Operációs rendszerek BSc

2. konzultáció gyakorlat

2020.02.26.

Készítette:

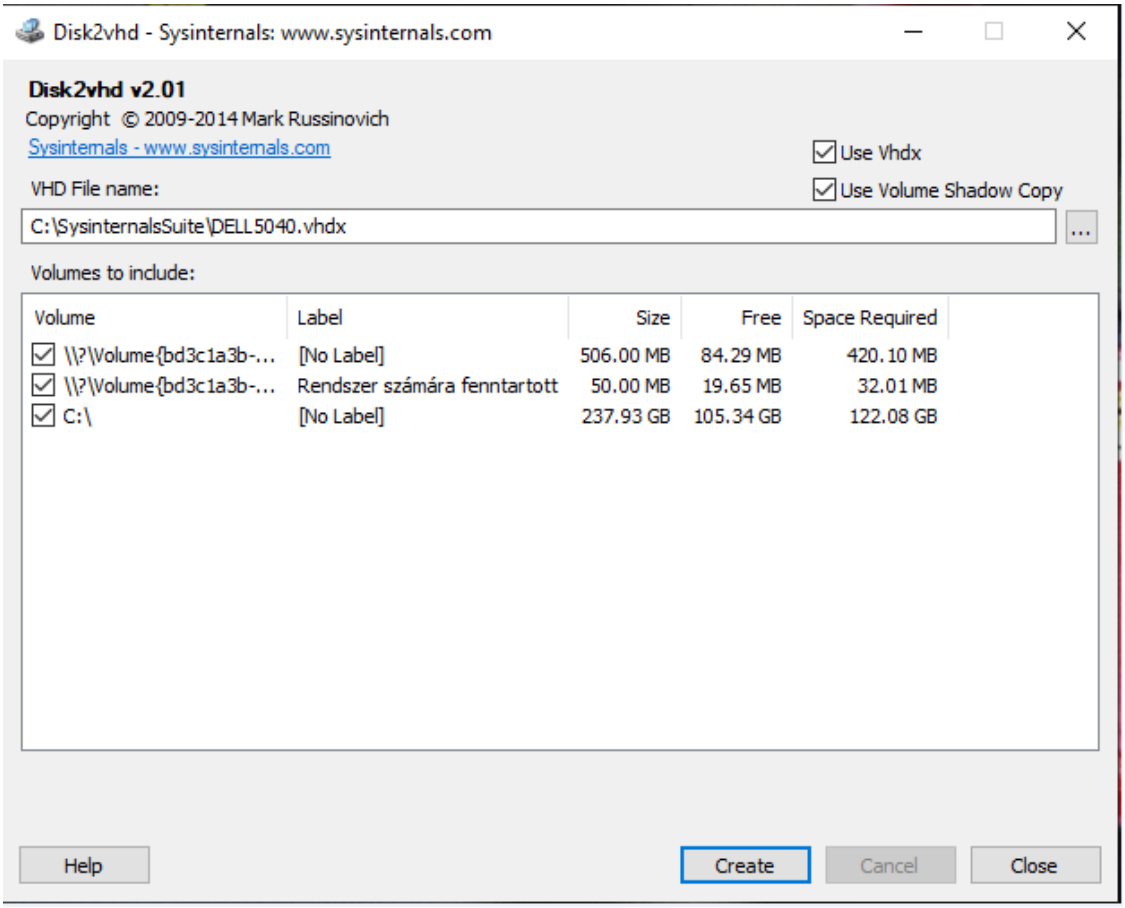
Hegedűs Attila László
Mérnök-informatikus
levelező
D2OVJ9

Miskolc, 2021

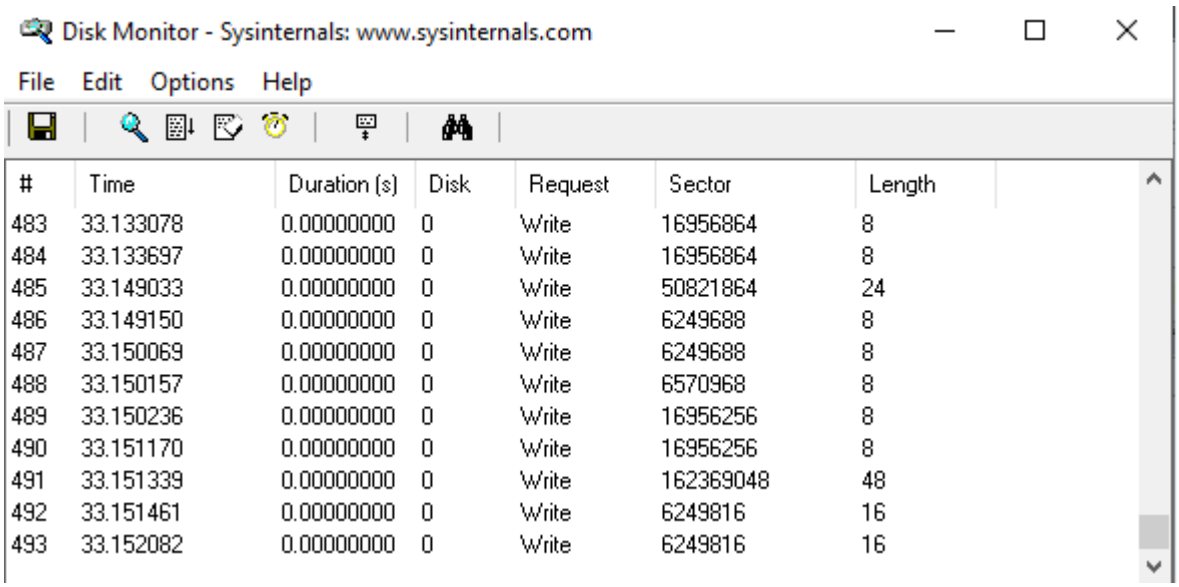
2. A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el: a) File and Disk Utilities (Disk2vhd) b) Networking Utilities (TCPView) c) Process Utilities (Process Explorer, Process Monitor, AutoRuns) d) Security Utilities (LogonSession) e) Information Utilities (RAMMap). A felsorolt eszközök közül minden eszköz esetén töltse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el a megadott dokumentumba (képernyőkép)

File and Disk Utilities

Disk2vhd – E program segítségével .vhd kiterjesztésű virtuális meghajtókat készíthetünk (Virtual Hard Drive) fizikai meghajtóinkról, akár úgy is, hogy közben fut a rendszer és aktívan használjuk azt. Ezeket például a VirtualBox, vagy Microsoft Virtual PC program segítségével hívhatjuk életre. A disk2vhd a Windows XP-ben bevezetett Volume Snapshot képesség segítségével pontos pillanatképeket készít az átalakításra kijelölt lemezkötetekről. A virtuális rendszereket használhatjuk biztonsági mentésre, tesztelésre, más gépekre való átvitelre, vagy akár biztonsági probléma miatti izolált-tesztelésre. A kezelőfelület felsorolja a célrendszer lemezköteteit jelölőnégyzetekkel, hogy kiválasszon egy bejegyzési mezőt a VHD lemeznévhez és könyvtárhoz. A Create gombbal kezdhetjük el a VHD létrehozását, ezen kívül egy Mégse, Bezárás és Help gomb tartozik a vezérlőelemekhez. A Help gomb a fejlesztő webhelyére irányít át minket.



