

Operációs Rendszerek BSc

2. Gyak.

2022. 02. 14

Készítette:

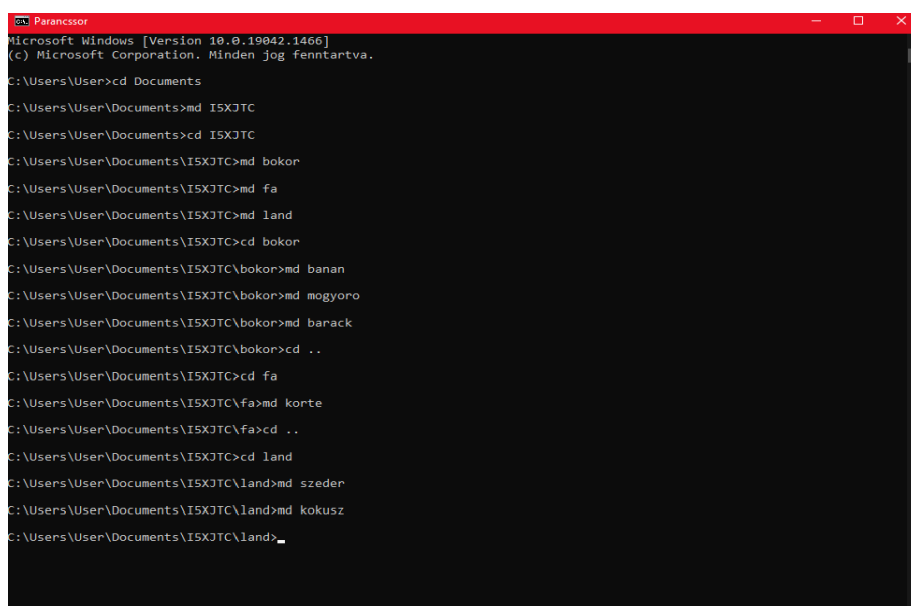
Katona Bence

Programtervezőinformatikus

I5XJTC

1.a. - Hozza létre a következő mappa szerkezetet!
neptunkod

```
|  
|- bokor  
|   |- banan  
|   |- mogyoro  
|   |- barack  
|- fa  
|   |- korte  
|- land  
    |- szeder  
    |- kokusz
```

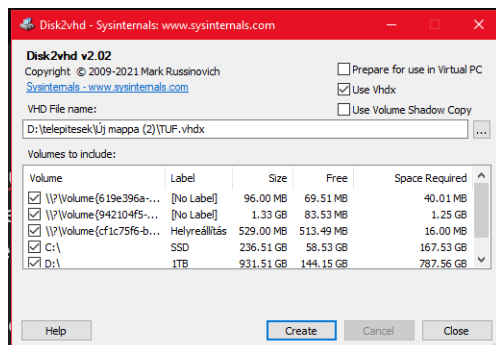


```
Microsoft Windows [Version 10.0.19042.1466]  
(c) Microsoft Corporation. Minden jog fenntartva.  
C:\Users\User>cd Documents  
C:\Users\User\Documents>md ISXJTC  
C:\Users\User\Documents>cd ISXJTC  
C:\Users\User\Documents\ISXJTC>md bokor  
C:\Users\User\Documents\ISXJTC>md fa  
C:\Users\User\Documents\ISXJTC>md land  
C:\Users\User\Documents\ISXJTC>cd bokor  
C:\Users\User\Documents\ISXJTC\bokor>md banan  
C:\Users\User\Documents\ISXJTC\bokor>md mogyoro  
C:\Users\User\Documents\ISXJTC\bokor>md barack  
C:\Users\User\Documents\ISXJTC\bokor>cd ..  
C:\Users\User\Documents\ISXJTC>cd fa  
C:\Users\User\Documents\ISXJTC\fa>md korte  
C:\Users\User\Documents\ISXJTC\fa>cd ..  
C:\Users\User\Documents\ISXJTC>cd land  
C:\Users\User\Documents\ISXJTC\land>md szeder  
C:\Users\User\Documents\ISXJTC\land>md kokusz  
C:\Users\User\Documents\ISXJTC\land>
```

