

```
Administrator: C:\Windows\System32\cmd.exe
Usage: ntfsinfo64 [-nobanner] [-accepteula] <drive letter>
-nobanner    Do not display the startup banner and copyright message.

D:\Doksik\2. félév\OS\utilities\NTFSInfo>ntfsinfo64 C

NtfsInfo v1.2 - NTFS Information Dump
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Volume Size
-----
Volume size          : 238117 MB
Total sectors        : 487663983
Total clusters       : 60957997
Free clusters        : 26538575
Free space           : 103666 MB (43% of drive)

Allocation Size
-----
Bytes per sector     : 512
Bytes per cluster    : 4096
Bytes per MFT record : 0
Clusters per MFT record: 0

MFT Information
-----
MFT size             : 587 MB (0% of drive)
MFT start cluster    : 786432
MFT zone clusters    : 46933632 - 46983072
MFT zone size        : 193 MB (0% of drive)
MFT mirror start     : 2

Meta-Data files
-----
D:\Doksik\2. félév\OS\utilities\NTFSInfo>
```

File and Disk Utilities közül: NTFSInfo

Ez a szoftver egy a partíciónk egyedi karakterét váró bemeneti paraméterrel különböző információkat ad az adott területről, amely szigorúan NTFS formátummal rendelkezik. (szektorok és klaszterek száma, szabad hely, allokalicázíós méret, MFT-vel kapcsolatos adatok, stb.)

```
Administrator: C:\Windows\System32\cmd.exe

Logon type: Interactive
Session: 5
Sid: S-1-5-21-3756175659-1382176547-1371571965-1001
Logon time: 2021. 02. 17. 7:45:26
Logon server: DESKTOP-VIIQUBJ
DNS Domain:
UPN:

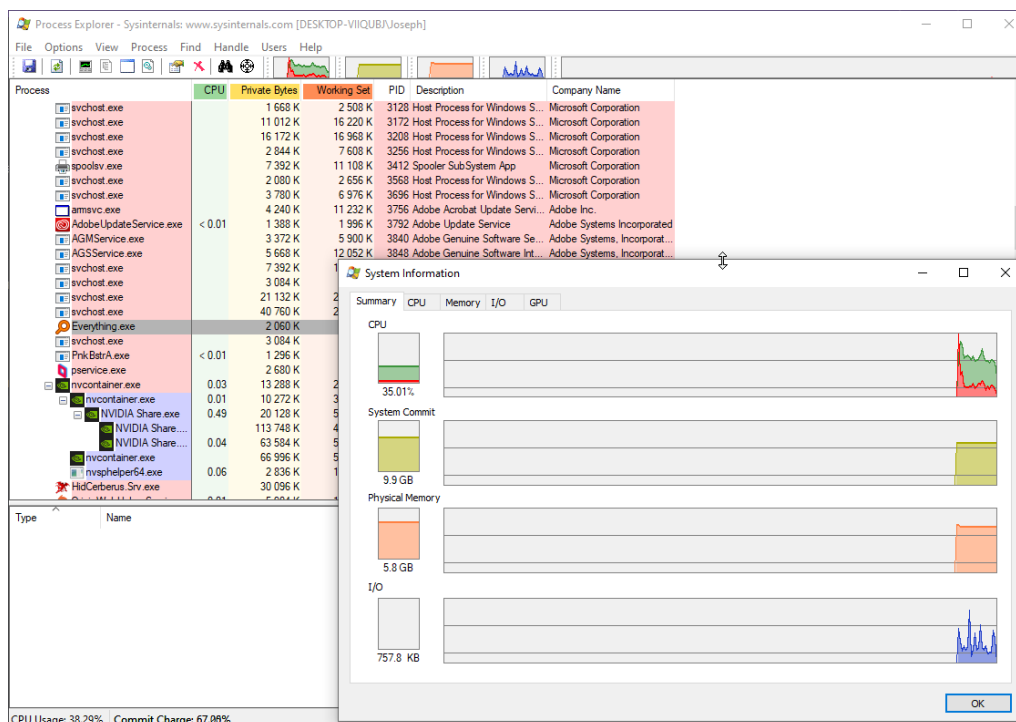
[14] Logon session 00000000:14eb23d4:
User name: DESKTOP-VIIQUBJ\Joseph
Auth package: NTLM
Logon type: Interactive
Session: 5
Sid: S-1-5-21-3756175659-1382176547-1371571965-1001
Logon time: 2021. 02. 17. 7:45:26
Logon server: DESKTOP-VIIQUBJ
DNS Domain:
UPN:

[15] Logon session 00000000:1b9a31c6:
User name: DESKTOP-VIIQUBJ\Joseph
Auth package: NTLM
Logon type: Interactive
Session: 6
Sid: S-1-5-21-3756175659-1382176547-1371571965-1001
Logon time: 2021. 02. 18. 9:43:52
Logon server: DESKTOP-VIIQUBJ
DNS Domain:
UPN:

[16] Logon session 00000000:1b9a3221:
User name: DESKTOP-VIIQUBJ\Joseph
Auth package: NTLM
Logon type: Interactive
Session: 6
Sid: S-1-5-21-3756175659-1382176547-1371571965-1001
Logon time: 2021. 02. 18. 9:43:52
```