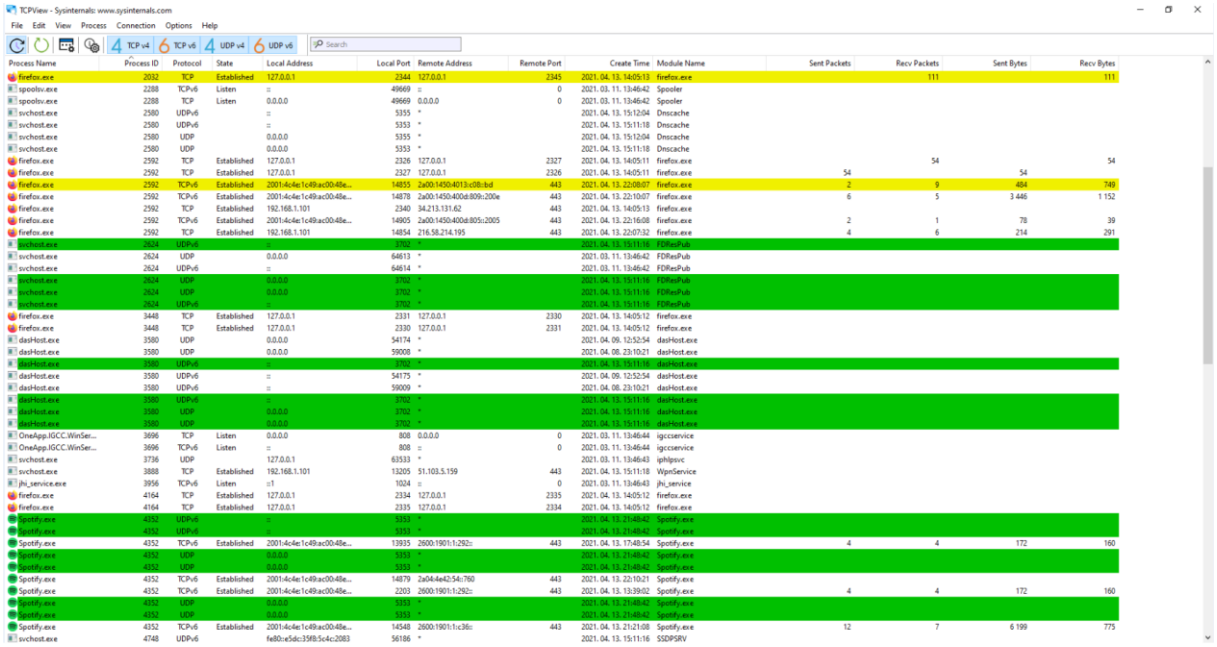
Diskmon – Megmutat minden eseményt, ami a fizikai merevlemezzel kapcsolatos. Minden írás / olvasás esetében jegyzi a lemez és használt szektor számát, az írott / olvasott adat mennyiségét, és annak időtartamát.



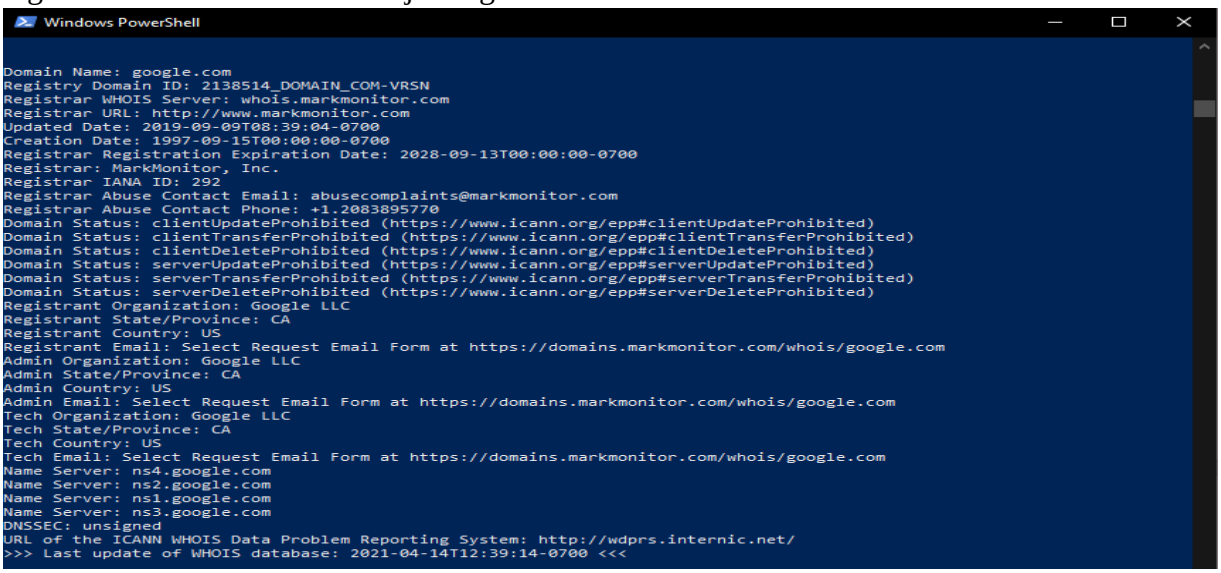
#	Time	Duration (s)	Disk	Request	Sector	Length
483	33.133078	0.00000000	0	Write	16956864	8
484	33.133697	0.00000000	0	Write	16956864	8
485	33.149033	0.00000000	0	Write	50821864	24
486	33.149150	0.00000000	0	Write	6249688	8
487	33.150069	0.00000000	0	Write	6249688	8
488	33.150157	0.00000000	0	Write	6570968	8
489	33.150236	0.00000000	0	Write	16956256	8
490	33.151170	0.00000000	0	Write	16956256	8
491	33.151339	0.00000000	0	Write	162369048	48
492	33.151461	0.00000000	0	Write	6249816	16
493	33.152082	0.00000000	0	Write	6249816	16