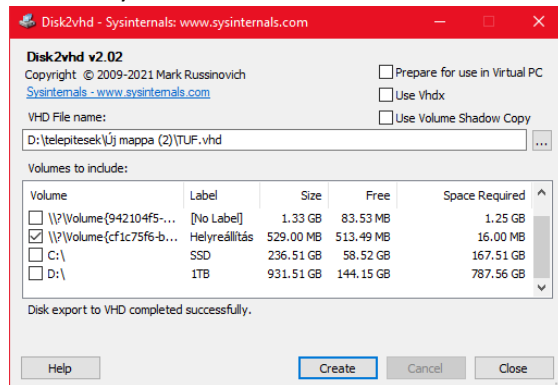
1.b. –

2.a. - Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít. A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el: a) File and Disk Utilities (Disk2vhd)

Virtuális merev lemezt hozz létre

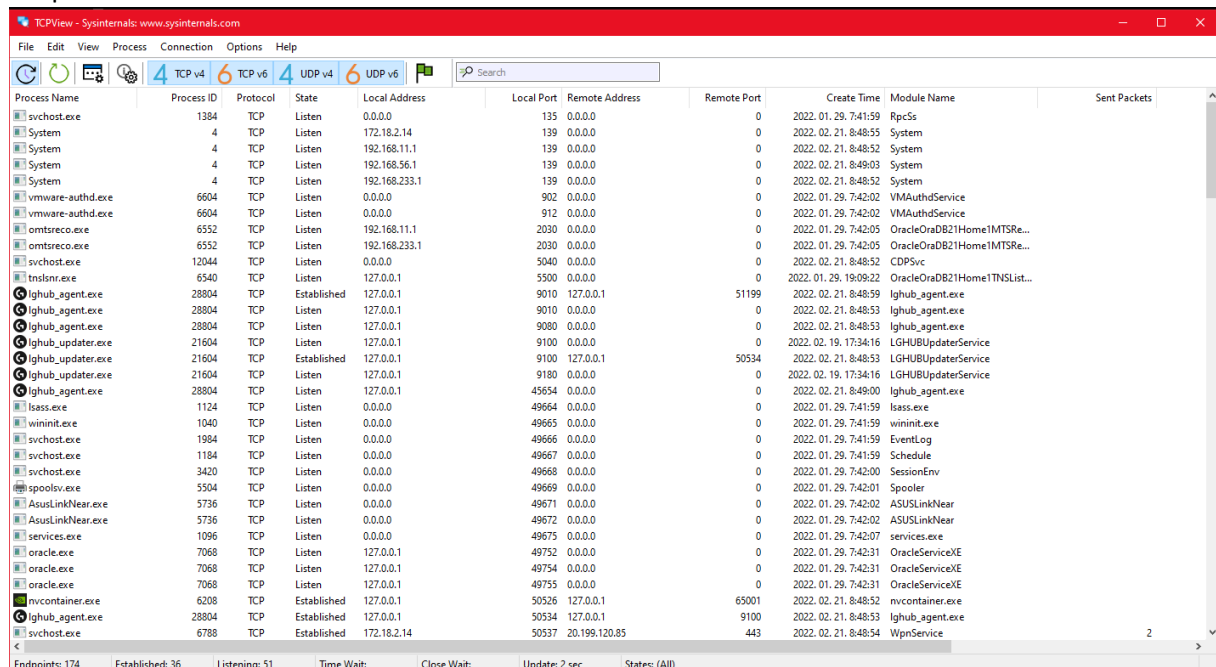


Eredmény:



2.b. - b) Networking Utilities (TCPView)

Megmutat egy listát amiben az UDP és TCP végpontok részletesen le vannak írva, beleértve a nevét, állapotát és a címét



2.c - c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)

A process explorer olyan mint a task manager csak annál több adatot jelenít meg, kilistázza a futó programokat és tulajdonságait

