

Operációs rendszerek BSc

3.gyakorlat

2021.02.24

Készítette:

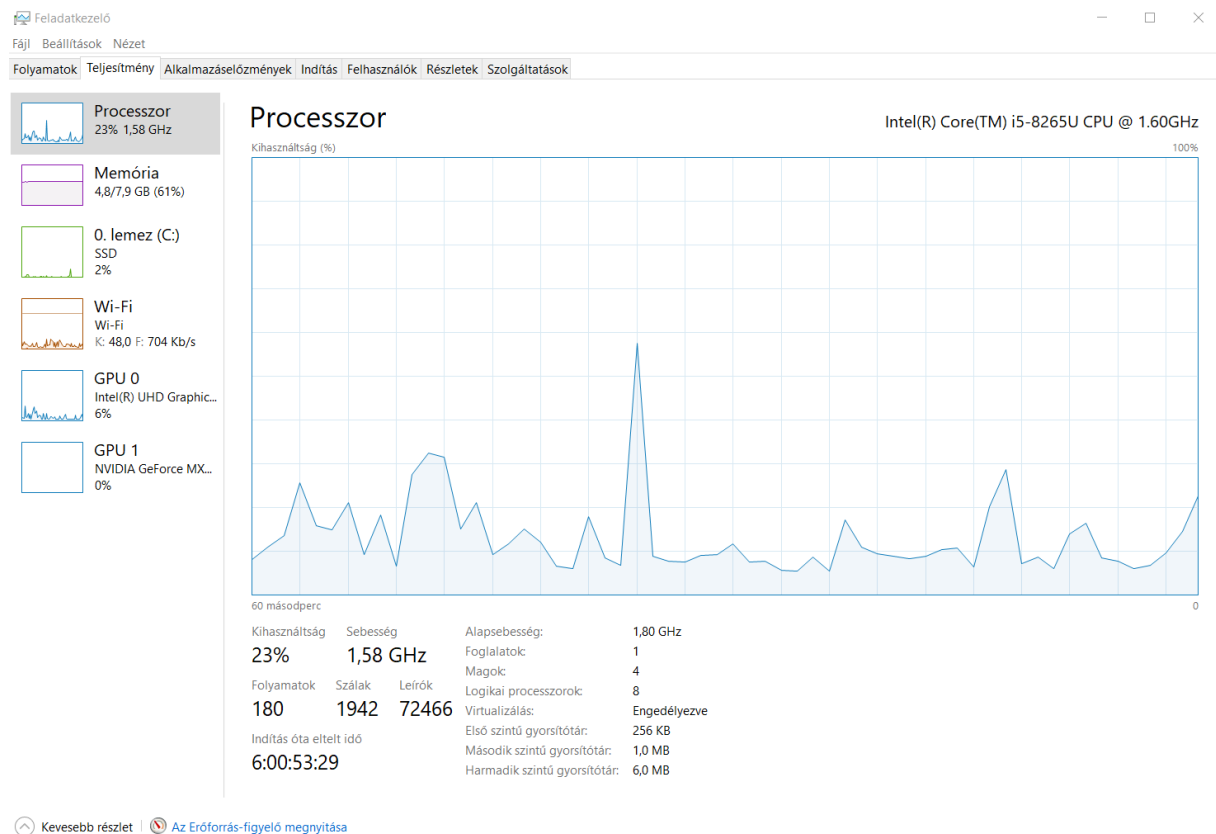
Szalontai Panna BSc

Programtervező Informatikus

GSACE9

1.Feladat: A Windows belső működésének a tanulmányozása.

