

# **Operációs rendszerek BSc**

## **2. konzultáció gyakorlat**

**2021.02.26.**

**Készítette:**

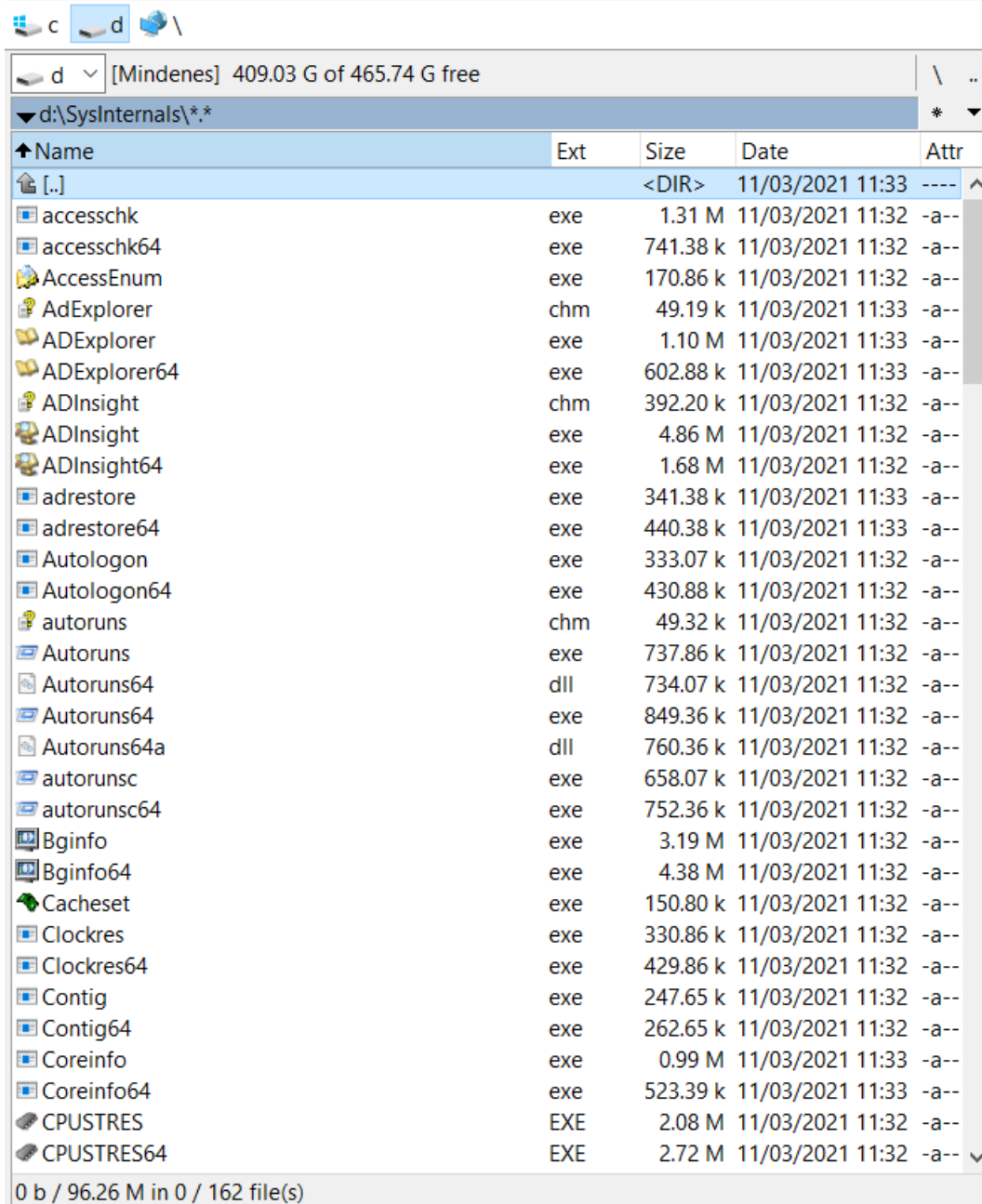
Szűcs Tamás Bsc

Mérnökinformatika

YSAZ4T

**Miskolc, 2021**

## 1. feladat – SysInternals megkeresése, letöltése és kibontása mappába



Name	Ext	Size	Date	Attr
[..]		<DIR>	11/03/2021 11:33	----
accesschk	exe	1.31 M	11/03/2021 11:32	-a--
accesschk64	exe	741.38 k	11/03/2021 11:32	-a--
AccessEnum	exe	170.86 k	11/03/2021 11:32	-a--
AdExplorer	chm	49.19 k	11/03/2021 11:33	-a--
ADExplorer	exe	1.10 M	11/03/2021 11:33	-a--
ADExplorer64	exe	602.88 k	11/03/2021 11:33	-a--
ADInsight	chm	392.20 k	11/03/2021 11:32	-a--
ADInsight	exe	4.86 M	11/03/2021 11:32	-a--
ADInsight64	exe	1.68 M	11/03/2021 11:32	-a--
adrestore	exe	341.38 k	11/03/2021 11:33	-a--
adrestore64	exe	440.38 k	11/03/2021 11:33	-a--
Autologon	exe	333.07 k	11/03/2021 11:32	-a--
Autologon64	exe	430.88 k	11/03/2021 11:32	-a--
autoruns	chm	49.32 k	11/03/2021 11:32	-a--
Autoruns	exe	737.86 k	11/03/2021 11:32	-a--
Autoruns64	dll	734.07 k	11/03/2021 11:32	-a--
Autoruns64	exe	849.36 k	11/03/2021 11:32	-a--
Autoruns64a	dll	760.36 k	11/03/2021 11:32	-a--
autorunsc	exe	658.07 k	11/03/2021 11:32	-a--
autorunsc64	exe	752.36 k	11/03/2021 11:32	-a--
Bginfo	exe	3.19 M	11/03/2021 11:32	-a--