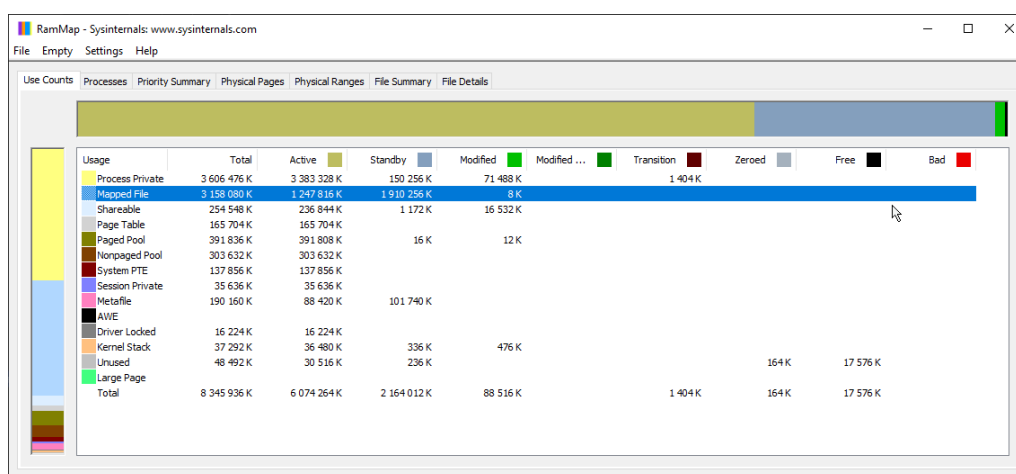
Security Utilities közül: LogonSessions

A program információt arról, hogy az adott végberendezés sessionjeit melyik felhasználó használja, mióta, milyen módon, melyik szerveren (ha a számítógép esetlegesen egy belső hálózaton lenne felkonfigurálva).



Process Utilities közül: Process Explorer

Ez a szoftver egy folyamat megfigyelő, mely a Task Manager-hez képest sokkal részletesebb leírást nyújt az adott processekről, rendszer információkról. Leginkább DLL verzió hibakezelésre alkalmazzák a leggyakrabban, mert ez a program segít abban, hogy kiszűrje mely processzek milyen DLL fájlt töltenek be.