Folyamatok										
Teljesítmény										
Alkalmazáselelmények										
Indítás										
Felhasználók										
Részletek										
Szolgáltatások										
Név	Állapot	15% Processzor	60% Memória	3% Lemez	1% Hálózat	6% GPU	GPU-motor	Energiafogyas...	Energiafogyas...	
Alkalmazások (5)										
Feladatkezelő		1,5%	24,2 MB	0,1 MB/s	0 Mb/s	0%		Alacsony	Nagyon alacso...	
Képmetsző		1,0%	3,4 MB	0,5 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
Microsoft Edge (10)		0,1%	307,0 MB	0 MB/s	0 Mb/s	0%	GPU 0 - 3D	Nagyon alacso...	Nagyon alacso...	
Microsoft Teams (10)		5,6%	812,9 MB	0 MB/s	1,1 Mb/s	3,6%	GPU 0 - Video Decode	Mérsékelt	Nagyon alacso...	
Microsoft Word		0%	59,7 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
Háttérfolyamatok (63)										
A Microsoft Windows Search sz...		0%	11,7 MB	0,1 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
Adobe Acrobat Update Service ...		0%	0,4 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
Application Frame Host		0%	5,6 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
AsLdrSvc64		0%	0,4 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
AsMonStartupTask64		0%	0,4 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
ASUS HID Access Service		0%	0,2 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
ASUS LiveUpdate Agent		0%	0,5 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
ASUS Optimization		0%	0,4 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
ASUS System Analysis		0%	1,4 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
ASUSSystemDiagnosis		0%	0,3 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
COM Surrogate		0%	1,8 MB	0,1 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
CTF-betöltő		0,3%	3,9 MB	0,2 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
Csatolt telefon		0%	0 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
Elan Service		0%	0,4 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	
Gazdafolyamat Windows-felad...		0%	2,8 MB	0 MB/s	0 Mb/s	0%		Nagyon alacso...	Nagyon alacso...	




2.Feladat: A Sysinternals Suite programcsomag tanulmányozása.

a, File and Disk Utilities (Disk2vhd)

Nem indult el.

b, Networking Utilities (TCPView)

 Kijelölés C:\Users\User\AppData\Local\Temp\Rar\$EXa6384.18590\Tcpvcon.exe

```
TCPView v3.01 - TCP/UDP endpoint viewer
Copyright (C) 1998-2010 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

[TCP] chrome.exe
      PID: 1536
      State: ESTABLISHED
      Local: desktop-hvbm1bs
      Remote: 142.250.27.188
[TCP] chrome.exe
      PID: 1536
      State: ESTABLISHED
      Local: desktop-hvbm1bs
      Remote: 1b-140-82-112-25-iad.github.com
[TCP] Teams.exe
      PID: 4656
      State: ESTABLISHED
      Local: desktop-hvbm1bs
      Remote: 52.111.231.0
[TCP] SearchApp.exe
      PID: 8268
      State: ESTABLISHED
      Local: desktop-hvbm1bs
      Remote: 52.96.191.98
[TCP] SearchApp.exe
      PID: 8268
      State: CLOSE_WAIT
      Local: desktop-hvbm1bs
      Remote: a87-245-215-22.deploy.akamaitechnologies.com
[TCP] msedge.exe
      PID: 10944
      State: ESTABLISHED
      Local: desktop-hvbm1bs
      Remote: cdn-185-199-108-133.github.com
```

c, Process Explorer v16.32

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-HVHM1BS\User]

