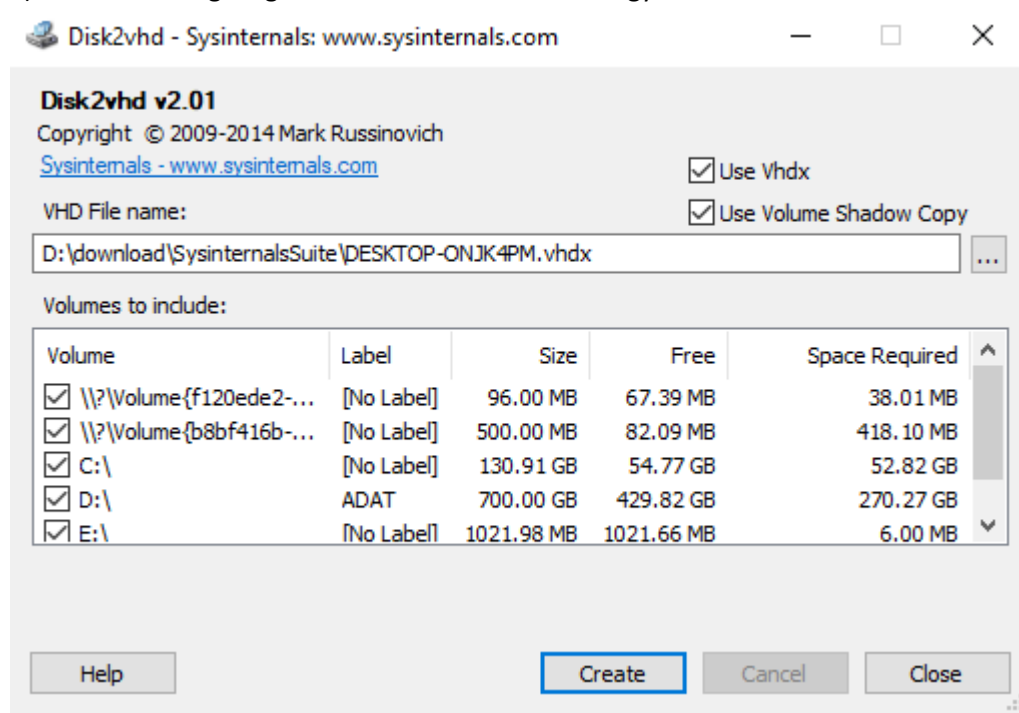
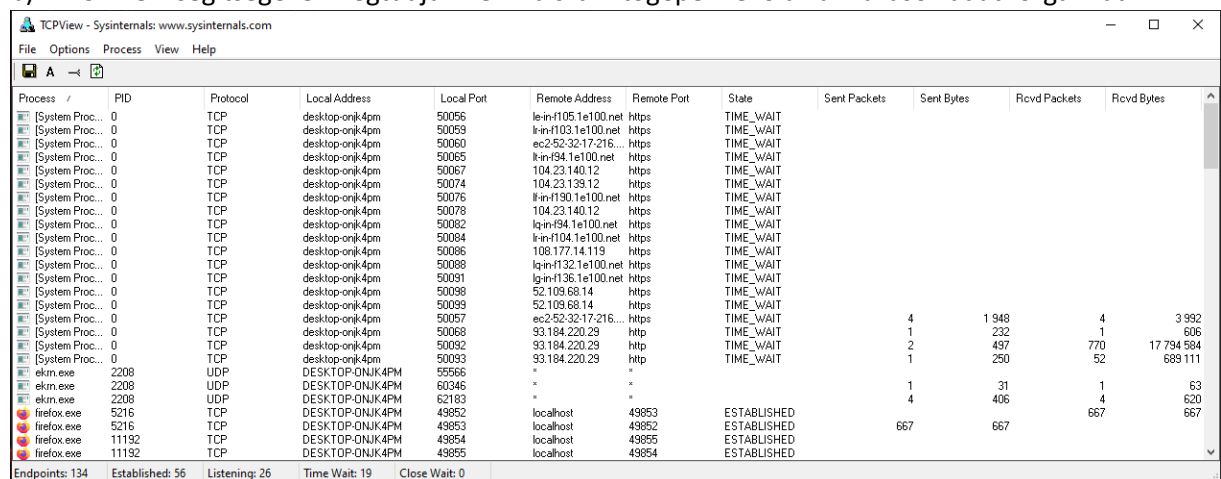


