

Operációs rendszerek BSc

2. konzultáció gyakorlat














2021.02.26

Készítette:

Bálint Gergely MSC
Mérnökinformatikus
LA3WXZ

Miskolc, 2021

- 1. Feladat .** Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít. A csomag magában foglal több diagnosztikai programot.

▼ ◀ \OS\Féléves feladat\kettő\programok\sysinternals-suite*.*			
↓Név	Kit.	Méret	Dátum
↑ [..]		<DIR>	2021.03.06 19:13
 Zoomlt64	exe	588 152	2020.04.30 17:49
 Zoomlt	exe	1 059 712	2020.04.30 17:50
 Winobj64	exe	1 366 928	2021.02.22 19:52
 WINOBJ	HLP	7 653	1999.12.30 20:26
 Winobj	exe	1 034 640	2021.02.22 19:52
 whois64	exe	523 632	2020.04.06 10:38
 whois	exe	398 712	2020.04.06 10:39
 Volumeid64	exe	169 648	2016.06.13 05:15
 Volumeid	exe	233 640	2016.06.13 05:18
 vmmap64	exe	719 232	2020.11.04 20:52
 vmmap	exe	1 312 640	2020.11.04 20:52
 Vmmap	chm	51 747	2020.11.04 20:52
 Testlimit64	exe	243 888	2016.11.18 16:38

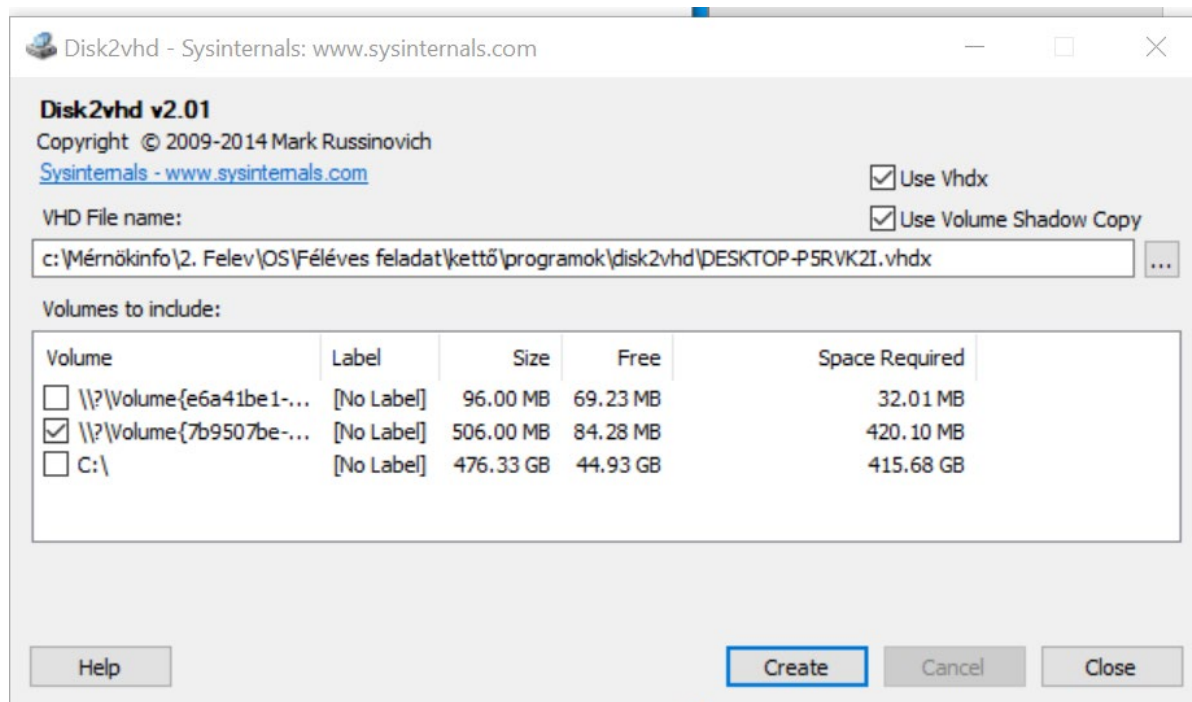
2. **feladat.** A felsorolt eszközök közül minden eszköz esetén töltsse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el a megadott dokumentumba (képernyőkép).





2.a

Disk2vhd

A program segítségével készíthetünk egy virtuális merevlemezt amit a Microsoft Virtual PC vagy Microsoft Hyper-V tud használni.

Létrehozta a DESKTOP-P5RVK2I.VHDX file-t.

