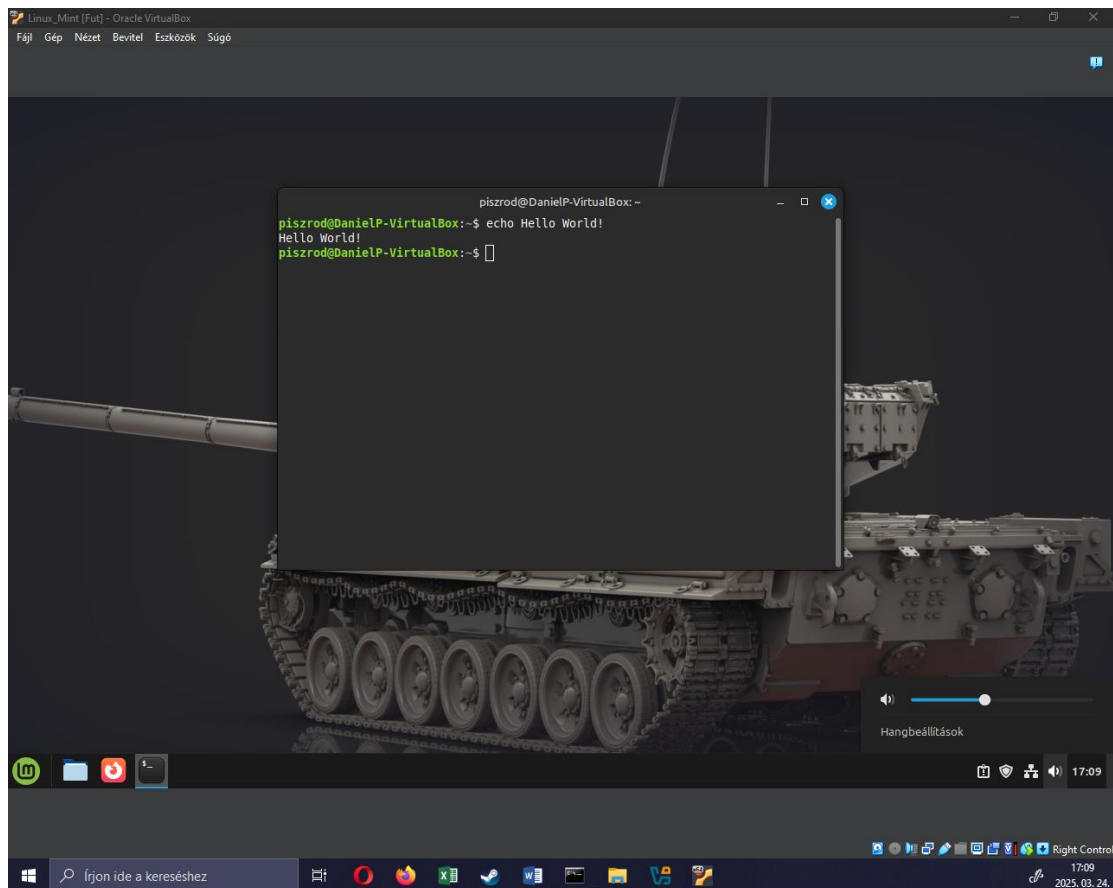
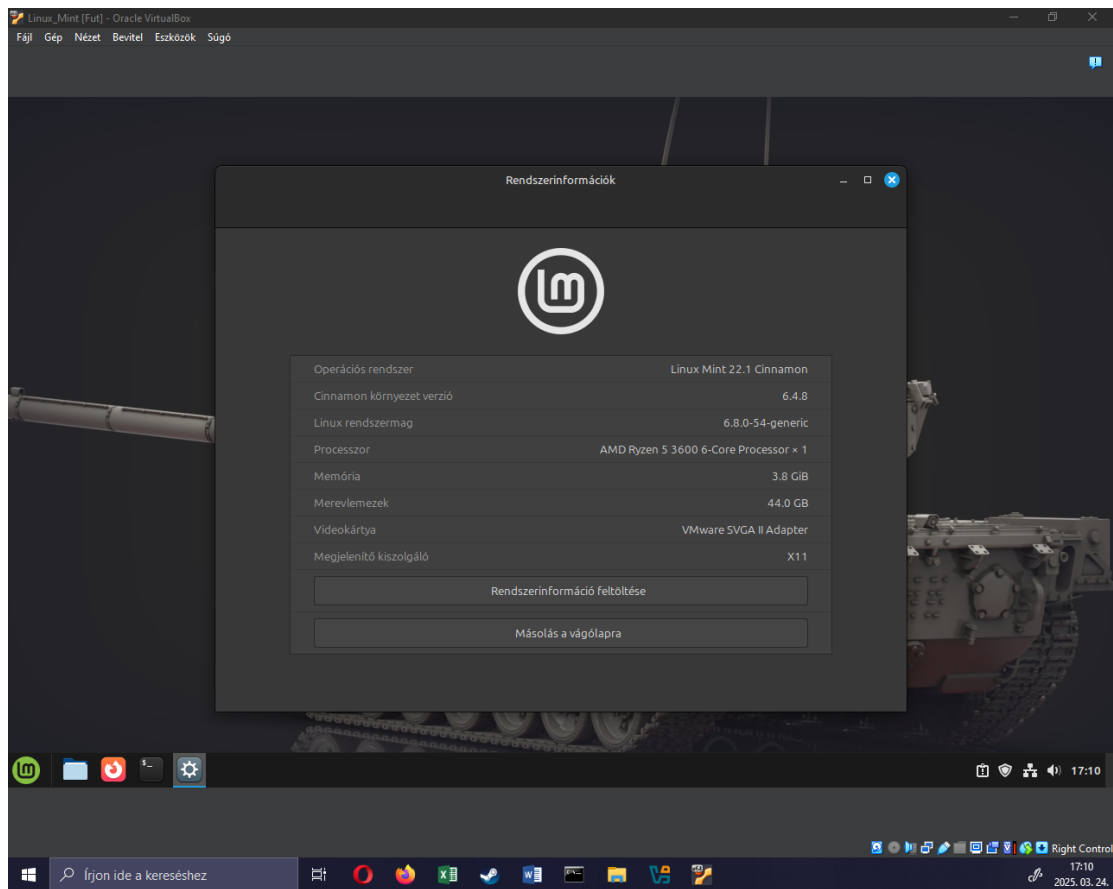