2. Operációs rendszerek gyakorlat

- 1) Letöltöttem a Sysinternals Suite.
- 2) a) A Disk2Vhd segítségével a fizikai lemezből lehet egy virtuális lemezt készíteni



- b) A TCPView segítségével megtudjuk nézni a számítógépen lévő alkalmazások adat forgalmát



c) Process Explorer: segítségével meg nézhetjük a számítógépünk processzorának a terheltségét

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-ONJK4PM\Attila]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		11 312 K	88 896 K	148		
System Idle Process	89.18	60 K	8 K	0		
System	0.96	208 K	2 796 K	4		
Interrupts	0.54	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 056 K	1 076 K	632		
csrss.exe	< 0.01	1 896 K	5 484 K	792		
wininit.exe		1 380 K	6 844 K	896		
services.exe	< 0.01	5 464 K	10 772 K	968		
svchost.exe	< 0.01	12 116 K	32 780 K	1108	Windows-szolgáltatások gaz...	Microsoft Corporation
dihost.exe		3 824 K	10 956 K	3852		
WmiPrvSE.exe		2 912 K	9 560 K	6876		
StartMenuExperienceHost.exe	0.01	35 892 K	92 308 K	8152		
RuntimeBroker.exe		6 636 K	25 172 K	6092	Runtime Broker	Microsoft Corporation
SearchApp.exe	0.18	171 540 K	251 436 K	6096	Search application	Microsoft Corporation
RuntimeBroker.exe	0.01	12 776 K	40 960 K	7012	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	23 476 K	47 804 K	7108	YourPhone	Microsoft Corporation
SettingSyncHost.exe		2 428 K	4 844 K	8364	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		3 668 K	17 636 K	9000	Runtime Broker	Microsoft Corporation
dihost.exe		5 776 K	14 384 K	9696	COM Surrogate	Microsoft Corporation
TextInputHost.exe	0.01	11 608 K	48 632 K	10048		
RuntimeBroker.exe		2 784 K	13 280 K	4500	Runtime Broker	Microsoft Corporation
UserOOBEBroker.exe		1 792 K	8 968 K	7096	User OOBEBroker	Microsoft Corporation
MoUseCoreWorker.exe		16 980 K	27 260 K	8632		
CompPkgSrv.exe		1 524 K	8 748 K	8936	Component Package Suppor...	Microsoft Corporation
ShellExperienceHost.exe	Susp...	12 300 K	44 424 K	8724	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2 968 K	19 092 K	7792	Runtime Broker	Microsoft Corporation
GameBar.exe	Susp...	14 592 K	38 480 K	9968	Xbox Game Bar	Microsoft Corporation
Video.UI.exe	Susp...	18 728 K	45 628 K	10140		
GameBarFTServer.exe		3 004 K	14 128 K	10532	Xbox Game Bar Full Trust C...	Microsoft Corporation

CPU Usage: 11.86% Commit Charge: 41.21% Processes: 175 Physical Usage: 67.29%

Process Monitor: Hasonló a Process Explorerhez de itt nem látjuk hogy az egyes programok százalékosan mennyire használják a számítógépünk proceszorát

