

Operációs rendszerek Bsc

3. gyakorlat (A)

2021. 02. 24.

Készítette:

Molnár Balázs Bsc

programtervező informatikus

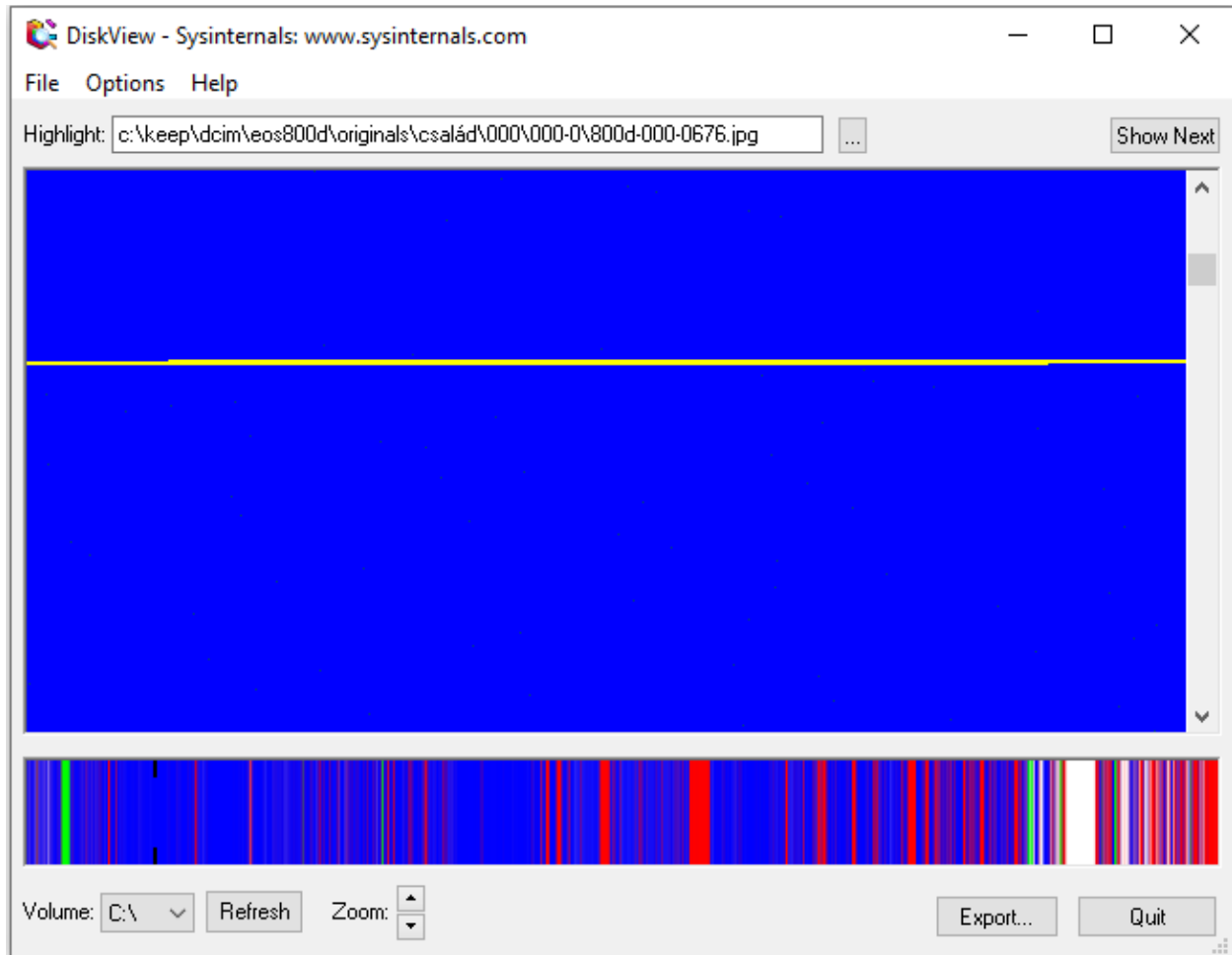
KFIXBJ

Miskolc, 2021

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.

