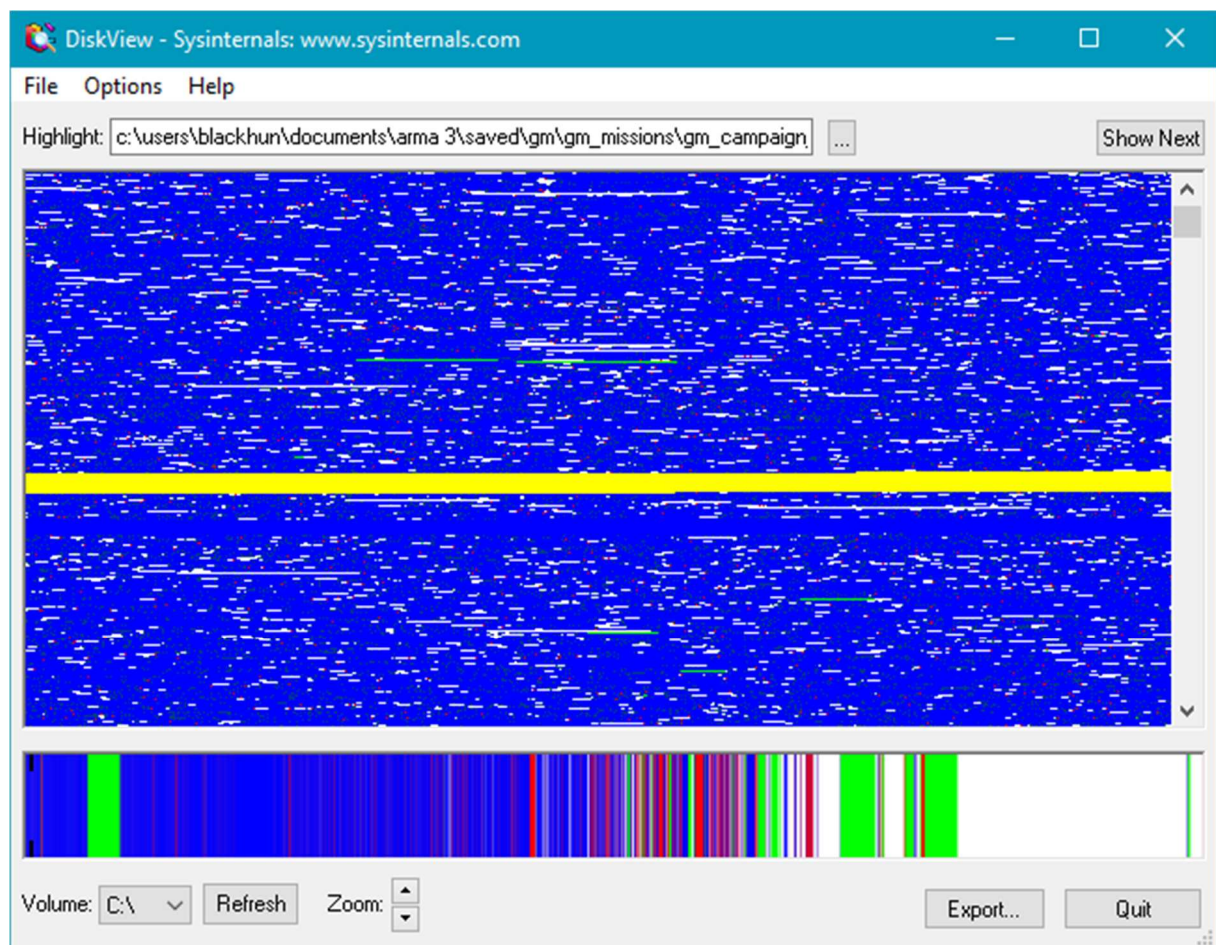