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:55:22.0841326	lsass.exe	744	Thread Create		SUCCESS	Thread ID: 3584
12:55:22.0873594	cfmon.exe	7520	ReadFile	C:\Windows\System32\inputService.dll	SUCCESS	Offset: 4 088 320, ...
12:55:22.0876866	cfmon.exe	7520	ReadFile	C:\Windows\System32\TextInputFramework.dll	SUCCESS	Offset: 878 080, Le...
12:55:22.0924279	Explorer.EXE	2184	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 212 480, Le...
12:55:22.0938871	Skype.exe	2896	UDP Receive	DESKTOP-ONJK4PM:6046 -> 40 68 35.123:3480	SUCCESS	Length: 201, seqn...
12:55:22.0950050	Explorer.EXE	2184	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
12:55:22.0950348	Explorer.EXE	2184	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
12:55:22.0950647	Explorer.EXE	2184	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
12:55:22.0950839	Explorer.EXE	2184	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
12:55:22.0952387	Explorer.EXE	2184	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
12:55:22.0952556	Explorer.EXE	2184	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Q...
12:55:22.0953211	Explorer.EXE	2184	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocCha...	SUCCESS	Type: REG_DWOW...
12:55:22.0953367	Explorer.EXE	2184	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	
12:55:22.0953489	Explorer.EXE	2184	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
12:55:22.0953596	Explorer.EXE	2184	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Q...
12:55:22.0953748	Explorer.EXE	2184	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocCha...	SUCCESS	Type: REG_DWOW...
12:55:22.0953864	Explorer.EXE	2184	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	
12:55:22.0954168	Explorer.EXE	2184	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:55:22.0954313	Explorer.EXE	2184	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:55:22.0954398	Explorer.EXE	2184	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:55:22.0954502	Explorer.EXE	2184	RegOpenKey	HKCU\Software\Classes\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	NAME NOT FOUND	Desired Access: R...
12:55:22.0954692	Explorer.EXE	2184	RegOpenKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Desired Access: R...
12:55:22.0954867	Explorer.EXE	2184	RegQueryKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Query: Name
12:55:22.0954988	Explorer.EXE	2184	RegQueryKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Query: HandleTag...
12:55:22.0955044	Explorer.EXE	2184	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
12:55:22.0955125	Explorer.EXE	2184	RegOpenKey	HKCU\Software\Classes\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}\Trea...	NAME NOT FOUND	Desired Access: Q...
12:55:22.0955247	Explorer.EXE	2184	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
12:55:22.0955258	Explorer.EXE	2184	RegQueryKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Query: HandleTag...
12:55:22.0955375	Explorer.EXE	2184	RegOpenKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}\TreatAs	NAME NOT FOUND	Desired Access: Q...
12:55:22.0955434	Explorer.EXE	2184	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
12:55:22.0955619	Explorer.EXE	2184	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
12:55:22.0955704	Explorer.EXE	2184	ReadFile	C:\Windows\System32\combase.dll	SUCCESS	Offset: 3 003 904, ...
12:55:22.0958840	Explorer.EXE	2184	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
12:55:22.0959024	Explorer.EXE	2184	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
12:55:22.0959209	Explorer.EXE	2184	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
12:55:22.0959381	Explorer.EXE	2184	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
12:55:22.0959537	Explorer.EXE	2184	RegQueryKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Query: Name
12:55:22.0959802	Explorer.EXE	2184	RegQueryKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Query: Name
12:55:22.0959957	Explorer.EXE	2184	RegQueryKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Query: HandleTag...
12:55:22.0960146	Explorer.EXE	2184	RegOpenKey	HKCU\Software\Classes\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	NAME NOT FOUND	Desired Access: M...
12:55:22.0960327	Explorer.EXE	2184	RegQueryValue	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}\ActivateOnHostFlags	SUCCESS	NAME NOT FOUND Length: 16
12:55:22.0960458	Explorer.EXE	2184	RegQueryKey	HKCR\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}	SUCCESS	Query: Name

Showing 418 467 of 887 576 events (47%) Backed by virtual memory

AutoRuns: A Windows környezetben történő automatikus futtatás vezérlés. A gépinek indításakor ez indítja el az automatikusan induló programokat illetve a harmadik féltől származó programokat

The screenshot shows the Autoruns application window with the following columns: Autorun Entry, Description, Publisher, Image Path, Timestamp, and VirusTotal. The list includes various system components and third-party applications.