Information Utilities közül: RAMMap

A program segít megértetni velünk, hogy a Windows hogyan kezeli a fizikai memóriát. Megmutatja, hogy az összes RAM-ból (az én esetemben 8 GB – 8 345 936 K) bizonyos részei milyen használat alatt van, mint például 3 GB körüli memóriaterület mapped file által lefoglalt terület van jelen, melyből ennek az 1/3-ad része aktív, azaz adott fájlok tárgya a virtuális memóriában aktív feldolgozás alatt vannak, míg a maradék 2/3-ad része még sorban áll.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

A P F

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets
chrome.exe	13400	TCP	desktop-viiqbu.jo...	59183	140.82.113.26	https	ESTABLISHED			
chrome.exe	1080	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	13400	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	1080	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	1080	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	13400	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	13400	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	13400	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	1080	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	1080	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	13400	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	13400	UDP	DESKTOP-VIIQBUJ	5353	*	*				
chrome.exe	13400	TCPV6	[2001::4::e:2184...	49644	[2001::1450::4025...	5228	ESTABLISHED			
chrome.exe	1080	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*				
chrome.exe	1080	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*				
chrome.exe	1080	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*				
chrome.exe	13400	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*				
chrome.exe	13400	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*				
chrome.exe	13400	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*				
Discord.exe	15460	TCP	DESKTOP-VIIQBUJ	6463	DESKTOP-VIIQBUJ	0	LISTENING			
Discord.exe	2176	TCP	desktop-viiqbu.jo...	58155	162.158.137.232	https	ESTABLISHED			
Discord.exe	2176	TCP	desktop-viiqbu.jo...	58006	162.158.137.235	https	ESTABLISHED			
Discord.exe	2176	TCP	desktop-viiqbu.jo...	59255	162.158.136.234	https	ESTABLISHED			
Discord.exe	15460	UDP	DESKTOP-VIIQBUJ	57329				319	286 605	
Discord.exe	2176	TCPV6	[2001::4::e:2184...	59486	[2001::1450::400d...	https	ESTABLISHED			
Discord.exe	2176	TCPV6	[2001::4::e:2184...	58533	[2001::1901::1452...	https	ESTABLISHED			
lsass.exe	976	TCP	DESKTOP-VIIQBUJ	49664	DESKTOP-VIIQBUJ	0	LISTENING			
lsass.exe	976	TCPV6	[0:0:0:0:0:0:0:0]	49664	[0:0:0:0:0:0:0:0]	0	LISTENING			
nvcontainer.exe	4112	TCP	DESKTOP-VIIQBUJ	64465	localhost	65001	ESTABLISHED			
nvcontainer.exe	4112	TCP	DESKTOP-VIIQBUJ	65001	localhost	64465	ESTABLISHED			
nvcontainer.exe	4112	UDP	DESKTOP-VIIQBUJ	65001	DESKTOP-VIIQBUJ	0	LISTENING			
nvcontainer.exe	4112	UDP	desktop-viiqbu.jo...	5353	*	*				
nvcontainer.exe	4112	UDP	desktop-viiqbu.jo...	5353	*	*				
nvcontainer.exe	4112	UDP	desktop-viiqbu.jo...	5353	*	*				

Endpoints: 246 Established: 30 Listening: 51 Time Wait: 26 Close Wait: 10

Networking Utilities közü: TCPView

Ez a szoftver leírást ad bizonyos folyamatokról, pontosan azok, amelyek TCP vagy UDP protollok szerint dolgoznak. A szoftver segít beazonosítani, hogy mely programok csatlakoznak az internetre, és mennyi adatot fogadtak/küldtek, lokálisan hol találhatóak meg, milyen a státuszuk.

Autoruns

Ez a program leírást ad, hogy mely szoftverek indulnak el miután az operációs rendszer bootolása befejeződött. Nem feltétlenül csak szoftverek listáját adja meg, hanem emellé megnézhetjük mely DLL fájlok, szolgáltatások, driverek, Codec-ek indulnak el. A lista indulás sorrendje szerint van prezentálva, és minden esetben a cmd.exe lesz az az alapprogram ami legelőször elindul.