Networking Utilities

TCPView – Segédprogram a valós idejű folyamatok megfigyelésére, amelyek TCP vagy UDP protokollokat használnak. A szoftver megjelenít egy listát azokról az aktív alkalmazásokról és szolgáltatásokról, amelyek most csatlakoznak az internethez, és információkat nyújtanak a helyi és távoli portokról, a protokollról és a kapcsolat állapotáról, a címekről, a küldött és fogadott csomagok számáról, stb. Használhatjuk a hálózati tevékenységek nyomon követésére, internetet használó potenciális vírusok észlelésére és információt nyújt a szerverről, amelyhez aktív folyamat kapcsolódik.

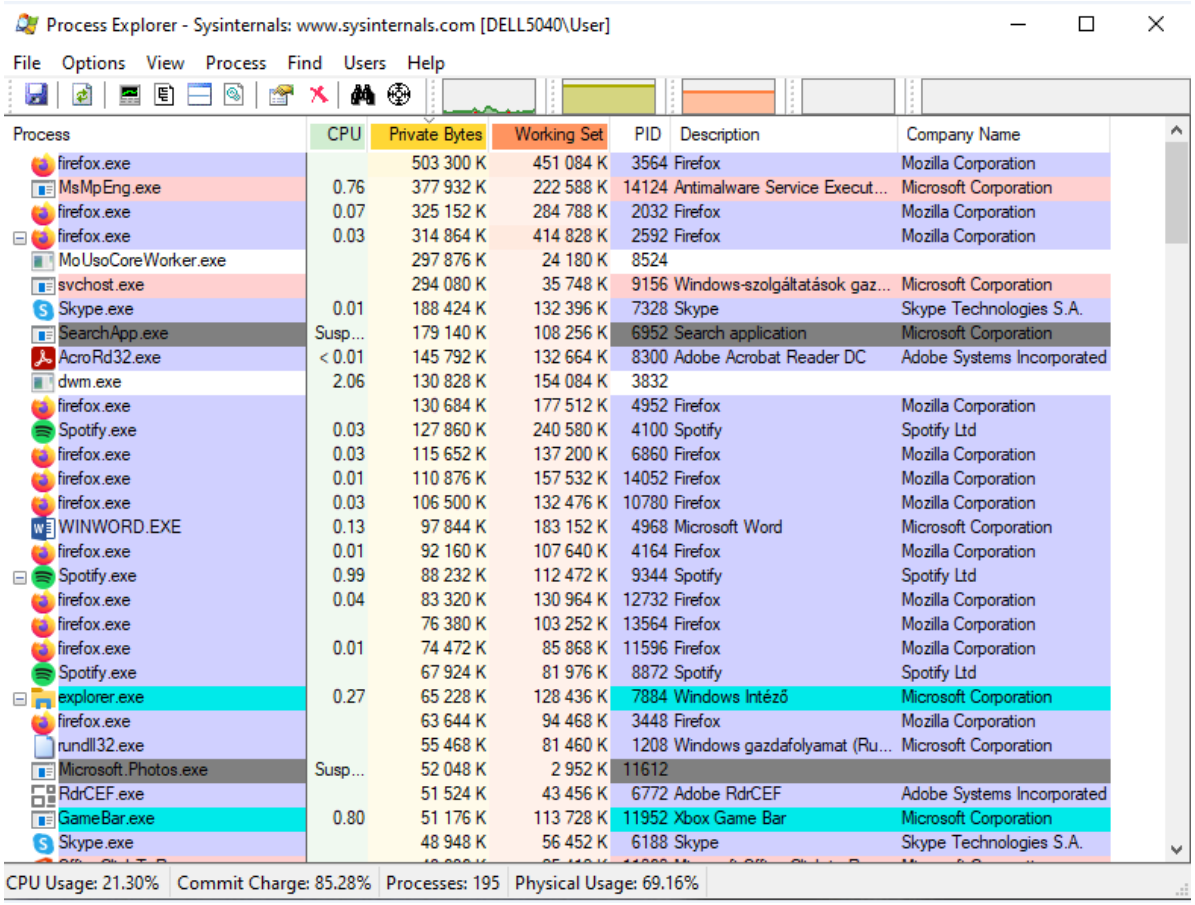


Whois – Hasonlóan a Unix parancsához, egy parancssori alkalmazás, egy domain regisztrációs információit mutatja meg.