Bginfo64	exe	4.38 M	11/03/2021 11:32	-a--
Cacheset	exe	150.80 k	11/03/2021 11:32	-a--
Clockres	exe	330.86 k	11/03/2021 11:32	-a--
Clockres64	exe	429.86 k	11/03/2021 11:32	-a--
Contig	exe	247.65 k	11/03/2021 11:32	-a--
Contig64	exe	262.65 k	11/03/2021 11:32	-a--
Coreinfo	exe	0.99 M	11/03/2021 11:33	-a--
Coreinfo64	exe	523.39 k	11/03/2021 11:33	-a--
CPUSTRES	EXE	2.08 M	11/03/2021 11:32	-a--
CPUSTRES64	EXE	2.72 M	11/03/2021 11:32	-a--

0 b / 96.26 M in 0 / 162 file(s)

## 2. feladat Segédprogramok letöltése és kibontása mappába

▼ d:\Segédprogramok\*.*					*	▼
↑ Name	Ext	Size	Date	Attr		
↑ [..]		<DIR>	11/03/2021 12:11	----		
[képek]		<DIR>	11/03/2021 12:11	----		
Disk2vhd	chm	39.76 k	17/12/2013 11:46	-a--		
disk2vhd	exe	6.80 M	20/01/2014 14:16	-a--		
Disk2vhd	zip	878.90 k	11/03/2021 11:34	-a--		
Eula	txt	6.84 k	28/07/2006 09:32	-a--		
logonSessions	zip	667.17 k	11/03/2021 11:35	-a--		
ProcessExplorer	zip	2.46 M	11/03/2021 11:35	-a--		
ProcessMonitor	zip	1.95 M	11/03/2021 11:35	-a--		
RAMMap	zip	488.39 k	11/03/2021 11:35	-a--		
SysinternalsSuite	zip	38.03 M	11/03/2021 11:32	-a--		
TCPView	zip	284.77 k	11/03/2021 11:34	-a--		

## 2.1 feladat Disk2VHD

Ez a segédprogram pillanatképet készít a rendszer jelenlegi állapotáról, melyet később a rendszer helyreállítására is felhasználhatunk.

