

A 2.)

- Process Utilities (Process Explorer, Process Monitor, AutoRuns): A process Explorer által megfigyelhetjük milyen handlerek és DLL vannak megnyitva és betöltve. A Process Monitor segítségével valós időben megfigyelhetjük a fájlrendszer, registryt, és folyamat/szál tevékenységet. Az AutoRuns segítségével a számítógéppel együtt automatikusan induló programot kezelhetünk, párat le is állítottam.

The image displays three Windows utility windows used for system monitoring and management.

Process Explorer: Shows a list of running processes. The 'svchost.exe' process is highlighted, showing its CPU usage (0.02%), Private Bytes (10,496 K), Working Set (25,020 K), and PID (828). Other processes like 'smss.exe', 'csrss.exe', and 'wininit.exe' are also visible.

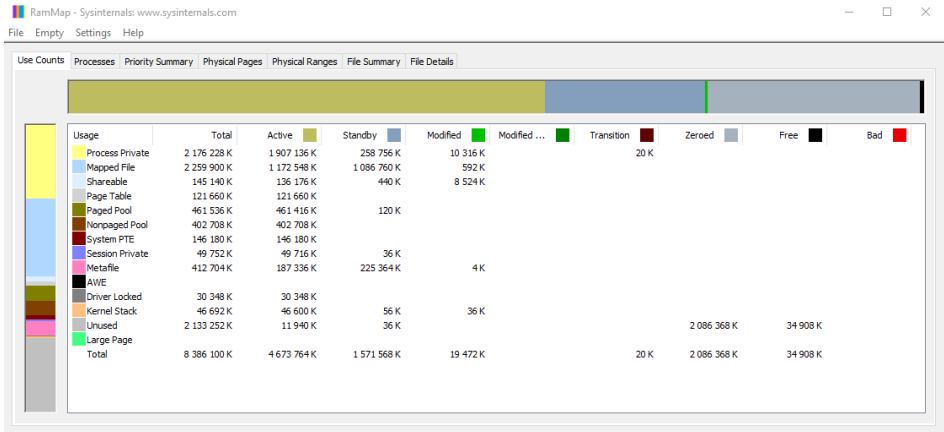
AutoRuns: Displays a list of programs and services that start automatically with the system. The 'HKLM\Software\Classes\ShellEx\ContextMenuHandlers' registry path is selected, showing various context menu handlers like 'Advanced SystemCare', 'Avast', and 'IObit Malware Fighter'.

Process Monitor: Shows a detailed log of system events, including file operations, registry changes, and process activities. The log is filtered to show events related to the 'HKLM\Software\Classes\ShellEx\ContextMenuHandlers' path.

- Security Utilities (LogonSession): Sajnos ez nekem nem működött.

```
C:\Users\juhet>logonsessions -p
'logonsessions' is not recognized as an internal or external command,
operable program or batch file.
```

- **Information Utilities (RAMMap):** Segítségével könnyű megfigyelni a adatmennyiségeket és a Ram használatot.



- Networking Utilities (TCPView): Segítségével a TCP és UDP protokollok futna.

[illegible]

- Cacheset: Szabadon választott, cache beállítások megváltoztatásában segít.

CacheSet - <http://www.sysinternals.com>

Cache Information

Current size	263728 KB
Peak size	378628 KB

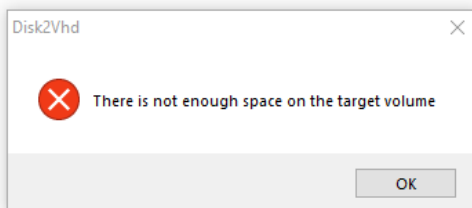
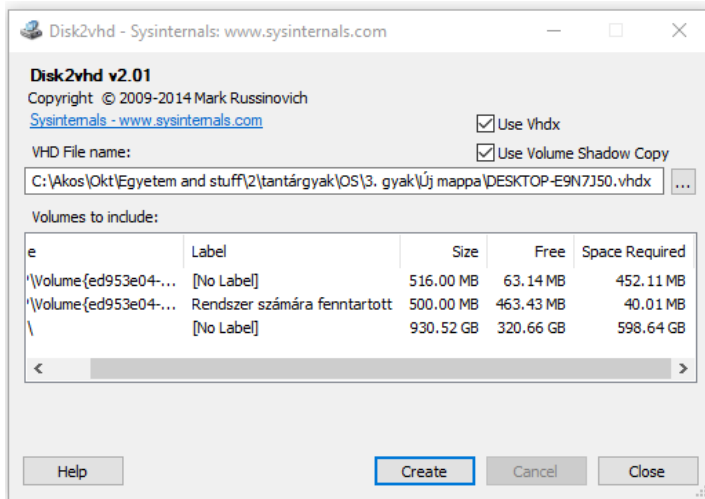
Adjust Cache Settings

Working set minimum	<input type="text" value="1024"/>	KB
Working set maximum	<input type="text" value="-4"/>	KB

