

Operációs rendszerek BSc

2. konzultáció gyakorlat

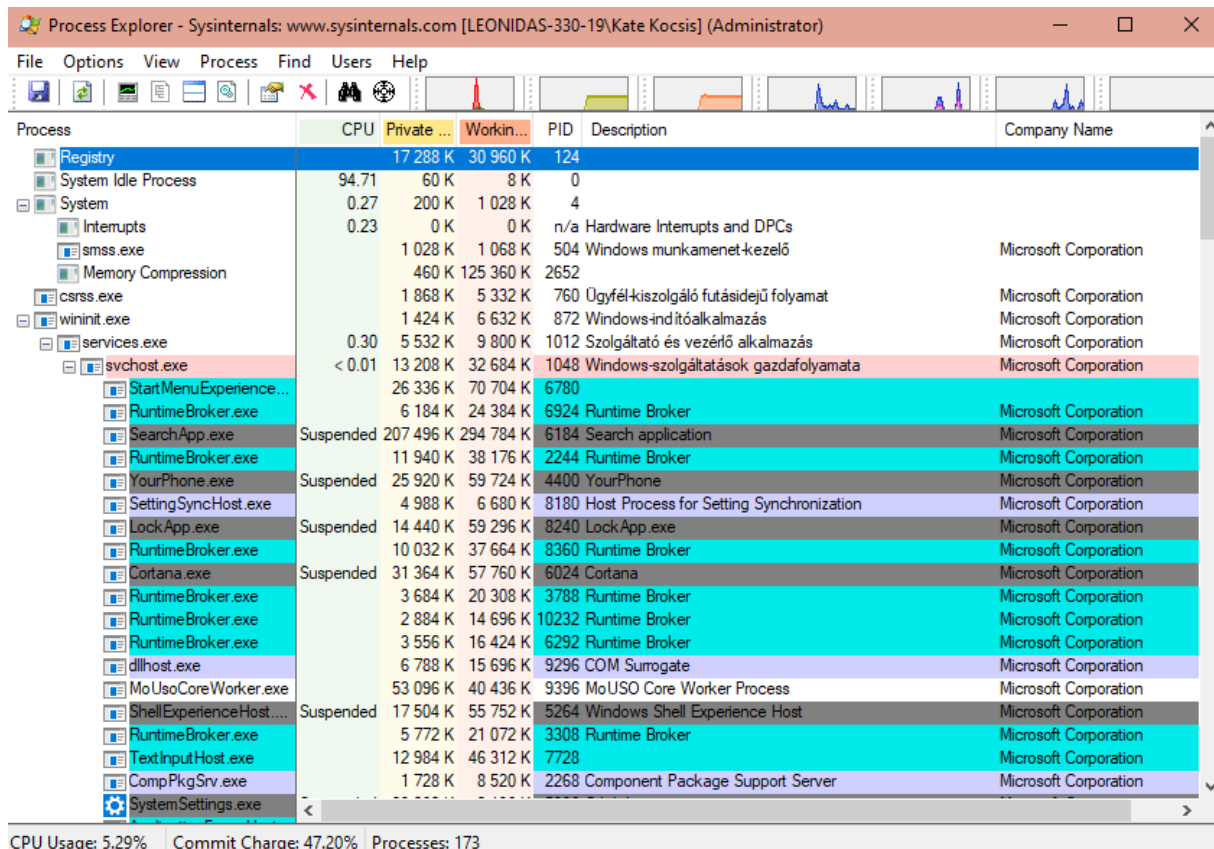
2021.02.26.

Készítette:
Kocsis Katalin Bsc
Mérnökinformatikus
WGOWUG

Miskolc, 2021

Operációs rendszerek – 3A. Gyakorlat

1. **Feladat:** Tölts le a *Sysinternals Suite* csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.



The screenshot shows the Process Explorer window from Sysinternals. The title bar reads 'Process Explorer - Sysinternals: www.sysinternals.com [LEONIDAS-330-19\Kate Kocsis] (Administrator)'. The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains icons for file operations, process management, and monitoring. The main window displays a list of processes with columns for Process, CPU, Private, Working Set, PID, Description, and Company Name. The 'Process' column is expanded, showing a tree view of system and user processes. The 'CPU' column shows usage percentages, and the 'Private' and 'Working Set' columns show memory usage in K. The 'PID' column shows the process ID, and the 'Description' column shows the process name and a brief description. The 'Company Name' column shows the manufacturer. The status bar at the bottom indicates 'CPU Usage: 5.29%', 'Commit Charge: 47.20%', and 'Processes: 173'.