Disk2vhd - Sysinternals: www.sysinternals.com

**Disk2vhd v2.01**  
Copyright © 2009-2014 Mark Russinovich  
[Sysinternals - www.sysinternals.com](http://www.sysinternals.com)

☒ Use Vhdx  
☒ Use Volume Shadow Copy

VHD File name:  
d:\Segédprogramok\DESKTOP-6JJR6LH.vhdx

Volumes to include:

Volume	Label	Size	Free	Space Required
<input type="checkbox"/> \\?\Volume{74671c5c-3f2e-4811-b1f3-...}	[No Label]	96.00 MB	69.58 MB	32.01 MB
<input type="checkbox"/> \\?\Volume{9a1bcc82-a5ff-452a-b80f-...}	[No Label]	507.00 MB	84.92 MB	422.10 MB
<input type="checkbox"/> \\?\Volume{6f23606b-69af-404b-82b8-...}	New Volume	97.66 GB	97.56 GB	98.21 MB
<input checked="" type="checkbox"/> C:\	[No Label]	140.21 GB	79.46 GB	47.08 GB
<input type="checkbox"/> D:\	Mindenes	465.75 GB	409.04 GB	56.73 GB

Help

Create

Cancel

Close

Copying volume C: on disk 1...

11/03/2021 12:37:52

Help

Create

Cancel

Close

## 2.2 TCPView

Ez a segédprogram a futó processzek folyamatait mutatja. Láthatjuk, hogy melyik processt (processz azonosítóval) melyik eszköz milyen protokollal, porton, milyen külső IP address felé. Ezen kívül láthatjuk, hogy hány csomag, byte lett küldve, illetve fogadva a process által.

 TCPView - Sysinternals: [www.sysinternals.com](http://www.sysinternals.com)[illegible]

## 2.3 Process Utilities

Ez a segédprogram megmutatja, hogy melyik process a CPU hány százalékát használja ki, látható a process ID-je, leírása és a „gyártó neve”.

