771,392 bytes free
```

h, Tegye mindenki számára olvashatóvá a felsorolas.txt fájlt!

Leírás: A feladat megoldásához az attrib parancsot használtam, ahol a “jogkörnek” a +r-t adtam meg, ami az olvashatóságot adja meg. Ezután ellenőriztem a művelet sikerességét.

```
Administrator: Command Prompt
C:\>cd UYSE1L
C:\UYSE1L>cd fa
C:\UYSE1L\fa>attrib +r felsorolas.txt
C:\UYSE1L\fa>attrib
A      R             C:\UYSE1L\fa\felsorolas.txt
C:\UYSE1L\fa>
```

i, Jelenítse meg, hogy mennyi helyet foglal.

Leírás: A dir parancsot használtam ismételten. A /a /s kapcsolók segítségével a mappa tartalma megjelenítésre kerül, illetve a mappában lévő almappák tartalmát is figyelembe veszi, így tehát a mappákban lévő fájlok méretét is megjeleníti. Ezeket összesítve a végén megkapjuk a teljes mappa méretét.

```
Administrator: Command Prompt
16/02/2022 19:18 <DIR> .
16/02/2022 19:18 <DIR> ..
16/02/2022 17:53 <DIR> banan
16/02/2022 17:53 <DIR> barack
16/02/2022 19:25      72 felsorolas.txt
16/02/2022 17:54 <DIR> kokusz
16/02/2022 17:54 <DIR> korte
16/02/2022 17:54 <DIR> szeder
                  1 File(s)      72 bytes

Directory of C:\UYSE1L\fa\banan
16/02/2022 17:53 <DIR> .
16/02/2022 17:53 <DIR> ..
                  0 File(s)      0 bytes

Directory of C:\UYSE1L\fa\barack
16/02/2022 17:53 <DIR> .
16/02/2022 17:53 <DIR> ..
                  0 File(s)      0 bytes

Directory of C:\UYSE1L\fa\kokusz
16/02/2022 17:54 <DIR> .
16/02/2022 17:54 <DIR> ..
                  0 File(s)      0 bytes

Directory of C:\UYSE1L\fa\korte
16/02/2022 17:54 <DIR> .
16/02/2022 17:54 <DIR> ..
                  0 File(s)      0 bytes

Directory of C:\UYSE1L\fa\szeder
16/02/2022 17:54 <DIR> .
16/02/2022 17:54 <DIR> ..
                  0 File(s)      0 bytes

Total Files Listed:
      2 File(s)      188 bytes
     29 Dir(s) 112,856,145,920 bytes free

C:\UYSE1L>dir /a /s
```

j, Rendezze ABC szerint a felsorolas.txt fájl tartalmát!

Leírás: A feladat megoldásához a “sort” parancsot használtam, ami automatikusan (szám nagyság/ABC rend szerint) rendezi például egy szöveges állomány sorait.

```
Administrator: Command Prompt
C:\UYSE1L>more fa\felsorolas.txt
Keresztes Iulia
Kormos Balazs
Szabo Alen
Berki Viktor
David Rebeke