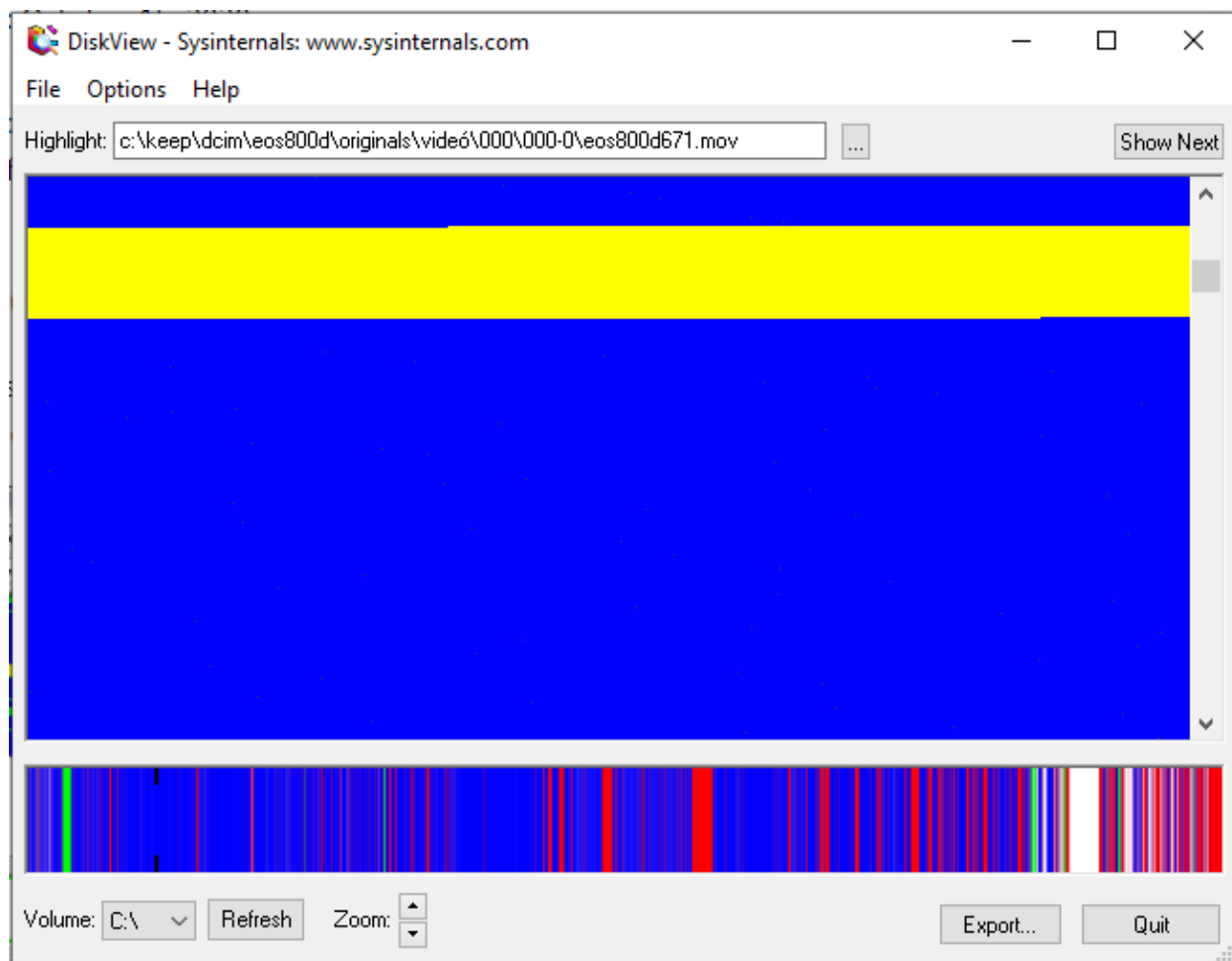
1 File and Disk Utilities

1.1 DiskView (külső segédprogram)



A segédprogramban a lemezünk egyes partícióin foglalt területeket vizsgálhatjuk.


