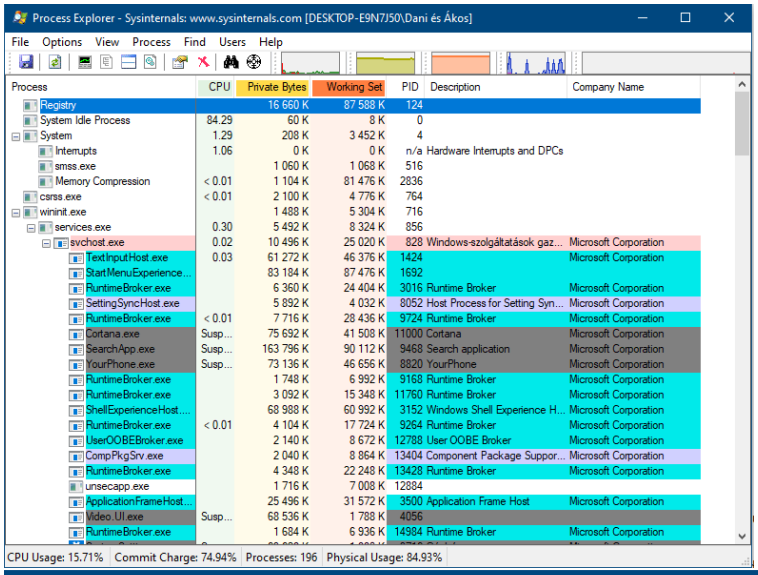
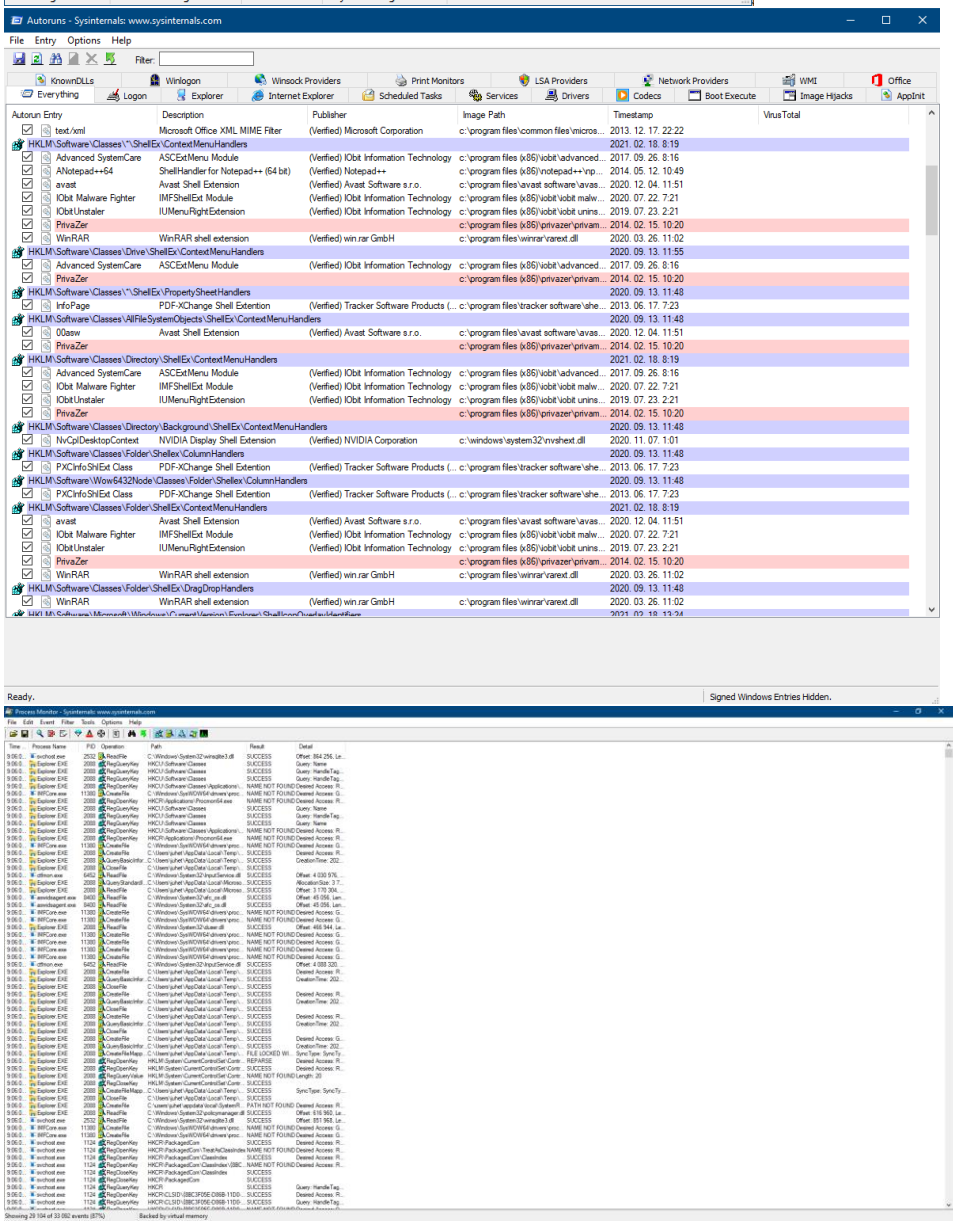
A 2.)