Buttons: Apply, Clear, Reset, Cancel

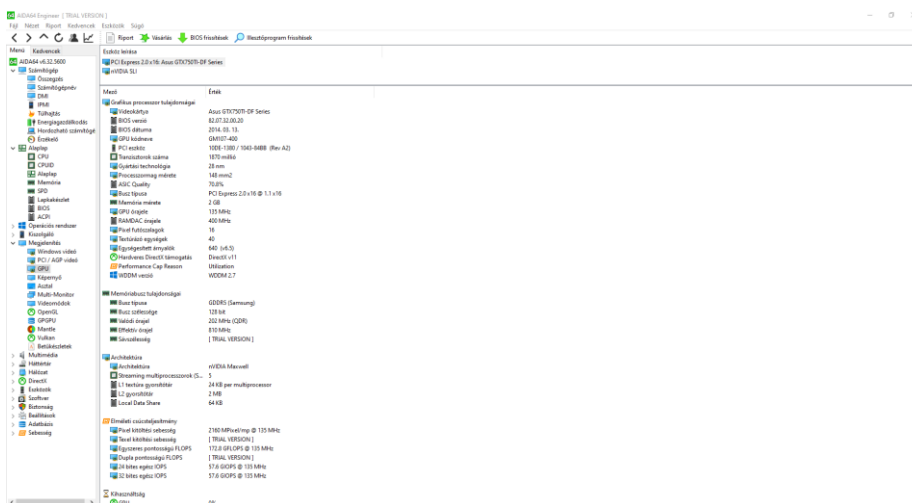
Sysinternals

- File and Disk Utilities (Disk2vhd): Sajnálatosan ez nekem nem működött.

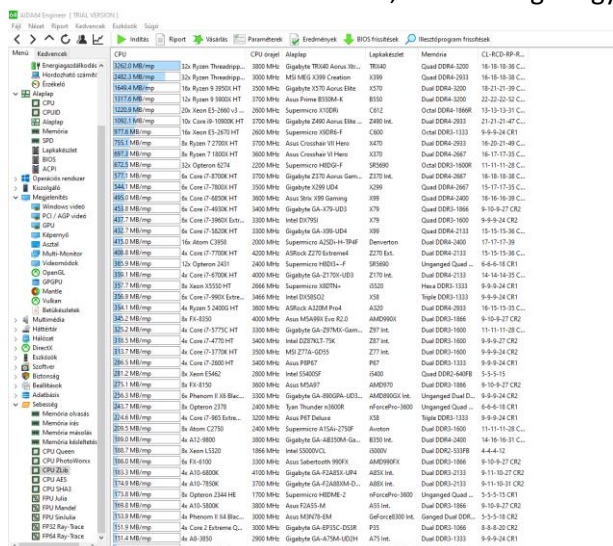


A 3.)

- GPU-Z: A számítógép beépített alkatrészeinek adatait és más paramétereket ír le.



- CPU-Z: A CPU különböző adatait, és sebességét figyelhetjük meg vele.



A 4.)

- API hívások:

- Ezeket használja:

API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL

API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL

API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL

- kernel32.dll

- függőségei:

	PI	Ordinal ^	Hint	Function	Entry Point
FSKQ8.EXE					
KERNEL32.DLL					
API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL					
NTDLL.DLL					
KERNELBASE.DLL					
NTDLL.DLL					
API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL					
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL					
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL					
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL					
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL					
EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL					
EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL					
EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL					
EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL					
EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL					
EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL					
EXT-MS-WIN-MRM-CORE-RESMANAGER-L1-1-0.DLL					
EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL					
EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL					
EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL					
EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL					
EXT-MS-WIN-ADVAPI32-NTMARTA-L1-1-0.DLL					
EXT-MS-WIN-SECURITY-CAPAUTHZ-L1-1-1.DLL					
EXT-MS-WIN-SECURITY-ENCRYPTEDFILE-L1-1-0.DLL					
EXT-MS-WIN-SECURITY-ENCRYPTEDFILE-L1-1-1.DLL					

	E	Ordinal ^	Hint	Function	Entry Point
		1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL_RtlAcquireSRWLockExclusive
		2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL_RtlAcquireSRWLockShared
		3 (0x0003)	2 (0x0002)	ActivateActCtx	0x00020080
		4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x0001B700
		5 (0x0005)	4 (0x0004)	AddAtomA	0x00059170
		6 (0x0006)	5 (0x0005)	AddAtomW	0x000128F0
		7 (0x0007)	6 (0x0006)	AddConsoleAliasA	0x00025640
		8 (0x0008)	7 (0x0007)	AddConsoleAliasW	0x00025650
		9 (0x0009)	8 (0x0008)	AddDllDirectory	api-ms-win-core-libraryloader-l1-1-0.AddDllDirectory
		10 (0x000A)	9 (0x0009)	AddIntegrityLabelToBoundaryDescriptor	0x0003BD10
		11 (0x000B)	10 (0x000A)	AddLocalAlternateComputerNameA	0x000592B0
		12 (0x000C)	11 (0x000B)	AddLocalAlternateComputerNameW	0x00059310
		13 (0x000D)	12 (0x000C)	AddRefActCtx	0x00022270

- NTDLL.DLL: Exportálja a Windows natív API-t.

[illegible]