Process	CPU	Private	Working Set	PID	Description	Company Name
Registry		17 288 K	30 960 K	124		
System Idle Process	94.71	60 K	8 K	0		
System	0.27	200 K	1 028 K	4		
Interrupts	0.23	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 028 K	1 068 K	504	Windows munkamenet-kezelő	Microsoft Corporation
Memory Compression		460 K	125 360 K	2652		
csrss.exe		1 868 K	5 332 K	760	Ügyfél-kiszolgáló futásidejű folyamat	Microsoft Corporation
wininit.exe		1 424 K	6 632 K	872	Windows-indítóalkalmazás	Microsoft Corporation
services.exe	0.30	5 532 K	9 800 K	1012	Szolgáltató és vezérlő alkalmazás	Microsoft Corporation
svchost.exe	< 0.01	13 208 K	32 684 K	1048	Windows-szolgáltatások gazdafolyamata	Microsoft Corporation
StartMenuExperience...		26 336 K	70 704 K	6780		
RuntimeBroker.exe		6 184 K	24 384 K	6924	Runtime Broker	Microsoft Corporation
SearchApp.exe	Suspended	207 496 K	294 784 K	6184	Search application	Microsoft Corporation
RuntimeBroker.exe		11 940 K	38 176 K	2244	Runtime Broker	Microsoft Corporation
YourPhone.exe	Suspended	25 920 K	59 724 K	4400	YourPhone	Microsoft Corporation
SettingSyncHost.exe		4 988 K	6 680 K	8180	Host Process for Setting Synchronization	Microsoft Corporation
LockApp.exe	Suspended	14 440 K	59 296 K	8240	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10 032 K	37 664 K	8360	Runtime Broker	Microsoft Corporation
Cortana.exe	Suspended	31 364 K	57 760 K	6024	Cortana	Microsoft Corporation
RuntimeBroker.exe		3 684 K	20 308 K	3788	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 884 K	14 696 K	10232	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 556 K	16 424 K	6292	Runtime Broker	Microsoft Corporation
dllhost.exe		6 788 K	15 696 K	9296	COM Surrogate	Microsoft Corporation
MoUsCoreWorker.exe		53 096 K	40 436 K	9396	MoUSO Core Worker Process	Microsoft Corporation
ShellExperienceHost...	Suspended	17 504 K	55 752 K	5264	Windows Shell Experience Host	Microsoft Corporation
RuntimeBroker.exe		5 772 K	21 072 K	3308	Runtime Broker	Microsoft Corporation
TextInputHost.exe		12 984 K	46 312 K	7728		Microsoft Corporation
CompPkgSrv.exe		1 728 K	8 520 K	2268	Component Package Support Server	Microsoft Corporation
SystemSettings.exe						

Letöltöttem a csomagot, kicsomagoltam, és áttanulmányoztam a Windows belső működését.

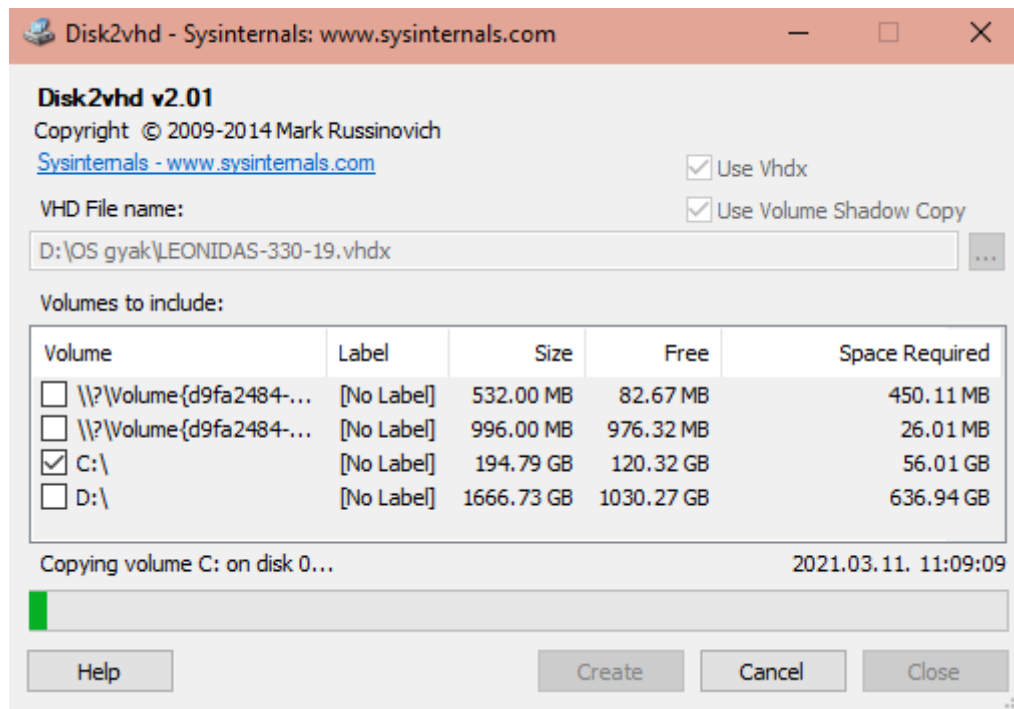
2. **Feladat:** A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

a) File and Disk Utilities (Disk2vhd)

Írja le a program szolgáltatásait:

Ez a program arra szolgál, hogy egy feltelepített rendszerből virtuális rendszert, képfájlt készít, amelyet tesztelésre, biztonsági mentésre, más gépekre való átvitelre vagy biztonsági probléma miatt izolált-tesztelésre használhatunk fel. Tehát .vhd kiterjesztésű Virtuális Meghajtókat készíthetünk (Virtual Hard Drive), akár úgy is, hogy közben fut a rendszer és aktívan használjuk azt. A kész képfájlt (képfájlokat) VirtualBox-al nyithatók meg.