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		20 428 K	73 440 K	148		
System Idle Process	97.97	60 K	8 K	0		
System	0.13	196 K	32 K	4		
Interrupts	0.51	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 068 K	588 K	912		
csrss.exe		2 944 K	533 572 K	3596		
wininit.exe		2 240 K	2 828 K	1008		
services.exe		2 128 K	3 568 K	1040		
svchost.exe		11 108 K	12 952 K	1096		
svchost.exe		86 432 K	80 280 K	1252	Windows-szolgáltatások gaz...	Microsoft Corporation
WmPrvSE.exe	< 0.01	15 272 K	9 904 K	4196		
dlh.exe		3 960 K	4 144 K	11840		
MoUsCoreWorker.exe		119 020 K	88 684 K	4148		
unsecapp.exe		1 824 K	2 860 K	15684		
WmPrvSE.exe		22 276 K	22 332 K	604		
StartMenuExperienceHost.exe	< 0.01	56 296 K	93 840 K	9804		
RuntimeBroker.exe		6 180 K	25 356 K	35436	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	174 472 K	243 292 K	26680	Search application	Microsoft Corporation
RuntimeBroker.exe		12 244 K	40 064 K	38328	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	56 280 K	45 520 K	38332		Microsoft Corporation
SettingSyncHost.exe		7 268 K	7 632 K	22824	Host Process for Setting Syn...	Microsoft Corporation
ShellExperienceHost.exe		14 184 K	55 576 K	30032	Windows Shell Experience H...	Microsoft Corporation
LockApp.exe	Susp...	34 180 K	48 180 K	24848	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		7 396 K	26 320 K	33984	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		10 504 K	36 272 K	17748	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 480 K	21 868 K	24828	Runtime Broker	Microsoft Corporation
TextInputHost.exe	< 0.01	32 132 K	48 072 K	5204		Microsoft Corporation
amsmiscreen.exe		8 372 K	23 600 K	27620	Windows Defender SmartScr...	Microsoft Corporation
Cortana.exe	< 0.01	54 940 K	69 872 K	30108	Cortana	Microsoft Corporation

CPU Usage: 2.02% Commit Charge: 56.31% Processes: 265 Physical Usage: 55.54%

A process monitor egy olyan program ami listázza a valós idejű file szerkezetet, a registry és a process aktivitását

Time	Process Name	PID	Operation	Path	Result	Detail
9:37.1	smss.exe	2180	ReadFile	D:\telepesek\U\mapa\Q\Procom64	SUCCESS	Offset: 1 441 792.
9:37.1	smss.exe	1124	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 607 600.
9:37.1	smss.exe	1124	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 591 296.
9:37.1	smss.exe	2180	ReadFile	D:\telepesek\U\mapa\Q\Procom64	SUCCESS	Offset: 1 507 328.
9:37.1	smss.exe	1124	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 513 844.
9:37.1	smss.exe	1124	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 579 008.
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query Name
9:37.1	Explorer.exe	2180	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 198 976.
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query HandleTag
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query HandleTag
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: R...
9:37.1	Explorer.exe	1426	RegOpenKey	D:\telepesek\U\mapa\Q\Procom64	SUCCESS	Offset: 1 572 864.
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query Name
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query HandleTag
9:37.1	smss.exe	1124	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 497 600.
9:37.1	Explorer.exe	2180	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 170 304.
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query Name
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: R...
9:37.1	Explorer.exe	1426	RegOpenKey	HKEY_CURRENT_USER\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: R...
9:37.1	Explorer.exe	1426	RegOpenKey	D:\telepesek\U\mapa\Q\Procom64	SUCCESS	CreationTime: 202...
9:37.1	smss.exe	1124	QueryNameInfo	D:\telepesek\U\mapa\Q\Procom64	SUCCESS	Name: telepesek...
9:37.1	smss.exe	1124	QueryNameInfo	D:\telepesek\U\mapa\Q\Procom64	SUCCESS	Name: telepesek...
9:37.1	smss.exe	2180	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 133 440.
9:37.1	Explorer.exe	1426	QueryStandard	C:\Users\User\AppData\Local\Microsoft...	SUCCESS	LocationSize: 3.7...
9:37.1	Explorer.exe	1426	ReadFile	C:\Users\User\AppData\Local\Microsoft...	SUCCESS	Offset: 3 055 616.
9:37.1	smss.exe	2180	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 2 899 968.
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query HandleTag
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Desired Access: R...
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query HandleTag
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Desired Access: R...
9:37.1	smss.exe	2180	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query HandleTag
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Desired Access: Q...
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Type: REG_DWORD
9:37.1	smss.exe	2180	UnlockFileSingle	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124 Length...
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Offset: 1 638 400.
9:37.1	smss.exe	2180	ReadFile	D:\telepesek\U\mapa\Q\Procom64	SUCCESS	Query HandleTag
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	CreationTime: 202...
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	NAME NOT FOUND	Desired Access: Q...
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	
9:37.1	smss.exe	5936	RegOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	

Showing 314 174 of 1 117 337 events (46%) Backed by virtual memory

Az Autoruns program megmutatja hogy mely programok vannak úgy beállítva hogy a rendszer felálltakor felálljon