Mint látható az alábbi képen, a System Idle Process (tétlenségi állapot) 90.39 értékkel van, vagyis a jelenleg futó processek a CPU-m kb. 10%-át használják ki. Ezen kívül a többi process esetén is látható a **suspended**, ami azt takarja, hogy a process jelenleg fel van függesztve futás alól.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-6JUR6LH\szucs]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Suspended	184 K	22,544 K	72		
Registry		5,720 K	46,380 K	132		
System Idle Process	90.39	60 K	8 K	0		
System	0.71	204 K	2,364 K	4		
Interrupts	0.38	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,064 K	1,172 K	496		
Memory Compression	< 0.01	1,548 K	71,160 K	2708		
csrss.exe	< 0.01	1,916 K	4,364 K	888		
wininit.exe		1,384 K	5,784 K	956		
services.exe	0.01	6,056 K	9,192 K	1076		
svchost.exe	0.13	13,460 K	32,968 K	1232	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		3,056 K	9,940 K	6024		
rundll32.exe		1,504 K	8,676 K	7840	Windows host process (Rund...	Microsoft Corporation
StartMenuExperienceHo...		37,156 K	65,972 K	8376		
RuntimeBroker.exe		6,816 K	26,956 K	8444	Runtime Broker	Microsoft Corporation
SearchApp.exe	Suspended	185,432 K	77,056 K	8564	Search application	Microsoft Corporation
RuntimeBroker.exe		32,156 K	41,044 K	8656	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		6,276 K	6,356 K	6736	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe		18,508 K	31,816 K	9352	LockApp.exe	Microsoft Corporation
dllhost.exe		5,520 K	12,888 K	9360	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		9,624 K	20,952 K	9456	Runtime Broker	Microsoft Corporation
YourPhone.exe	Suspended	27,336 K	2,872 K	10080	YourPhone	Microsoft Corporation
RuntimeBroker.exe		3,540 K	17,384 K	11184	Runtime Broker	Microsoft Corporation
MoUsoCoreWorker.exe		26,184 K	23,740 K	12512		
SystemSettings.exe	Suspended	22,832 K	2,980 K	12628	Settings	Microsoft Corporation
ApplicationFrameHost.e...		23,888 K	33,348 K	12384	Application Frame Host	Microsoft Corporation
WinStore.App.exe	Suspended	20,348 K	2,716 K	5412	Store	Microsoft Corporation
RuntimeBroker.exe		2,088 K	9,628 K	12308	Runtime Broker	Microsoft Corporation
Microsoft.Photos.exe	Suspended	42,564 K	3,088 K	644		
RuntimeBroker.exe	< 0.01	5,552 K	19,296 K	4276	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		1,812 K	9,040 K	9236	Runtime Broker	Microsoft Corporation
TextInputHost.exe		16,232 K	27,492 K	6656		
ShellExperienceHost.exe	Suspended	27,916 K	40,748 K	6488	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5,472 K	20,724 K	2924	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.e...		7,800 K	18,680 K	8788	System Settings Broker	Microsoft Corporation
RtkUWP.exe	Suspended	11,984 K	38,336 K	9516	Realtek Audio Console	Realtek Semiconductor
RuntimeBroker.exe		4,348 K	16,024 K	6620	Runtime Broker	Microsoft Corporation
smartscreen.exe		8,972 K	26,612 K	5024	Windows Defender SmartScr...	Microsoft Corporation
ScreenClippingHost.exe	1.89	13,068 K	38,856 K	3076		Microsoft Corporation
svchost.exe	0.11	9,324 K	15,836 K	1356	Host Process for Windows S	Microsoft Corporation

## Process Monitor

Ez a segédprogram megmutatja, hogy melyik process (ID-vel együtt látható), mikor lett elindítva, milyen műveletet végez, a process útvonalát is látni, illetve sikeresen végrehajtódott-e a művelet. Az utolsó oszlop a részleteket takarja.