Mentse el a megadott dokumentumba (képernyőkép):

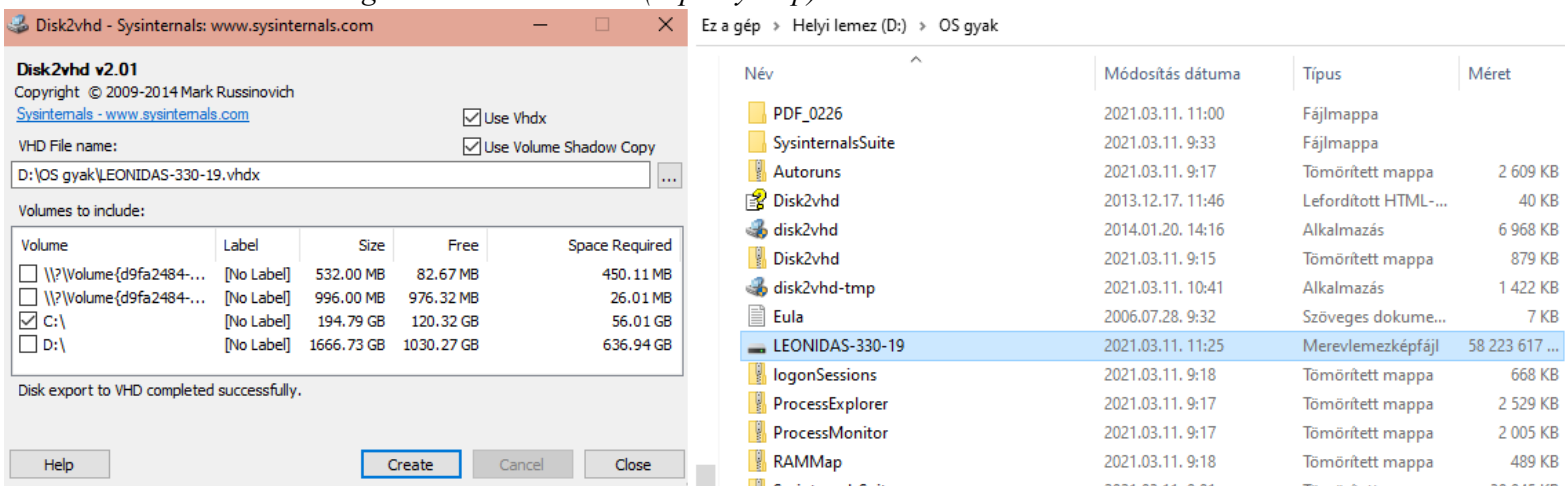


Megjegyzés: Én most csak a C meghajtóról készítek képfájlt, mert sok ideig tartana, ha a mindent bepipáltam volna, és túl sok területet vett volna el. A képen látszik, hogy a képfájl kb. felére nyomja össze, mint amekkora az eredeti.

Írja le a program futtatás eredményét:

A kiválasztott könyvtárba készített egy lemezképfájlt, a file neve pedig a gépem nevét kapta meg.

Mentse el a megadott dokumentumba (képernyőkép):

