

1. Elsőként a SysInternalsSuite csomagból a diskext.exe programot vizsgáltam meg. Ez a IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS parancsot demonstrálja, ami azt írja ki, hogy az egyes partíciók melyik meghajtón helyezkednek el. Ehhez nem találtam beépített Windowsos programot.

The screenshot shows the Firehawk Total Commander interface. A command prompt window titled "Administrator: C:\WINDOWS\system32\cmd.exe" is open, displaying the output of the command `diskext.exe` run from the directory `c:\Firehawk\Suli\Operációs Rendszerek\2. Gyak\sysinternalsSuite`. The output lists disk extents for three volumes, showing their disk, offset, and length.

```
Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.

c:\Firehawk\Suli\Operációs Rendszerek\2. Gyak\sysinternalsSuite>diskext.exe

DiskExt v1.2 - Disk extent dumper
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Volume: \\?\Volume{ad2fd1a3-5331-43df-b32e-9daaa9a57f51}\
Mounted at: <unmounted>
Extent [1]:
Disk: 0
Offset: 1048576
Length: 554696704

Volume: \\?\Volume{2f57a662-f1dd-4d1d-a7ea-7d9145895eff}\
Mounted at: C:\
Extent [1]:
Disk: 0
Offset: 676331520
Length: 255383830528

Volume: \\?\Volume{4e3bfc29-93ce-494d-8c4a-d5d74ff44e09}\
Mounted at: <unmounted>
Extent [1]:
Disk: 0
Offset: 555745280
Length: 103809024

c:\Firehawk\Suli\Operációs Rendszerek\2. Gyak\sysinternalsSuite>
```

The background shows the Total Commander file list with columns for Name, Size, Date, and Attributes. The status bar at the bottom indicates file and directory counts.

2. Másodjára a TCPView-t néztem meg, ami részletesen kilistázza a TCP és UDP végpontokat a rendszeren. Ehhez a megfelelő beépített parancs a “netstat”.