2. Feladat



3.Feladat

3/a

```
Parancssor
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\Scirocco>cd C:\

C:\>MD ELJUVY

C:\>cd ELJUVY

C:\ELJUVY>MD bokor

C:\ELJUVY>MD fa

C:\ELJUVY>MD land

C:\ELJUVY>cd bokor

C:\ELJUVY\bokor>md banan

C:\ELJUVY\bokor>md mogyoro

C:\ELJUVY\bokor>md barack

C:\ELJUVY\bokor>cd fa
A rendszer nem találja a megadott elérési utat.

C:\ELJUVY\bokor>cd ELJUVY
A rendszer nem találja a megadott elérési utat.

C:\ELJUVY\bokor>cd C:\ELJUVY

C:\ELJUVY>cd fa

C:\ELJUVY\fa>md korte

C:\ELJUVY\fa>cd C:\ELJUVY

C:\ELJUVY>cd land

C:\ELJUVY\land>md szeder

C:\ELJUVY\land>md kokusz

C:\ELJUVY\land>
```

3/b

```
Parancssor
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\Scirocco>xcopy "C:\ELJUVY\land\szeder" "C:\ELJUVY\fa\szeder" /e
Does C:\ELJUVY\fa\szeder specify a file name
or directory name on the target
(F = file, D = directory)? d
0 File(s) copied

C:\Users\Scirocco>xcopy "C:\ELJUVY\bokor\banan" "C:\ELJUVY\fa\banan" /e
Does C:\ELJUVY\fa\banan specify a file name
or directory name on the target
(F = file, D = directory)? d
0 File(s) copied

C:\Users\Scirocco>
```

3/c

```
Parancssor

C:\Users\Scirocco>move "C:\ELJUVY\bokor\barack" "C:\ELJUVY\fa\barack"
1 dir(s) moved.

C:\Users\Scirocco>move "C:\ELJUVY\land\kokusz" "C:\ELJUVY\fa\kokusz"
1 dir(s) moved.

C:\Users\Scirocco>
```

3/d

```
Parancssor

C:\Users\Scirocco>rmdir /s "C:\ELJUVY\land"
C:\ELJUVY\land, Are you sure (Y/N)? y

C:\Users\Scirocco>copy NUL "C:\ELJUVY\bokor\banan\leiras.txt"
1 file(s) copied.

C:\Users\Scirocco>copy NUL "C:\ELJUVY\fa\felsorolas.txt"
1 file(s) copied.

C:\Users\Scirocco>
```

3/e

```
Parancssor

C:\ELJUVY\bokor\banan>copy con leiras.txt
a barack kerek
Overwrite leiras.txt? (Yes/No/All): y
a barack puha
a barack finom^Z
        1 file(s) copied.

C:\ELJUVY\bokor\banan>cd C:\ELJUVY\fa

C:\ELJUVY\fa>copy con felsorolas.txt
Csaba
Lili
Tibor
Vencel
Viola^Z
        1 file(s) copied.

C:\ELJUVY\fa>
```

3/f

```
Parancssor

C:\ELJUVY>tree /f
Folder PATH listing
Volume serial number is 924E-9547
C:..
|_ bokor
|   |_ banan
|       leiras.txt
|   |_ mogyoro
|_ fa
    |_ felsorolas.txt
    |_ banan
    |_ barack
    |_ kokusz
    |_ korte
    |_ szeder

C:\ELJUVY>
```

3/g

```
Parancssor
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\Scirocco>cd C:\ELJUVY

C:\ELJUVY>dir ?e* /s
Volume in drive C has no label.
Volume Serial Number is 924E-9547

Directory of C:\ELJUVY\bokor\banan

2025. 03. 18.  00:47                45 leiras.txt
                1 File(s)                45 bytes

Directory of C:\ELJUVY\fa

2025. 03. 18.  00:50                33 felsorolas.txt
                1 File(s)                33 bytes

Total Files Listed:
                2 File(s)                78 bytes
                0 Dir(s)  374 540 374 016 bytes free

C:\ELJUVY>
```