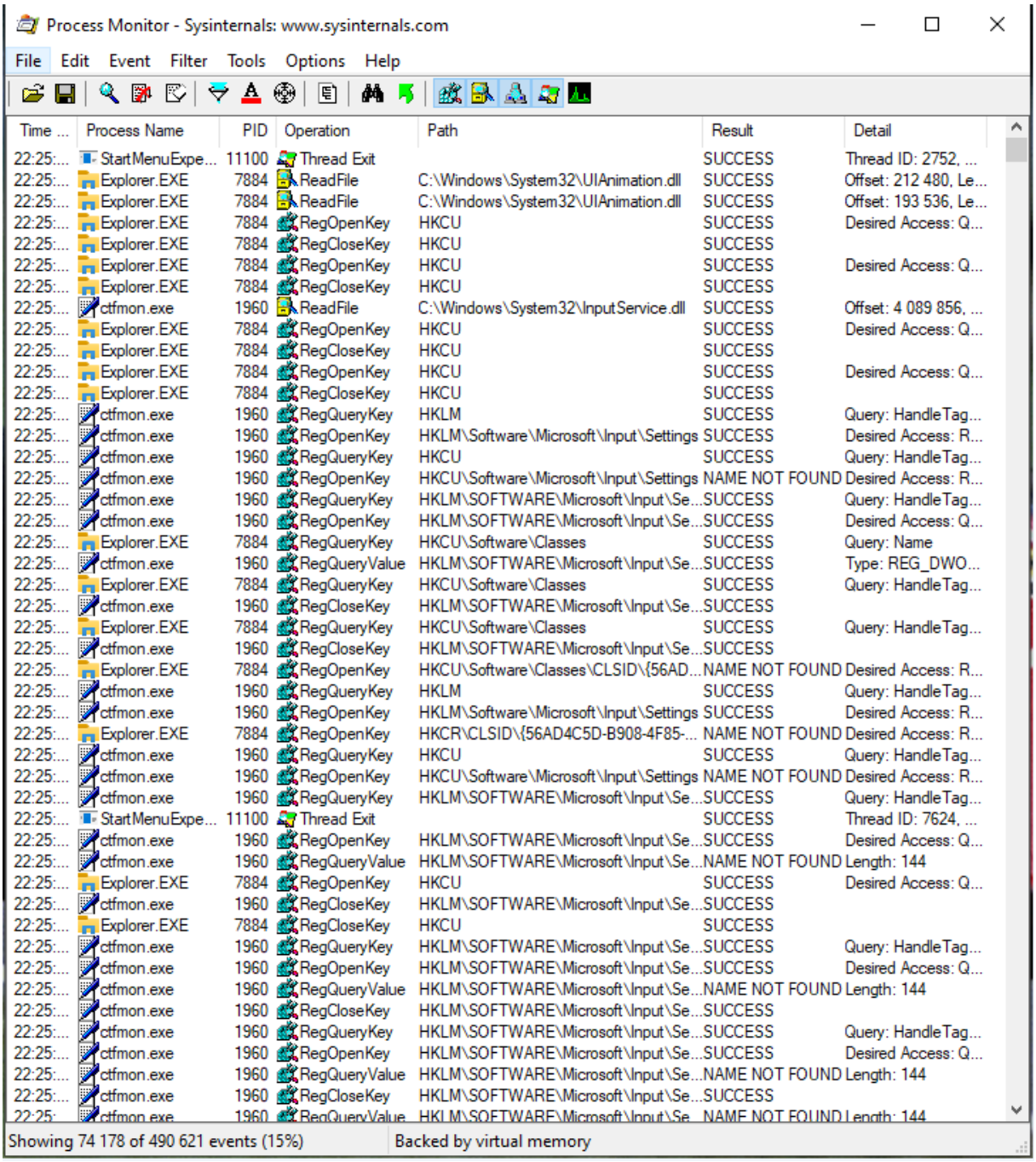
Process Utilities

Process Explorer – Fejlett figyelőeszköz, lehetővé teszi a rendszeren futó összes folyamat részletes információinak megtekintését. Segítségével részletesen nyomon követhetjük, lebonthatjuk a futó processzeket, a DLL eljárásokat vagy éppen a szolgáltatásokat. Ezeket leállíthatjuk, módosíthatjuk a prioritásukat, jellemzőit, vagy vizuálisan láthatjuk gépünk működését a monitor ablak segítségével. A felhasználói felületén megismerhetjük a folyamatok neveit, PID-jeit, az általuk igénybe vett CPU időt (CPU), a folyamat által allokált bájtok mennyiségét, melyek nem oszthatóak meg más folyamatokkal (Private Bytes), a memory manager által a folyamatnak elkülönített fizikai memória mennyiségét (Working Set), valamint a folyamat jellemzését és fejlesztőjét (Description, Company Name)



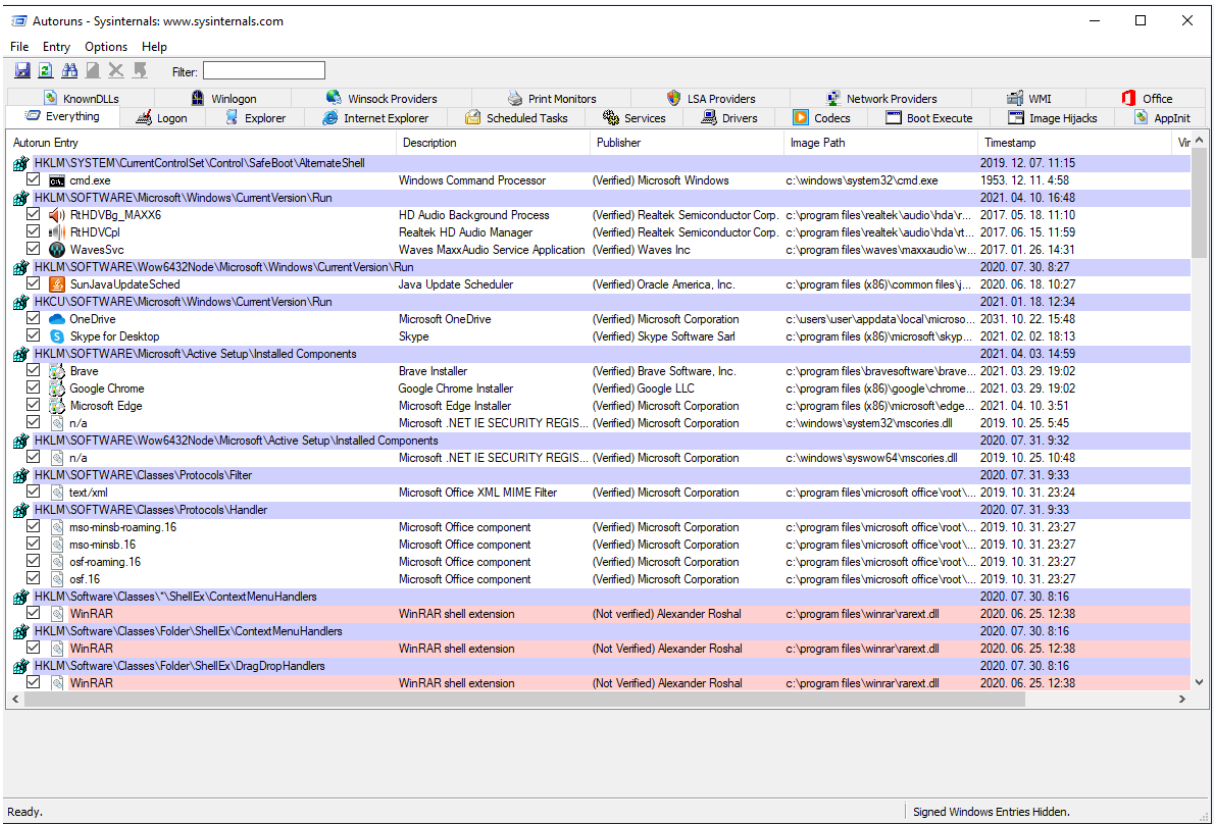
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
firefox.exe		503 300 K	451 084 K	3564	Firefox	Mozilla Corporation
MsMpEng.exe	0.76	377 932 K	222 588 K	14124	Antimalware Service Execut...	Microsoft Corporation
firefox.exe	0.07	325 152 K	284 788 K	2032	Firefox	Mozilla Corporation
firefox.exe	0.03	314 864 K	414 828 K	2592	Firefox	Mozilla Corporation
MoUsoCoreWorker.exe		297 876 K	24 180 K	8524		
svchost.exe		294 080 K	35 748 K	9156	Windows-szolgáltatások gaz...	Microsoft Corporation
Skype.exe	0.01	188 424 K	132 396 K	7328	Skype	Skype Technologies S.A.
SearchApp.exe	Susp...	179 140 K	108 256 K	6952	Search application	Microsoft Corporation
AcroRd32.exe	< 0.01	145 792 K	132 664 K	8300	Adobe Acrobat Reader DC	Adobe Systems Incorporated
dwm.exe	2.06	130 828 K	154 084 K	3832		
firefox.exe		130 684 K	177 512 K	4952	Firefox	Mozilla Corporation
Spotify.exe	0.03	127 860 K	240 580 K	4100	Spotify	Spotify Ltd
firefox.exe	0.03	115 652 K	137 200 K	6860	Firefox	Mozilla Corporation
firefox.exe	0.01	110 876 K	157 532 K	14052	Firefox	Mozilla Corporation
firefox.exe	0.03	106 500 K	132 476 K	10780	Firefox	Mozilla Corporation
WINWORD.EXE	0.13	97 844 K	183 152 K	4968	Microsoft Word	Microsoft Corporation
firefox.exe	0.01	92 160 K	107 640 K	4164	Firefox	Mozilla Corporation
Spotify.exe	0.99	88 232 K	112 472 K	9344	Spotify	Spotify Ltd
firefox.exe	0.04	83 320 K	130 964 K	12732	Firefox	Mozilla Corporation
firefox.exe		76 380 K	103 252 K	13564	Firefox	Mozilla Corporation
firefox.exe	0.01	74 472 K	85 868 K	11596	Firefox	Mozilla Corporation
Spotify.exe		67 924 K	81 976 K	8872	Spotify	Spotify Ltd
explorer.exe	0.27	65 228 K	128 436 K	7884	Windows Intéző	Microsoft Corporation
firefox.exe		63 644 K	94 468 K	3448	Firefox	Mozilla Corporation
rundll32.exe		55 468 K	81 460 K	1208	Windows gazdafolyamat (Ru...	Microsoft Corporation
Microsoft.Photos.exe	Susp...	52 048 K	2 952 K	11612		
RdrCEF.exe		51 524 K	43 456 K	6772	Adobe RdrCEF	Adobe Systems Incorporated
GameBar.exe	0.80	51 176 K	113 728 K	11952	Xbox Game Bar	Microsoft Corporation
Skype.exe		48 948 K	56 452 K	6188	Skype	Skype Technologies S.A.