TCPView - Sysinternals: www.sysinternals.com											
File Options Process View Help											
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	desktop-5ir6n9p	56537	172.217.20.14	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-5ir6n9p	56543	74.125.133.157	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-5ir6n9p	56563	51.130.106.75	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-5ir6n9p	56564	162.159.129.233	https	TIME_WAIT				
chrome.exe	10948	TCP	desktop-5ir6n9p	55199	142.250.27.188	5228	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	55348	52.114.92.45	https	ESTABLISHED	2	270	2	673
chrome.exe	10948	TCP	desktop-5ir6n9p	55350	edge-star-shv-01...	https	ESTABLISHED	13	574	14	324
chrome.exe	10948	TCP	desktop-5ir6n9p	55399	52.114.92.66	https	ESTABLISHED	2	116	2	94
chrome.exe	10948	TCP	desktop-5ir6n9p	55493	52.114.72.3	https	ESTABLISHED	1	156	1	52
chrome.exe	10948	TCP	desktop-5ir6n9p	55494	52.114.72.3	https	ESTABLISHED	1	165	1	81
chrome.exe	10948	TCP	desktop-5ir6n9p	56406	dns.google	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56459	bud02s26-in-f14.1...	https	ESTABLISHED	8	5,096	16	2,225
chrome.exe	10948	TCP	desktop-5ir6n9p	56529	185.199.108.133	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56516	91.83.14.72	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56640	40.117.256.250	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56641	52.114.74.115	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56670	52.114.159.112	https	ESTABLISHED	2	8,598	1	465
chrome.exe	10948	TCP	desktop-5ir6n9p	56678	185.60.218.35	https	ESTABLISHED	1	637	6	40,380
chrome.exe	10948	TCP	desktop-5ir6n9p	56683	77.234.91.145	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56685	8.8.8.8	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56687	185.60.218.35	https	CLOSE_WAIT			2	63
chrome.exe	10948	TCP	desktop-5ir6n9p	56694	31.13.91.13	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56695	172.217.20.10	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56696	172.217.20.10	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56701	172.217.16.99	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56704	172.217.16.99	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56705	31.13.91.13	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56706	185.60.218.24	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56708	185.60.218.24	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56708	31.13.91.13	https	ESTABLISHED				
chrome.exe	10948	TCP	desktop-5ir6n9p	56710	52.113.193.114	https	ESTABLISHED	3	2,145	3	892
chrome.exe	10948	UDP	DESKTOP-SIR6N9P	5353	*	*				4	176
chrome.exe	11388	UDP	DESKTOP-SIR6N9P	5353	*	*				4	176
chrome.exe	10948	UDP	DESKTOP-SIR6N9P	5353	*	*					
chrome.exe	10948	UDP	DESKTOP-SIR6N9P	5353	*	*					
chrome.exe	10948	UDP	desktop-5ir6n9p	61314	*	*		1,015	37,776	4,810	1,648,603
chrome.exe	10948	UDP	DESKTOP-SIR6N9P	5353	*	*					
chrome.exe	11388	UDP	DESKTOP-SIR6N9P	5353	*	*					
chrome.exe	11388	UDPv6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	10948	UDPv6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	10948	UDPv6	[2620:9b:0:0:0:0:1::61312]	*	*						
Discord.exe	10160	TCP	DESKTOP-SIR6N9P	6463	DESKTOP-SIR6N9P	0	LISTENING				
Discord.exe	5616	TCP	desktop-5ir6n9p	49820	162.159.136.234	https	ESTABLISHED	2	108	39	4,894
ekm.exe	2932	TCP	desktop-5ir6n9p	56552	91.228.167.67	53535	CLOSE_WAIT				
ekm.exe	2932	UDP	DESKTOP-SIR6N9P	55028	*	*					
ekm.exe	2932	UDP	DESKTOP-SIR6N9P	55027	*	*					
ekm.exe	2932	UDP	DESKTOP-SIR6N9P	55028	*	*					
ekm.exe	2932	UDP	DESKTOP-SIR6N9P	56825	*	*					
ekm.exe	2932	UDP	DESKTOP-SIR6N9P	45617	*	*					
Endpoints: 134 Established: 40 Listening: 26 Time Wait: 4 Close Wait: 2											