3/h

```
Parancssor

C:\ELJUVY>attrib -r C:\ELJUVY\fa\felsorolas.txt

C:\ELJUVY>
```

```
Parancssor

C:\ELJUVY>dir /s
Volume in drive C has no label.
Volume Serial Number is 924E-9547

Directory of C:\ELJUVY

2025. 03. 18.  00:24    <DIR>        .
2025. 03. 18.  00:24    <DIR>        ..
2025. 03. 18.  00:11    <DIR>        bokor
2025. 03. 18.  00:36    <DIR>        fa
                0 File(s)                0 bytes

Directory of C:\ELJUVY\bokor

2025. 03. 18.  00:11    <DIR>        .
2025. 03. 18.  00:11    <DIR>        ..
2025. 03. 18.  00:34    <DIR>        banan
2025. 03. 17.  23:27    <DIR>        mogyoro
                0 File(s)                0 bytes

Directory of C:\ELJUVY\bokor\banan

2025. 03. 18.  00:34    <DIR>        .
2025. 03. 18.  00:34    <DIR>        ..
2025. 03. 18.  00:47                45 leiras.txt
                1 File(s)                45 bytes

Directory of C:\ELJUVY\bokor\mogyoro

2025. 03. 17.  23:27    <DIR>        .
2025. 03. 17.  23:27    <DIR>        ..
                0 File(s)                0 bytes

Directory of C:\ELJUVY\fa

2025. 03. 18.  00:36    <DIR>        .
2025. 03. 18.  00:36    <DIR>        ..
2025. 03. 17.  23:27    <DIR>        banan
2025. 03. 17.  23:27    <DIR>        barack
2025. 03. 18.  00:50                33 felsorolas.txt
2025. 03. 17.  23:29    <DIR>        kokusz
2025. 03. 17.  23:28    <DIR>        korte
2025. 03. 17.  23:29    <DIR>        szeder
                1 File(s)                33 bytes

Directory of C:\ELJUVY\fa\banan
```

```
Kijelölés Parancssor

Directory of C:\ELJUVY\fa\banan
2025. 03. 17. 23:27 <DIR> .
2025. 03. 17. 23:27 <DIR> ..
                0 File(s)          0 bytes

Directory of C:\ELJUVY\fa\barack
2025. 03. 17. 23:27 <DIR> .
2025. 03. 17. 23:27 <DIR> ..
                0 File(s)          0 bytes

Directory of C:\ELJUVY\fa\kokusz
2025. 03. 17. 23:29 <DIR> .
2025. 03. 17. 23:29 <DIR> ..
                0 File(s)          0 bytes

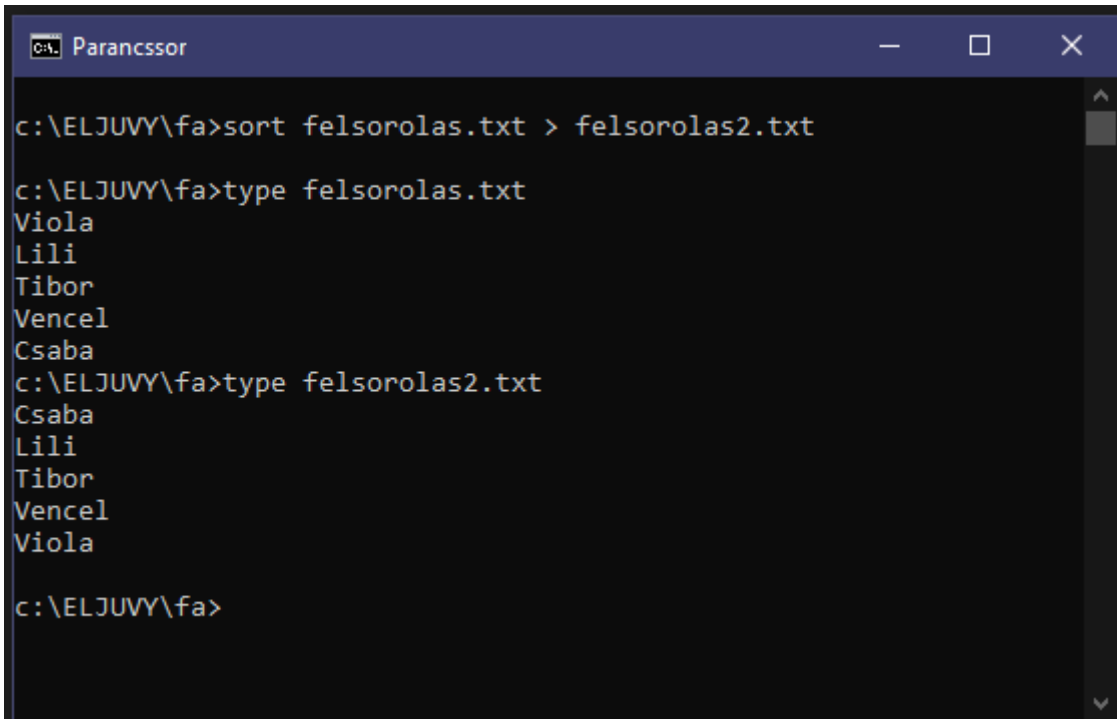
Directory of C:\ELJUVY\fa\korte
2025. 03. 17. 23:28 <DIR> .
2025. 03. 17. 23:28 <DIR> ..
                0 File(s)          0 bytes

Directory of C:\ELJUVY\fa\szeder
2025. 03. 17. 23:29 <DIR> .
2025. 03. 17. 23:29 <DIR> ..
                0 File(s)          0 bytes

Total Files Listed:
                2 File(s)          78 bytes
                29 Dir(s)  290 155 794 432 bytes free

C:\ELJUVY>
```