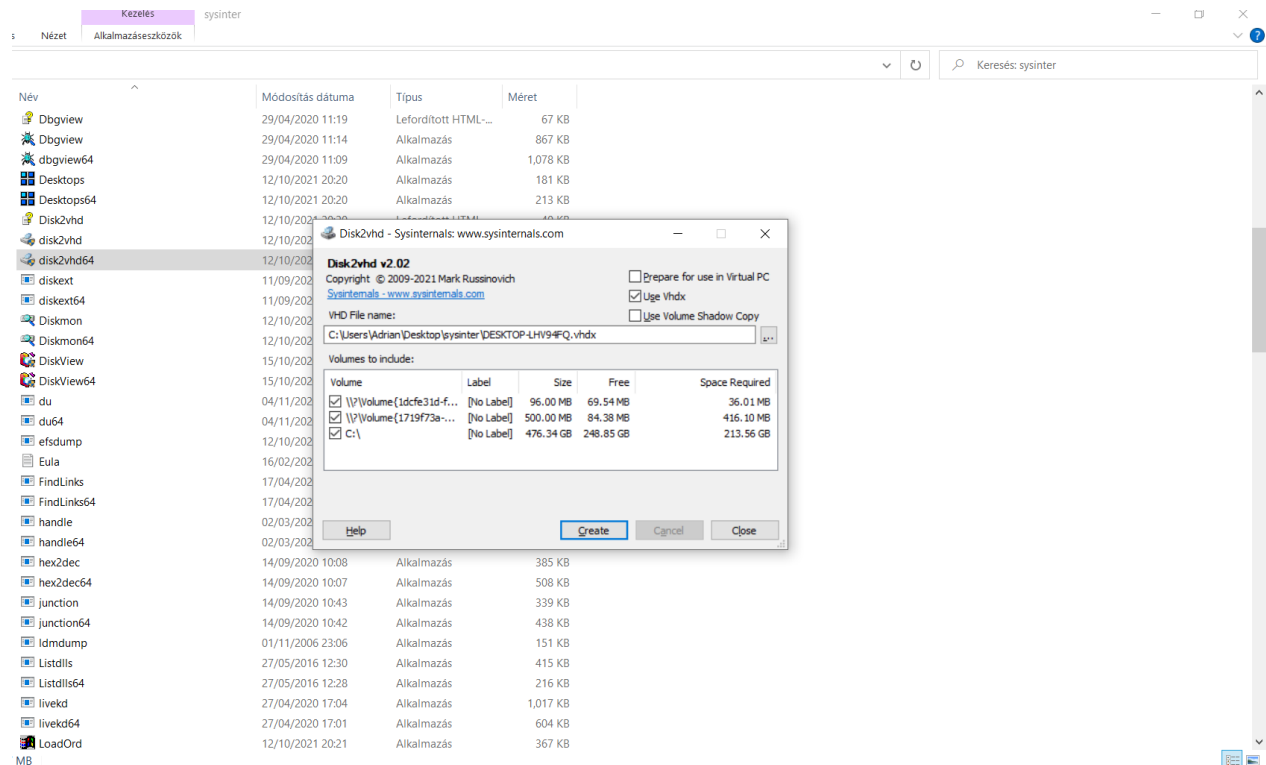
C:\UYSE1L>sort < fa\felsorolas.txt
Berki Viktor
David Rebeke
Keresztes Iulia
Kormos Balazs
Szabo Alen
C:\UYSE1L>
```

2. feladat – Töltse le a megadott programokat, majd futtassa őket..

a, Disk2vhd

Leírás:

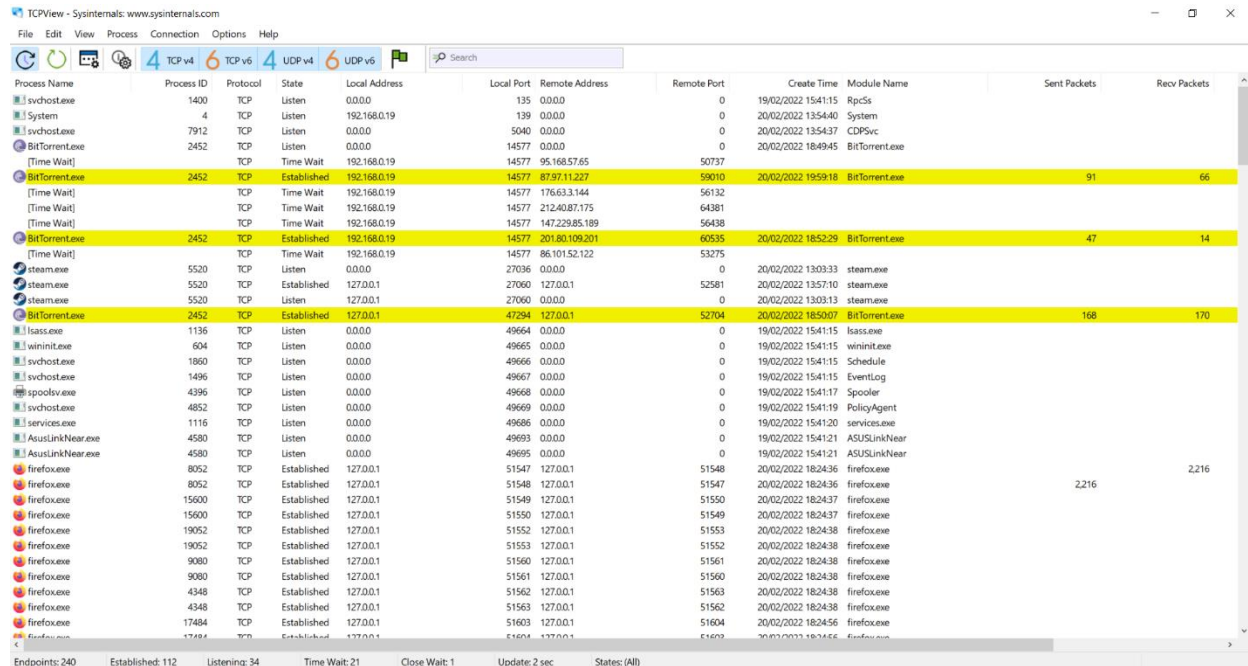
A program a kiválasztott fizikai lemezekhez létrehoz egy virtuális merevlemez.



b, TCPView

Leírás:

A TCPView program egy bizonyos felsorolást mutat a számítógépen futó processzekről, a TCP-kről és az UDP-kről, a processzek helyi és távoli ip címéről...



Process Name Process ID Protocol State Local Address Local Port Remote Address Remote Port Create Time Module Name Sent Packets Recv Packets

svchost.exe	1400	TCP	Listen	192.168.0.19	135	0.0.0.0	0	19/02/2022 15:41:15	RpcSs		
System	4	TCP	Listen	192.168.0.19	139	0.0.0.0	0	20/02/2022 13:54:40	System		
svchost.exe	7912	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	20/02/2022 13:54:37	CDPSvc		
BitTorrent.exe	2452	TCP	Time Wait	192.168.0.19	14577	95.168.57.65	50737	20/02/2022 18:49:45	BitTorrent.exe		
BitTorrent.exe	2452	TCP	Established	192.168.0.19	14577	87.97.11.227	59010	20/02/2022 19:59:18	BitTorrent.exe	91	66
[Time Wait]		TCP	Time Wait	192.168.0.19	14577	176.63.3.144	56132				
[Time Wait]		TCP	Time Wait	192.168.0.19	14577	212.40.87.175	64381				
[Time Wait]		TCP	Time Wait	192.168.0.19	14577	147.228.85.189	56438				
BitTorrent.exe	2452	TCP	Established	192.168.0.19	14577	201.80.109.201	60535	20/02/2022 18:52:29	BitTorrent.exe	47	14
[Time Wait]		TCP	Time Wait	192.168.0.19	14577	86.101.52.122	53275				
steam.exe	5520	TCP	Listen	0.0.0.0	27036	0.0.0.0	0	20/02/2022 13:03:33	steam.exe		
steam.exe	5520	TCP	Established	127.0.0.1	27060	127.0.0.1	52581	20/02/2022 13:57:10	steam.exe		
steam.exe	5520	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	20/02/2022 13:03:13	steam.exe		
BitTorrent.exe	2452	TCP	Established	127.0.0.1	47294	127.0.0.1	52704	20/02/2022 18:50:07	BitTorrent.exe	168	170
lsass.exe	1136	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	19/02/2022 15:41:15	lsass.exe		
wininit.exe	604	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	19/02/2022 15:41:15	wininit.exe		
svchost.exe	1860	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	19/02/2022 15:41:15	Schedule		
svchost.exe	1496	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	19/02/2022 15:41:15	EventLog		
spoolsv.exe	4396	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	19/02/2022 15:41:17	Spooler		
svchost.exe	4852	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	19/02/2022 15:41:19	PolicyAgent		