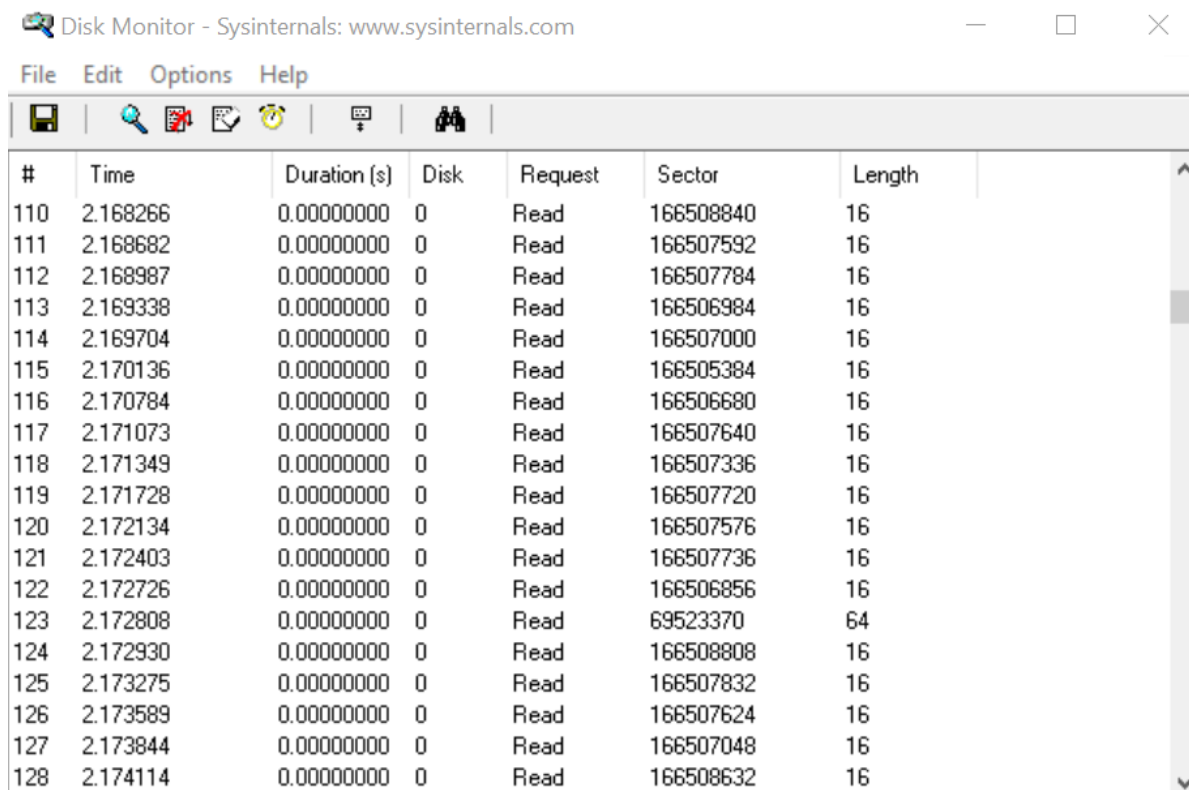


 Eula	txt	7 005	2021.03.06 18:47	-a--
 disk2vhd	exe	7 134 400	2021.03.06 18:47	-a--
 Disk2vhd	chm	40 717	2021.03.06 18:47	-a--
 DESKTOP-P5RVK2I	VHDX	42 992 128	2021.03.06 20:11	-a--



DiskMon

Naplózza és megjeleníti a merevlemez aktivitásait a Windowsban. Folyamatosan listázza a futó aktivitásokat.



Disk Monitor - Sysinternals: www.sysinternals.com

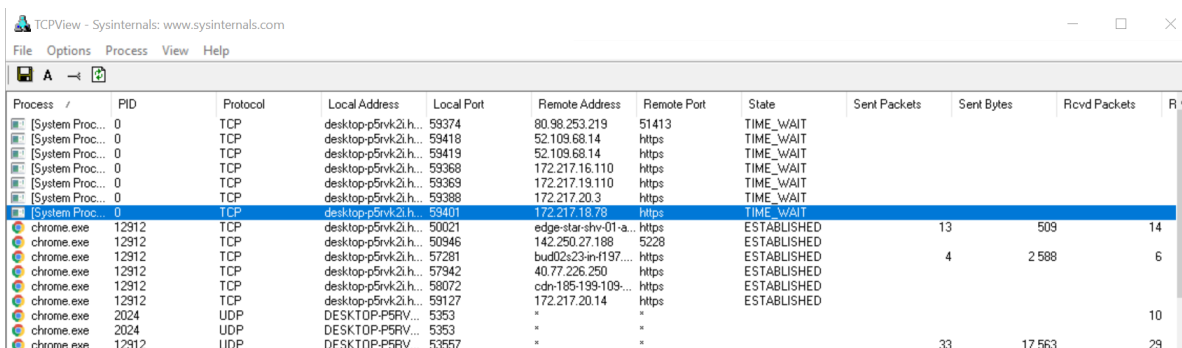
File Edit Options Help

#	Time	Duration (s)	Disk	Request	Sector	Length
110	2.168266	0.00000000	0	Read	166508840	16
111	2.168682	0.00000000	0	Read	166507592	16
112	2.168987	0.00000000	0	Read	166507784	16
113	2.169338	0.00000000	0	Read	166506984	16
114	2.169704	0.00000000	0	Read	166507000	16
115	2.170136	0.00000000	0	Read	166505384	16
116	2.170784	0.00000000	0	Read	166506680	16
117	2.171073	0.00000000	0	Read	166507640	16
118	2.171349	0.00000000	0	Read	166507336	16
119	2.171728	0.00000000	0	Read	166507720	16
120	2.172134	0.00000000	0	Read	166507576	16
121	2.172403	0.00000000	0	Read	166507736	16
122	2.172726	0.00000000	0	Read	166506856	16
123	2.172808	0.00000000	0	Read	69523370	64
124	2.172930	0.00000000	0	Read	166508808	16
125	2.173275	0.00000000	0	Read	166507832	16
126	2.173589	0.00000000	0	Read	166507624	16
127	2.173844	0.00000000	0	Read	166507048	16
128	2.174114	0.00000000	0	Read	166508632	16