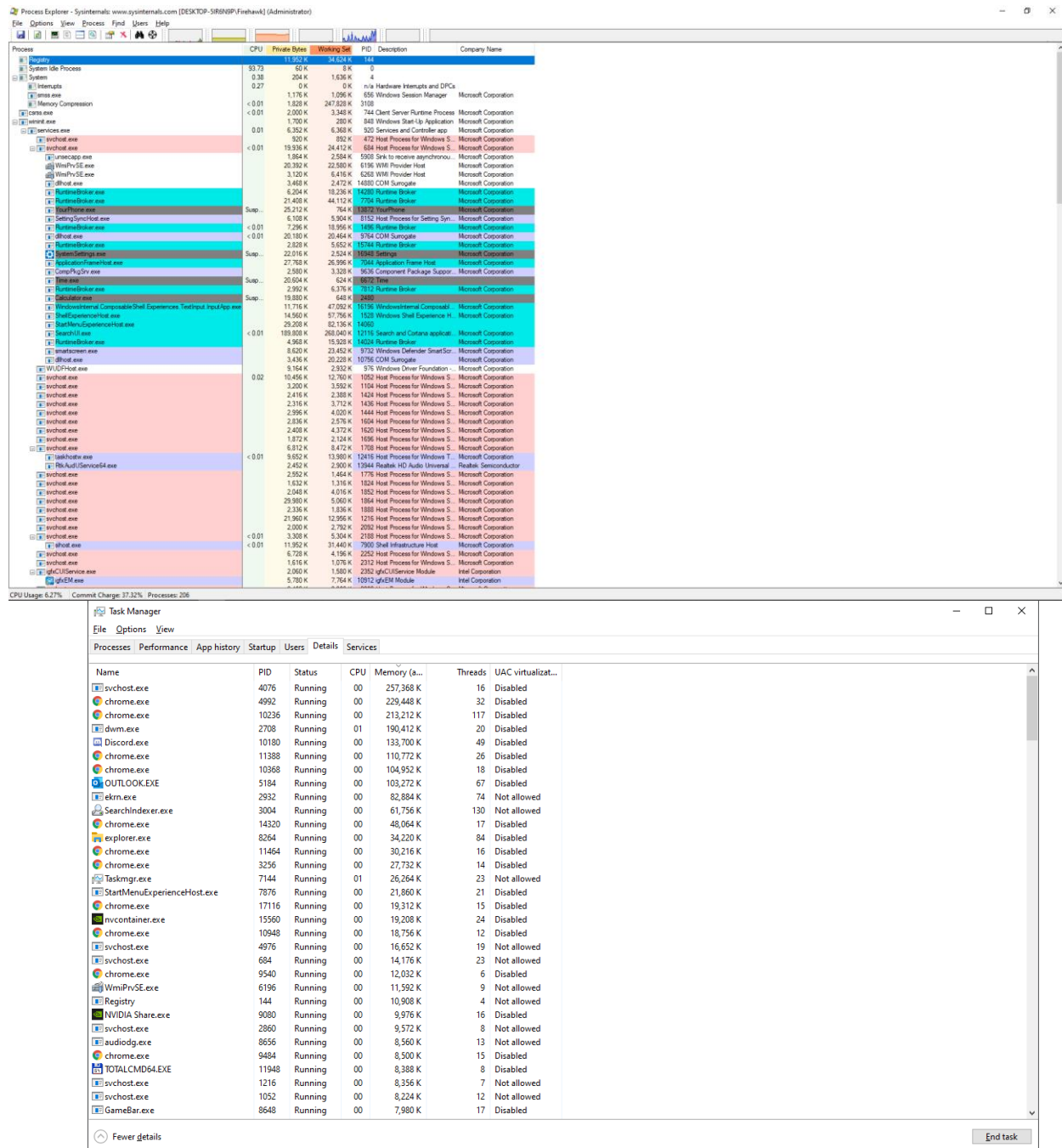
```
Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Firehawk>netstat

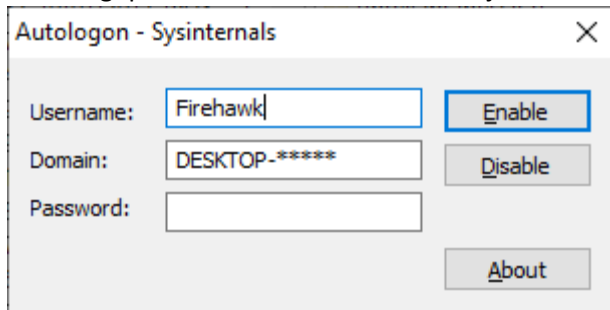
Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:64995           DESKTOP-SIR6N9P:65001  ESTABLISHED
TCP    127.0.0.1:65001           DESKTOP-SIR6N9P:64995  ESTABLISHED
TCP    127.0.0.1:65044           DESKTOP-SIR6N9P:65063  ESTABLISHED
TCP    127.0.0.1:65063           DESKTOP-SIR6N9P:65044  ESTABLISHED
TCP    192.168.0.162:49820       162.159.136.234:https  ESTABLISHED
TCP    192.168.0.162:55199       142.250.27.188:5228    ESTABLISHED
TCP    192.168.0.162:55348       52.114.92.45:https      ESTABLISHED
TCP    192.168.0.162:55350       edge-star-shv-01-waw1:https ESTABLISHED
TCP    192.168.0.162:55399       52.114.92.66:https      ESTABLISHED
TCP    192.168.0.162:55493       52.114.72.3:https       ESTABLISHED
TCP    192.168.0.162:55494       52.114.72.3:https       ESTABLISHED
TCP    192.168.0.162:56406       dns:https               ESTABLISHED
TCP    192.168.0.162:56459       bud02s26-in-f14:https  ESTABLISHED
TCP    192.168.0.162:56512       52.97.176.2:https       ESTABLISHED
TCP    192.168.0.162:56529       cdn-185-199-108-133:https ESTABLISHED
TCP    192.168.0.162:56895       40.101.12.66:https      ESTABLISHED
TCP    192.168.0.162:57017       52.114.104.9:https      ESTABLISHED
TCP    192.168.0.162:57054       52.97.163.2:https       ESTABLISHED
TCP    192.168.0.162:57082       52.97.163.2:https       ESTABLISHED
```