3/j



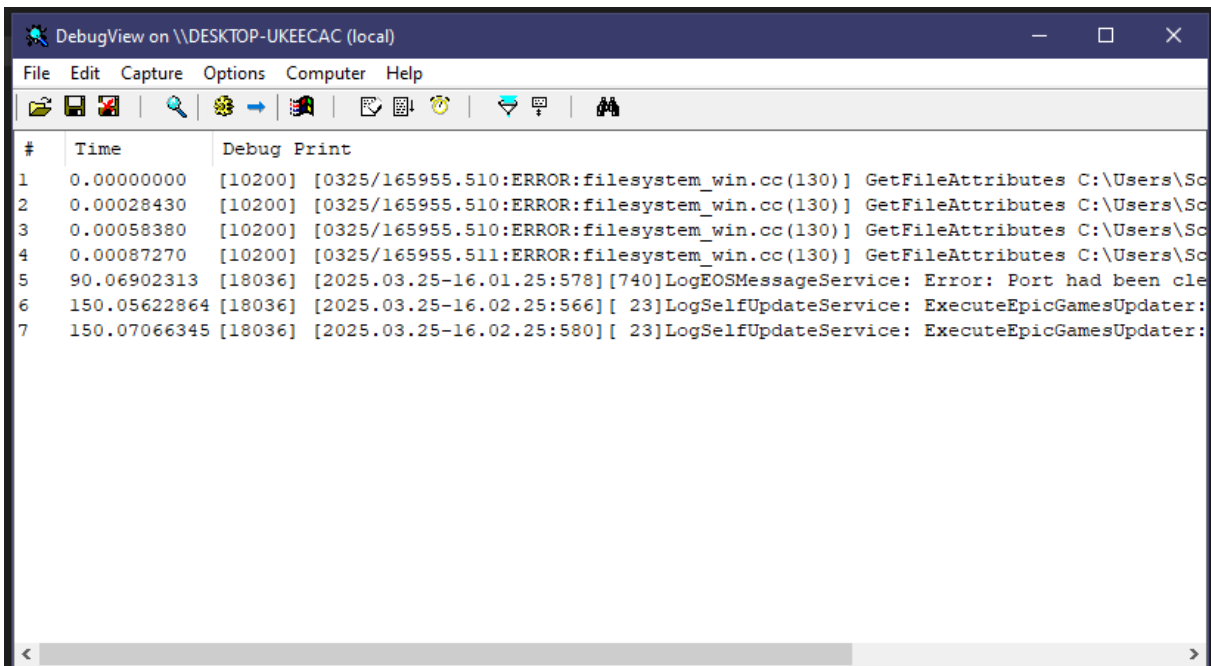
```
c:\ELJUVY\fa>sort felsorolas.txt > felsorolas2.txt

c:\ELJUVY\fa>type felsorolas.txt
Viola
Lili
Tibor
Vencel
Csaba
c:\ELJUVY\fa>type felsorolas2.txt
Csaba
Lili
Tibor
Vencel
Viola

c:\ELJUVY\fa>
```

4.Feladat

4/a



#	Time	Debug Print
1	0.00000000	[10200] [0325/165955.510:ERROR:filesystem_win.cc(130)] GetFileAttributes C:\Users\Sc
2	0.00028430	[10200] [0325/165955.510:ERROR:filesystem_win.cc(130)] GetFileAttributes C:\Users\Sc
3	0.00058380	[10200] [0325/165955.510:ERROR:filesystem_win.cc(130)] GetFileAttributes C:\Users\Sc
4	0.00087270	[10200] [0325/165955.511:ERROR:filesystem_win.cc(130)] GetFileAttributes C:\Users\Sc
5	90.06902313	[18036] [2025.03.25-16.01.25:578] [740]LogEOSMessageService: Error: Port had been cle
6	150.05622864	[18036] [2025.03.25-16.02.25:566] [23]LogSelfUpdateService: ExecuteEpicGamesUpdater:
7	150.07066345	[18036] [2025.03.25-16.02.25:580] [23]LogSelfUpdateService: ExecuteEpicGamesUpdater:

A **DebugView** egy olyan alkalmazás, amely lehetővé teszi a hibakeresési kimenet monitorozását a helyi rendszeren vagy a hálózaton található bármely számítógépen.

4/b

Process Name	Process ID	Protocol	State	Local Address	Local Port
svchost.exe	1196	TCP	Listen	0.0.0.0	135
System	4	TCP	Listen	26.11.128.202	139
System	4	TCP	Listen	192.168.0.12	139
System	4	TCP	Listen	192.168.56.1	139
svchost.exe	836	TCP	Listen	0.0.0.0	5040
Discord.exe	13168	TCP	Listen	127.0.0.1	6463
steam.exe	9052	TCP	Listen	0.0.0.0	27036
steam.exe	9052	TCP	Listen	127.0.0.1	27060
steam.exe	9052	TCP	Established	127.0.0.1	27060
lsass.exe	968	TCP	Listen	0.0.0.0	49664
wininit.exe	876	TCP	Listen	0.0.0.0	49665
svchost.exe	1652	TCP	Listen	0.0.0.0	49666
svchost.exe	1812	TCP	Listen	0.0.0.0	49667

Endpoints: 141 Established: 30 Listening: 27 Time Wait: 5 Close Wait: 3 Update: 2

A **TCPView** részletesen megjeleníti a rendszer összes TCP- és UDP-végpontját, beleértve a helyi és távoli címeket, valamint a TCP kapcsolatok állapotát.