2.b

TCPview

Egy részletes listát mutat az összes TCP és DUP végpontról a rendszerben. Futtatás után, több a hálózatot használó programról kilistázza nevét, a távoli címét és az állapotát a TCP kapcsolatnak



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
[System Proc...	0	TCP	desktop-p5rvk2i.h...	59374	80.98.253.219	51413	TIME_WAIT			
[System Proc...	0	TCP	desktop-p5rvk2i.h...	59418	52.109.68.14	https	TIME_WAIT			
[System Proc...	0	TCP	desktop-p5rvk2i.h...	59419	52.109.68.14	https	TIME_WAIT			
[System Proc...	0	TCP	desktop-p5rvk2i.h...	59368	172.217.16.110	https	TIME_WAIT			
[System Proc...	0	TCP	desktop-p5rvk2i.h...	59369	172.217.19.110	https	TIME_WAIT			
[System Proc...	0	TCP	desktop-p5rvk2i.h...	59388	172.217.20.3	https	TIME_WAIT			
[System Proc...	0	TCP	desktop-p5rvk2i.h...	59401	172.217.18.78	https	TIME_WAIT			
chrome.exe	12912	TCP	desktop-p5rvk2i.h...	50021	edge-star-shw-01-a...	https	ESTABLISHED	13	509	14
chrome.exe	12912	TCP	desktop-p5rvk2i.h...	50946	142.250.27.188	5228	ESTABLISHED			
chrome.exe	12912	TCP	desktop-p5rvk2i.h...	57281	bud02s23m-f197...	https	ESTABLISHED	4	2 588	6
chrome.exe	12912	TCP	desktop-p5rvk2i.h...	57942	40.77.226.250	https	ESTABLISHED			
chrome.exe	12912	TCP	desktop-p5rvk2i.h...	58072	cdn-185-199-109-...	https	ESTABLISHED			
chrome.exe	12912	TCP	desktop-p5rvk2i.h...	59127	172.217.20.14	https	ESTABLISHED			
chrome.exe	2024	UDP	DESKTOP-P5RV...	5353	*	*				10
chrome.exe	2024	UDP	DESKTOP-P5RV...	5353	*	*				
chrome.exe	12912	UDP	DESKTOP-P5RV...	53557	*	*		33	17 563	29

2.c

Process Explorer

Nyomon követhetjük és felfedezhetjük a futó processzeket, DLL eljárásokat vagy szolgáltatásokat.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8 176 K	43 908 K	124		
System Idle Process	89.06	60 K	8 K	0		
System	0.40	196 K	52 K	4		
Interrupts	0.31	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 052 K	292 K	552		
Memory Compression	0.02	3 876 K	383 052 K	2284		
csrss.exe		2 052 K	3 112 K	656		
wininit.exe		1 412 K	2 684 K	768		
services.exe	0.67	6 076 K	7 052 K	840		
svchost.exe	< 0.01	15 988 K	20 944 K	88	Windows-szolgáltatások gaz...	Microsoft Corporation
unsecapp.exe		1 996 K	4 736 K	5264		
StartMenuExperienceHos...		34 160 K	23 808 K	8460		
RuntimeBroker.exe		6 824 K	7 804 K	8636	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	159 160 K	1 960 K	8780	Search application	Microsoft Corporation
RuntimeBroker.exe		19 204 K	11 284 K	9028	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	29 124 K	3 392 K	9608	YourPhone	Microsoft Corporation
SettingSyncHost.exe		10 264 K	5 772 K	9772	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		7 056 K	6 876 K	10188	Runtime Broker	Microsoft Corporation
LockApp.exe	Susp...	16 320 K	14 044 K	9300	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10 540 K	18 700 K	9896	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		5 308 K	8 260 K	10432	Runtime Broker	Microsoft Corporation
dllhost.exe		3 208 K	6 168 K	8792		
RuntimeBroker.exe		5 152 K	10 404 K	12816	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe		32 248 K	25 088 K	12976	Application Frame Host	Microsoft Corporation
WinStore.App.exe	Susp...	54 936 K	1 836 K	13000	Store	Microsoft Corporation
MoUsoCoreWorker.exe		52 448 K	8 520 K	11332		
UserOOBEBroker.exe		2 260 K	6 236 K	5012	User OOBEBroker	Microsoft Corporation
TextInputHost.exe		13 388 K	13 616 K	4156		Microsoft Corporation
CompPkgSrv.exe		2 832 K	7 180 K	400	Component Package Suppor...	Microsoft Corporation
Calculator.exe	Susp...	22 912 K	1 300 K	12924		
RuntimeBroker.exe		1 548 K	3 752 K	8528	Runtime Broker	Microsoft Corporation
dllhost.exe		4 128 K	7 016 K	12612	COM Surrogate	Microsoft Corporation
Microsoft.Photos.exe	Susp...	55 320 K	544 K	12132		
RuntimeBroker.exe		11 060 K	13 096 K	6816	Runtime Broker	Microsoft Corporation
GameBarFTServer.exe	0.04	13 500 K	17 520 K	7056	Xbox Game Bar Full Trust CO...	Microsoft Corporation
SystemSettings.exe	Susp...	27 128 K	1 700 K	12516	Gépház	Microsoft Corporation
ShellExperienceHost.exe		15 208 K	62 396 K	6204	Windows Shell Experience H...	Microsoft Corporation
GameBar.exe	0.04	24 640 K	27 712 K	25208	Xbox Game Bar	Microsoft Corporation
RuntimeBroker.exe	< 0.01	6 280 K	17 224 K	27656	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 840 K	17 508 K	12852	Runtime Broker	Microsoft Corporation
smartscreen.exe		9 420 K	26 640 K	29644	Windows Defender SmartScr...	Microsoft Corporation
WUDFHost.exe		8 676 K	8 924 K	764		
svchost.exe	0.01	11 032 K	13 424 K	1084	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	0.01	2 896 K	4 068 K	1148	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	< 0.01	1 676 K	2 604 K	1372	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	0.02	7 792 K	6 856 K	1400	Windows-szolgáltatások gaz...	Microsoft Corporation