services.exe	1116	TCP	Listen	0.0.0.0	49686	0.0.0.0	0	19/02/2022 15:41:20	services.exe		
ASUSLinkNear.exe	4580	TCP	Listen	0.0.0.0	49693	0.0.0.0	0	19/02/2022 15:41:21	ASUSLinkNear		
ASUSLinkNear.exe	4580	TCP	Listen	0.0.0.0	49695	0.0.0.0	0	19/02/2022 15:41:21	ASUSLinkNear		
firefox.exe	8052	TCP	Established	127.0.0.1	51547	127.0.0.1	51548	20/02/2022 18:24:36	firefox.exe		
firefox.exe	8052	TCP	Established	127.0.0.1	51548	127.0.0.1	51547	20/02/2022 18:24:36	firefox.exe	2,216	2,216
firefox.exe	15600	TCP	Established	127.0.0.1	51549	127.0.0.1	51550	20/02/2022 18:24:37	firefox.exe		
firefox.exe	15600	TCP	Established	127.0.0.1	51550	127.0.0.1	51549	20/02/2022 18:24:37	firefox.exe		
firefox.exe	19052	TCP	Established	127.0.0.1	51552	127.0.0.1	51553	20/02/2022 18:24:38	firefox.exe		
firefox.exe	19052	TCP	Established	127.0.0.1	51553	127.0.0.1	51552	20/02/2022 18:24:38	firefox.exe		
firefox.exe	9080	TCP	Established	127.0.0.1	51560	127.0.0.1	51561	20/02/2022 18:24:38	firefox.exe		
firefox.exe	9080	TCP	Established	127.0.0.1	51561	127.0.0.1	51560	20/02/2022 18:24:38	firefox.exe		
firefox.exe	4348	TCP	Established	127.0.0.1	51562	127.0.0.1	51563	20/02/2022 18:24:38	firefox.exe		
firefox.exe	4348	TCP	Established	127.0.0.1	51563	127.0.0.1	51562	20/02/2022 18:24:38	firefox.exe		
firefox.exe	17484	TCP	Established	127.0.0.1	51603	127.0.0.1	51604	20/02/2022 18:24:56	firefox.exe		
firefox.exe	17484	TCP	Established	127.0.0.1	51604	127.0.0.1	51603	20/02/2022 18:24:56	firefox.exe		

Endpoints: 240 Established: 112 Listening: 34 Time Wait: 21 Close Wait: 1 Update: 2 sec States: (All)

c, Process Explorer

Leírás:

A process explorer megmutatja, hogy mely processzek aktívak, és ezekhez milyen további processzek töltődnek be. Továbbá jelzi a CPU használatot, memória használatot.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-LHV94FQ\Adrian]

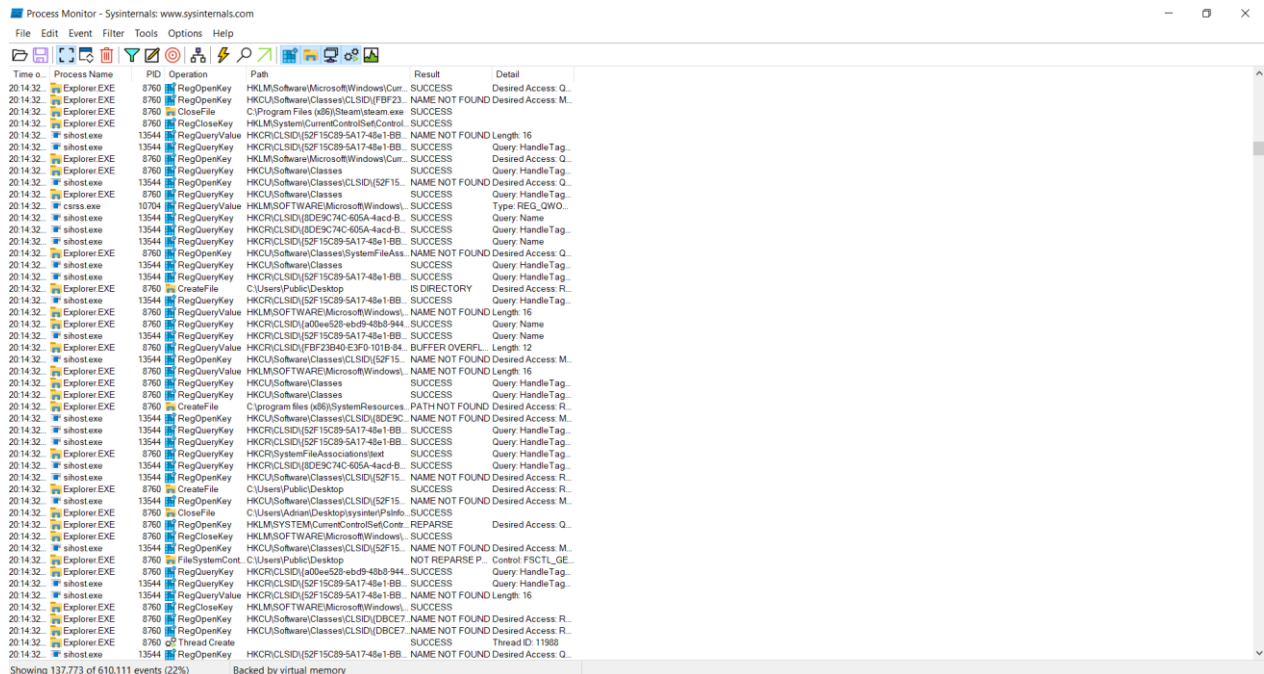
FileOptionsViewProcessFindUsersHelp

<

d, Process monitor

Leírás:

A process monitor valós idejűen jeleníti meg a fájlrendszert, a beállításjegyzéket (operation), az elérési útvonalat (path), illetve az ellenőrzés eredményét (result).



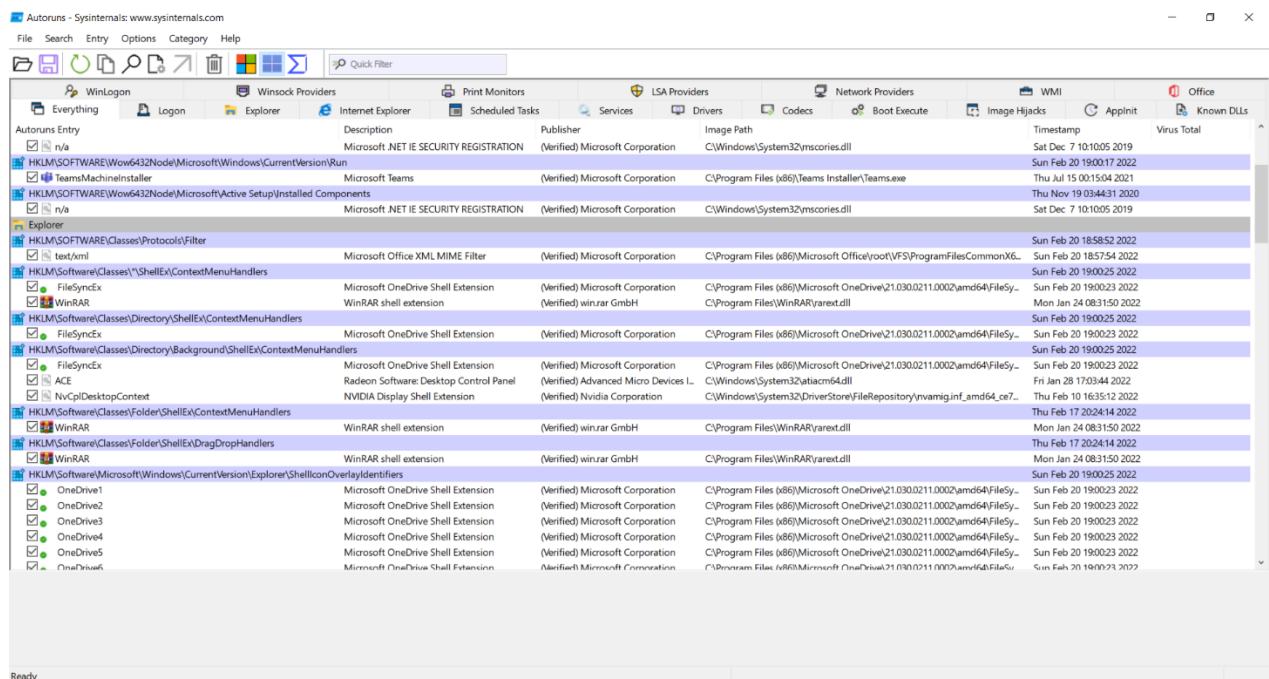
The screenshot shows the Process Monitor application window. The main pane displays a list of events with columns for Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show only those related to the Explorer.exe process. The list includes various operations such as RegOpenKey, RegCloseKey, RegQueryValue, and FileOpen, with details like the path and the result of the operation.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