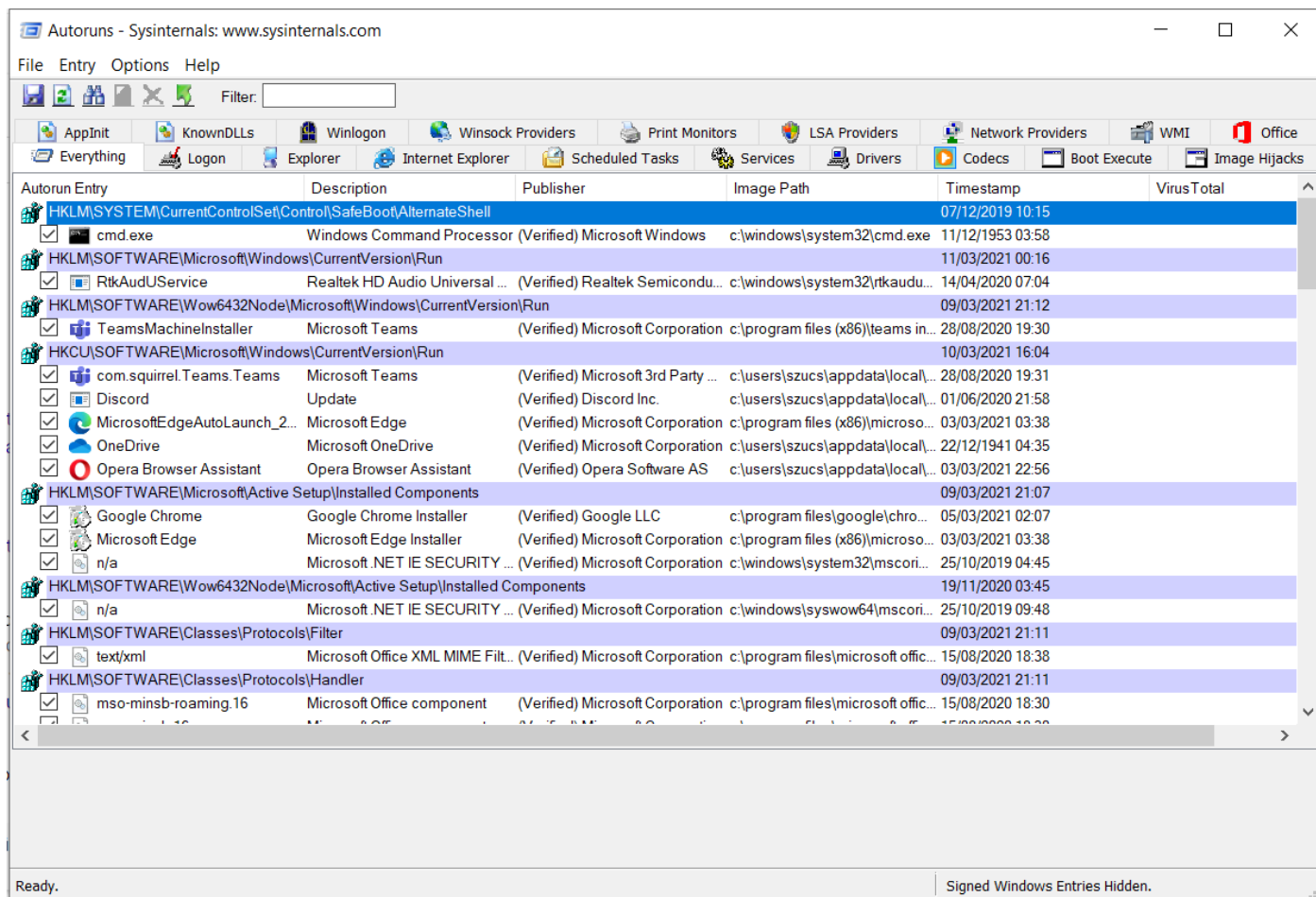
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:56:53.5085722	MsMpEng.exe	2904	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5E4A33A1-584A-49C3-98BE-9D6FE2D91C1B}\mpengine.dll	SUCCESS	Offset: 14,958,592. Length: 12,288. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5088542	MsMpEng.exe	2904	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5E4A33A1-584A-49C3-98BE-9D6FE2D91C1B}\mpengine.dll	SUCCESS	Offset: 14,934,016. Length: 4,096. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5091363	MsMpEng.exe	2904	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5E4A33A1-584A-49C3-98BE-9D6FE2D91C1B}\mpengine.dll	SUCCESS	Offset: 14,151,680. Length: 8,192. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5093971	MsMpEng.exe	2904	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5E4A33A1-584A-49C3-98BE-9D6FE2D91C1B}\mpengine.dll	SUCCESS	Offset: 14,438,400. Length: 16,384. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5096756	MsMpEng.exe	2904	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5E4A33A1-584A-49C3-98BE-9D6FE2D91C1B}\mpengine.dll	SUCCESS	Offset: 14,180,352. Length: 16,384. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5097037	svchost.exe	2344	ReadFile	C:\Windows\System32\StateRepository\Core.dll	SUCCESS	Offset: 690,688. Length: 15,872. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5099153	svchost.exe	2904	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5E4A33A1-584A-49C3-98BE-9D6FE2D91C1B}\mpengine.dll	SUCCESS	Offset: 14,422,016. Length: 16,384. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5101149	MsMpEng.exe	2904	LockFile	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine\edb\db-shm	SUCCESS	Exclusive: False. Offset: 124. Length: 1. Fail Immediately: True