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953. 12. 11. 3:58	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	ESET command line interface	(Verified) ESET, spol. s r.o.	c:\program files\eset\eset security\...	2020. 10. 26. 9:30	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\...	2020. 09. 16. 21:51	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Cleaner	(Verified) Piriform Software Ltd	d:\prog file\ccleaner\ccleaner64.exe	2021. 01. 06. 17:54	
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\attila\appdata\local\microso...	2020. 10. 02. 13:48	
Discord	Update	(Verified) Discord Inc.	c:\users\attila\appdata\local\discord...	2020. 06. 01. 21:58	
Skype for Desktop	Skype	(Verified) Skype Software Sarl	c:\program files (x86)\microsoft\skyp...	2020. 04. 01. 23:51	
Spotify	Spotify	(Verified) Spotify AB	c:\users\attila\appdata\roaming\spot...	2021. 01. 20. 0:18	
Steam	Steam Client Bootstrapper	(Verified) Valve	d:\prog file\game\steam\steam.exe	2021. 02. 13. 0:23	
C:\Users\Attila\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	Send to OneNote Tool	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft office...	2021. 02. 15. 20:15	
MEGASync.Lnk	MEGASync	(Verified) Mega Limited	c:\programdata\megasync\megasy...	2020. 12. 21. 4:33	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021. 02. 17. 4:41	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2019. 10. 25. 4:45	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	2019. 10. 25. 9:48	
n/a	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft office...	2020. 12. 28. 23:39	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	d:\prog file\notepad plus\notepad++...	2014. 05. 12. 10:49	
ANotepad++64	ESET Shell Extension	(Verified) ESET, spol. s r.o.	c:\program files\eset\eset security\...	2020. 10. 26. 9:30	
MEGA (Context menu)	WinRAR shell extension	(Verified) win.rar GmbH	d:\prog file\winrar\winrar.exe	2020. 12. 01. 19:00	
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				2021. 01. 27. 17:40	

d) LogonSession: Segítségével megnézhetjük hogy mikor jelentkeztek be a számítógépünkbe

```
Administrator: Parancssor
Microsoft Windows [Version 10.0.19042.804]
(c) 2020 Microsoft Corporation. Minden jog fenntartva.

C:\Windows\system32>D:\download\SysinternalsSuite\logonsessions64

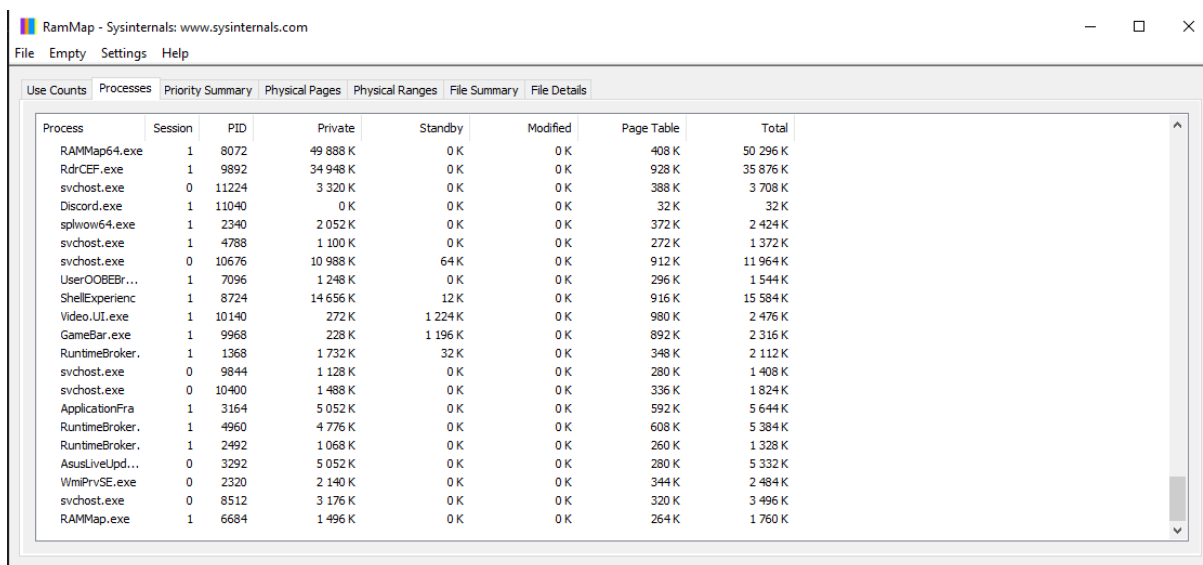
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\DESKTOP-ONJ4KPM$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2021. 02. 25. 12:04:21
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:0001203b:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2021. 02. 25. 12:04:22
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:00012592:
User name: Font Driver Host\UMFD-0
Auth package: Negotiate
Logon type: Interactive
Session: 0
Sid: S-1-5-96-0-0
Logon time: 2021. 02. 25. 12:04:23
Logon server:
DNS Domain:
UPN:
```