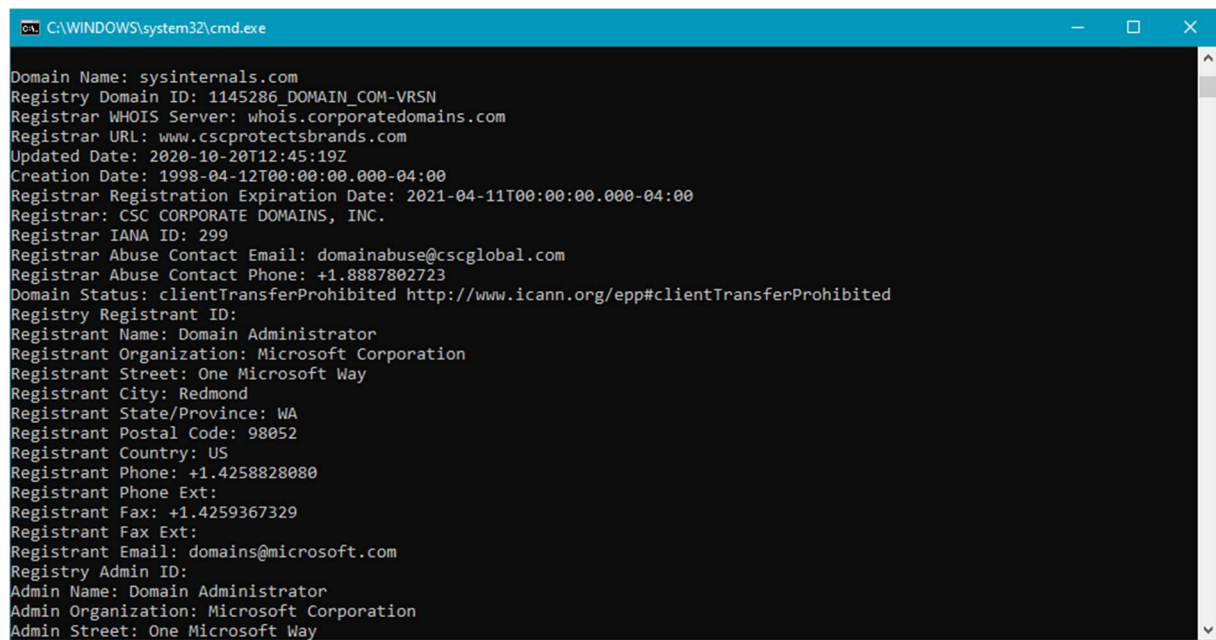