Process Monitor - A Process Monitor segítségével a fájl és rendszerleíró adatbázis hozzáféréseket lehet megnézni valós időben. Ha nem futtatunk semmit a rendszerben, akkor is rengeteg háttérművelet zajlik, így érdemes mindig szűrni a rögzített műveleteket a Filter (Ctrl + L) segítségével. A leggyakoribb szűrési feltétel a folyamat neve, de rengeteg más opció beállítható. A Process Monitort különösen rejtélyes hozzáférési hibák esetén jön jól. Ilyenkor érdemes a Highlight segítségével kiemelni az érdekes sorokat, pl. ahol a Result értéke ACCESS DENIED.



Time ...	Process Name	PID	Operation	Path	Result	Detail
22:25:...	StartMenuExpe...	11100	Thread Exit		SUCCESS	Thread ID: 2752, ...
22:25:...	Explorer.EXE	7884	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 212 480, Le...
22:25:...	Explorer.EXE	7884	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 193 536, Le...
22:25:...	Explorer.EXE	7884	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
22:25:...	Explorer.EXE	7884	RegCloseKey	HKCU	SUCCESS	
22:25:...	Explorer.EXE	7884	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
22:25:...	Explorer.EXE	7884	RegCloseKey	HKCU	SUCCESS	
22:25:...	ctfmon.exe	1960	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4 089 856, ...
22:25:...	Explorer.EXE	7884	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
22:25:...	Explorer.EXE	7884	RegCloseKey	HKCU	SUCCESS	
22:25:...	Explorer.EXE	7884	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
22:25:...	Explorer.EXE	7884	RegCloseKey	HKCU	SUCCESS	
22:25:...	ctfmon.exe	1960	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
22:25:...	ctfmon.exe	1960	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: R...
22:25:...	ctfmon.exe	1960	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
22:25:...	Explorer.EXE	7884	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
22:25:...	ctfmon.exe	1960	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
22:25:...	Explorer.EXE	7884	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
22:25:...	Explorer.EXE	7884	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
22:25:...	Explorer.EXE	7884	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
22:25:...	ctfmon.exe	1960	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
22:25:...	Explorer.EXE	7884	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
22:25:...	ctfmon.exe	1960	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: R...
22:25:...	ctfmon.exe	1960	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
22:25:...	StartMenuExpe...	11100	Thread Exit		SUCCESS	Thread ID: 7624, ...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
22:25:...	ctfmon.exe	1960	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
22:25:...	Explorer.EXE	7884	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
22:25:...	ctfmon.exe	1960	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
22:25:...	Explorer.EXE	7884	RegCloseKey	HKCU	SUCCESS	
22:25:...	ctfmon.exe	1960	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
22:25:...	ctfmon.exe	1960	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
22:25:...	ctfmon.exe	1960	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
22:25:...	ctfmon.exe	1960	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
22:25:...	ctfmon.exe	1960	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
22:25:...	ctfmon.exe	1960	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
22:25:...	ctfmon.exe	1960	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
22:25:...	ctfmon.exe	1960	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144

AutoRuns – Autostart-nak nevezzük azokat a szoftvereket, melyek automatikusan indulnak el, anélkül, hogy a felhasználó saját akaratából indítaná el azokat. Ezek lehetnek driverek, szolgáltatások, melyek a gép bootolása után indulnak. Ezek nagyon hasznosak lehetnek, de programok telepítése közben nem kívánt felesleges kiegészítők is települhetnek a gépre, gondolok itt például a vicces több, soros Internet Explorer bővítmény sorokra. Feleslegesek lehetnek azok a háttérben futó rejtett folyamatok, melyek a programok gyorsabb elindításáért felelősek, ezen kívül akár malware-ek is működhetnek a felhasználó tudta nélkül a háttérben. Az AutoRuns segítségével azonosíthatunk minden magától induló szoftvert, folyamatot, megkönnyíti azok leállítását, autostartok kikapcsolását.