e) RAMMap: Segítségével megnézhetjük a számítógépünkben lévő ramnak a hasznátságát



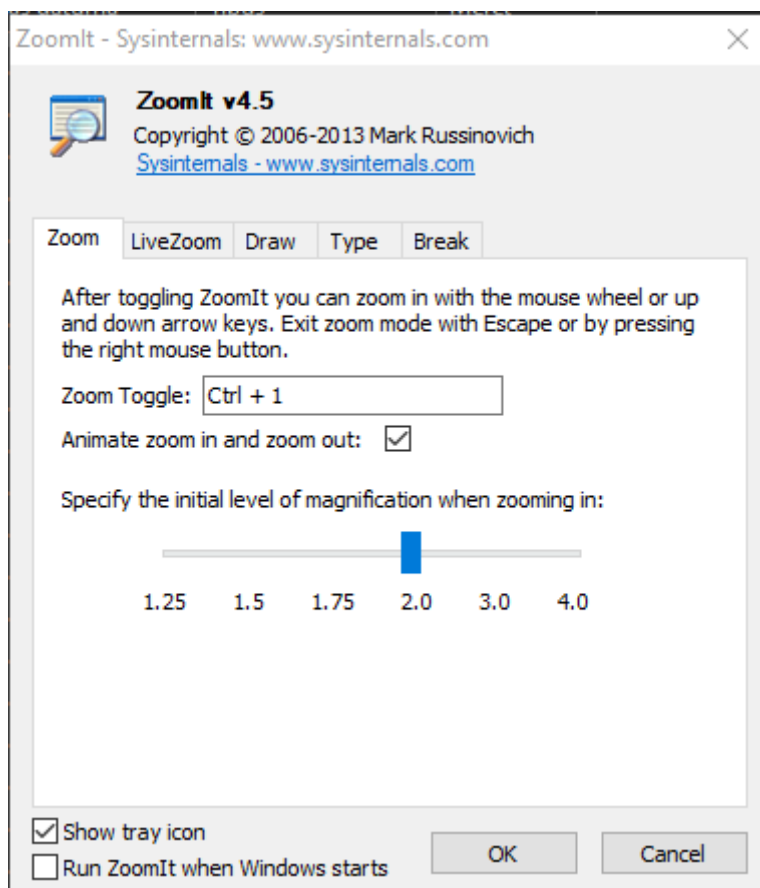
RAMMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