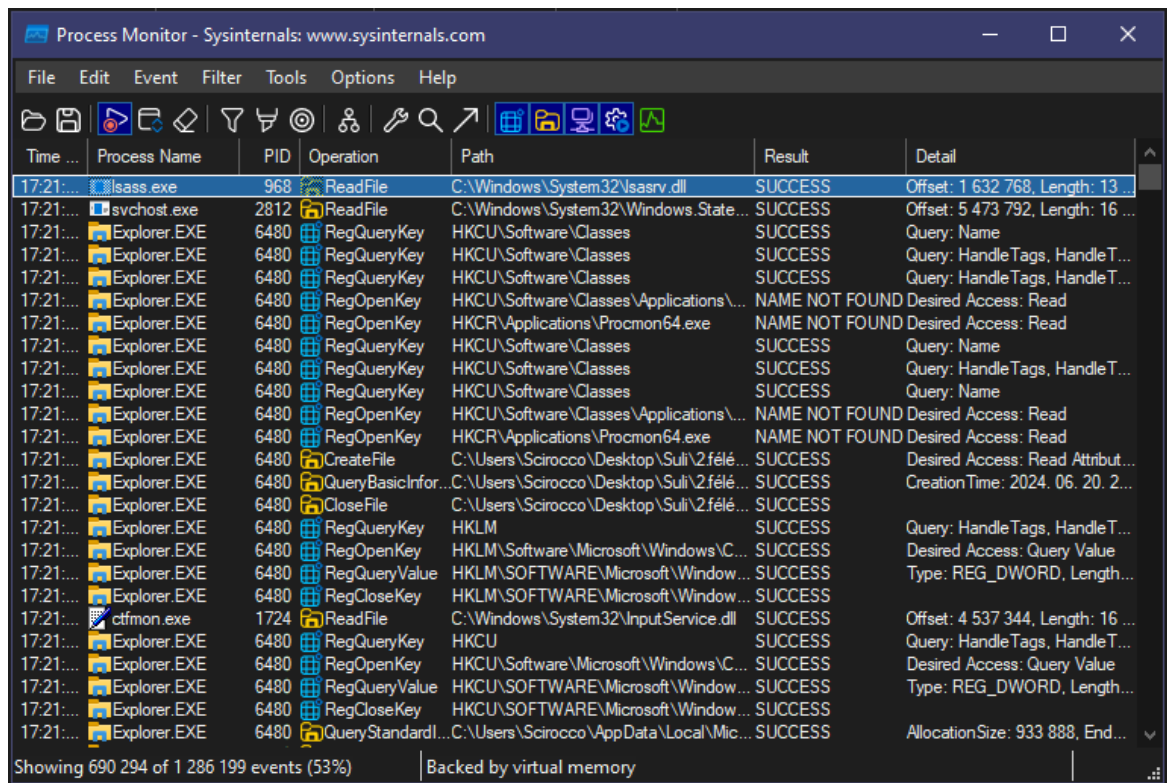
4/c (1/3)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		15 776 K	43 968 K	148		
System Idle Process	100.00	60 K	8 K	0		
System	< 0.01	228 K	12 344 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 076 K	144 K	628		
Memory Compression		1 700 K	383 548 K	2572		
csrss.exe		2 132 K	2 508 K	760		
csrss.exe	< 0.01	3 692 K	4 796 K	852		
wininit.exe		1 440 K	584 K	876		
services.exe	< 0.01	6 484 K	7 972 K	924		
svchost.exe		18 292 K	25 600 K	1076	Windows-szolgáltatások gazdafolya...	Microsoft Corporation
dllhost.exe		4 904 K	4 976 K	6844	COM Surrogate	Microsoft Corporation
WmiPrvSE.exe		10 336 K	9 592 K	960	WMI Provider Host	Microsoft Corporation
TextInputHost.exe		44 276 K	17 088 K	6344		Microsoft Corporation
StartMenuExperienceHos...		72 280 K	80 648 K	3824		
RuntimeBroker.exe		9 456 K	21 764 K	8188	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		18 588 K	30 244 K	8572	Runtime Broker	Microsoft Corporation
UserOOBEBroker.exe		2 396 K	4 552 K	8652	User OOBE Broker	Microsoft Corporation
RuntimeBroker.exe		2 388 K	2 548 K	10040	Runtime Broker	Microsoft Corporation
CompPkgSrv.exe		2 216 K	1 980 K	8704	Component Package Support Server	Microsoft Corporation
SearchApp.exe	Susp...	48 684 K	4 952 K	7200	Search application	Microsoft Corporation
msedgewebview2.exe	Susp...	37 528 K	6 476 K	6048	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2 164 K	692 K	2116	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	Susp...	69 364 K	2 520 K	10948	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	Susp...	11 852 K	2 616 K	5868	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	Susp...	8 276 K	1 100 K	2516	Microsoft Edge WebView2	Microsoft Corporation

CPU Usage: 0.13% Commit Charge: 59.85% Processes: 238 Physical Usage: 52.76%

A **ProcessExplorer** információkat jelenít meg arról, hogy mely leírók és DLL-folyamatok lettek megnyitva és betöltve.