File Options View Process Find Users Help

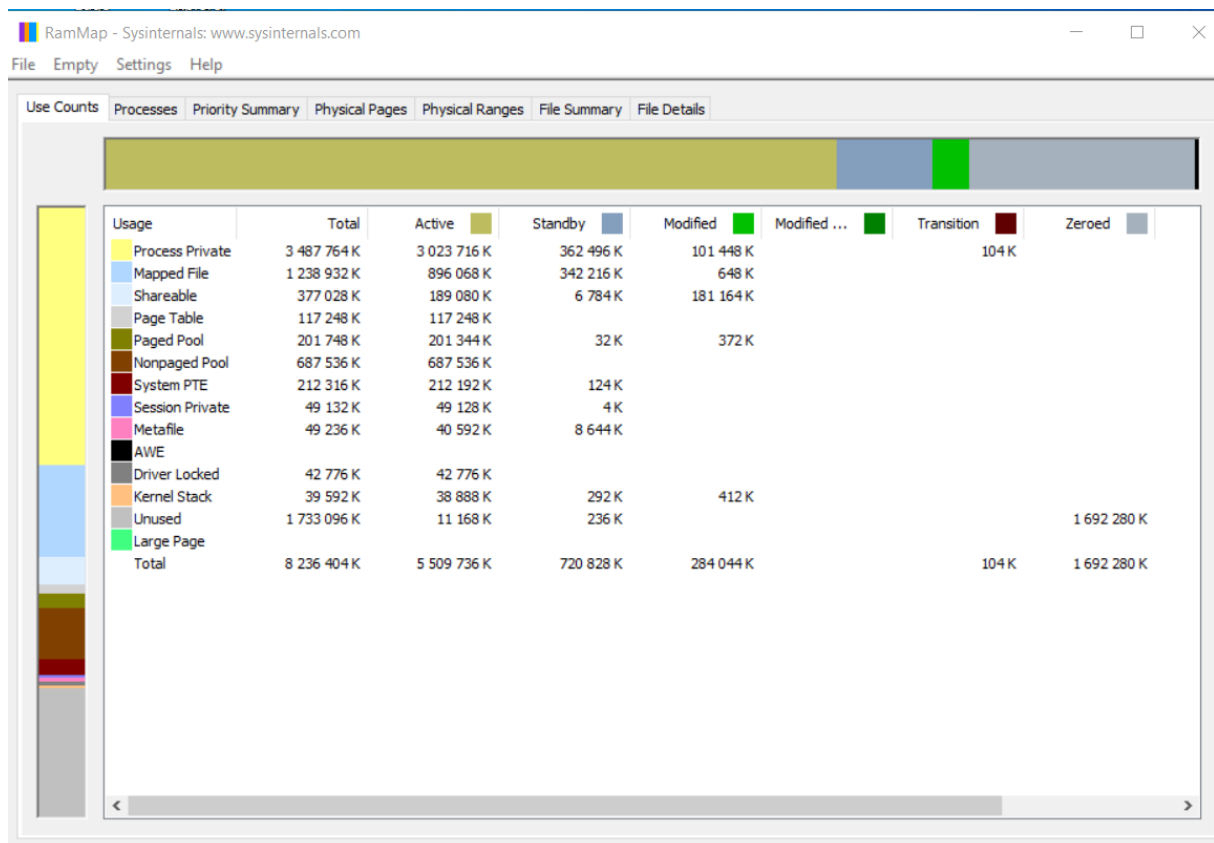
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry	0.03	3 016 K	70 528 K	124		
System Idle Process	77.46	60 K	8 K	0		
System	0.89	196 K	1 264 K	4		
Interrupts	0.90	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 068 K	652 K	568		
Memory Compression	< 0.01	312 K	104 196 K	2840		
csrss.exe	< 0.01	1 888 K	4 784 K	656		
wininit.exe		1 716 K	6 048 K	864		
services.exe	0.56	5 756 K	8 604 K	936		
svchost.exe	< 0.01	12 996 K	32 572 K	1028	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe	0.01	34 044 K	44 420 K	4232		
unsecapp.exe		1 572 K	6 284 K	8984		
SettingSyncHost.exe		2 468 K	5 260 K	9740	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperienceHost.exe		30 832 K	86 464 K	4912		
RuntimeBroker.exe		6 312 K	26 144 K	8156	Runtime Broker	Microsoft Corporation
SearchApp.exe	0.05	189 516 K	281 172 K	8268	Search application	Microsoft Corporation
RuntimeBroker.exe		13 736 K	41 552 K	7284	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	24 708 K	1 996 K	2928	YourPhone	Microsoft Corporation
RuntimeBroker.exe	< 0.01	3 172 K	16 628 K	10712	Runtime Broker	Microsoft Corporation
TextInputHost.exe		13 916 K	46 828 K	2680		Microsoft Corporation
dllhost.exe	< 0.01	5 552 K	13 760 K	9548	COM Surrogate	Microsoft Corporation
SystemSettings.exe	Susp...	23 828 K	2 544 K	6332	Gépház	Microsoft Corporation
ApplicationFrameHost.exe		21 568 K	29 704 K	1648	Application Frame Host	Microsoft Corporation
RtkUWP.exe	Susp...	10 700 K	36 588 K	9920		
RuntimeBroker.exe		2 344 K	13 956 K	11304	Runtime Broker	Microsoft Corporation
GameBar.exe	0.02	28 704 K	71 028 K	11688	Xbox Game Bar	Microsoft Corporation
GameBarFTServer.exe		9 992 K	19 644 K	8468	Xbox Game Bar Full Trust CO...	Microsoft Corporation
RuntimeBroker.exe		4 200 K	22 468 K	11200	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	18 032 K	55 356 K	2332	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2 032 K	11 712 K	11424	Runtime Broker	Microsoft Corporation
WmiPrvSE.exe		2 704 K	10 116 K	5952		
WmiPrvSE.exe	< 0.01	7 736 K	14 976 K	2820		
smartscreen.exe	< 0.01	8 192 K	23 184 K	11096	Windows Defender SmartScr...	Microsoft Corporation
WUDFHost.exe		4 240 K	6 096 K	1104		
svchost.exe		9 376 K	17 456 K	1200	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2 964 K	7 416 K	1260	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		1 888 K	5 768 K	1440	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		1 616 K	9 320 K	1448	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		3 036 K	10 676 K	1476	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2 496 K	8 888 K	1564	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2 032 K	10 200 K	1572	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		6 560 K	13 764 K	1672	Windows-szolgáltatások gaz...	Microsoft Corporation
MicrosoftEdgeUpdate.e...		1 892 K	832 K	4540		
taskhostw.exe	< 0.01	8 376 K	18 960 K	8808	Gazdafolyamat Windows-fela...	Microsoft Corporation
RtkAudUService64.exe		2 640 K	2 952 K	9556	Realtek HD Audio Universal ...	Realtek Semiconductor