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

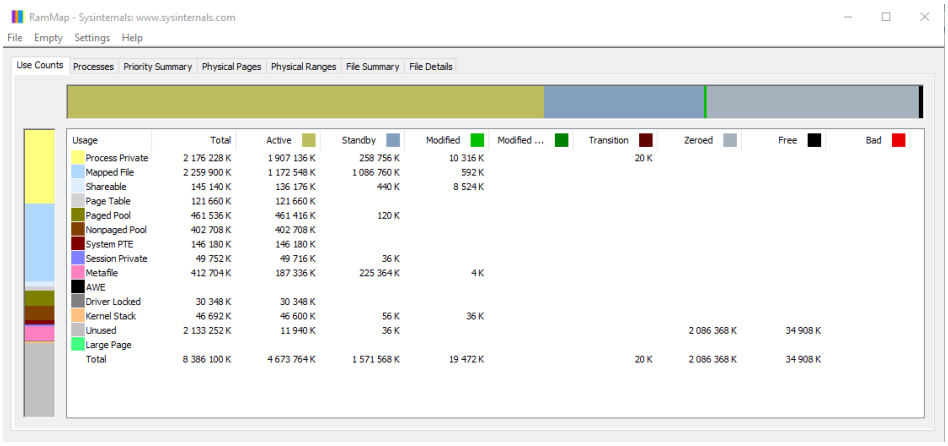




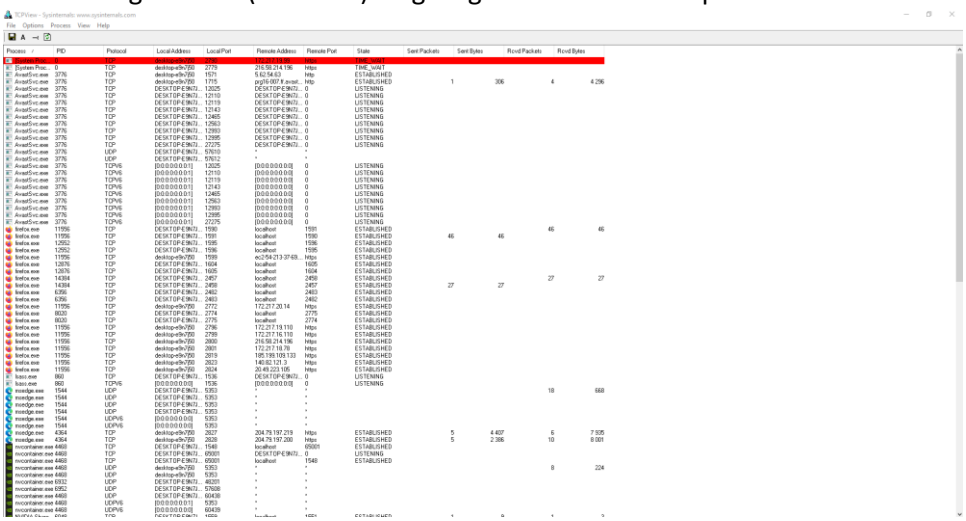
- Security Utilities (LogonSession): Sajnos ez nekem nem működött.