Process Monitor

Statisztikákat láthatunk a futó folyamatokról (indítás, befejezés, DLL betöltések)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
21:31:5...	NVDisplay.Cont...	3416	ReadFile	C:\Windows\System32\DriverStore\FileR...	SUCCESS	Offset: 4 565 504, ...
21:31:5...	svchost.exe	2780	Thread Create		SUCCESS	Thread ID: 21388
21:31:5...	NVDisplay.Cont...	3416	ReadFile	C:\Windows\System32\DriverStore\FileR...	SUCCESS	Offset: 4 504 064, ...
21:31:5...	MsMpEng.exe	5640	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 14 958 592,...
21:31:5...	svchost.exe	2780	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
21:31:5...	NVDisplay.Cont...	3416	ReadFile	C:\Windows\System32\DriverStore\FileR...	SUCCESS	Offset: 4 540 928, ...
21:31:5...	Explorer.EXE	1348	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
21:31:5...	svchost.exe	2780	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678 400, Le...
21:31:5...	Explorer.EXE	1348	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags...
21:31:5...	MsMpEng.exe	5640	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 14 934 016,...
21:31:5...	Explorer.EXE	1348	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags...
21:31:5...	Explorer.EXE	1348	RegOpenKey	HKCU\Software\Classes\CLSID\{11659...	NAME NOT FOUND	Desired Access: R...
21:31:5...	Explorer.EXE	1348	RegOpenKey	HKCR\CLSID\{11659A23-5884-4D1B-9...	SUCCESS	Desired Access: R...
21:31:5...	Explorer.EXE	1348	RegQueryKey	HKCR\CLSID\{11659a23-5884-4d1b-9cf...	SUCCESS	Query: Name
21:31:5...	Explorer.EXE	1348	RegQueryKey	HKCR\CLSID\{11659a23-5884-4d1b-9cf...	SUCCESS	Query: HandleTags...
21:31:5...	Explorer.EXE	1348	RegOpenKey	HKCU\Software\Classes\CLSID\{11659a...	NAME NOT FOUND	Desired Access: Q...
21:31:5...	Explorer.EXE	1348	RegQueryKey	HKCR\CLSID\{11659a23-5884-4d1b-9cf...	SUCCESS	Query: HandleTags...
21:31:5...	Explorer.EXE	1348	RegOpenKey	HKCR\CLSID\{11659a23-5884-4d1b-9cf...	NAME NOT FOUND	Desired Access: Q...
21:31:5...	Explorer.EXE	1348	ReadFile	C:\Windows\System32\combase.dll	SUCCESS	Offset: 3 003 904, ...
21:31:5...	NVDisplay.Cont...	3416	ReadFile	C:\Windows\System32\DriverStore\FileR...	SUCCESS	Offset: 4 557 312

AutoRuns

Megmutatja, hogy milyen folyamatok indulnak automatikusan a Windows bootoláskor.