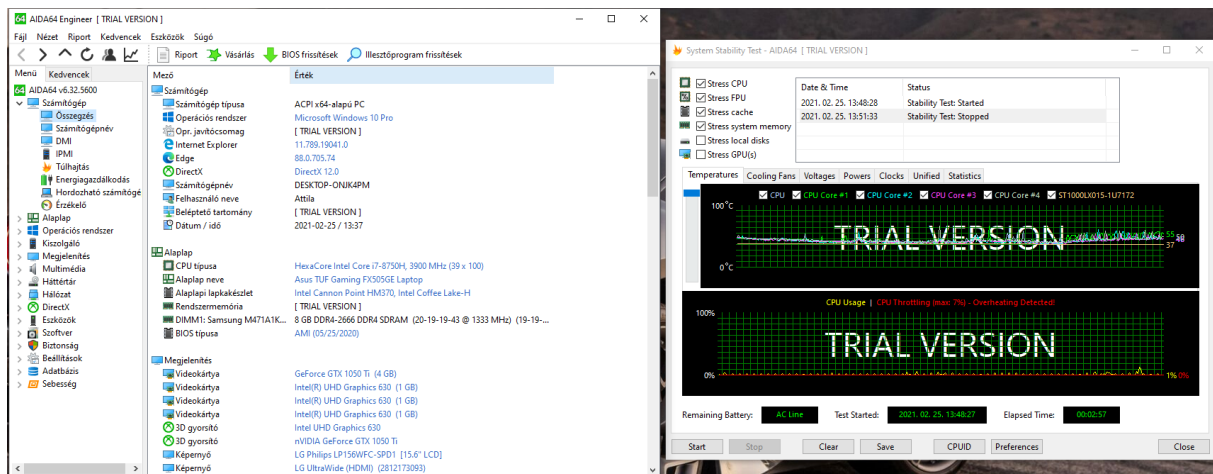
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Process	Session	PID	Private	Standby	Modified	Page Table	Total
RAMMap64.exe	1	8072	49 888 K	0 K	0 K	408 K	50 296 K
RdrCEF.exe	1	9892	34 948 K	0 K	0 K	928 K	35 876 K
svchost.exe	0	11224	3 320 K	0 K	0 K	388 K	3 708 K
Discord.exe	1	11040	0 K	0 K	0 K	32 K	32 K
splwow64.exe	1	2340	2 052 K	0 K	0 K	372 K	2 424 K
svchost.exe	1	4788	1 100 K	0 K	0 K	272 K	1 372 K
svchost.exe	0	10676	10 988 K	64 K	0 K	912 K	11 964 K
UserOOBEBr...	1	7096	1 248 K	0 K	0 K	296 K	1 544 K
ShellExperienc	1	8724	14 656 K	12 K	0 K	916 K	15 584 K
Video.UI.exe	1	10140	272 K	1 224 K	0 K	980 K	2 476 K
GameBar.exe	1	9968	228 K	1 196 K	0 K	892 K	2 316 K
RuntimeBroker.	1	1368	1 732 K	32 K	0 K	348 K	2 112 K
svchost.exe	0	9844	1 128 K	0 K	0 K	280 K	1 408 K
svchost.exe	0	10400	1 488 K	0 K	0 K	336 K	1 824 K
ApplicationFra	1	3164	5 052 K	0 K	0 K	592 K	5 644 K
RuntimeBroker.	1	4960	4 776 K	0 K	0 K	608 K	5 384 K
RuntimeBroker.	1	2492	1 068 K	0 K	0 K	260 K	1 328 K
AsusLiveUpd...	0	3292	5 052 K	0 K	0 K	280 K	5 332 K
WmiPrvSE.exe	0	2320	2 140 K	0 K	0 K	344 K	2 484 K
svchost.exe	0	8512	3 176 K	0 K	0 K	320 K	3 496 K
RAMMap.exe	1	6684	1 496 K	0 K	0 K	264 K	1 760 K