A fenti képen egy fénykép fájl látható, a program kiírja az elérési útvonalat is.



A lemezen a fényképeket tartalmazó mappa több fájlja is egymás után helyezkedik el, így találtam egy videófelvételt, amely láthatóan több helyet foglal a lemezen, ami logikus.

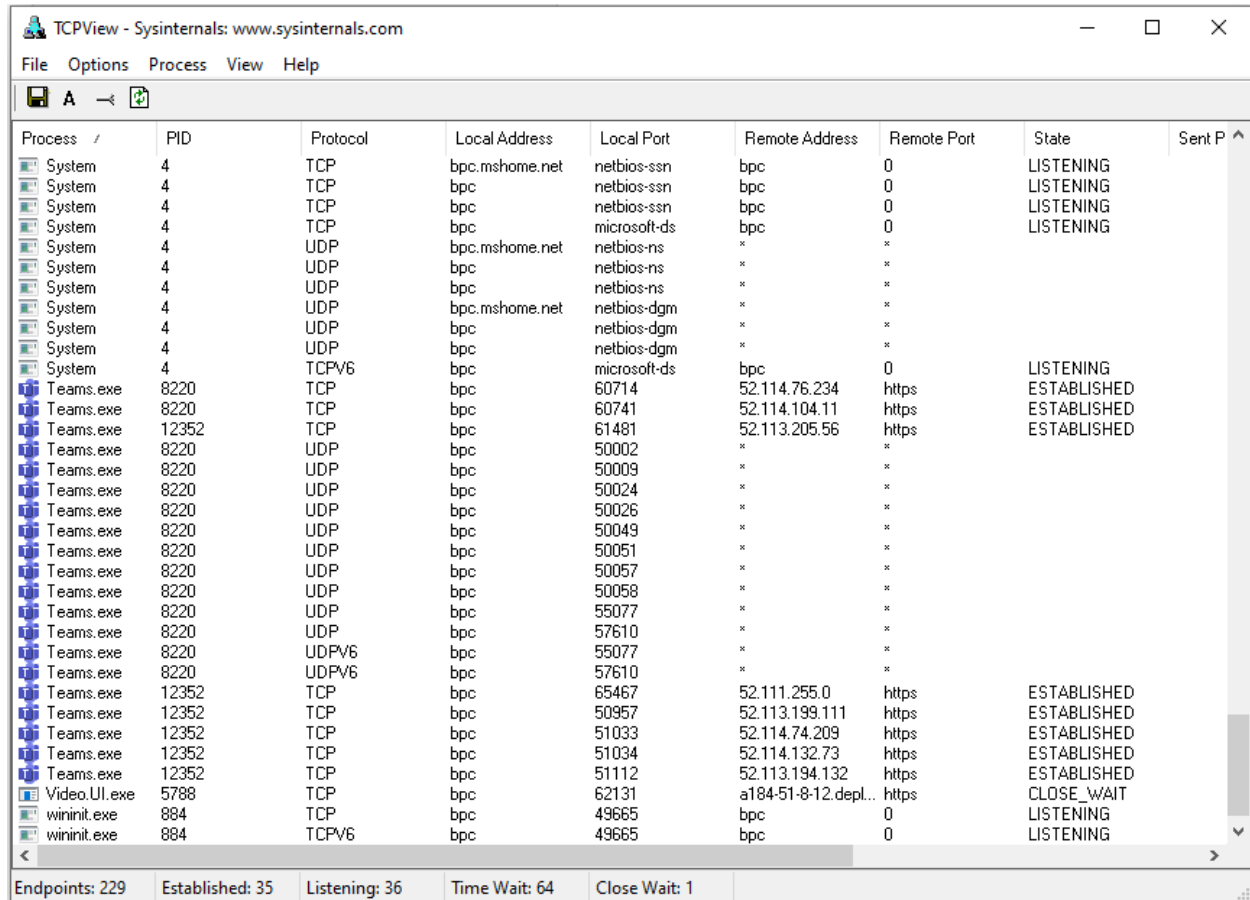
Belső segédprogramokkal ilyen részletességgel nem vizsgálható a lemezünkön a fájlok elhelyezkedése, a fájlkezelő csak elérési útjuk szerint jeleníti meg a fájlokat.