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

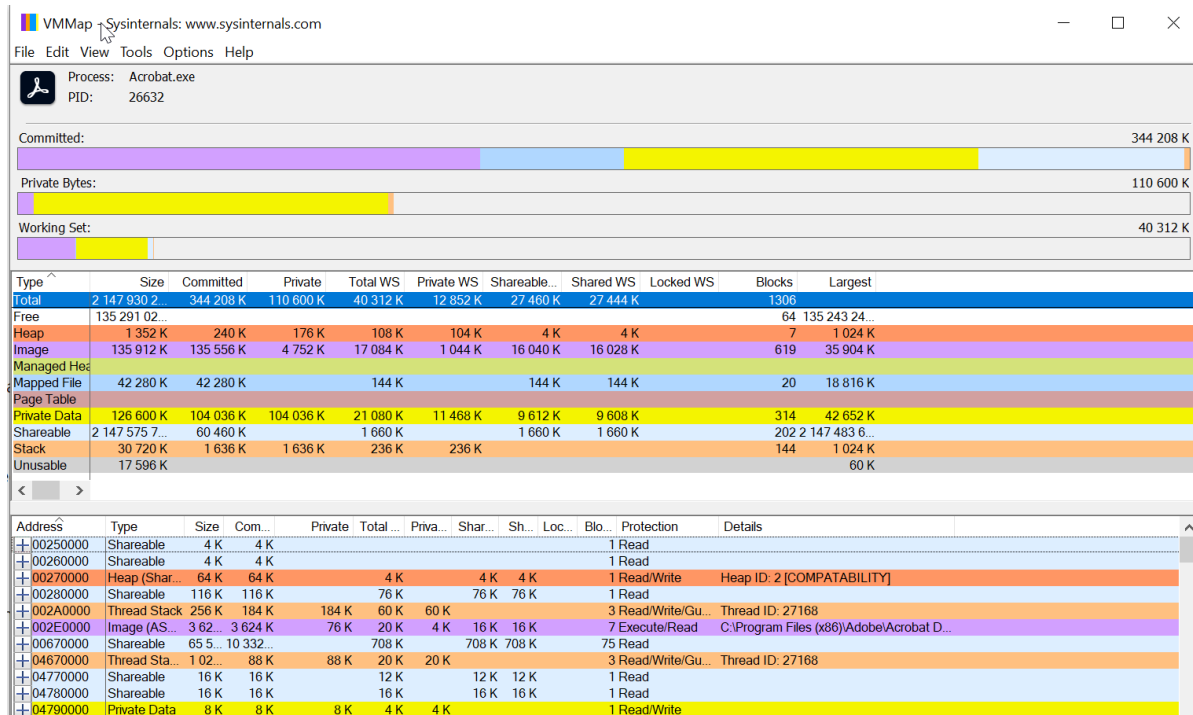
Filter:

Winsock Providers Logon Explorer Internet Explorer Scheduled Tasks LSA Providers Services Drivers Codecs Network

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 Pro...	(Verified) Microsoft Wind...	c:\windows\system32\cm...	1953. 12. 11. 3:58	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 03. 07. 18:03	
<input checked="" type="checkbox"/> AdobeAAM...	Adobe Updater Startup ...	(Verified) Adobe System...	c:\program files (x86)\co...	2018. 04. 11. 8:32	
<input checked="" type="checkbox"/> AdobeGCIn...	Adobe GC Invoker Utility	(Verified) Adobe Inc.	c:\program files (x86)\co...	2021. 02. 17. 4:27	
<input checked="" type="checkbox"/> Greenshot	Greenshot	(Verified) Open Source ...	c:\program files\greensh...	2017. 08. 09. 16:34	
<input checked="" type="checkbox"/> Logitech Do...	Logitech Download Assi...	(Verified) Logitech	c:\windows\system32\log...	2012. 09. 13. 23:51	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021. 02. 07. 17:55	
<input checked="" type="checkbox"/> Acrobat Assi...	AcroTray	(Not verified) Adobe Sys...	c:\program files (x86)\ad...	2020. 11. 18. 22:04	
<input checked="" type="checkbox"/> DualControl	DualControlStartupApp	(Verified) LG Electronics...	c:\program files (x86)\lg ...	2018. 12. 27. 5:41	

VMMMap

Egy folyamatnak a virtuális és fizikai memóriaelemzésére használható segédprogram.



2.d

LogonSession

Megmutatja az aktív bejelentkezési munkameneteket és megmutathatja az futó folyamatok listáját is a munkamenetekhez.

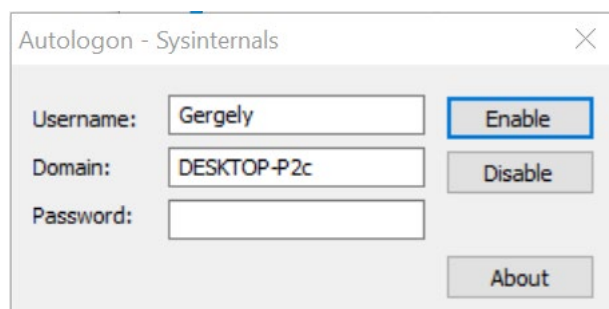
```
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
  User name:      WORKGROUP\DESKTOP-P5RVK2I$
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            S-1-5-18
  Logon time:     2021. 03. 07. 18:03:49
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:000113ee:
  User name:
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            (none)
  Logon time:     2021. 03. 07. 18:03:49
  Logon server:
  DNS Domain:
  UPN:
```