2014.12.12 14:32	Explorer.exe	8760	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Q...
2014.12.12 14:32	Explorer.exe	8760	RegOpenKey	HKCU\Software\Classes\CLSID\{F0F3F3F3-F0F3-F0F3-F0F3-F0F3}	NAME NOT FOUND	Desired Access: M...
2014.12.12 14:32	Explorer.exe	8760	CloseFile	C:\Program Files (x86)\Steam\steam.exe	SUCCESS	
2014.12.12 14:32	Explorer.exe	8760	RegCloseKey	HKLM\System\CurrentControlSet\Control\...	SUCCESS	
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKLM\Software\Microsoft\Windows\...	SUCCESS	Desired Access: Q...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCU\Software\Classes\CLSID\{52F15...	NAME NOT FOUND	Desired Access: Q...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Name
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCU\Software\Classes\SystemFileAss...	NAME NOT FOUND	Desired Access: Q...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	8760	CreateFile	C:\Users\Public\Desktop	IS DIRECTORY	Desired Access: R...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKLM\Software\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: M...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCR\CLSID\{a00e528-ebd9-48b6-944...	SUCCESS	Query: Name
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Name
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCR\CLSID\{F0F3F3F3-F0F3-F0F3-F0F3-F0F3}	NAME NOT FOUND	Desired Access: M...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKLM\Software\Classes	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	C:\Program Files (x86)\SystemResources	PATH NOT FOUND	Desired Access: R...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCU\Software\Classes\CLSID\{BDEC...	NAME NOT FOUND	Desired Access: M...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCR\Software\Classes\CLSID\{52F15...	NAME NOT FOUND	Desired Access: R...
2014.12.12 14:32	shost.exe	13544	CreateFile	C:\Users\Public\Desktop	SUCCESS	Desired Access: R...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCU\Software\Classes\CLSID\{52F15...	NAME NOT FOUND	Desired Access: M...
2014.12.12 14:32	shost.exe	8760	CloseFile	C:\Users\Adrian\Desktop\sysinternals\PsInfo...	SUCCESS	
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Cont...	REPARSE	Desired Access: Q...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKLM\Software\Microsoft\Windows\...	SUCCESS	
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCU\Software\Classes\CLSID\{52F15...	NAME NOT FOUND	Desired Access: M...
2014.12.12 14:32	shost.exe	8760	FileSystemCont...	C:\Users\Public\Desktop	NOT REPARSE P...	Control: FSCTL_GE...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCR\CLSID\{a00e528-ebd9-48b6-944...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	SUCCESS	Query: Handle Tag...