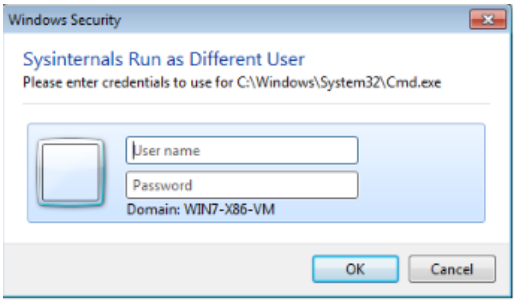
Security Utilities

LogonSession – Ha azt hisszük, mikor bejelentkezünk a számítógépünkre, akkor ez az egyetlen aktív logon session, ez az alkalmazás nagy meglepetést okozhat. A LogonSessions listáz minden aktív bejelentkezést, a -p opcióval visszatéríti a session-ök által futtatott processzeket. Az én számítógépem esetében összesen 71 logon session-t mértem.

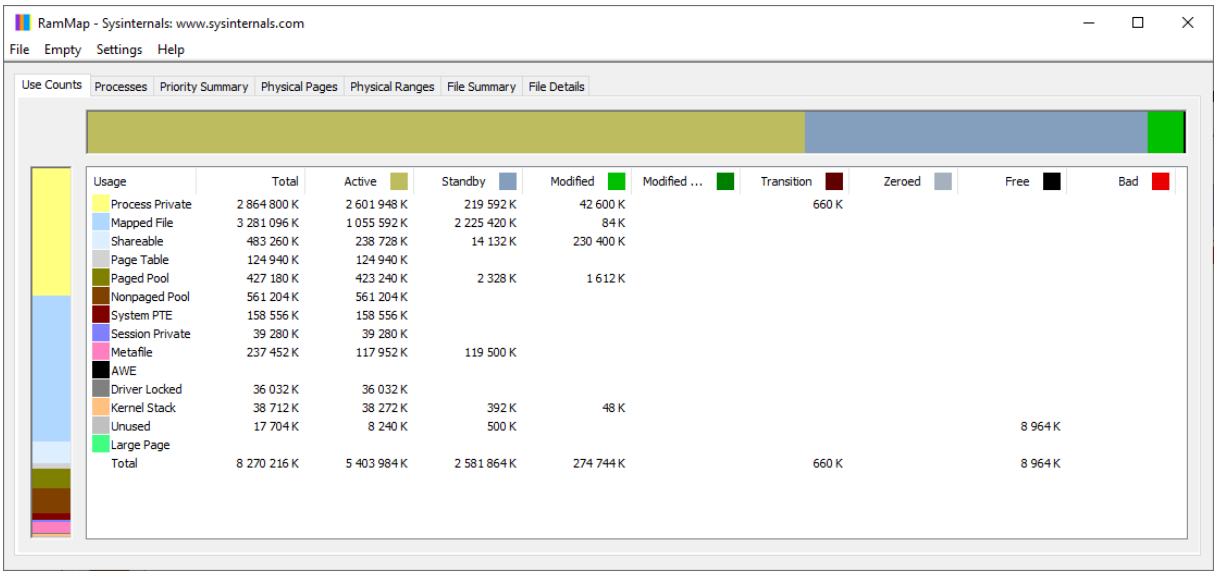
```
Administrator: Windows PowerShell
PS C:\SysinternalsSuite> .\logonsessions.exe -p

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\DELL5040$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   2021. 03. 11. 13:46:41
    Logon server:
    DNS Domain:
    UPN:
      764: lsass.exe
      968: svchost.exe
      752: svchost.exe
     1248: svchost.exe
     1264: svchost.exe
     1272: svchost.exe
     1436: IntelCpHDCPSvc.exe
     1452: svchost.exe
     1500: svchost.exe
     1652: IntelCpHeciSvc.exe
     1884: svchost.exe
     1904: svchost.exe
     1060: svchost.exe
     2104: igfxCUIService.exe
     2172: svchost.exe
     2676: RtkAudioService64.exe
     2780: svchost.exe
     2848: svchost.exe
     2988: svchost.exe
     2288: spoolsv.exe
     3504: svchost.exe
     3612: armsvc.exe
     3624: svchost.exe
     3696: OneApp.IGCC.WinService.exe
     3736: svchost.exe
     3800: svchost.exe
     3860: RstMwService.exe
     3888: svchost.exe
     3956: jhi_service.exe
     3992: svchost.exe
     4228: WmiPrvSE.exe
     4456: svchost.exe
     5012: svchost.exe
```

```
Administrator: Windows PowerShell
PS C:\SysinternalsSuite> .\logonsessions.exe

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\DELL5040$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   2021. 03. 11. 13:46:41
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000bdc3:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   2021. 03. 11. 13:46:41
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:0000c1d0:
    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. 03. 11. 13:46:41
    Logon server:
    DNS Domain:
    UPN:

[3] Logon session 00000000:000003e4:
    User name:    WORKGROUP\DELL5040$
    Auth package: Negotiate
    Logon type:   Service
    Session:      0
    Sid:          S-1-5-20
    Logon time:   2021. 03. 11. 13:46:41
    Logon server:
    DNS Domain:
    UPN:
```

ShellRunAs – Segítségével más felhasználóként indíthatunk el programokat.