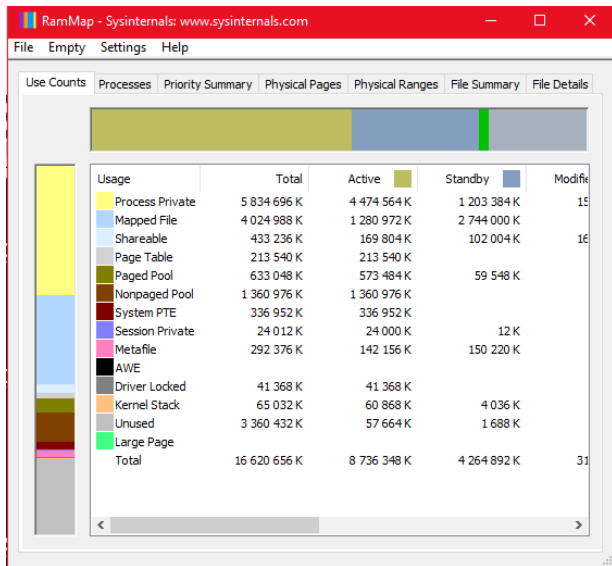
Name	Description	Publisher	Image Path	Timestamp
Logon				
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Tue Feb 1 10:12:58 2022
Adobe Reader Synchronizer	Adobe Collaboration Synchronizer 21.11	(Verified) Adobe Inc.	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollab...	Fri Dec 24 20:03:22 2021
DAEMON Tools Lite	DAEMON Tools Lite	(Verified) Disc Soft Ltd	C:\Program Files\DAEMON Tools Lite\DTAgent.exe	Mon Nov 21 13:01:56 2016
Gainet Net Updater	Gainet Net Updater	(Verified) Gainet Network Ltd	C:\Users\User\AppData\Local\Gainet\Program Files (x86)\NetAgent\gia...	Thu Dec 3 17:17:43 2020
LGHUB	LGHUB	(Verified) Logitech Inc	C:\Program Files\LGHUB\Lghub.exe	Sat Feb 19 10:50:37 2022
Microsoft Edge	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Sun Dec 19 16:06:26 2021
HP State Message Application	HP State Message Application	(Verified) Hewlett-Packard	C:\Program Files\HP\Shared\hpdlfe.exe	Sat Aug 29 12:02:00 2015
Logitech Gaming Framework	Logitech Gaming Framework	(Verified) Logitech Inc	C:\Program Files\Logitech Gaming Software\LCore.exe	Fri Oct 5 10:43:56 2018
Pentabilet Service	Pentabilet Service	(Verified) Guangzhou Ugee Comp...	C:\Program Files\Pentabilet\PentabiletService.exe	Mon Jul 20 16:33:02 2020
Vanguard tray notification	Vanguard tray notification	(Verified) Riot Games, Inc.	C:\Program Files\Riot Vanguard\vgtray.exe	Tue Nov 30 03:48:00 2021
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sat Dec 7 10:15:08 2019
Google Chrome	Google Chrome	(Verified) Google LLC	C:\Program Files (x86)\Google\Chrome\Application\98.0.4758.102\insta...	Sat May 15 02:22:00 2021
Microsoft Edge	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.56\Insta...	Sat Feb 19 08:33:53 2022
n/a	Microsoft .NET 10 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Dec 7 10:10:05 2019
Java Update Scheduler	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Sat May 15 02:32:01 2021
Acrobat Install On Demand	Acrobat Install On Demand	(Verified) Adobe Inc.	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Est\Aldt\ltdi.dll	Fri Apr 9 05:29:36 2021
n/a	Microsoft .NET 10 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Dec 7 10:10:05 2019

2.d - d) Security Utilities (LogonSession)

Nem fut le a program

2.e - e) Information Utilities (RAMMap)

Egy olyan alkalmazás ami kilistázza hogy a ramokat mik használják föl, mennyire használják és még számos adatot



3. Készítsen egy neptunkod.c nevű forráskódot, amely egy vezeteknev.txt fájl létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc.

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

int main()
{
    FILE *fp;
    fp = fopen("neptunkod.txt", "w");
    if (fp == NULL)
    {
        printf("Nem lehet létrehozni a fájlt!\n");
        return 1;
    }
    fprintf(fp, "Kutató neve: Szak neve: Neptunkod: Információk: stb.\n");
    fclose(fp);
    return 0;
}
```

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