A következő két program belső segédprogram, azonban a lemez karbantartásával foglalkoznak, részletes információkat nem kapunk a fájlokról.

 Defragment and Optimize Drives	12/7/2019 10:09 AM	Shortcut	2 KB
 Disk Cleanup	12/7/2019 10:09 AM	Shortcut	2 KB

2 Networking Utilities

2.1 TCPView (külső segédprogram)



The screenshot shows the TCPView application window with the following data:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent P
System	4	TCP	bpc.mshome.net	netbios-ssn	bpc	0	LISTENING	
System	4	TCP	bpc	netbios-ssn	bpc	0	LISTENING	
System	4	TCP	bpc	netbios-ssn	bpc	0	LISTENING	
System	4	TCP	bpc	microsoft-ds	bpc	0	LISTENING	
System	4	UDP	bpc.mshome.net	netbios-ns	*	*		
System	4	UDP	bpc	netbios-ns	*	*		
System	4	UDP	bpc	netbios-ns	*	*		
System	4	UDP	bpc.mshome.net	netbios-dgm	*	*		
System	4	UDP	bpc	netbios-dgm	*	*		
System	4	UDP	bpc	netbios-dgm	*	*		
System	4	TCPV6	bpc	microsoft-ds	bpc	0	LISTENING	
Teams.exe	8220	TCP	bpc	60714	52.114.76.234	https	ESTABLISHED	
Teams.exe	8220	TCP	bpc	60741	52.114.104.11	https	ESTABLISHED	
Teams.exe	12352	TCP	bpc	61481	52.113.205.56	https	ESTABLISHED	
Teams.exe	8220	UDP	bpc	50002	*	*		
Teams.exe	8220	UDP	bpc	50009	*	*		
Teams.exe	8220	UDP	bpc	50024	*	*		
Teams.exe	8220	UDP	bpc	50026	*	*		
Teams.exe	8220	UDP	bpc	50049	*	*		
Teams.exe	8220	UDP	bpc	50051	*	*		
Teams.exe	8220	UDP	bpc	50057	*	*		
Teams.exe	8220	UDP	bpc	50058	*	*		
Teams.exe	8220	UDP	bpc	55077	*	*		
Teams.exe	8220	UDP	bpc	57610	*	*		
Teams.exe	8220	UDPV6	bpc	55077	*	*		
Teams.exe	8220	UDPV6	bpc	57610	*	*		
Teams.exe	12352	TCP	bpc	65467	52.111.255.0	https	ESTABLISHED	
Teams.exe	12352	TCP	bpc	50957	52.113.199.111	https	ESTABLISHED	
Teams.exe	12352	TCP	bpc	51033	52.114.74.209	https	ESTABLISHED	
Teams.exe	12352	TCP	bpc	51034	52.114.132.73	https	ESTABLISHED	
Teams.exe	12352	TCP	bpc	51112	52.113.194.132	https	ESTABLISHED	
Video.UI.exe	5788	TCP	bpc	62131	a184-51-8-12.depl...	https	CLOSE_WAIT	
wininit.exe	884	TCP	bpc	49665	bpc	0	LISTENING	
wininit.exe	884	TCPV6	bpc	49665	bpc	0	LISTENING	

Summary statistics at the bottom:

Endpoints: 229	Established: 35	Listening: 36	Time Wait: 64	Close Wait: 1
----------------	-----------------	---------------	---------------	---------------

A TCPView programban a Gyakorlat Teams hívásának kapcsolatait kerestem ki, láthatóak TCP és UDP kapcsolatok is.