Autologon

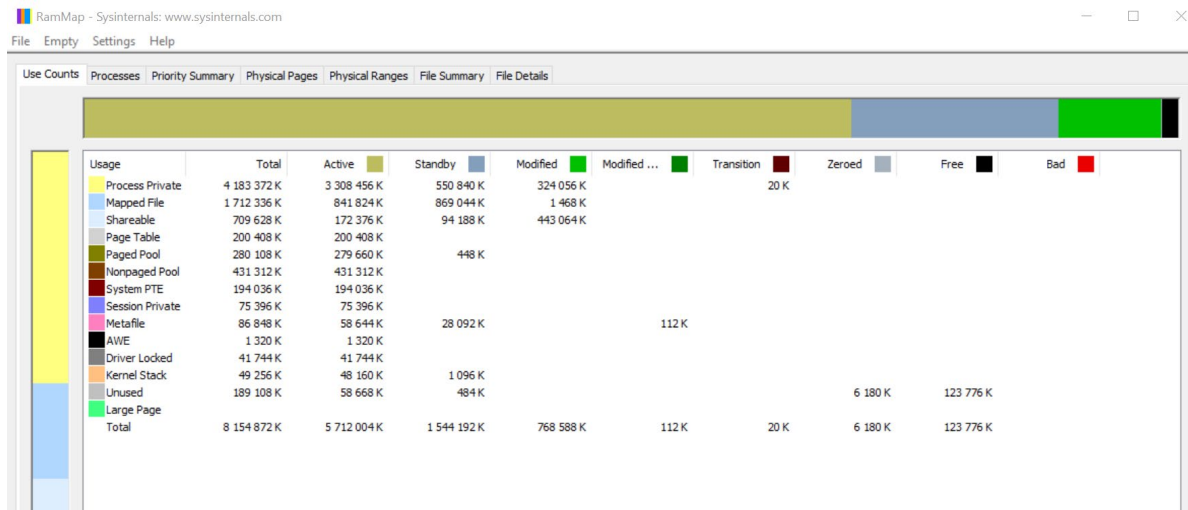
Segíti az automatikus bejelentkezést, ahelyett, hogy várna a felhasználó nevének és jelszavának megadására.



2.e

RamMap

Több különböző módon tudja megjeleníteni az információkat a fizikai memóriahasználatról elemzés céljából



ClockRes

A segítségével megtudhatjuk a rendszeróra, időzítő maximális felbontását.

```
C:\>Clockres64.exe

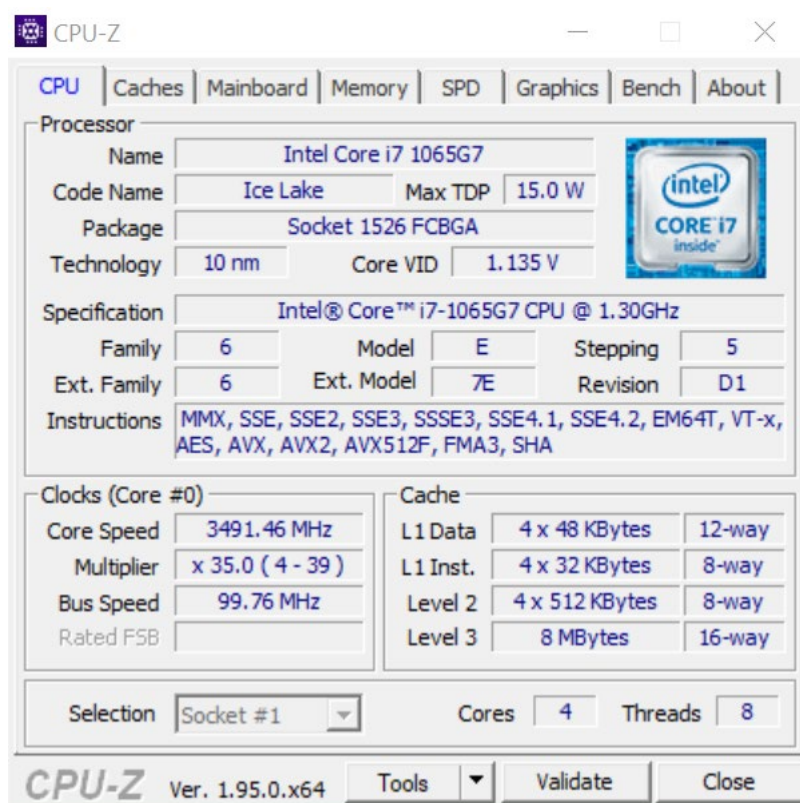
Clockres v2.1 - Clock resolution display utility
Copyright (C) 2016 Mark Russinovich
Sysinternals

Maximum timer interval: 15.625 ms
Minimum timer interval: 0.500 ms
Current timer interval: 1.000 ms
```

3. Töltse le és végezzen vizsgálatot az AIDA64_Engineer_v5.98.4800_Portable, CPU-Z, GPU-Z programokkal. A felsorolt segédprogramoknak írja le a szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el az alábbi dokumentumba (képernyőkép is).

CPU-Z

Információkat szerezhetünk róla a számítógépben lévő hardverekről és a legfontosabb összetevőkről úgy mint processzor, alaplap, videokártya, SPD, Cache, RAM, BIOS.



GPU-Z

Ezzel a programmal a videokártyáról és a grafikus processzorról kaphatunk információkat amit akár egy report fájlba is menthetünk. Típus, órajel, hőmérséklet stb.