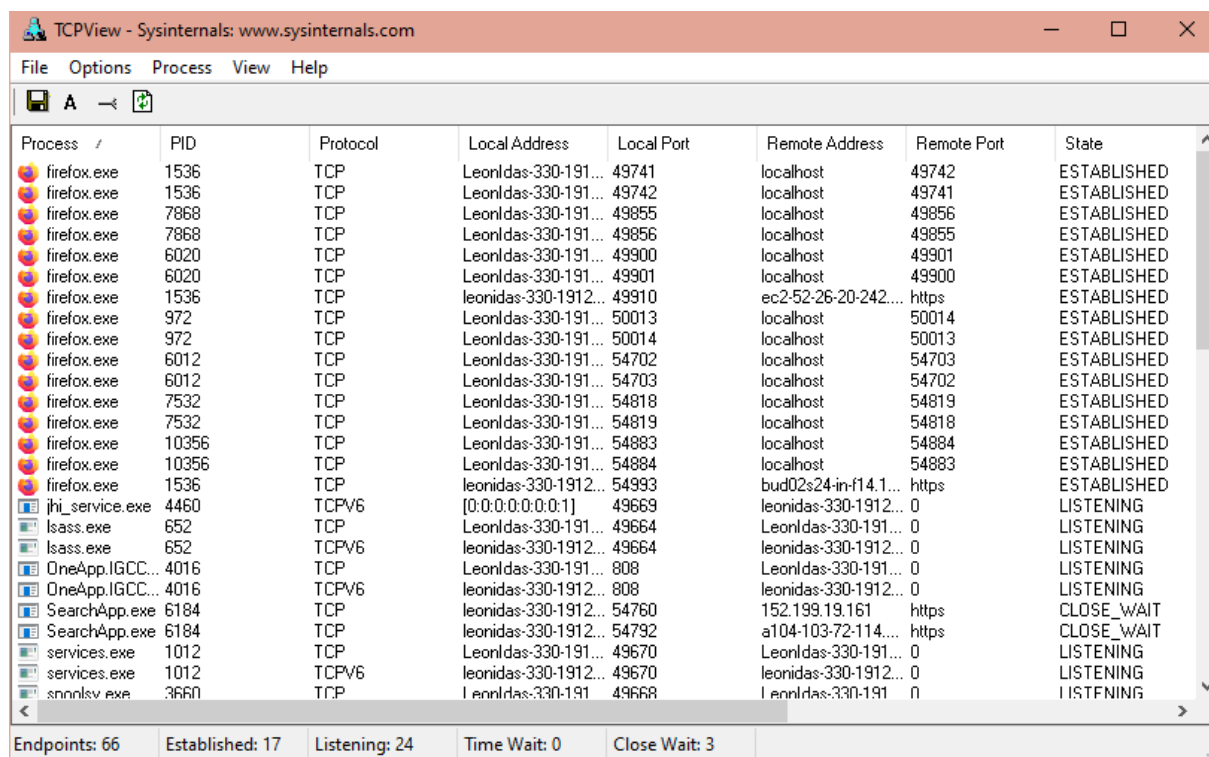


b) Networking Utilities (TCPView)

Írja le a program szolgáltatásait:

Ez egy hatékony segédprogram, amely a TCP és UDP végpontok széles listáját jeleníti meg a rendszeren. Az összes releváns információt több információs oszlopban jeleníti meg a folyamat, a PID, a protokoll, a helyi és a távoli cím, az elküldött csomagok, a fogadott csomagok stb. között. Lehetővé teszi az összes információ valós idejű megtekintését, hogy megőrizze frissítve az összes futó eljárással.

Mentse el a megadott dokumentumba (képernyőkép):



The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu is a toolbar with icons for saving, refreshing, and zooming. The main area is a table with the following columns: Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State. The table lists various processes and their network connections. At the bottom, there is a summary bar with the following data: Endpoints: 66, Established: 17, Listening: 24, Time Wait: 0, Close Wait: 3.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
firefox.exe	1536	TCP	Leonidas-330-191...	49741	localhost	49742	ESTABLISHED
firefox.exe	1536	TCP	Leonidas-330-191...	49742	localhost	49741	ESTABLISHED
firefox.exe	7868	TCP	Leonidas-330-191...	49855	localhost	49856	ESTABLISHED
firefox.exe	7868	TCP	Leonidas-330-191...	49856	localhost	49855	ESTABLISHED
firefox.exe	6020	TCP	Leonidas-330-191...	49900	localhost	49901	ESTABLISHED
firefox.exe	6020	TCP	Leonidas-330-191...	49901	localhost	49900	ESTABLISHED
firefox.exe	1536	TCP	leonidas-330-1912...	49910	ec2-52-26-20-242...	https	ESTABLISHED
firefox.exe	972	TCP	Leonidas-330-191...	50013	localhost	50014	ESTABLISHED
firefox.exe	972	TCP	Leonidas-330-191...	50014	localhost	50013	ESTABLISHED
firefox.exe	6012	TCP	Leonidas-330-191...	54702	localhost	54703	ESTABLISHED
firefox.exe	6012	TCP	Leonidas-330-191...	54703	localhost	54702	ESTABLISHED
firefox.exe	7532	TCP	Leonidas-330-191...	54818	localhost	54819	ESTABLISHED
firefox.exe	7532	TCP	Leonidas-330-191...	54819	localhost	54818	ESTABLISHED
firefox.exe	10356	TCP	Leonidas-330-191...	54883	localhost	54884	ESTABLISHED
firefox.exe	10356	TCP	Leonidas-330-191...	54884	localhost	54883	ESTABLISHED
firefox.exe	1536	TCP	leonidas-330-1912...	54993	bud02s24-in-f14.1...	https	ESTABLISHED
jhi_service.exe	4460	TCPV6	[0:0:0:0:0:0:1]	49669	leonidas-330-1912...	0	LISTENING
lsass.exe	652	TCP	Leonidas-330-191...	49664	Leonidas-330-191...	0	LISTENING
lsass.exe	652	TCPV6	leonidas-330-1912...	49664	leonidas-330-1912...	0	LISTENING
OneApp.IGCC...	4016	TCP	Leonidas-330-191...	808	Leonidas-330-191...	0	LISTENING
OneApp.IGCC...	4016	TCPV6	leonidas-330-1912...	808	leonidas-330-1912...	0	LISTENING
SearchApp.exe	6184	TCP	leonidas-330-1912...	54760	152.199.19.161	https	CLOSE_WAIT
SearchApp.exe	6184	TCP	leonidas-330-1912...	54792	a104-103-72-114...	https	CLOSE_WAIT
services.exe	1012	TCP	Leonidas-330-191...	49670	Leonidas-330-191...	0	LISTENING
services.exe	1012	TCPV6	leonidas-330-1912...	49670	leonidas-330-1912...	0	LISTENING
snmnlsv.exe	3660	TCP	Leonidas-330-191...	49668	Leonidas-330-191...	0	LISTENING

Írja le a program futtatás eredményét:

A program elkezdje felsorolni az összes TCP és UDP végpontot és a megfelelő tartománynév-verziók IP-címeinek megoldását. A lista a háttérben futó összes folyamatot fogja feltölteni.

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

Process Explorer:

Írja le a program szolgáltatásait:

Ennek a programnak a segítségével részletesen nyomon lehet követni, le lehet bontani a futó processzeket, a DLL eljárásokat vagy éppen a szolgáltatásokat. Ezeket le tudjuk állítani, módosítani tudjuk a prioritásukat, jellemzőit, vagy vizuálisan láthatjuk gépünk működését a monitor ablak segítségével.