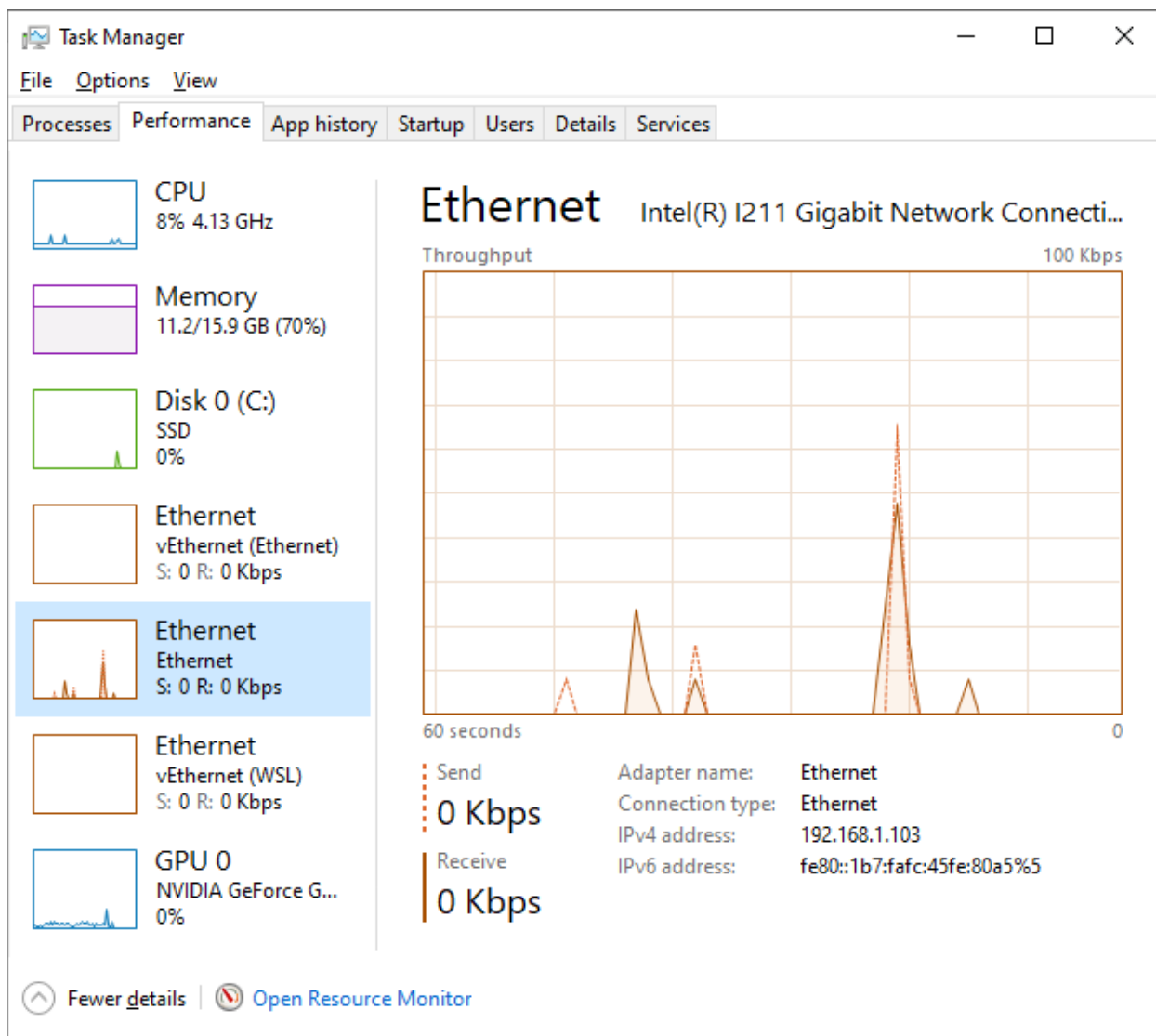
A TCP kapcsolatok általában a szöveges állományok, dokumentumok küldéséért felelősek.