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

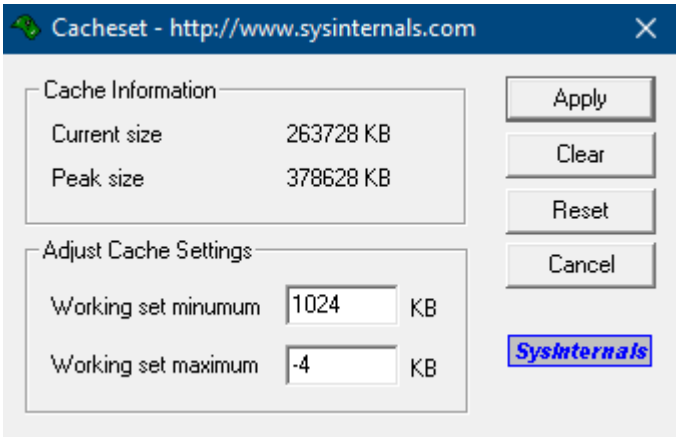
- Information Utilities (RAMMap): Segítségével könnyű megfigyelni a adatmennyiségeket és a Ram használatot.



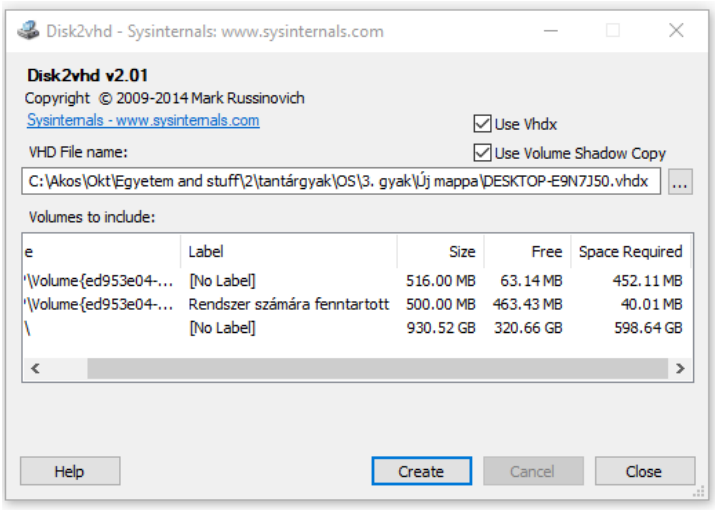
- Networking Utilities (TCPView): Segítségével a TCP és UDP protokollok futna.

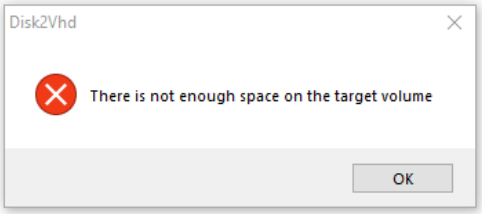


- Cacheset: Szabadon választott, cache beállítások megváltoztatásában segít.