Mentse el a megadott dokumentumba (képernyőkép):

Process Explorer - Sysinternals: www.sysinternals.com [LEONIDAS-330-19\Kate Kocsis]

File Options View Process Find Users Help

Process	CPU	Private ...	Workin...	PID	Description	Company Name
Registry		19 692 K	38 828 K	124		
System Idle Process	85.12	60 K	8 K	0		
System	0.35	276 K	36 872 K	4		
Interrupts	0.20	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 028 K	1 116 K	504		
Memory Compression		924 K	238 948 K	2652		
csrss.exe		1 884 K	5 256 K	760		
wininit.exe		1 424 K	6 380 K	872		
services.exe	0.53	5 404 K	9 644 K	1012		
svchost.exe	0.02	13 480 K	33 120 K	1048	Windows-szolgáltatások gazdafolyamata	Microsoft Corporation
StartMenuExperienceHost.exe		26 384 K	71 788 K	6780		
RuntimeBroker.exe		6 140 K	24 548 K	6924	Runtime Broker	Microsoft Corporation
SearchApp.exe	Suspended	222 084 K	308 800 K	6184	Search application	Microsoft Corporation
RuntimeBroker.exe	< 0.01	11 708 K	37 572 K	2244	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe	< 0.01	4 960 K	6 480 K	8180	Host Process for Setting Synchronization	Microsoft Corporation
LockApp.exe	Suspended	14 648 K	59 360 K	8240	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10 076 K	38 004 K	8360	Runtime Broker	Microsoft Corporation
Cortana.exe	Suspended	31 364 K	56 252 K	6024	Cortana	Microsoft Corporation
RuntimeBroker.exe		3 752 K	20 136 K	3788	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		5 620 K	23 520 K	6292	Runtime Broker	Microsoft Corporation
dllhost.exe		5 536 K	13 728 K	9296	COM Surrogate	Microsoft Corporation
MoUsCoreWorker.exe		55 800 K	41 292 K	9396		
ShellExperienceHost.exe	Suspended	17 504 K	55 864 K	5264	Windows Shell Experience Host	Microsoft Corporation
RuntimeBroker.exe		5 772 K	20 232 K	3308	Runtime Broker	Microsoft Corporation
TextInputHost.exe		13 144 K	46 196 K	7728		
CompPkgSrv.exe		1 992 K	8 764 K	2268	Component Package Support Server	Microsoft Corporation
SystemSettings.exe	Suspended	23 080 K	1 920 K	5936	Gépház	Microsoft Corporation
ApplicationFrameHost.exe		9 364 K	26 840 K	8200	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe						

CPU Usage: 14.88% Commit Charge: 57.41% Processes: 176 Physical Usage: 55.45%

Írja le a program futtatás eredményét:

A program megnyitásakor sok vizuális adat jelenik meg azonnal - a számítógépen futó folyamatokról hierarchikus fa nézet jelenik meg (színek segítségével), beleértve a CPU és a RAM használatát az egyes folyamatok számértékeivel. Van néhány kis mini aktivitási grafikon az eszköztár tetején, amelyek megmutatják a CPU használatát, amelyre kattintva külön ablakban megjeleníthető.

Process monitor:

Írja le a program szolgáltatásait:

Ez a program egy fejlett figyelő eszköz a Windows segédprogramok Windows Sysinternals csomagjában. Lehetővé teszi a rendszerén futó összes folyamat részletes információinak megtekintését. Ezek a konkrét folyamatok által kiváltott események részletei.

Mentse el a megadott dokumentumba (képernyőkép):

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path
12:29:...	svchost.exe	2140	Lock File	C:\ProgramData\Microsoft\Windows\A...
12:29:...	svchost.exe	2140	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...
12:29:...	svchost.exe	2140	Unlock FileSingle	C:\ProgramData\Microsoft\Windows\A...
12:29:...	Explorer.EXE	5648	ReadFile	C:\Windows\System32\NPSMDesktop...
12:29:...	svchost.exe	2140	RegOpenKey	HKLM\Software\Policies\Microsoft\...
12:29:...	svchost.exe	2140	RegOpenKey	HKU\S-1-5-18
12:29:...	svchost.exe	2140	RegOpenKey	HKU\DEFAULT
12:29:...	svchost.exe	5256	Lock File	C:\Users\Kate Kocsis\AppData\Local\...
12:29:...	svchost.exe	2140	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...
12:29:...	svchost.exe	2140	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop

Showing 227 347 of 603 109 events (37%) Backed by virtual memory

Írja le a program futtatás eredményét:

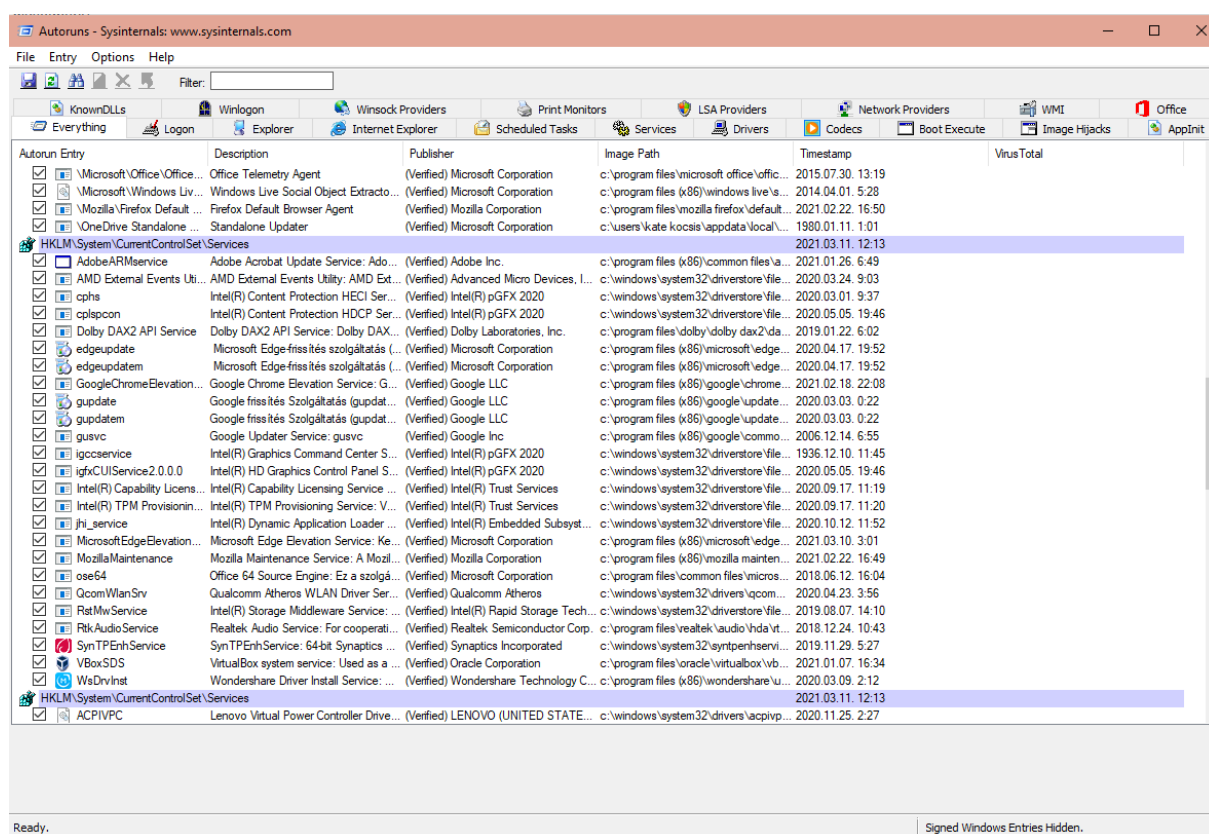
Amikor megnyitjuk először ezt a programot akkor hatalmas számú adatsort jelenik meg. Nem rögzít minden olyan dolgot, ami a számítógépen történik. Nem követi nyomon, hogy mely folyamatok vannak nyitva és pazarolják a CPU-t a számítógépen. Képes bármilyen típusú I / O műveletet rögzíteni, függetlenül attól, hogy ez történik-e a rendszerleíró adatbázisban, a fájlrendszeren vagy akár a hálózaton keresztül.

AutoRuns:

Írja le a program szolgáltatásait:

Az AutoRuns program automatikusan induló folyamatokat kezeli Windows rendszereken. Érthetjük ezalatt az automatikusan induló programokat, drivereket, beépülőket és tulajdonképpen mindent, amit indít Windowsunk rendszerinduláskor vagy fut jelenleg is.

Mentse el a megadott dokumentumba (képernyőkép):



Írja le a program futtatás eredményét:

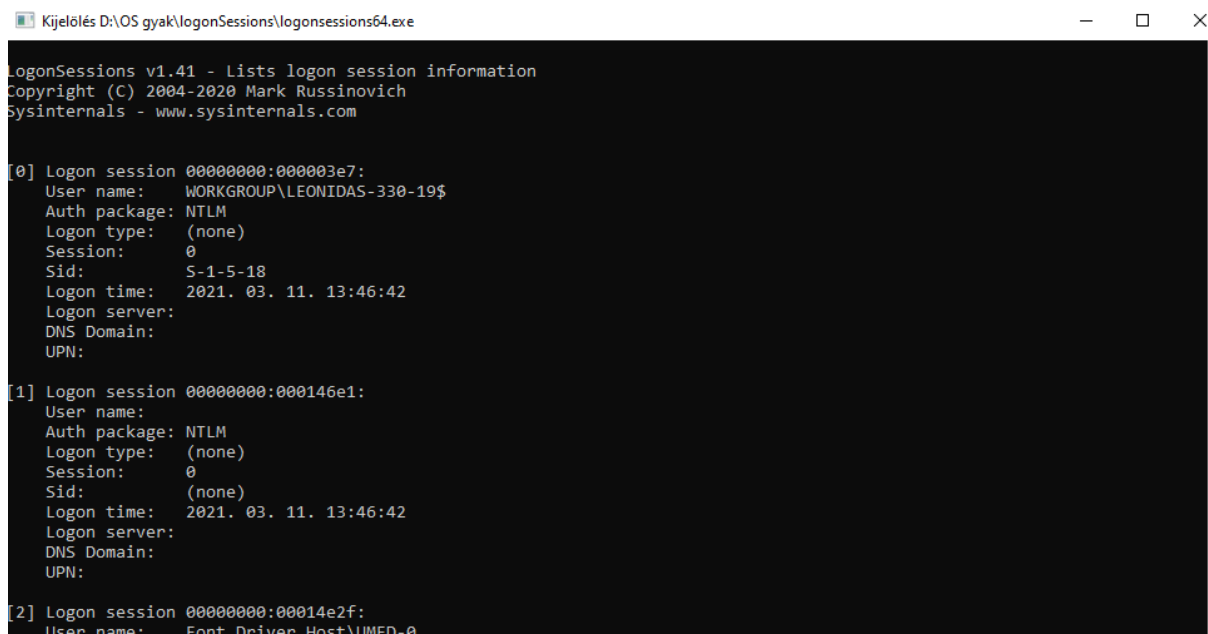
Amikor megnyitjuk a programot akkor megjelenik egy csomó lap és egy lista a számítógépen automatikusan elindított dolgok listájáról. Az alapértelmezett Minden fül mindent megjelenít minden lapról. A listában lévő elemek különböző színekkel rendelkezhetnek.