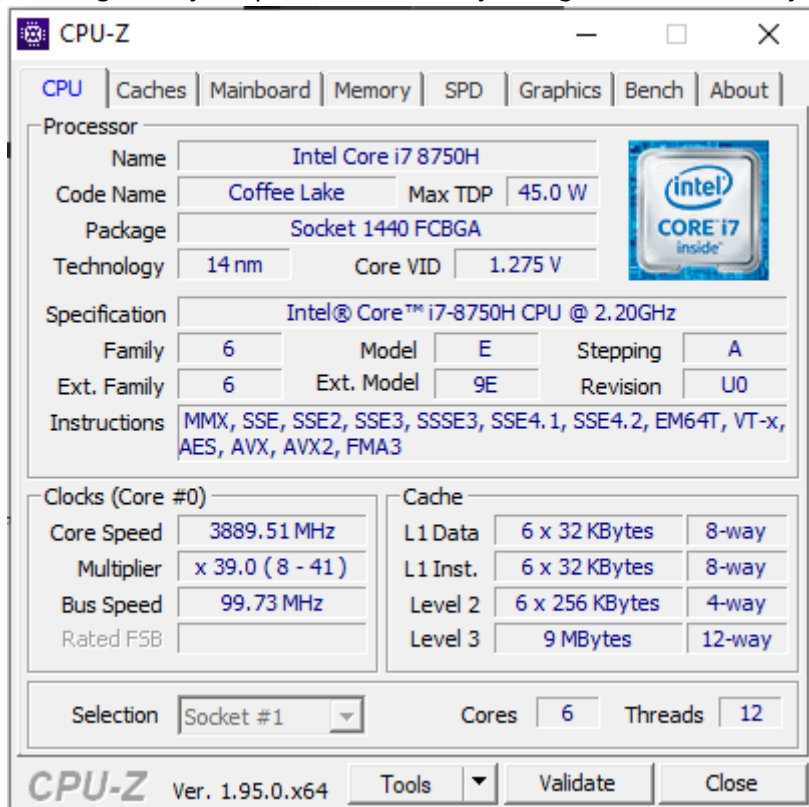
f) ZoomIt64: Segítségével bele nagyíthatunk a képernyőnkbe



3) AIDA64: Segítségével megnézhetjük hogy a számítógépünkben milyen alkatrészek vannak és végezhetünk egy stabilitás tesztet is



CPUZ: segítségével megnézhetjük a processzorunk tulajdonságait és monitorozhatjuk is




GPUZ: segítségével megnézhetjük a GPU tulajdonságait

TechPowerUp GPU-Z 2.37.0


Graphics Card | Sensors | Advanced | Validation

Name: Intel(R) UHD Graphics 630 [Lookup](#)

GPU: Coffee Lake GT2 Revision: N/A

Technology: 14 nm Die Size: Unknown 

Release Date: Oct 5, 2017 Transistors: Unknown

BIOS Version: 1010 PC 14.34 04/18/2018 22:21:46  ☒ UEFI

Subvendor: ASUS Device ID: 8086 3E9B - 1043 1A4E

ROPs/TMUs: 8 / 16 Bus Interface: N/A ?

Shaders: 24 Unified DirectX Support: 12 (12_1)

Pixel Fillrate: 8.8 GPixel/s Texture Fillrate: 17.6 GTexel/s

Memory Type: DDR4 Bus Width: 64 bit

Memory Size: N/A Bandwidth: 21.3 GB/s

Driver Version: 25.20.100.6577 DCH / Win10 64

Driver Date: Feb 07, 2019 Digital Signature: WHQL

GPU Clock: 350 MHz Memory: 1333 MHz Boost: 1100 MHz

Default Clock: 350 MHz Memory: 1333 MHz Boost: 1100 MHz

Multi-GPU: Disabled

Computing: ☒ OpenCL ☐ CUDA ☒ DirectCompute ☒ DirectML

Technologies: ☒ Vulkan ☐ Ray Tracing ☒ PhysX ☒ OpenGL 4.6

Intel(R) UHD Graphics 630 [Close](#)

- 4) a) A kernel32.dll a API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL és a
API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL hívásokat használja
b) A kernel32.dll-nek az alábbi függőségei vannak:

Dependency Walker - [neptonkod]