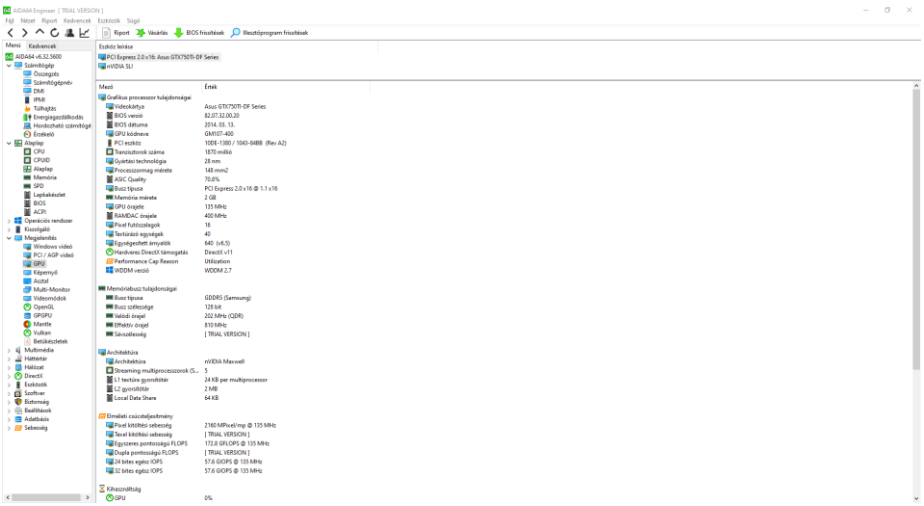
- File and Disk Utilities (Disk2vhd): Sajnálatosan ez nekem nem működött.



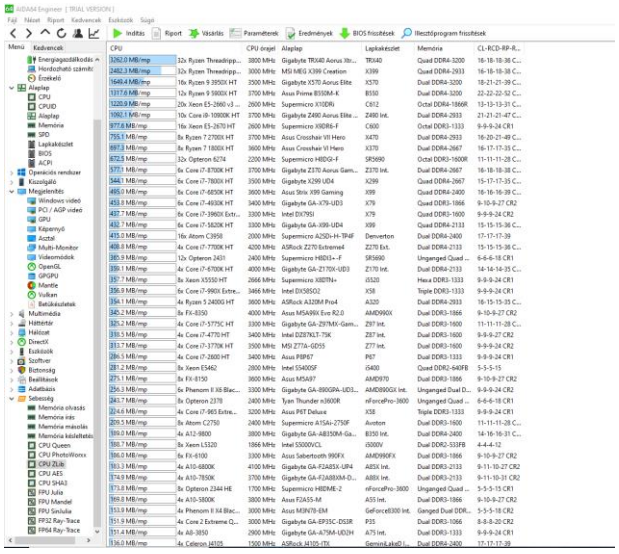


A 3.)

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



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

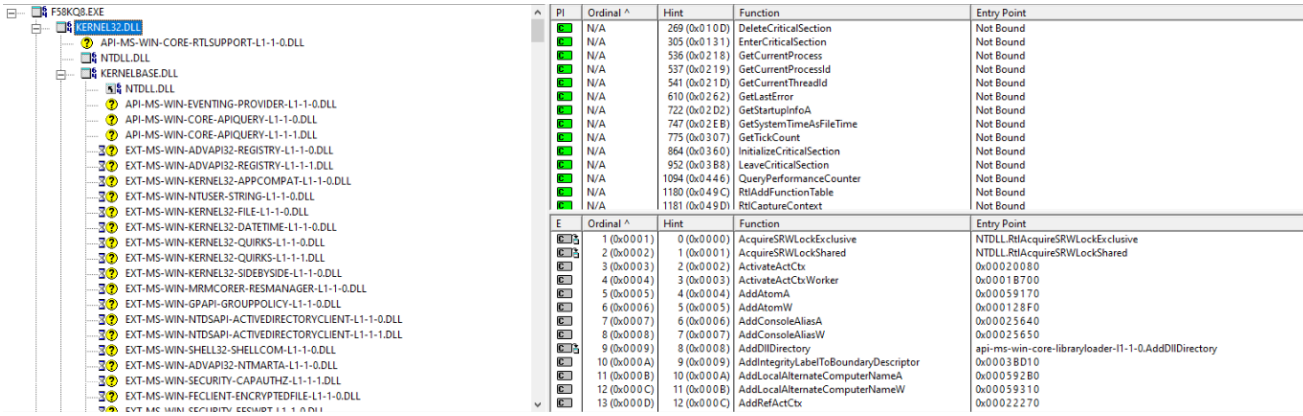


A 4.)

- 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:



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