12:56:53.5101583	svchost.exe	2344	ReadFile	C:\Windows\System32\StateRepository\Core.dll	SUCCESS	Offset: 678,400. Length: 12,288. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5108535	Explorer.EXE	6196	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 312,832. Length: 9,728. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5108543	svchost.exe	2344	ReadFile	C:\Windows\System32\StateRepository\Core.dll	SUCCESS	Offset: 635,904. Length: 16,384. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5112751	Explorer.EXE	6196	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 257,536. Length: 8,192. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5112983	svchost.exe	2344	ReadFile	C:\Windows\System32\StateRepository\Core.dll	SUCCESS	Offset: 623,616. Length: 12,288. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5116219	svchost.exe	2344	ReadFile	C:\Windows\System32\StateRepository.dll	SUCCESS	Offset: 5,471,744. Length: 16,384. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5117344	cmdmon.exe	7084	ReadFile	C:\Windows\System32\inputservice.dll	SUCCESS	Offset: 4,089,856. Length: 16,384. (IO Flags: Non-cached, Paging I/O, Sync
12:56:53.5117975	MsMpEng.exe	2904	UnlockFileSingle	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine\edb\db-shm	SUCCESS	Offset: 124. Length: 1
12:56:53.5118116	Explorer.EXE	6196	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
12:56:53.5118711	Explorer.EXE	6196	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Handle Tags. Handle Tags: 0x0
12:56:53.5118950	Explorer.EXE	6196	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Handle Tags. Handle Tags: 0x0
12:56:53.5119240	Explorer.EXE	6196	RegOpenKey	HKCU\Software\Classes\Applications\Procmon64.exe	NAME NOT FOUND	NAME NOT FOUND Desired Access: Read
12:56:53.5119587	Explorer.EXE	6196	RegOpenKey	HKCU\Software\Classes	NAME NOT FOUND	NAME NOT FOUND Desired Access: Read
12:56:53.5120064	Explorer.EXE	6196	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
12:56:53.5120335	Explorer.EXE	6196	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Handle Tags. Handle Tags: 0x0