CPU Usage: 22.54% Commit Charge: 66.81% Processes: 192 Physical Usage: 66.45%

d, Security Utilities (LogonSession)

Nem hozott be semmit.

e, Information Utilities (RAMMap)



RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Process	Session	PID	Private	Standby	Modified	Page Table	Total
System	-1	4	0 K	0 K	0 K	84 K	84 K
Registry	-1	124	1 980 K	0 K	0 K	244 K	2 224 K
msedge.exe	6	3048	6 816 K	0 K	0 K	916 K	7 732 K
RuntimeBroker.	6	10712	3 048 K	0 K	0 K	508 K	3 556 K
TextInputHost.	6	2680	3 344 K	4 K	2 324 K	832 K	6 504 K
dllhost.exe	6	9548	2 012 K	0 K	0 K	344 K	2 356 K
svchost.exe	0	3900	3 456 K	0 K	0 K	452 K	3 908 K
svchost.exe	0	3908	1 040 K	16 K	0 K	304 K	1 360 K
GameBarFTS...	2	6964	0 K	0 K	0 K	36 K	36 K
taskhostw.exe	6	8808	3 188 K	64 K	0 K	400 K	3 652 K
svchost.exe	0	2364	904 K	0 K	0 K	264 K	1 168 K
chrome.exe	6	10556	92 568 K	228 K	24 K	1 352 K	94 172 K
chrome.exe	6	1536	8 592 K	8 K	4 K	740 K	9 344 K
svchost.exe	0	7760	308 K	0 K	4 K	236 K	548 K
ctfmon.exe	6	7152	7 368 K	236 K	0 K	468 K	8 072 K
NVDisplay.Cont	0	2408	2 144 K	96 K	0 K	404 K	2 644 K
svchost.exe	0	2472	356 K	0 K	0 K	252 K	608 K
smartscreen.ex	6	5852	5 424 K	0 K	0 K	516 K	5 940 K
svchost.exe	0	1672	2 852 K	604 K	4 K	348 K	3 808 K
svchost.exe	0	2664	1 028 K	44 K	0 K	356 K	1 428 K
svchost.exe	0	2652	340 K	0 K	0 K	256 K	596 K
software_repor	6	5148	0 K	0 K	0 K	36 K	36 K
svchost.exe	0	1784	812 K	0 K	0 K	236 K	1 048 K
svchost.exe	0	2704	9 948 K	0 K	0 K	304 K	10 252 K
svchost.exe	0	2796	724 K	24 K	0 K	320 K	1 068 K
svchost.exe	0	2812	536 K	8 K	0 K	268 K	812 K
msedge.exe	6	10284	369 732 K	0 K	4 K	1 996 K	371 732 K
svchost.exe	0	8064	780 K	16 K	0 K	328 K	1 124 K
MemCompres...	-1	2840	178 904 K	12 436 K	38 112 K	520 K	229 972 K

3.Feladat: Dependency Walker