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	NAME NOT FOUND	Length: 16
2014.12.12 14:32	shost.exe	8760	RegCloseKey	HKLM\Software\Microsoft\Windows\...	SUCCESS	
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCU\Software\Classes\CLSID\{BDEC7...	NAME NOT FOUND	Desired Access: R...
2014.12.12 14:32	shost.exe	8760	RegOpenKey	HKCU\Software\Classes\CLSID\{BDEC7...	NAME NOT FOUND	Desired Access: R...
2014.12.12 14:32	shost.exe	8760	Thread Create		SUCCESS	Thread ID: 11988
2014.12.12 14:32	shost.exe	13544	RegOpenKey	HKCR\CLSID\{52F15C89-5A17-48a1-B8...	NAME NOT FOUND	Desired Access: Q...

e, Autoruns

Leírás:

A program a rendszerindításkor automatikusan elinduló programokat kezeli, jeleníti meg. Ezek lehetnek manuálisan telepített- vagy beépített windows alkalmazások.



The screenshot shows the Autoruns application window. The main pane displays a list of system services and startup items with columns for Name, Description, Publisher, Image Path, and Timestamp. The list includes various services such as WinLogon, Winsock Providers, Internet Explorer, and Print Monitors. The list is filtered to show only those related to the Explorer.exe process.

Name	Description	Publisher	Image Path	Timestamp
WinLogon	WinLogon	Microsoft Corporation	C:\Windows\System32\winlogon.dll	Sat Dec 7 10:10:05 2019
Winsock Providers	Winsock Providers	Microsoft Corporation	C:\Windows\System32\winsock.dll	Sun Feb 20 18:58:52 2022
Internet Explorer	Internet Explorer	Microsoft Corporation	C:\Program Files (x86)\Internet Explorer\iexplore.exe	Sun Feb 20 18:57:54 2022
Print Monitors	Print Monitors	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Services	Services	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Drivers	Drivers	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Codecs	Codecs	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Boot Execute	Boot Execute	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Image Hijacks	Image Hijacks	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
WMI	WMI	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Appinit	Appinit	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Office	Office	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022
Known DLLs	Known DLLs	Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF\ProgramFilesCommonX64\...	Sun Feb 20 19:00:25 2022

f, LogonSession

Leírás:

Listát jelenít meg a jelenleg aktív bejelentkezési munkamenetekről. A -p beállítással pedig a munkamenetekben futó folyamatokat is listázza.