Az UDP kapcsolatokon keresztül valószínűleg a hívás hang és videó stream-jei kapcsolódnak.

Egyéb hálózati kapcsolatokat elemző programra példa a Wireshark.

2.2 Task Manager (belső segédprogram)

A hálózatot a Task Managerből is vizsgálhatjuk, de itt csak összesített használatot látunk, az egyes kapcsolatokat nem tudjuk megvizsgálni.

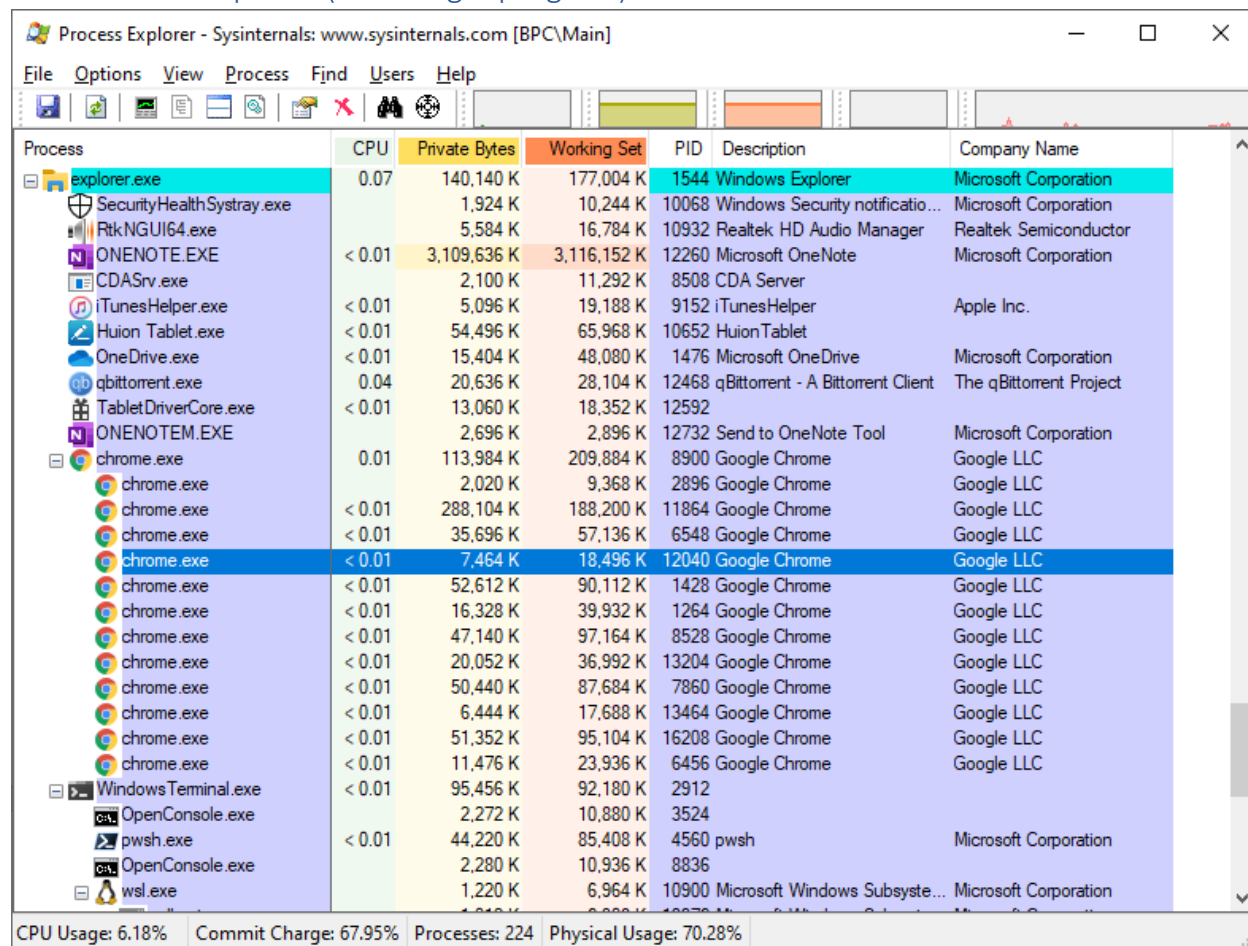


Illetve az egyes alkalmazások hálózathasználatát is követketjük, szintén összesítve, Mbps-ban.