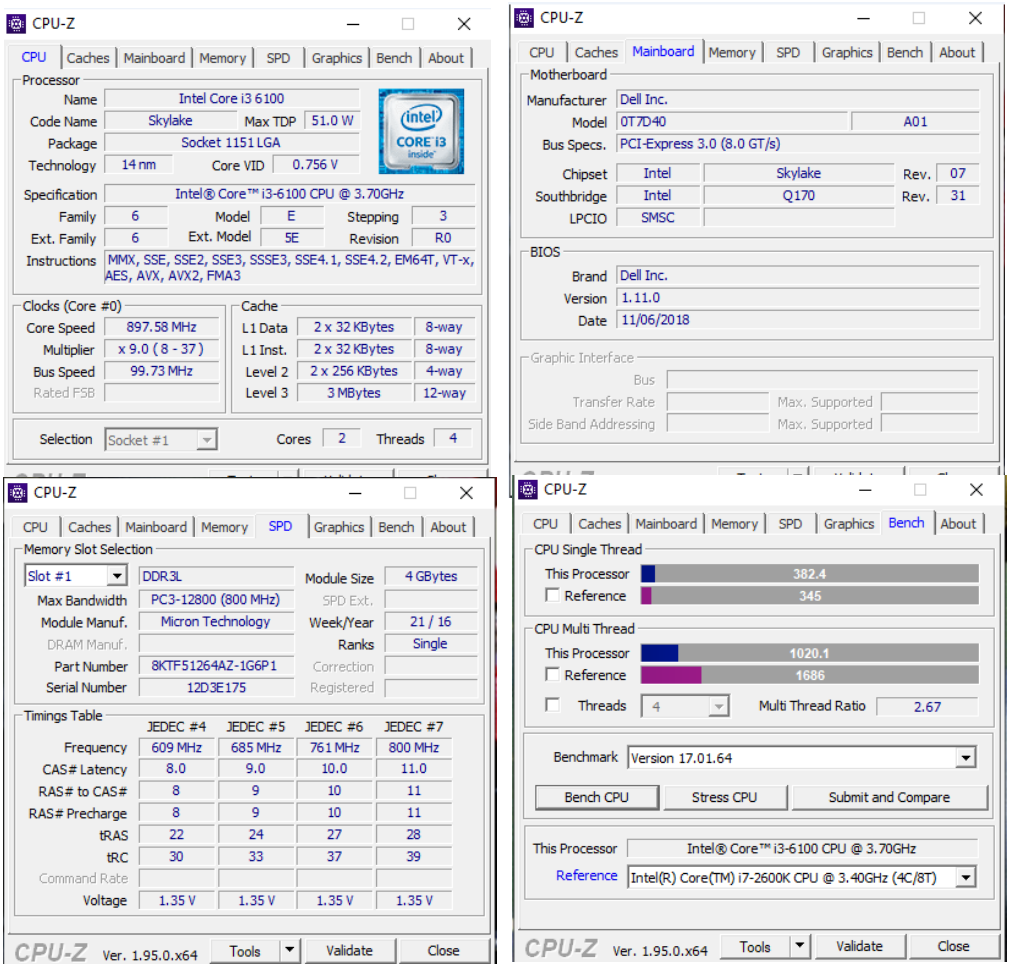


RAMMap – Egy fejlett fizikai memória használat elemző alkalmazás Windows-ra, különböző módokon keresztül ábrázolja a memória használatára vonatkozó információkat. A felületén 7 fület találunk, 1.Use Counts: memóriahasználat összegzése típusonként és lapozólistákként, 2.Processes: folyamatok és általuk felhasznált memória, 3.Priority Summary: prioritás szerinti összegzés, 4.Physical Pages: az összes fizikai memória használata laponként, 5.Physical Ranges: a fizikai memória címek szerint, 6.File Summary: file adatok a RAM-ban fájlonként, 7.File Details: az egyéni fizikai lapok fájlonként.

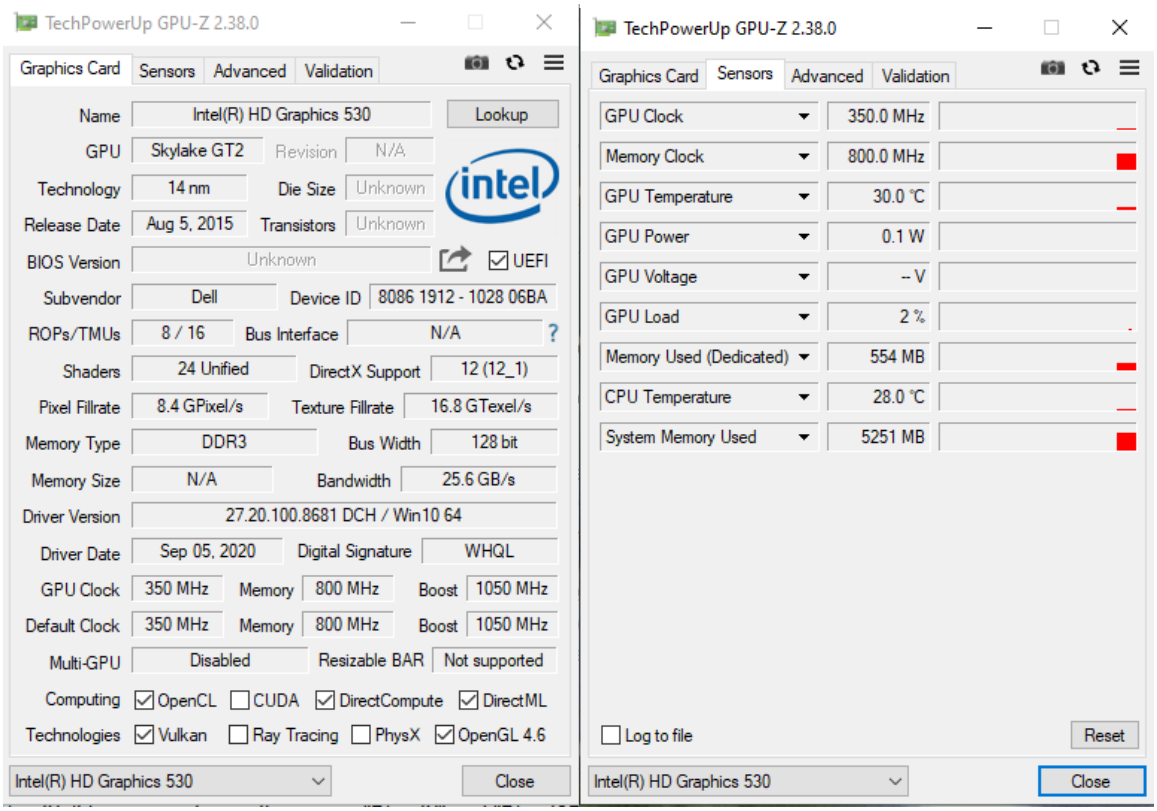


Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	2 864 800 K	2 601 948 K	219 592 K	42 600 K		660 K			
Mapped File	3 281 096 K	1 055 592 K	2 225 420 K	84 K					
Shareable	483 260 K	238 728 K	14 132 K	230 400 K					
Page Table	124 940 K	124 940 K							
Paged Pool	427 180 K	423 240 K	2 328 K	1 612 K					
Nonpaged Pool	561 204 K	561 204 K							
System PTE	158 556 K	158 556 K							
Session Private	39 280 K	39 280 K							
Metafile	237 452 K	117 952 K	119 500 K						
AWE									
Driver Locked	36 032 K	36 032 K							
Kernel Stack	38 712 K	38 272 K	392 K	48 K					
Unused	17 704 K	8 240 K	500 K					8 964 K	
Large Page									
Total	8 270 216 K	5 403 984 K	2 581 864 K	274 744 K		660 K		8 964 K	