d) Security Utilities (LogonSession):

Írja le a program szolgáltatásait:

Felsorolja az éppen aktív bejelentkezési munkameneteket.

Mentse el a megadott dokumentumba (képernyőkép):



```
Kijelölés D:\OS gyak\logonSessions\logonsessions64.exe

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

[0] Logon session 00000000:00003e7:
  User name:      WORKGROUP\LEONIDAS-330-19$
  Auth package:   NTLM
  Logon type:      (none)
  Session:        0
  Sid:            S-1-5-18
  Logon time:      2021. 03. 11. 13:46:42
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:000146e1:
  User name:
  Auth package:   NTLM
  Logon type:      (none)
  Session:        0
  Sid:            (none)
  Logon time:      2021. 03. 11. 13:46:42
  Logon server:
  DNS Domain:
  UPN:

[2] Logon session 00000000:00014e2f:
  User name:      Font Driver Host\UMFD-0
```

Írja le a program futtatás eredményét:

A program elindítása után egy parancssor jelenik meg. Különböztetve részleteket jelenít meg a Windows korábbi bejelentkezési kísérleteiről

e) Information Utilities (RAMMap):

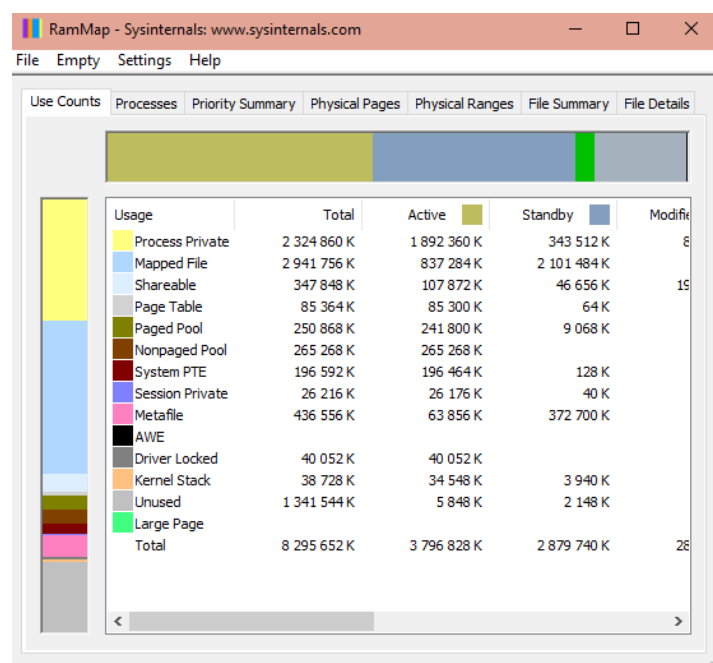
Írja le a program szolgáltatásait:

Ez a program betekintést nyújt a Windows memóriakezelésébe, megmutatja, hogy a memóriát hogyan használják a különböző szolgáltatások.

Mentse el a megadott dokumentumba (képernyőkép):

Írja le a program futtatás eredményét:

A program első indításakor egy füllapú felület jelenik meg, amely információkat tartalmaz a folyamatokról, a számlálásokról, a fizikai oldalakról és a fájl összefoglalásáról. A fájlösszefoglaló lapon megjelennek a memóriában lévő fájl adatok.