Name	Status	10% CPU	70% Memory	0% Disk	0% Network
Apps (12)					
> Autostart program viewer (32 bit)		0%	26.6 MB	0 MB/s	0 Mbps
> Google Chrome (13)		0%	438.8 MB	0 MB/s	0.1 Mbps
> Microsoft OneNote		0%	2,936.7 MB	0 MB/s	0 Mbps
> Microsoft Teams (7)		0%	1,036.5 MB	0 MB/s	0 Mbps
> Microsoft Word		0.2%	96.9 MB	0 MB/s	0 Mbps
> Sysinternals Diskview		0%	970.5 MB	0 MB/s	0 Mbps

3 Process Utilities

3.1 Process Explorer (külső segédprogram)



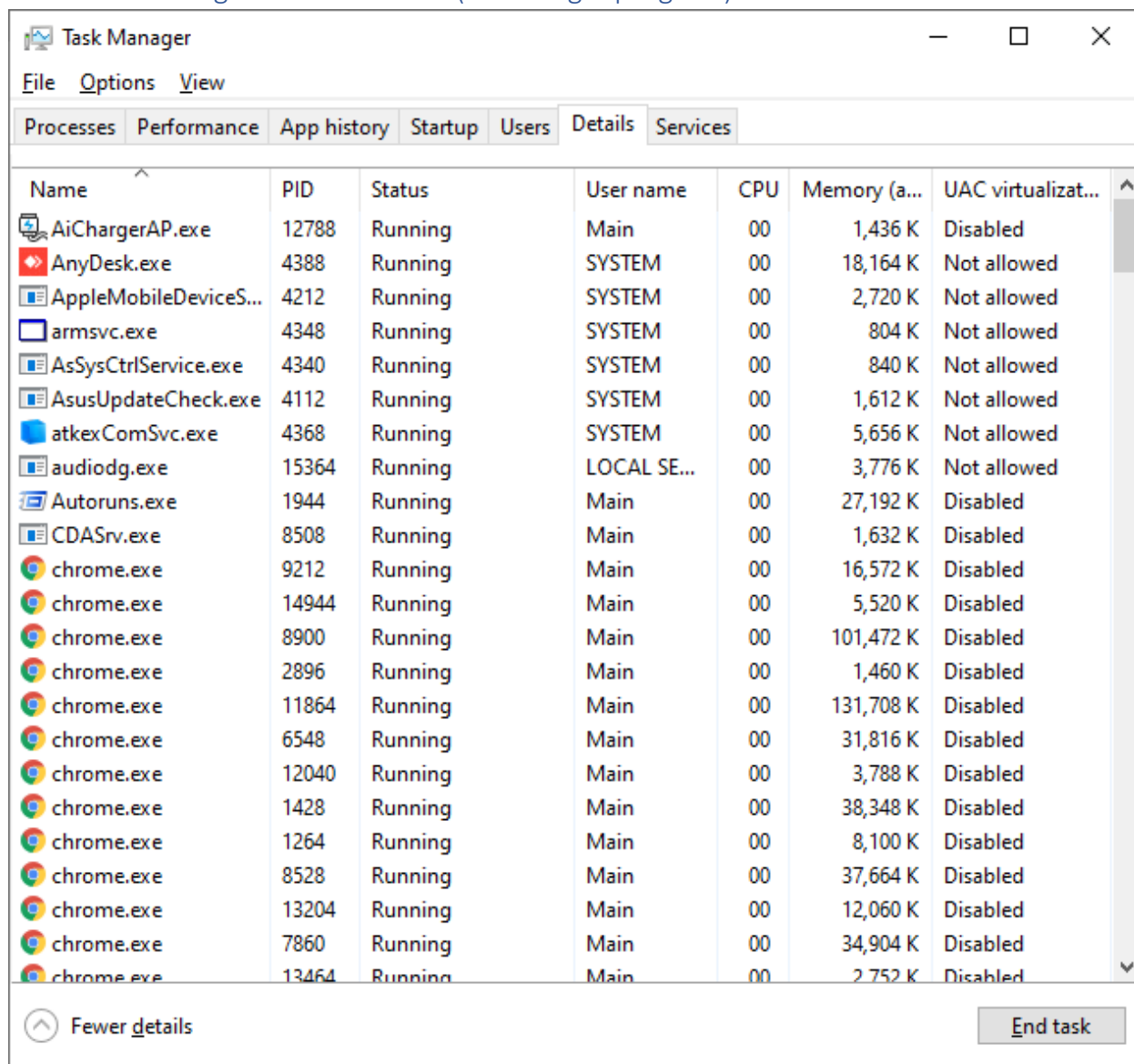
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
explorer.exe	0.07	140,140 K	177,004 K	1544	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,924 K	10,244 K	10068	Windows Security notificatio...	Microsoft Corporation
RtkNGUI64.exe		5,584 K	16,784 K	10932	Realtek HD Audio Manager	Realtek Semiconductor
ONENOTE.EXE	< 0.01	3,109,636 K	3,116,152 K	12260	Microsoft OneNote	Microsoft Corporation
CDASrv.exe		2,100 K	11,292 K	8508	CDA Server	
iTunesHelper.exe	< 0.01	5,096 K	19,188 K	9152	iTunesHelper	Apple Inc.
Huion Tablet.exe	< 0.01	54,496 K	65,968 K	10652	HuionTablet	
OneDrive.exe	< 0.01	15,404 K	48,080 K	1476	Microsoft OneDrive	Microsoft Corporation
qbittorrent.exe	0.04	20,636 K	28,104 K	12468	qBittorrent - A Bittorrent Client	The qBittorrent Project