```
Administrator: Parancssor
C:\Users\Adrian\Desktop>sysinter\logonsessions

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-LHV94FQ$
    Auth package: NTLM
    Logon type:   (none)
    Session:     0
    Sid:         S-1-5-18
    Logon time:   19/02/2022 15:41:14
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000f789:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:     0
    Sid:         (none)
    Logon time:   19/02/2022 15:41:14
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:0000fb5f:
    User name:   Font Driver Host\UPFD-0
    Auth package: Negotiate
    Logon type:   Interactive
    Session:     0
    Sid:         S-1-5-96-0-0
    Logon time:   19/02/2022 15:41:14
    Logon server:
    DNS Domain:
    UPN:

[3] Logon session 00000000:0000fb6f:
    User name:   Font Driver Host\UPFD-1
    Auth package: Negotiate
    Logon type:   Interactive
    Session:     1
    Sid:         S-1-5-96-0-1
    Logon time:   19/02/2022 15:41:14
    Logon server:
    DNS Domain:
```

```
Administrator: Parancssor
Microsoft Windows [Version 10.0.19042.1526]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Windows\system32>cd C:\Users\Adrian\Desktop>sysinter

C:\Users\Adrian\Desktop>sysinter\logonsessions -p

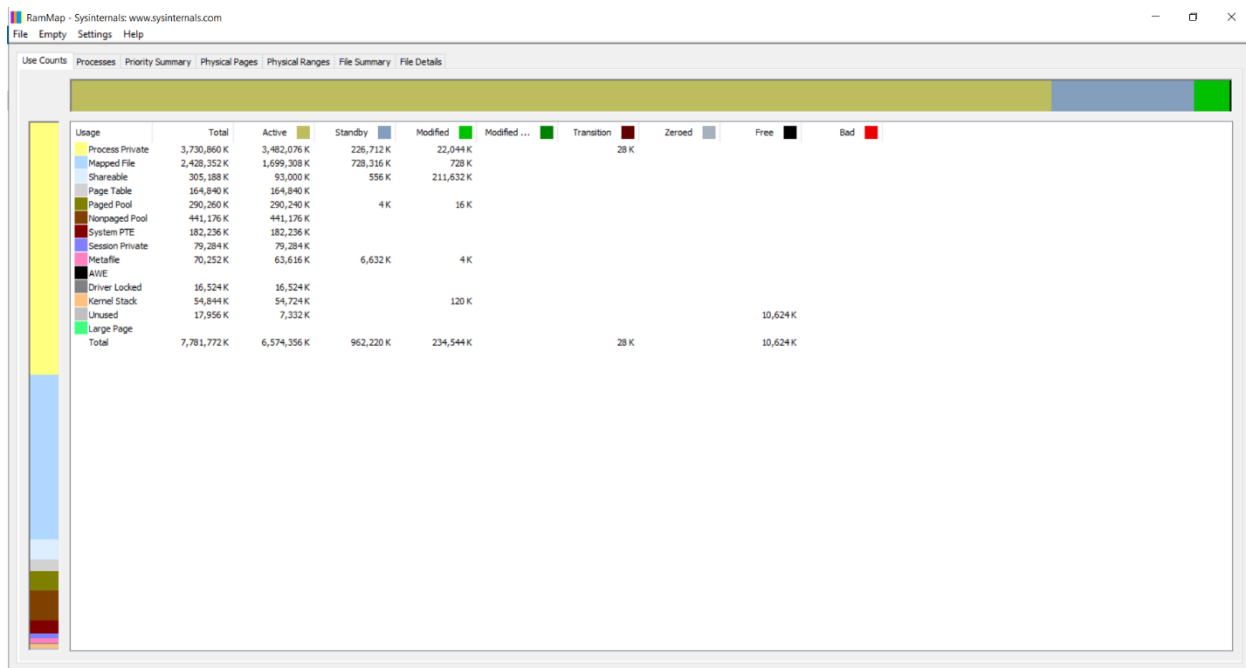
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name:   WORKGROUP\DESKTOP-LHV94FQ$