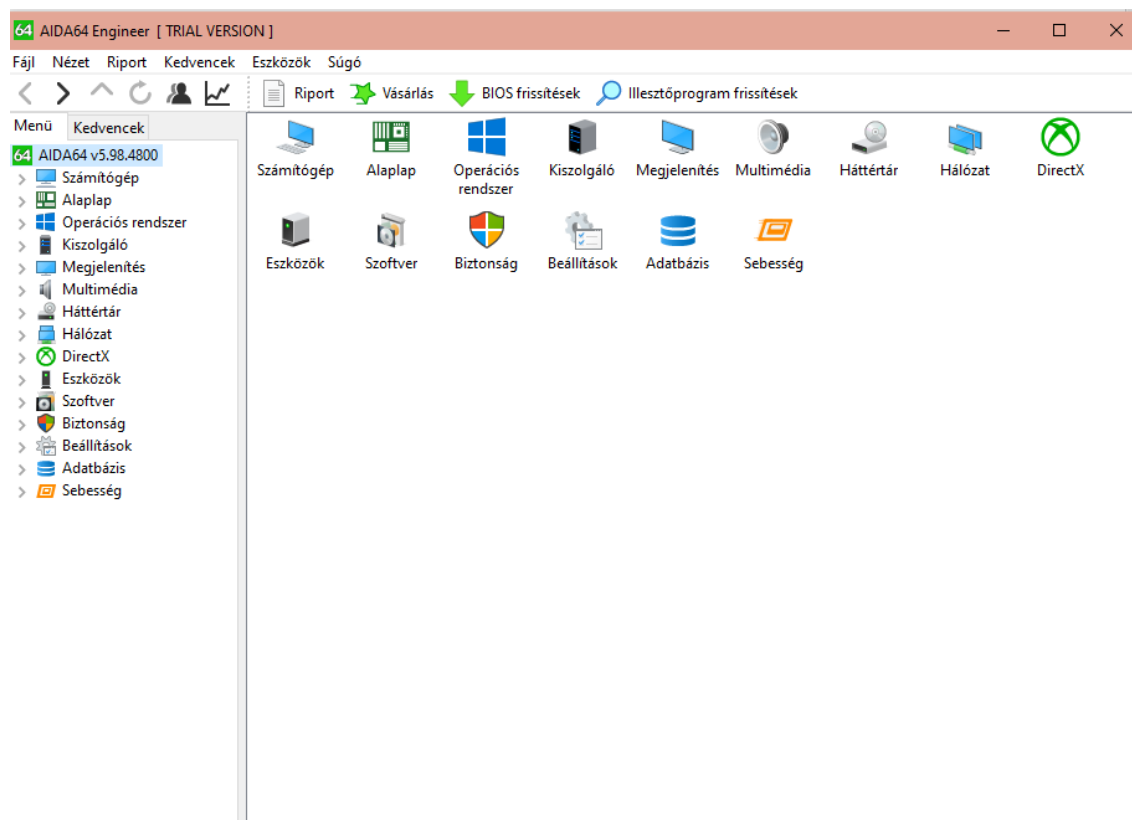
3. **Feladat:** Töltse le és végezzen vizsgálatot az *AIDA64_Engineer_v5.98.4800_Portable*, *CPU-Z*, *GPU-Z* programokkal.

AIDA64_Engineer_v5.98.4800_Portable:

Írja le a program szolgáltatásait:

Ez egy rendszerinformációs szoftver, mely részletes információkat szolgáltat a hardverkomponensekről és a telepített programokról, képes a gép teljesítményének mérésére, és segíti a hibák felderítését.

Mentse el a megadott dokumentumba (képernyőkép):



Írja le a program futtatás eredményét:

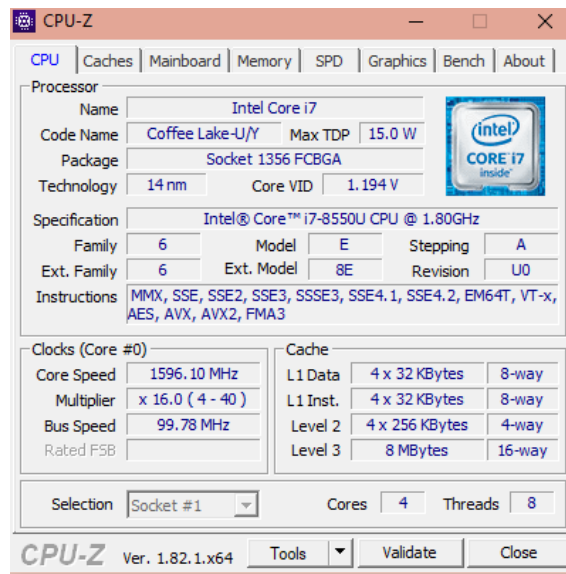
A program megnyitását követően megjelenik egy ablak, amiben a program fő funkciói a felső menüsorból érhetők el. Ez alatt található az eszköztár, amelynek segítségével navigálhatunk az AIDA64 oldalai között. Az ez alatt bal oldalt látható oldalmenü egy összesítő listát tartalmaz a hardver- és szoftverkategóriákról, melyek részleteit a képernyő nagy részét kitöltő információs ablakok mutatják.

CPU-Z:

Írja le a program szolgáltatásait:

A programmal gyorsan információt kapunk a számítógép hardware elemeiről, a CPU, memória, alaplap és videokártya főbb tulajdonságait bemutató füleken

Mentse el a megadott dokumentumba (képernyőkép):



Írja le a program futtatás eredményét

Amikor megnyitottam a programot akkor egy kis ablak jelent meg amiben elemzi a program a chip, az alaplap, a RAM és a grafikus adapter állapotát. Diagnosztizálva a processzort, megtudtam annak nevét, architektúráját és aljzatát. Frekvenciákról, a feszültségekről, a magok számáról, a gyorsítótárról és a szorzóról is tartalmaz adatokat.

GPU-Z:

Írja le a program szolgáltatásait:

A tesztprogrammal megtudhatjuk milyen típusú, sebességű és egyéb technikai jellemzőkkel rendelkező videokártya található a számítógépünkben.

Mentse el a megadott dokumentumba (képernyőkép):