4/c (2/3)



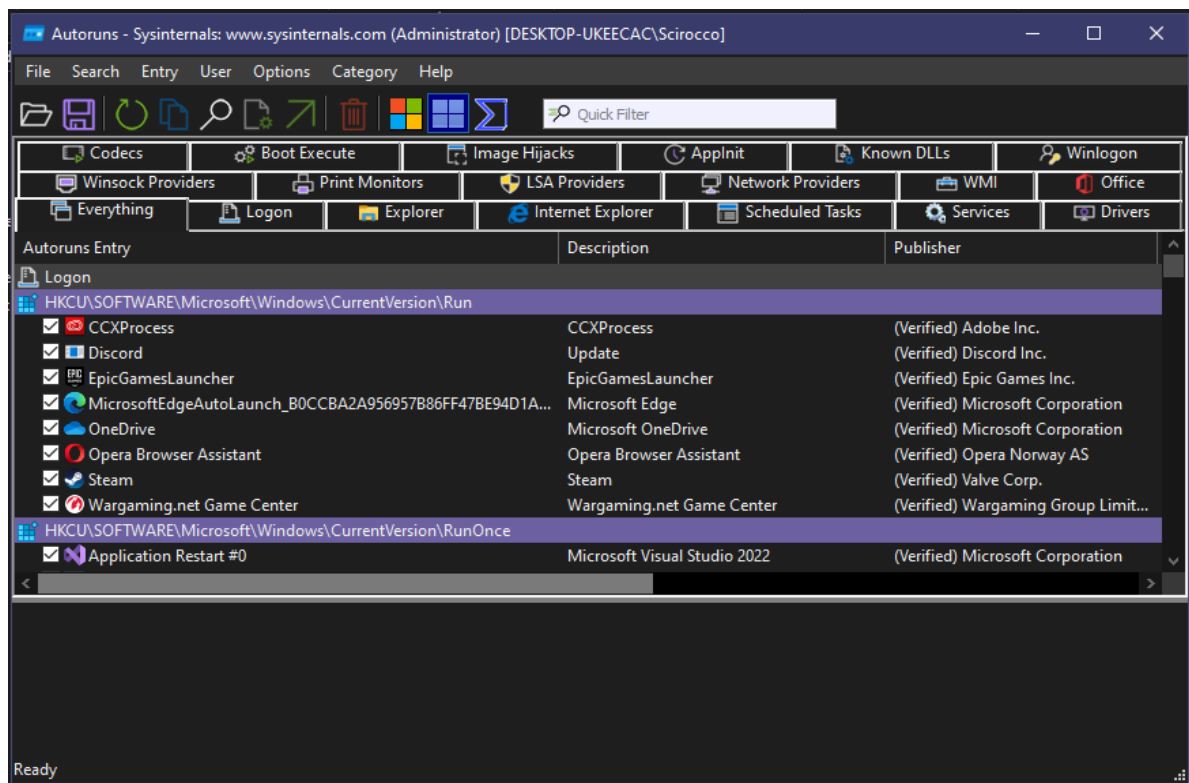
Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
17:21:...	lsass.exe	968	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 632 768, Length: 13 ...
17:21:...	svchost.exe	2812	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 5 473 792, Length: 16 ...
17:21:...	Explorer.EXE	6480	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
17:21:...	Explorer.EXE	6480	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleT...
17:21:...	Explorer.EXE	6480	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: Read
17:21:...	Explorer.EXE	6480	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: Read
17:21:...	Explorer.EXE	6480	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
17:21:...	Explorer.EXE	6480	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleT...
17:21:...	Explorer.EXE	6480	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
17:21:...	Explorer.EXE	6480	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: Read
17:21:...	Explorer.EXE	6480	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: Read
17:21:...	Explorer.EXE	6480	CreateFile	C:\Users\Scirocco\Desktop\Suli\2.félé...	SUCCESS	Desired Access: Read Attribut...
17:21:...	Explorer.EXE	6480	QueryBasicInfor...	C:\Users\Scirocco\Desktop\Suli\2.félé...	SUCCESS	CreationTime: 2024. 06. 20. 2...
17:21:...	Explorer.EXE	6480	CloseFile	C:\Users\Scirocco\Desktop\Suli\2.félé...	SUCCESS	
17:21:...	Explorer.EXE	6480	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleT...
17:21:...	Explorer.EXE	6480	RegOpenKey	HKLM\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Query Value
17:21:...	Explorer.EXE	6480	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWORD, Length...
17:21:...	Explorer.EXE	6480	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
17:21:...	ctfmon.exe	1724	ReadFile	C:\Windows\System32\inputService.dll	SUCCESS	Offset: 4 537 344, Length: 16 ...
17:21:...	Explorer.EXE	6480	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleT...
17:21:...	Explorer.EXE	6480	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Query Value
17:21:...	Explorer.EXE	6480	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWORD, Length...
17:21:...	Explorer.EXE	6480	RegCloseKey	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	
17:21:...	Explorer.EXE	6480	QueryStandardl...	C:\Users\Scirocco\AppData\Local\Mic...	SUCCESS	AllocationSize: 933 888, End...