    Auth package: NTLM
    Logon type:   (none)
    Session:     0
    Sid:         S-1-5-18
    Logon time:   19/02/2022 15:41:14
    Logon server:
    DNS Domain:
    UPN:
    1136: lsass.exe
    1268: svchost.exe
    1448: svchost.exe
    1776: svchost.exe
    1860: svchost.exe
    1968: svchost.exe
    1996: svchost.exe
    980:  svchost.exe
    2076: svchost.exe
    2404: svchost.exe
    2516: WdDisplay.Container.exe
    2640: svchost.exe
    2756: atiesrxx.exe
    2768: svchost.exe
    2256: svchost.exe
    2400: svchost.exe
    3196: svchost.exe
    3260: svchost.exe
    3432: svchost.exe
    4252: svchost.exe
    4332: svchost.exe
    4340: AsusOptimization.exe
    4396: spoolsv.exe
    4820: WmiPrvSE.exe
    4832: svchost.exe
    5112: AsusAppService.exe
    4508: AsusLinkRemote.exe
    4460: AsusSoftwareManager.exe
```

g, RAMMap

Leírás:

A rendszer memóriahasználatát jellemzi, többféle leírást ad róla. Például a memóriacímeket, a fájlok adatait a memóriában, fájlként.



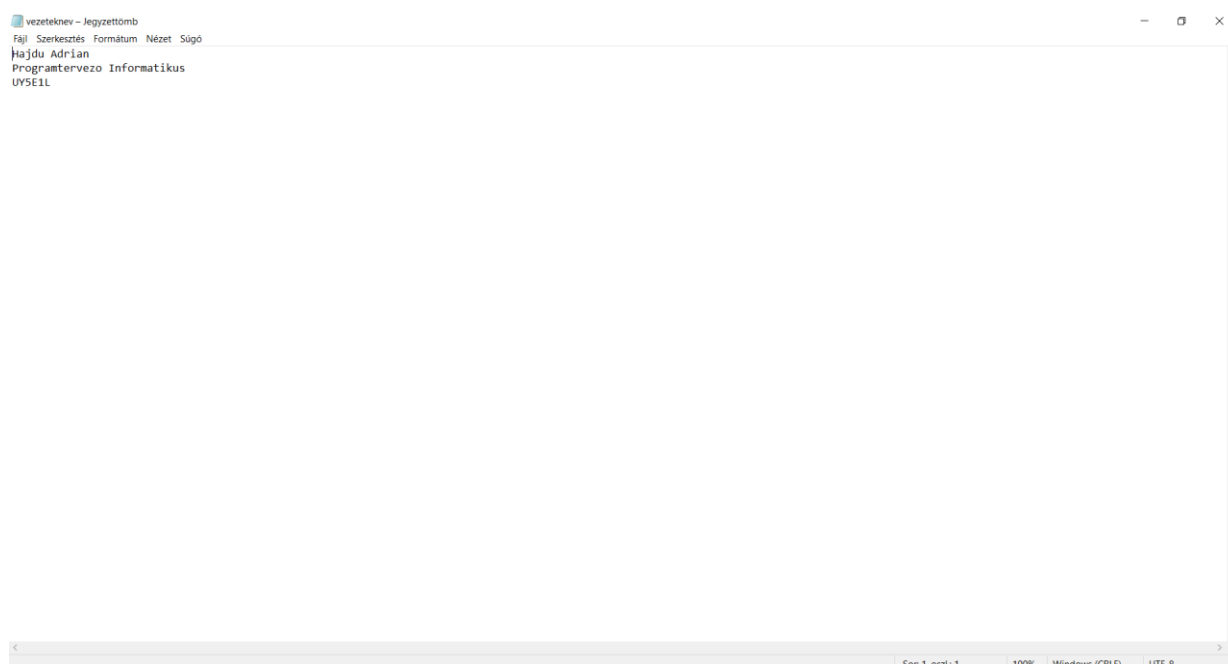
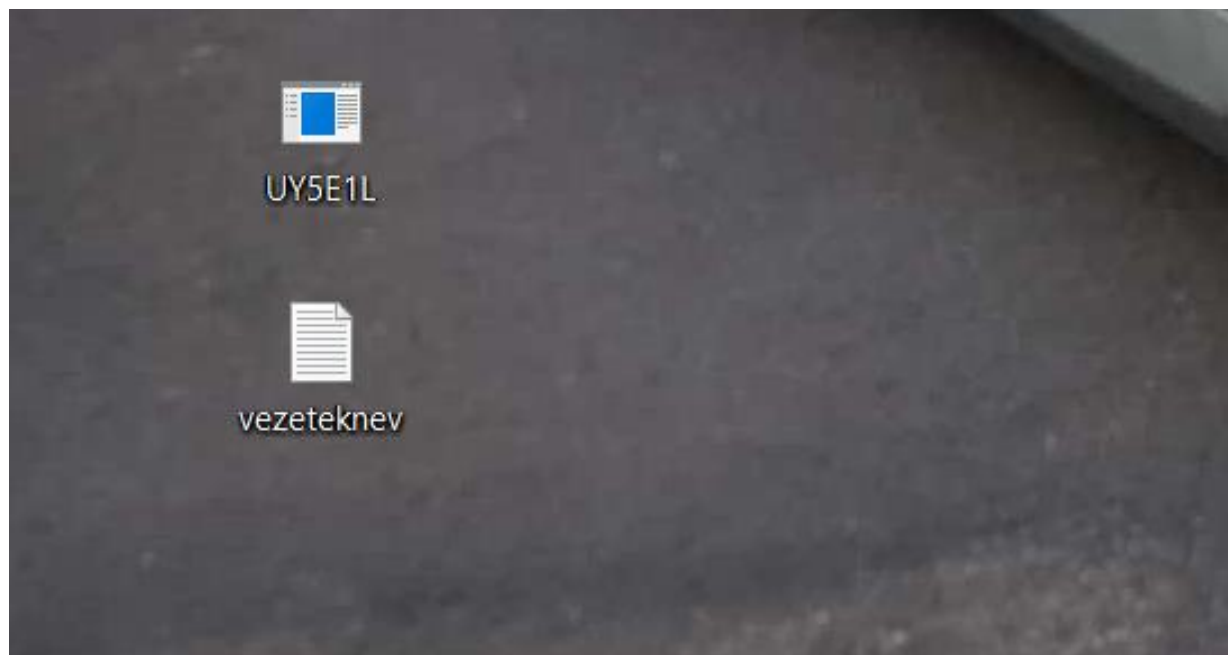
3. feladat – Töltse le a következő programot: Dependency Walker...

a, Készítsen C programot, mely létrehoz egy fájlt, majd olvassa.

The screenshot shows the Code::Blocks IDE with a C program open in the editor. The program is named 'main.c' and is located in the 'main0' project. The code is as follows:

```
1 #include <stdio.h>
2 #include <stdlib.h>
3
4 int main()
5 {
6     FILE *fp;
7
8     fp = fopen("vezeteknev.txt", "w+");
9
10    fprintf(fp, "Hajdu Adrian\n");
11    fprintf(fp, "Programtervező Informatikus\n");
12    fprintf(fp, "UYSEIL\n");
13
14    fclose(fp);
15    return 0;
16 }
17
```

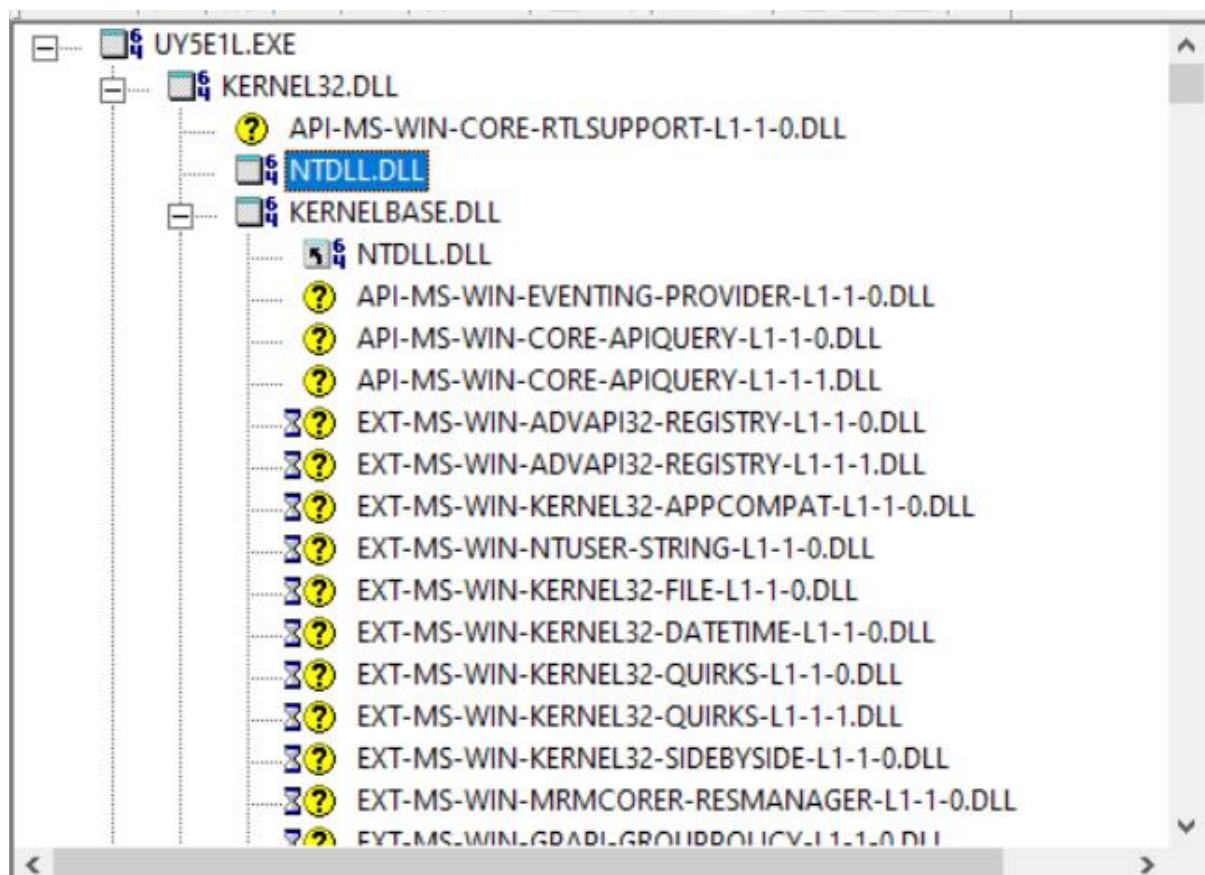
The output window at the bottom shows the execution results. It indicates that the program was terminated with status -1073741810 (0 minute(s), 1 second(s)).



b, Vizsgálja meg, hogy a program milyen api hívásokat használ a kernel32.dll-ből!



c, Mire jó az ntdll.dll?



Az NTDLL.DLL kernel függvényeket tartalmaz, amelyek elősegítik az operációs rendszer megfelelő működését.