## File & Disk Utilities: Diskview



Vizualizálja a kiválasztott lemezen található szektorokat, és megmutatja hogy a kiválasztott fájl mekkora területet foglal el.

## Networking Utilities: Whois



```
C:\WINDOWS\system32\cmd.exe

Domain Name: sysinternals.com
Registry Domain ID: 1145286_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2020-10-20T12:45:19Z
Creation Date: 1998-04-12T00:00:00.000-04:00
Registrar Registration Expiration Date: 2021-04-11T00:00:00.000-04:00
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: domains@microsoft.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way
```

whois \*webcím\* paranccsal rákérdezhetünk weboldalak regisztrációs információira

## Process Utilities: Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-BLACKHUN\BlackHUN]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
winlogon.exe		2 540 K	10 716 K	15340		
dwm.exe	0.59	94 044 K	70 064 K	1040		
fontdrvhost.exe		7 712 K	21 488 K	16904		
explorer.exe	0.57	93 708 K	142 608 K	8	Windows Intéző	Microsoft Corporation
SecurityHealthSystray.exe		1 712 K	9 708 K	8872	Windows Security notificatio...	Microsoft Corporation
RAVCpl64.exe		4 208 K	14 304 K	13588	Realtek HD Audio Manager	Realtek Semiconductor
OneDrive.exe		31 168 K	65 712 K	12528	Microsoft OneDrive	Microsoft Corporation
E_IATICDE.EXE	< 0.01	1 752 K	8 444 K	8024	EPSON Status Monitor 3	SEIKO EPSON CORPOR...
steam.exe	0.29	80 484 K	88 468 K	7192	Steam Client Bootstrapper	Valve Corporation
steamwebhelper.exe	< 0.01	23 444 K	45 024 K	11576	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		9 904 K	14 236 K	16320	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe	< 0.01	54 564 K	46 996 K	12844	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		13 776 K	26 104 K	2580	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		61 776 K	58 428 K	9684	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		27 604 K	38 152 K	12488	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		88 904 K	94 852 K	4372	Steam Client WebHelper	Valve Corporation
DTAgent.exe	< 0.01	80 564 K	55 332 K	3548	DAEMON Tools Lite Agent	Disc Soft Ltd
wgc.exe	0.18	45 548 K	62 368 K	1360	Wargaming.net Game Center	Wargaming.net
wargamingerrormonitor.exe	< 0.01	10 192 K	16 612 K	12416	Wargaming.net Error Monitor	Wargaming.net
wgc_renderer_host.exe	0.62	89 984 K	58 452 K	13136	Wargaming.net Game Center	Wargaming.net
wgc_renderer_host.exe	< 0.01	7 680 K	21 004 K	2700	Wargaming.net Game Center	Wargaming.net
wgc_renderer_host.exe	1.56	55 552 K	83 724 K	8704	Wargaming.net Game Center	Wargaming.net
DMT.exe	< 0.01	25 676 K	30 492 K	15860	Dual Monitor Tools	GNE
GalaxyClient.exe	0.10	53 636 K	74 984 K	9004	GOG Galaxy	GOG.com
GalaxyClient Helper.exe	< 0.01	81 560 K	41 036 K	13260	GalaxyClient Helper Applicati...	GOG.com
GalaxyClient Helper.exe		102 552 K	83 372 K	3832	GalaxyClient Helper Applicati...	GOG.com
GOG Galaxy Notifications Ren...	0.01	41 780 K	64 412 K	9592	GOG Galaxy Notifications Re...	GOG.com
python.exe	< 0.01	22 392 K	21 912 K	5936	Python	Python Software Foundation
conhost.exe		6 312 K	6 296 K	3516	Konzolablak-kezelő	Microsoft Corporation

CPU Usage: 25.52% Commit Charge: 39.83% Processes: 266 Physical Usage: 48.65%

A process explorer megmutatja a futó programokhoz kapcsolódó folyamatokat

[illegible]