## Autoruns

Ez a segédprogram segít eligazodni az automatikusan futó programok/processek között. Különböző tabok között váltogatva láthatjuk szeparálva a folyamatokat/programokat. Látható egy-egy adott szolgáltatás bejegyzését, leírását, a program „kiadóját”, az adott process elérési útját és telepítési idejét.



## 2.4 Security Utilities

A LogonSession segédprogram nem fut. Kipróbáltam több módon is, nem indult.

## 2.5 RAMMAP

Ez a segédprogram memórialhasználati statisztikát készít. A különböző TAB-ok leírása:

Use counts: típus és lapozófájl szerinti megjelenítés

Processzek: méret szerinti megjelenítés

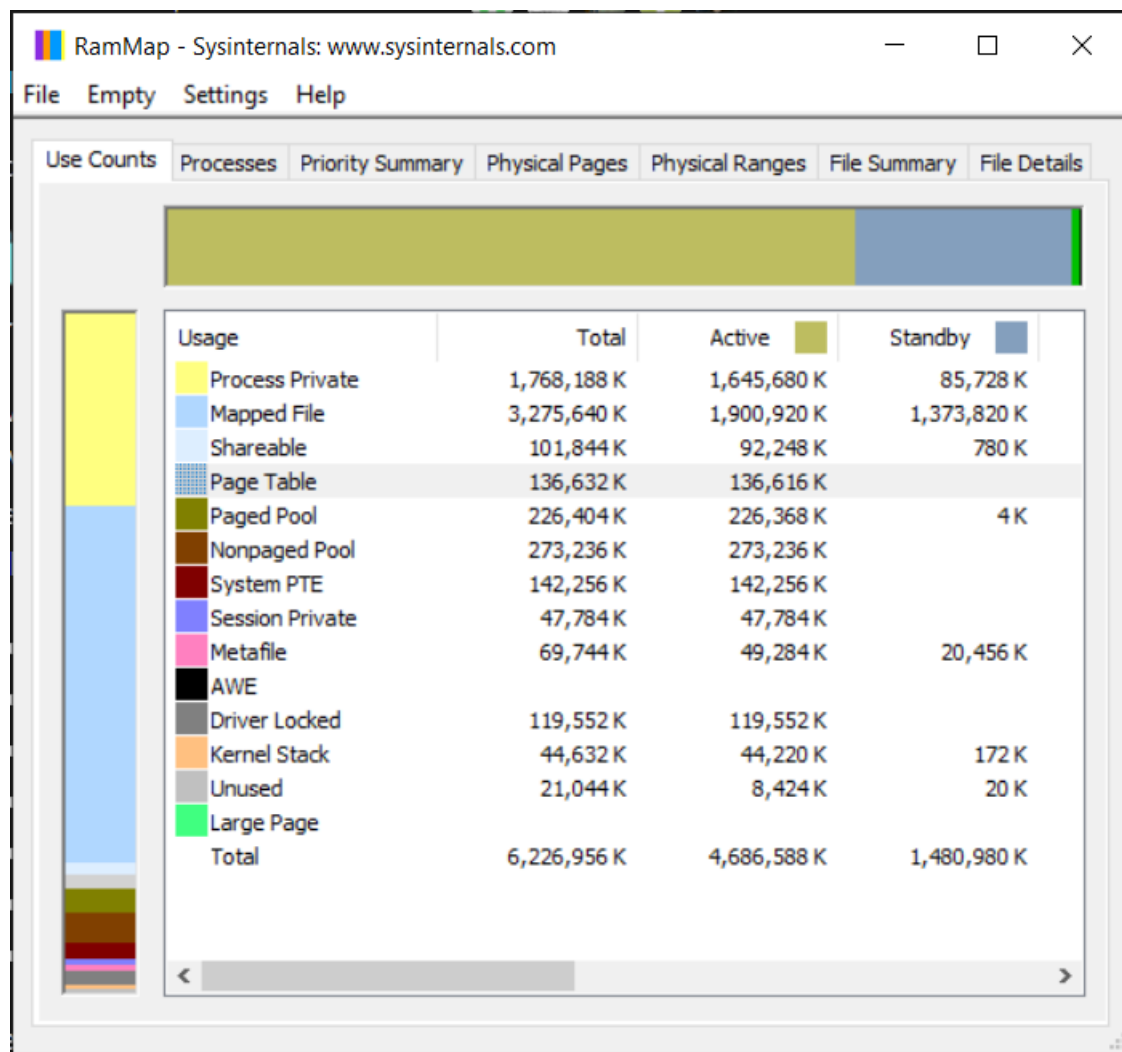
Priority Summary: prioritás szerinti megjelenítés

Physical Pages: fizikai memória használat szerinti megjelenítés

File Summary: RAM-ban lévő méret szerinti megjelenítés

File Details: hol található az adott process

- *Use Counts*: usage summary by type and paging list
- *Processes*: process working set sizes
- *Priority Summary*: prioritized standby list sizes
- *Physical Pages*: per-page use for all physical memory
- *Physical Ranges*: physical memory addresses
- *File Summary*: file data in RAM by file
- *File Details*: individual physical pages by file





### 3. Feladat

#### 3.1 AIDA64

Az AIDA64 majdnem teljes részletességgel szolgál a szoftverekkel/hardverekkel kapcsolatban. Meg tudjuk nézni pl. a memória adatait, milyen órajelen működik, stb. Ugyanígy a CPU, grafikus kártya (esetemben APU – Accelerated Processing Unit), alaplap, háttértár adatait is kiolvashatjuk. Ezen túlmenően készíthetünk egy átfogó riportot is, mely tartalmazza a számunkra releváns adatokat a gépünkkel kapcsolatban.