3. Ezután a Process Explorert vizsgáltam. Itt szülő-gyermek hierarchiában lehet látni részletesen, hogy milyen folyamatok is futnak a gépen. A processzeket a feladatkezelőben is tudjuk listázni.



4. Security Utility-k közül az AutoLogons programot vizsgáltam meg, amivel belehet állítani, hogy számítógép indításnál automatikusan bejelentkezzen a beállított felhasználóval.



5. Information Utilitynek a CoreInfo programot néztem meg, ami rengeteg infót listáz ki a processzorról. Nem találtam ennek se megfelelő beépített programot.

```
Administrator C:\WINDOWS\system32\cmd.exe
EIST * Supports Enhanced Intel Speedstep
ACPI * Implements ACPI for power management
TM * Implements thermal monitor circuitry
TM2 * Implements Thermal Monitor 2 control
APIC * Implements software-accessible local APIC
x2APIC * Supports x2APIC

CNXT-ID - L1 data cache mode adaptive or BIOS

MCE * Supports Machine Check, INIT and CM-MCE
MCA * Implements Machine Check Architecture
PBE * Supports use of FERRO/PBE pin

PSN - Implements 96-bit processor serial number

PREFETCHW * Supports PREFETCHW instruction

Maximum implemented CPUID leaves: 00000016 (Basic), 00000008 (Extended).
Maximum implemented address width: 48 bits (virtual), 39 bits (physical).
Processor signature: 000906EA

Logical to Physical Processor Map:
**----- Physical Processor 0 (Hyperthreaded)
**----- Physical Processor 1 (Hyperthreaded)
**----- Physical Processor 2 (Hyperthreaded)
**----- Physical Processor 3 (Hyperthreaded)
**----- Physical Processor 4 (Hyperthreaded)
**----- Physical Processor 5 (Hyperthreaded)

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
**----- Instruction Cache
**----- Unified Cache
0, Level 1, 32 KB, Assoc 8, LineSize 64
0, Level 2, 256 KB, Assoc 4, LineSize 64
1, Level 1, 32 KB, Assoc 8, LineSize 64
1, Level 2, 256 KB, Assoc 4, LineSize 64
2, Level 1, 32 KB, Assoc 8, LineSize 64
2, Level 2, 256 KB, Assoc 4, LineSize 64
3, Level 1, 32 KB, Assoc 8, LineSize 64
3, Level 2, 256 KB, Assoc 4, LineSize 64
4, Level 1, 32 KB, Assoc 8, LineSize 64
4, Level 2, 256 KB, Assoc 4, LineSize 64
5, Level 1, 32 KB, Assoc 8, LineSize 64
5, Level 2, 256 KB, Assoc 4, LineSize 64
6, Level 1, 32 KB, Assoc 8, LineSize 64
6, Level 2, 256 KB, Assoc 4, LineSize 64

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

C:\Firehawk\Gull10Operációs Rendszerek\2. Gyak\sysinternals\Suite>
```

6. Végül az AutoRuns-ban néztem meg, hogy a Windowssal együtt milyen programok indulnak is el automatikusan. Ezt láthatjuk a Feladatkezelőben is.