The screenshot shows the TechPowerUp GPU-Z 2.37.0 application window. The 'Graphics Card' tab is selected, displaying a comprehensive list of GPU specifications. The interface includes a top navigation bar with tabs for 'Graphics Card', 'Sensors', 'Advanced', and 'Validation'. The main content area is organized into a grid of fields, each with a label and a corresponding value. A 'Lookup' button is located next to the GPU name field. The Intel logo is prominently displayed on the right side of the window. At the bottom, there is a dropdown menu showing the current GPU and a 'Close' button.

TechPowerUp GPU-Z 2.37.0			
Graphics Card Sensors Advanced Validation			
Name	Intel(R) Iris(R) Plus Graphics		
GPU	Ice Lake GT2	Revision	N/A
Technology	10 nm	Die Size	177 mm²
Release Date	Aug 1, 2019	Transistors	Unknown
BIOS Version	Unknown		UEFI <input checked="" type="checkbox"/>
Subvendor	Acer	Device ID	8086 8A52 - 1025 1407
ROPs/TMUs	8 / 16	Bus Interface	N/A
Shaders	64 Unified	DirectX Support	12 (12_1)
Pixel Fillrate	8.8 GPixel/s	Texture Fillrate	17.6 GTexel/s
Memory Type	DDR4	Bus Width	128 bit
Memory Size	N/A	Bandwidth	32.0 GB/s
Driver Version	27.20.100.8783 DCH / Win10 64		
Driver Date	Sep 24, 2020	Digital Signature	WHQL
GPU Clock	300 MHz	Memory	1000 MHz
Default Clock	300 MHz	Memory	1000 MHz
Boost	1100 MHz	Boost	1100 MHz
Multi-GPU	Disabled		
Computing	<input checked="" type="checkbox"/> OpenCL	<input type="checkbox"/> CUDA	<input checked="" type="checkbox"/> DirectCompute
Technologies	<input checked="" type="checkbox"/> Vulkan	<input type="checkbox"/> Ray Tracing	<input checked="" type="checkbox"/> PhysX
			<input checked="" type="checkbox"/> OpenGL 4.6
Intel(R) Iris(R) Plus Graphics			

Aida64 Engineer

Szolgáltatásai között szerepel a hardverfelismerés, részletes adatokkal szolgál a telepített szoftvekről, a számítógép érzékelői segítségével adatokat kapunk a hőmérsékletről, feszültségről, ventilátorok fordulatszámáról. Továbbá tartalmaz benchmarkmodulokat is.

The screenshot displays the AIDA64 Engineer [TRIAL VERSION] window. The interface includes a menu bar (Fájl, Nézet, Riport, Kedvencek, Eszközök, Súgó), a toolbar with navigation icons, and a main panel with three tabs: Menü, Kedvencek, and Riport. The Menü tab is active, showing a tree view of system components. The 'CPU' section is expanded, revealing various CPU-related metrics. The 'Mező' (Field) column lists the metrics, and the 'Érték' (Value) column shows the corresponding values.

Mező	Érték
CPU tulajdonságai	
CPU típusa	QuadCore , 3500 MHz (35 x 100)
CPU alias	Ice Lake-U
Utasításkészlet	x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, AVX, AVX2,...
Eredeti órajel	[TRIAL VERSION]
Min / Max CPU szorzó	4x / 15x
Engineering Sample	Nem
L1 kód gyorsítótár	32 KB per core
L1 adat gyorsítótár	[TRIAL VERSION]
L2 gyorsítótár	512 KB per core (On-Die, ECC, Full-Speed)
L3 gyorsítótár	8 MB (On-Die, ECC, Full-Speed)
CPU fizikai információk	
Tokozás típusa	1526 Ball BGA
Tokozás mérete	50 mm x 25 mm
Gyártási technológia	10 nm, CMOS, Cu, High-K + Metal Gate
Processzormag mérete	[TRIAL VERSION] mm2
PCH: Processzormag mérete	[TRIAL VERSION] mm2
Tipikus teljesítmény felvétel	15 W
Multi CPU	
CPU #1	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz
CPU #2	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz
CPU #3	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz
CPU #4	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz
CPU #5	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz
CPU #6	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz
CPU #7	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz
CPU #8	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz, 1498 MHz

4. Feladat

Töltse le a következő programot: Dependency Walker

Készítsen egy *neptunkod.c* nevű forráskódot, amely egy *vezeteknev.txt* fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc.

Fordítsa le kódot a C fordító, amely létrehoz egy objektum kódot, ezután egy linker segítségével készítsen egy végrehajtó állományt: *neptunkod.exe*