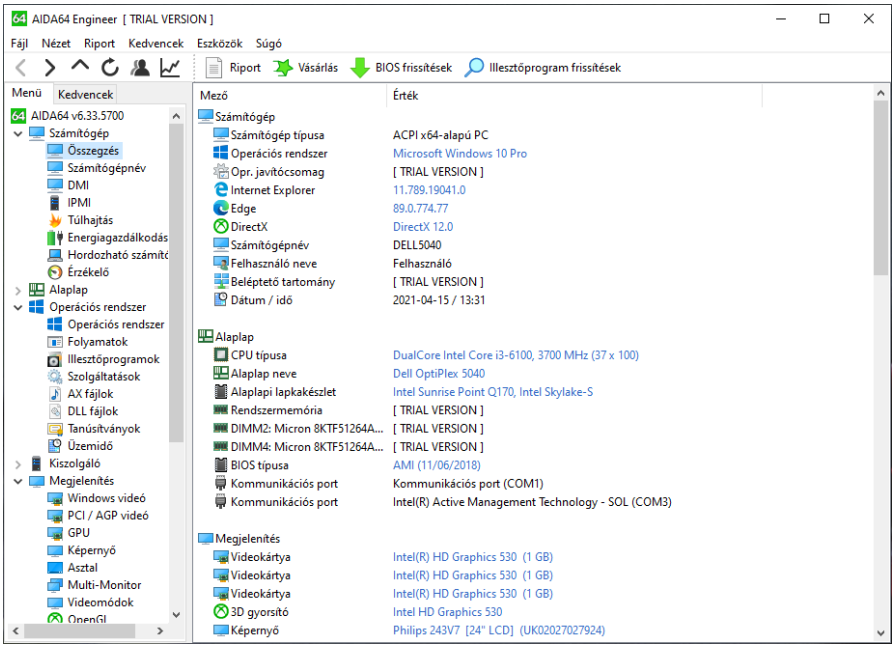
CPU-Z – Egy ingyenes hardveranalizáló szoftver, mely központjában a processzor áll. A CPU fülben megtalálható minden információ a processzorról, megjelenik például a pontos típusa, foglalata, a magok aktuális sebessége, feszültsége, adatok az instrukciókészletéről, a cache-re vonatkozó adatok. A Caches fülön ugyanezeket láthatjuk, megfigyelhetjük, hogy a Level 1 Data-Cache a legkisebb méretű, és leggyorsabb elérésű, a Level 3 Cache pedig nagyobb kapacitású, ugyanakkor lassabb adatátvitelt tesz lehetővé. A Mainboard fül az alaplapra vonatkozó adatokat ábrázolja, láthatjuk a gyártót, a modell nevét, a busz specifikációját, fontos lehet még a BIOS-ra vonatkozó információ, egy gyors keresés után rögtön megtudhatjuk, hogy a legfrissebb verzióval rendelkezik-e a számítógépünk. A Memory fülön a memóriáról kapunk általános információkat, mint a típusa, mérete, sebessége, single vagy dual channel, és az időzítésükre vonatkozó információk. Itt észrevételezhetjük, ha a memóriánk lassabban működik, mint az képes lenne, felmerülhet, hogy elfelejtettük beállítani a BIOS-ban az XMP-t. A következő az SPD(Serial Presence Detect) fül, melyen az egyes memória moduljainkról kapunk részletes információt. A Graphics fül a videókártyáról, grafikus vezérlőről nyújt információkat. A Bench fülön pedig rövid benchmarkot futtathatunk és stress testelhetünk, akár referenciaként megadott processzorok „ellen” is.



GPU-Z – Hasonlóan a CPU-Z-hez egy ingyenes szoftver, a tárgya azonban a CPU helyett a GPU részletes elemzése. A Graphics Card fülön a videókártyánkról kapunk részletbemenő információkat, láthatjuk például a típusát, adatátviteli képességeit, órajelét, memória méretét stb. A Sensors fülön a kártyánk szenzorainak méréseit olvashatjuk le, órajel, memória órajel, hőmérséklet, áramerősség, feszültség, terhelés. Érdekes, hogy esetemben egy integrált grafikus vezérlőről beszélünk, szenzorok azonban +/- 1-2 fok eltérést mutatnak a processzor és a GPU hőmérséklete között. Az Advanced fülön részletesebb információkat kaphatunk a driverünkről, API támogatásainkról stb. A Validation fülön a GPU-Z általi méréseket oszthatjuk meg.



AIDA64 – Windows-felhasználóknak szánt rendszerinformációs, -diagnosztikai és sebességmérő alkalmazás. A program rettentően széleskörű, szinte bármit megtalálhatunk benne, amit a hardverünkről és operációs rendszerünkről tudni lehet. Az információkon kívül képes stressztesztre, a komplett számítógép sebességmérésére, és a kapott eredmények összehasonlítására más AIDA64 felhasználókkal, megmutathatja nekünk az összes futó folyamatot és azok erőforrás használatát, láthatjuk segítségével az összes .dll fájlt, ami a gépünkön van stb. A bal oldali hasáb Menü fülén találunk minden elérhető opciót.



Források:

Mark Russinovich, Aaron Margosis: Windows Sysinternals Administrator's Reference
https://numlockholmes.blog.hu/2010/03/21/fizikai_gep_virtualizacioja
https://hu.multipurposeweb.com/software/669035
https://hu.vessoft.com/software/windows/download/tcpview
http://hu.tipsandtricks.tech/a-process-monitor-es-a-process-explorer-hasznalata
http://www.szoftverbazis.hu/szoftver/microsoft-process-explorer-v11-32-AI14.html
http://mit.bme.hu/~micskeiz/education/meres4/meres-labor-4-windows-segedlet.pdf
https://community.chocolatey.org/packages/logonsessions
https://www.aida64.hu/kezikonyv/aida64-kezikonyv
https://itcafe.hu/cikk/hardver_diagnosztika_aida_hds_ashampoo_speccy_ahdm/aida64.html
https://docs.microsoft.com/en-us/sysinternals/downloads/rammap