File Edit View Options Profile Window Help

Module	PI	Ordinal	Hint	Function	Entry Point
NEPTONKOD.EXE					
KERNEL32.DLL					
API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL		N/A	207 (0x00CF)	DeleteCriticalSection	Not Bound
API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL		N/A	236 (0x00EC)	EnterCriticalSection	Not Bound
NTDLL.DLL		N/A	279 (0x0117)	ExitProcess	Not Bound
KERNELBASE.DLL		N/A	300 (0x012C)	FindClose	Not Bound
NTDLL.DLL		N/A	304 (0x0130)	FindFirstFileA	Not Bound
API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL		N/A	321 (0x0141)	FindNextFileA	Not Bound
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL		N/A	352 (0x0160)	FreeLibrary	Not Bound
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL		N/A	388 (0x0184)	GetCommandLineA	Not Bound
EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL		N/A	510 (0x01FE)	GetLastError	Not Bound
EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL		N/A	529 (0x0211)	GetModuleHandleA	Not Bound
EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL		N/A	577 (0x0241)	GetProcAddress	Not Bound
EXT-MS-WIN-KERNEL32-QUICKS-L1-1-0.DLL		N/A	734 (0x02DE)	InitializeCriticalSection	Not Bound
EXT-MS-WIN-KERNEL32-SIDEWAYSIDE-L1-1-0.DLL		N/A	814 (0x032E)	LeaveCriticalSection	Not Bound
EXT-MS-WIN-KERNEL32-SIDEWAYSIDE-L1-1-0.DLL		N/A	817 (0x0331)	LoadLibraryA	Not Bound
EXT-MS-WIN-KERNEL32-SIDEWAYSIDE-L1-1-0.DLL		N/A	1140 (0x0474)	SetUnhandledExceptionFilter	Not Bound
EXT-MS-WIN-KERNEL32-SIDEWAYSIDE-L1-1-0.DLL		N/A	1173 (0x0495)	TlsGetValue	Not Bound
EXT-MS-WIN-KERNEL32-SIDEWAYSIDE-L1-1-0.DLL		N/A	1213 (0x04BF)	VirtualProtect	Not Bound
EXT-MS-WIN-KERNEL32-SIDEWAYSIDE-L1-1-0.DLL		N/A	1215 (0x04BF)	VirtualQuery	Not Bound

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base
KERNEL32.DLL	2021/02/12 11:48	2036/02/11 2:40	632 544	A	0x0009D946	0x0009D946	x86	Console	CV,Unknown	0x6B800000	Unknown
KERNELBASE.DLL	2021/02/12 11:48	2066/10/17 17:03	2 182 176	A	0x00217A60	0x00217A60	x86	Console	CV,Unknown	0x10000000	Unknown
MSVCRT.DLL	2020/11/19 3:49	2037/09/12 14:10	775 256	A	0x000C7C0A	0x000C7C0A	x86	GUI	CV,Unknown	0x10100000	Unknown
NEPTONKOD.EXE	2021/02/27 18:11	2021/02/27 18:11	44 411	A	0x00012C56	0x00012C56	x86	Console	None	0x00400000	Unknown
NTDLL.DLL	2021/02/12 11:48	1971/11/30 5:23	1 696 248	A	0x001A9CBA	0x001A9CBA	x86	Console	CV,Unknown	0x4B280000	Unknown
BCRYPTPRIMITIVES.DLL	2021/01/27 12:23	2087/04/18 22:20	375 000	A	0x0006422D	0x0006422D	x86	Console	CV,Unknown	0x10000000	Unknown
CRYPTBASE.DLL	2020/11/19 3:49	2076/02/03 8:21	31 528	A	0x0000FBFE	0x0000FBFE	x86	Console	CV,Unknown	0x10000000	Unknown
CRYPTSP.DLL	2020/11/19 3:49	2062/07/07 22:20	72 736	A	0x0001551C	0x0001551C	x86	Console	CV,Unknown	0x52600000	Unknown

Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.

For Help, press F1

c) Az NTDLL.DLL az a dinamikusan kapcsolódó könyvtár (Dinamically Linked Library – DLL), amin keresztül a felhasználói módú folyamatok elérhetik az NT-t. Mivel az egyes objektumok közötti kapcsolattartás az LPC mechanizmuson keresztül történik, így minden felhasználói objektum az NTDLL.DLL-en keresztül éri el a környezetét.

Az NTDLL által megvalósított működés egyszerű. Ha egy hívás érkezik, ellenőrzi a hívás paramétereit, és megvalósítja a user–kernel módváltást, majd meghívja az NT kért funkciót megvalósító függvényét.