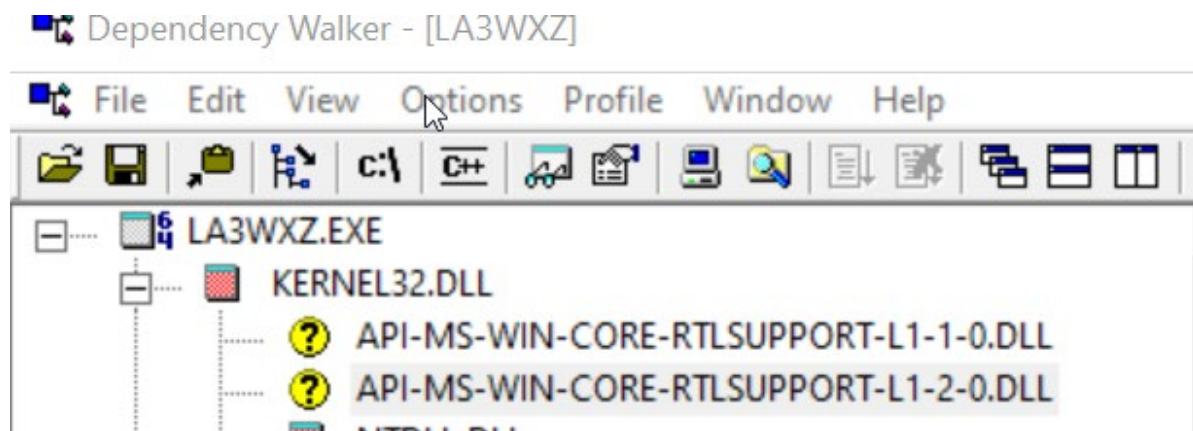
A Dependency Walker segítségével végezze el a következő feladatokat.

Nyissa meg a *neptunkod.exe* fájlt!

4.a Vizsgálja meg, hogy a *neptunkod.exe* milyen API hívásokat használ a kernel32.dll-ből

API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL

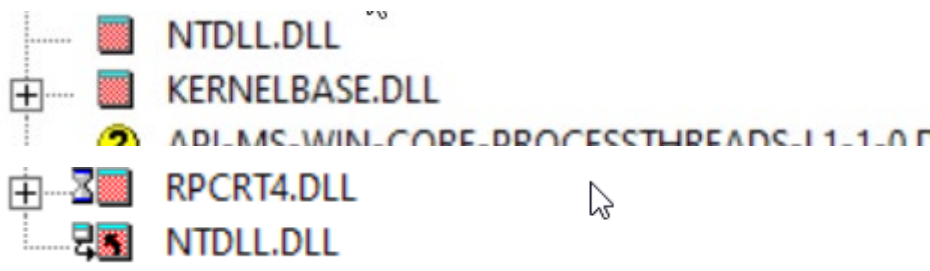


4.b Milyen függőségei vannak a kernel32.dll-nek!

NTDLL.DLL

KERNELBASE.DLL

RPCRT4.DLL



4.c Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról!

Az NTDLL.DLL file exportálja a Windows natív API-t

E	Ordinal ^	Hint	Function	Entry Point
	239 (0x00EF)	224 (0x00E0)	NtAlpcCreatePortSection	0x00073350
	240 (0x00F0)	225 (0x00E1)	NtAlpcCreateResourceReserve	0x00073360
	241 (0x00F1)	226 (0x00E2)	NtAlpcCreateSectionView	0x00073370
	242 (0x00F2)	227 (0x00E3)	NtAlpcCreateSecurityContext	0x00073380
	243 (0x00F3)	228 (0x00E4)	NtAlpcDeletePortSection	0x00073390
	244 (0x00F4)	229 (0x00E5)	NtAlpcDeleteResourceReserve	0x000733A0
	245 (0x00F5)	230 (0x00E6)	NtAlpcDeleteSectionView	0x000733B0
	246 (0x00F6)	231 (0x00E7)	NtAlpcDeleteSecurityContext	0x000733C0
	247 (0x00F7)	232 (0x00E8)	NtAlpcDisconnectPort	0x000733D0
	248 (0x00F8)	233 (0x00E9)	NtAlpcImpersonateClientContainerOfPort	0x000733E0
	249 (0x00F9)	234 (0x00EA)	NtAlpcImpersonateClientOfPort	0x000733F0
	250 (0x00FA)	235 (0x00EB)	NtAlpcOpenSenderProcess	0x00073400
	251 (0x00FB)	236 (0x00EC)	NtAlpcOpenSenderThread	0x00073410
	252 (0x00FC)	237 (0x00ED)	NtAlpcQueryInformation	0x00073420
	253 (0x00FD)	238 (0x00EE)	NtAlpcQueryInformationMessage	0x00073430
	254 (0x00FE)	239 (0x00EF)	NtAlpcRevokeSecurityContext	0x00073440
	255 (0x00FF)	240 (0x00F0)	NtAlpcSendWaitReceivePort	0x00073450
	256 (0x0100)	241 (0x00F1)	NtAlpcSetInformation	0x00073460
	257 (0x0101)	242 (0x00F2)	NtApphelpCacheControl	0x00073050
	258 (0x0102)	243 (0x00F3)	NtAreMappedFilesTheSame	0x00073470
	259 (0x0103)	244 (0x00F4)	NtAssignProcessToJobObject	0x00073480
	260 (0x0104)	245 (0x00F5)	NtAssociateWaitCompletionPacket	0x00073490
	261 (0x0105)	246 (0x00F6)	NtCallEnclave	0x000734A0
	262 (0x0106)	247 (0x00F7)	NtCallbackReturn	0x00072BC0
	263 (0x0107)	248 (0x00F8)	NtCancelIoFile	0x00073160