Showing 690 294 of 1 286 199 events (53%) | Backed by virtual memory

A **ProcessMonitor** egy monitorozási eszköz, amely valós idejű fájlrendszert, beállításjegyzéket és folyamat-/száltevékenységet jelenít meg.

4/c (3/3)



Autoruns - Sysinternals: www.sysinternals.com (Administrator) [DESKTOP-UKKECAC\Scirocco]

Autoruns Entry	Description	Publisher
Logon		
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
<input checked="" type="checkbox"/> CCXProcess	CCXProcess	(Verified) Adobe Inc.
<input checked="" type="checkbox"/> Discord	Update	(Verified) Discord Inc.
<input checked="" type="checkbox"/> EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.
<input checked="" type="checkbox"/> MicrosoftEdgeAutoLaunch_B0CCBA2A956957B86FF47BE94D1A...	Microsoft Edge	(Verified) Microsoft Corporation
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation
<input checked="" type="checkbox"/> Opera Browser Assistant	Opera Browser Assistant	(Verified) Opera Norway AS
<input checked="" type="checkbox"/> Steam	Steam	(Verified) Valve Corp.
<input checked="" type="checkbox"/> Wargaming.net Game Center	Wargaming.net Game Center	(Verified) Wargaming Group Limit...
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce		
<input checked="" type="checkbox"/> Application Restart #0	Microsoft Visual Studio 2022	(Verified) Microsoft Corporation

Ready

Az **Autoruns** megmutatja, hogy milyen programok futnak a rendszerindítás vagy bejelentkezés során.

4/d

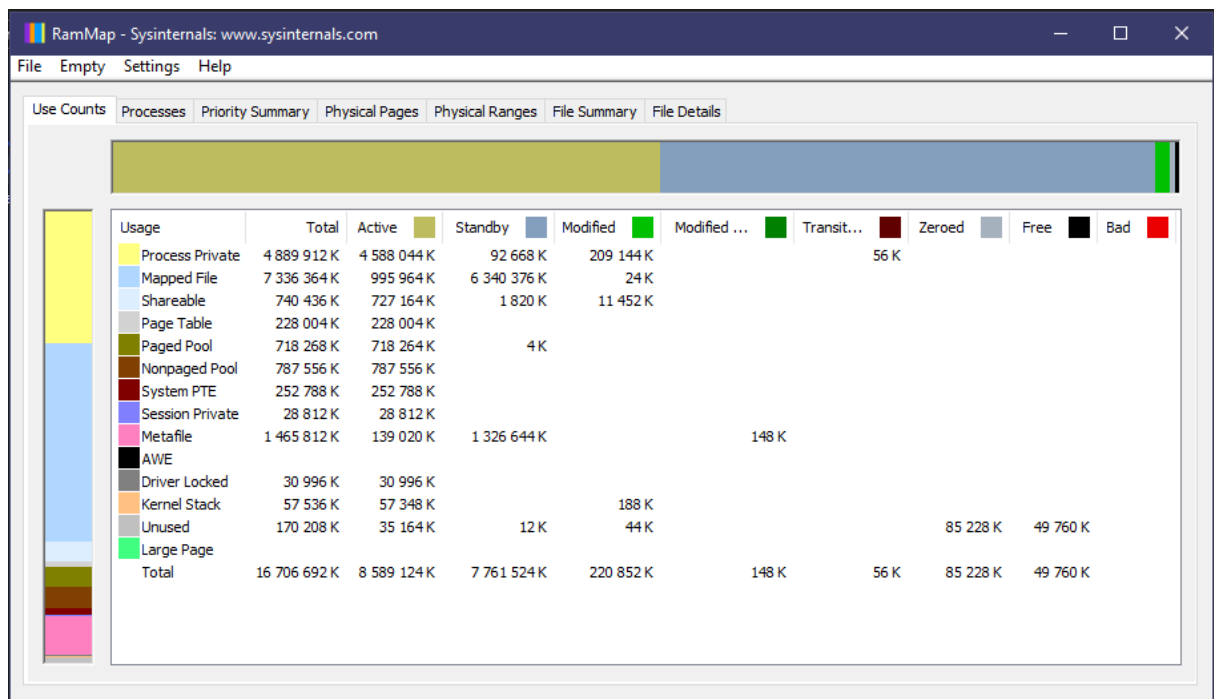
```
Administrator: Parancssor
c:\logonSessions>logonsessions64 -p

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\DESKTOP-UKEECAC$
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            S-1-5-18
  Logon time:     2025. 03. 17. 11:04:25
  Logon server:
  DNS Domain:
  UPN:
    968: lsass.exe
    100: winlogon.exe
    1076: svchost.exe
    1248: svchost.exe
    1364: svchost.exe
```

A **LogonSessions** felsorolja az aktuális aktív bejelentkezési munkameneteket és a **-p** beállítással az egyes munkamenetekben futó folyamatokat.