## System information: CoreInfo

```
C:\WINDOWS\system32\cmd.exe

Intel(R) Core(TM) i5-7600K CPU @ 3.80GHz
Intel64 Family 6 Model 158 Stepping 9, GenuineIntel
Microcode signature: 000000B4
HTT          *      Hyperthreading enabled
HYPERVISOR    -      Hypervisor is present
VMX           *      Supports Intel hardware-assisted virtualization
SVM           -      Supports AMD hardware-assisted virtualization
X64           *      Supports 64-bit mode

SMX           -      Supports Intel trusted execution
SKINIT        -      Supports AMD SKINIT

NX            *      Supports no-execute page protection
SMEP          *      Supports Supervisor Mode Execution Prevention
SMAP          *      Supports Supervisor Mode Access Prevention
PAGE1GB       *      Supports 1 GB large pages
PAE           *      Supports > 32-bit physical addresses
PAT           *      Supports Page Attribute Table
PSE           *      Supports 4 MB pages
PSE36         *      Supports > 32-bit address 4 MB pages
PGE           *      Supports global bit in page tables
SS            *      Supports bus snooping for cache operations
VME           *      Supports Virtual-8086 mode
RDWRFSGBASE   *      Supports direct GS/FS base access

FPU           *      Implements i387 floating point instructions
MMX           *      Supports MMX instruction set
MMXEXT        -      Implements AMD MMX extensions
3DNow         -      Supports 3DNow! instructions
```

```
C:\WINDOWS\system32\cmd.exe

*--- Physical Processor 0
*--- Physical Processor 1
--*- Physical Processor 2
---* Physical Processor 3

Logical Processor to Socket Map:
**** Socket 0

Logical Processor to NUMA Node Map:
**** NUMA Node 0

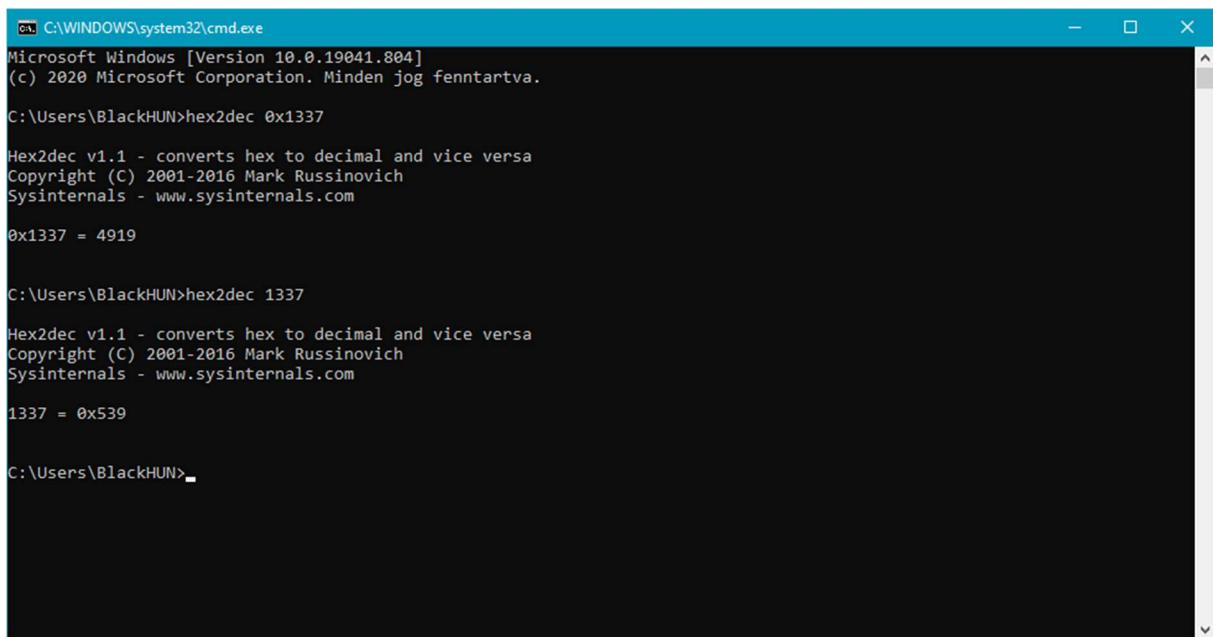
No NUMA nodes.

Logical Processor to Cache Map:
*--- Data Cache          0, Level 1,  32 KB, Assoc 8, LineSize 64
*--- Instruction Cache    0, Level 1,  32 KB, Assoc 8, LineSize 64
*--- Unified Cache        0, Level 2, 256 KB, Assoc 4, LineSize 64
**** Unified Cache        1, Level 3,   6 MB, Assoc 12, LineSize 64
*--- Data Cache          1, Level 1,  32 KB, Assoc 8, LineSize 64
*--- Instruction Cache    1, Level 1,  32 KB, Assoc 8, LineSize 64
*--- Unified Cache        2, Level 2, 256 KB, Assoc 4, LineSize 64
--*- Data Cache          2, Level 1,  32 KB, Assoc 8, LineSize 64
--*- Instruction Cache    2, Level 1,  32 KB, Assoc 8, LineSize 64
--*- Unified Cache        3, Level 2, 256 KB, Assoc 4, LineSize 64
---* Data Cache          3, Level 1,  32 KB, Assoc 8, LineSize 64
---* Instruction Cache    3, Level 1,  32 KB, Assoc 8, LineSize 64
---* Unified Cache        4, Level 2, 256 KB, Assoc 4, LineSize 64

Logical Processor to Group Map:
**** Group 0
```

Processzorinformációk listázása

## Miscellaneous: Hex2dec



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.804]
(c) 2020 Microsoft Corporation. Minden jog fenntartva.

C:\Users\BlackHUN>hex2dec 0x1337

Hex2dec v1.1 - converts hex to decimal and vice versa
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

0x1337 = 4919

C:\Users\BlackHUN>hex2dec 1337

Hex2dec v1.1 - converts hex to decimal and vice versa
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