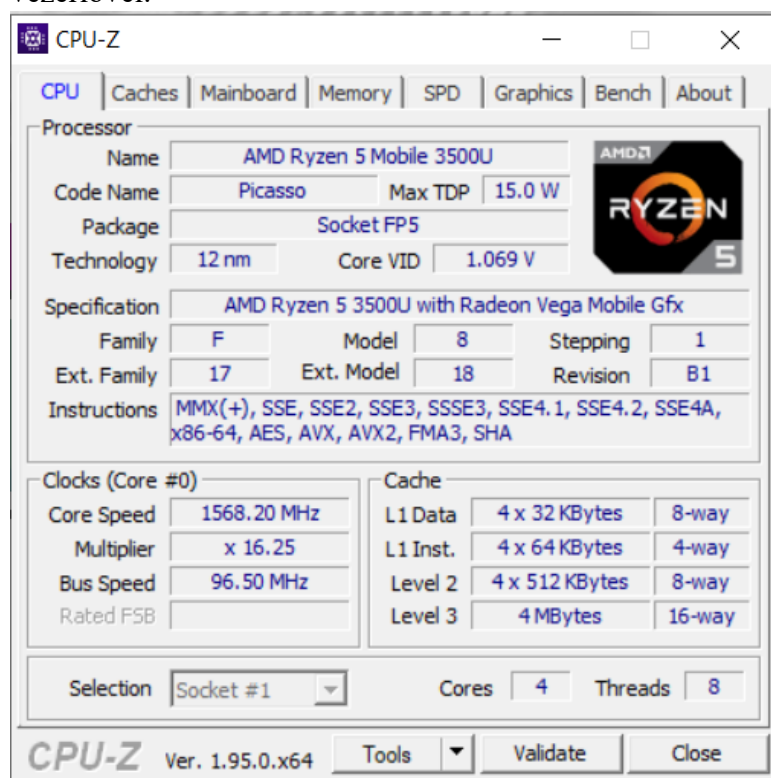
The screenshot displays the AIDA64 Engineer [ TRIAL VERSION ] interface. The left sidebar shows a tree view of system components, with 'Computer' expanded. The main window displays a list of system fields and their corresponding values.

Field	Value
Computer	
Computer Type	ACPI x64-based PC (Mobile)
Operating System	Microsoft Windows 10 Pro
OS Service Pack	[ TRIAL VERSION ]
Internet Explorer	11.789.19041.0
Edge	89.0.774.45
DirectX	DirectX 12.0
Computer Name	DESKTOP-6JUR6LH
User Name	szucs
Logon Domain	[ TRIAL VERSION ]
Date / Time	2021-03-11 / 13:38
Motherboard	
CPU Type	Mobile QuadCore AMD Ryzen 5 3500U, 3325 MHz (33.25 x 100)
Motherboard Name	Acer Aspire A314-22
Motherboard Chipset	AMD K17.1 FCH, AMD K17.1 IMC
System Memory	[ TRIAL VERSION ]
DIMM1: SK hynix HMA851S6...	4 GB DDR4-2666 DDR4 SDRAM (20-19-19-43 @ 1333 MHz) (19-19-1...
BIOS Type	Unknown (01/06/2021)
Display	
Video Adapter	AMD Radeon(TM) Vega 8 Graphics (2 GB)
Video Adapter	AMD Radeon(TM) Vega 8 Graphics (2 GB)
Video Adapter	AMD Radeon(TM) Vega 8 Graphics (2 GB)
Video Adapter	AMD Radeon(TM) Vega 8 Graphics (2 GB)
3D Accelerator	AMD Picasso
Monitor	CMN N140HGA-EA1 [14" LCD]



### 3.2 CPU-Z

Ez a program a CPU/cache/alaplap/memória/sebesség/grafikus kártya alap adatait olvassa ki. Jelen esetben látható, hogy a notebookomban egy AMD Ryzen 5-ös APU található, Vega 8-as grafikus vezérlővel.



### 3.3 GPU-Z

Ez a program a grafikus vezérlőről ad alapvető információkat. Jelen esetben látható, hogy a notebookomban egy AMD Radeon Vega 8-as grafikus vezérlő van.