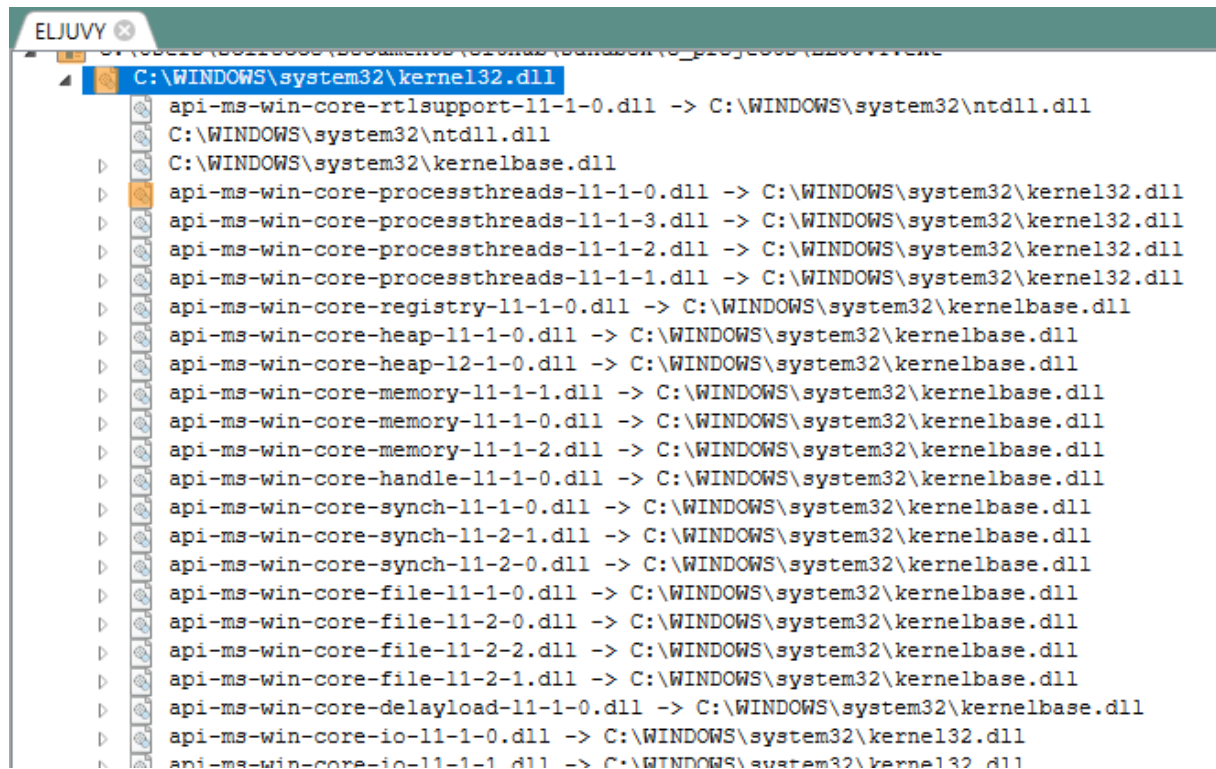
4/e



A **RAMMap** egy fizikai memóriahasználat elemző segédprogram. Támogatja a memória pillanatképeinek mentését és betöltését.

5. feladat

5/a



5/b

PI	Ordinal	Hint	Function	Module
	N/A	1260 (0x04ec)	RtlLookupFunctionEntry	C:\WINDOWS\system32\ntdll.dll
	N/A	1552 (0x0610)	RtlUnwind	C:\WINDOWS\system32\ntdll.dll
	N/A	1579 (0x062b)	RtlVirtualUnwind	C:\WINDOWS\system32\ntdll.dll
	N/A	757 (0x02f5)	RtlCaptureContext	C:\WINDOWS\system32\ntdll.dll
	N/A	1553 (0x0611)	RtlUnwindEx	C:\WINDOWS\system32\ntdll.dll
	N/A	1299 (0x0513)	RtlPcToFileHeader	C:\WINDOWS\system32\ntdll.dll

E	Ordinal	Hint	Function	VirtualAddress
	8 (0x0008)		N/A Ordinal_8	0x0007fb10
	9 (0x0009)		N/A A_SHAFinal	0x00040240
	10 (0x000a)		N/A A_SHAInit	0x00041070
	11 (0x000b)		N/A A_SHAUpdate	0x000410b0
	12 (0x000c)		N/A AlpcAdjustCompletionListConcurren	0x000e07e0
	13 (0x000d)		N/A AlpcFreeCompletionListMessage	0x00071730
	14 (0x000e)		N/A AlpcGetCompletionListLastMessageI	0x000e0810
	15 (0x000f)		N/A AlpcGetCompletionListMessageAttri	0x000e0830
	16 (0x0010)		N/A AlpcGetHeaderSize	0x00071460
	17 (0x0011)		N/A AlpcGetMessageAttribute	0x00071420
	18 (0x0012)		N/A AlpcGetMessageFromCompletionList	0x00010a60
	19 (0x0013)		N/A AlpcGetOutstandingCompletionListM	0x00086380
	20 (0x0014)		N/A AlpcInitializeMessageAttribute	0x000713c0
	21 (0x0015)		N/A AlpcMaxAllowedMessageLength	0x00084d20
	22 (0x0016)		N/A AlpcRegisterCompletionList	0x00086200
	23 (0x0017)		N/A AlpcRegisterCompletionListWorkerT	0x00076240
	24 (0x0018)		N/A AlpcRunDownCompletionList	0x00086340