1337 = 0x539

C:\Users\BlackHUN>
```

Hexadecimális és decimális számok közötti gyors átváltás

# Autoruns

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office  
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019. 12. 07. 10:15	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953. 12. 11. 3:58	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2020. 10. 04. 22:56	
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	(Verified) Realtek Semiconductor Corp.	c:\program files\realtek\audio\hda\rt...	2016. 09. 06. 9:31	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021. 01. 30. 12:44	
<input checked="" type="checkbox"/> amd_dc_opt	AMD Dual-Core Optimizer	(Not verified) AMD	c:\program files (x86)\amd\dual-core...	2008. 07. 22. 19:53	
<input checked="" type="checkbox"/> iOne	Cerberus Keyboard		c:\program files (x86)\cerberus\cerbe...	2017. 06. 22. 9:26	
<input checked="" type="checkbox"/> LogMeIn Hamachi UI	Hamachi Client Application	(Verified) LogMeIn, Inc.	c:\program files (x86)\logmein\hamac...	2019. 04. 02. 15:58	
<input checked="" type="checkbox"/> SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\j...	2020. 12. 09. 15:24	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 01. 14. 13:13	
<input checked="" type="checkbox"/> CiscoMeetingDaemon	Cisco Webex Meeting	(Verified) Cisco WebEx LLC	c:\users\blackhun\appdata\local\w...	2021. 02. 05. 14:55	
<input checked="" type="checkbox"/> DAEMON Tools Lite Aut...	DAEMON Tools Lite Agent	(Verified) AVB Disc Soft, SIA	c:\program files\daemon tools lite\da...	2019. 05. 06. 14:08	
<input checked="" type="checkbox"/> Discord	Update	(Verified) Discord Inc.	c:\users\blackhun\appdata\local\dis...	2020. 06. 01. 21:58	
<input checked="" type="checkbox"/> EPSON Stylus DX7400 ...	EPSON Status Monitor 3	(Verified) SEIKO EPSON Corporation	c:\windows\system32\spool\drivers\...	2007. 04. 12. 6:18	
<input checked="" type="checkbox"/> GNE_DualMonitorTools	Dual Monitor Tools	(Not verified) GNE	c:\program files (x86)\dual monitor to...	2018. 06. 04. 19:46	
<input checked="" type="checkbox"/> GogGalaxy	GOG Galaxy	(Verified) GOG Sp. z o.o.	d:\program files (x86)\gog galaxy\gal...	2020. 12. 22. 11:52	
<input checked="" type="checkbox"/> LGHUB	LGHUB	(Verified) Logitech Inc	c:\program files\lg hub\lg hub.exe	2020. 11. 18. 14:33	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\blackhun\appdata\local\mi...	1958. 02. 05. 12:59	
<input checked="" type="checkbox"/> Steam	Steam Client Bootstrapper	(Verified) Valve	d:\program files (x86)\steam\steam.exe	2021. 02. 13. 0:23	
<input checked="" type="checkbox"/> Wargaming.net Game C...	Wargaming.net Game Center	(Verified) Wargaming.net Limited	d:\programdata\wargaming.net\gam...	2021. 02. 02. 16:40	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce				2021. 02. 07. 12:48	
<input checked="" type="checkbox"/> Application Restart #0	Brave Browser	(Verified) Brave Software, Inc.	c:\program files\bravesoftware\brave...	2021. 02. 04. 6:06	
<input checked="" type="checkbox"/> Application Restart #2	Brave Browser	(Verified) Brave Software, Inc.	c:\program files\bravesoftware\brave...	2021. 02. 04. 6:06	
C:\Users\BlackHUN\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2020. 10. 04. 22:04	
<input checked="" type="checkbox"/> GIGABYTE AORUS GR...			c:\program files (x86)\gigabyte\aurus...	2017. 01. 14. 17:01	
<input checked="" type="checkbox"/> MEGAAsyncLink	MEGAAsync	(Verified) Mega Limited	c:\users\blackhun\appdata\local\vm...	2020. 11. 17. 23:08	
<input checked="" type="checkbox"/> Voicemeeter (VB-Audio)...	VB-AUDIO Virtual Audio Device Mixin...	(Verified) Vincent Burel	c:\program files (x86)\vb\voicemeete...	2019. 06. 20. 6:56	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 10. 07. 20:59	
<input checked="" type="checkbox"/> Brave	Brave Installer	(Verified) Brave Software, Inc.	c:\program files\bravesoftware\brave...	2021. 02. 04. 6:06	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome...	2021. 02. 04. 1:31	
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021. 02. 10. 21:20	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2019. 10. 25. 4:45	

Ready. Signed Windows Entries Hidden.