TabletDriverCore.exe	< 0.01	13,060 K	18,352 K	12592		
ONENOTEM.EXE		2,696 K	2,896 K	12732	Send to OneNote Tool	Microsoft Corporation
chrome.exe	0.01	113,984 K	209,884 K	8900	Google Chrome	Google LLC
chrome.exe		2,020 K	9,368 K	2896	Google Chrome	Google LLC
chrome.exe	< 0.01	288,104 K	188,200 K	11864	Google Chrome	Google LLC
chrome.exe	< 0.01	35,696 K	57,136 K	6548	Google Chrome	Google LLC
chrome.exe	< 0.01	7,464 K	18,496 K	12040	Google Chrome	Google LLC
chrome.exe	< 0.01	52,612 K	90,112 K	1428	Google Chrome	Google LLC
chrome.exe	< 0.01	16,328 K	39,932 K	1264	Google Chrome	Google LLC
chrome.exe	< 0.01	47,140 K	97,164 K	8528	Google Chrome	Google LLC
chrome.exe	< 0.01	20,052 K	36,992 K	13204	Google Chrome	Google LLC
chrome.exe	< 0.01	50,440 K	87,684 K	7860	Google Chrome	Google LLC
chrome.exe	< 0.01	6,444 K	17,688 K	13464	Google Chrome	Google LLC
chrome.exe	< 0.01	51,352 K	95,104 K	16208	Google Chrome	Google LLC
chrome.exe	< 0.01	11,476 K	23,936 K	6456	Google Chrome	Google LLC
Windows Terminal.exe	< 0.01	95,456 K	92,180 K	2912		
OpenConsole.exe		2,272 K	10,880 K	3524		
pwsh.exe	< 0.01	44,220 K	85,408 K	4560	pwsh	Microsoft Corporation
OpenConsole.exe		2,280 K	10,936 K	8836		
WSL.exe		1,220 K	6,964 K	10900	Microsoft Windows Subsystem...	Microsoft Corporation

CPU Usage: 6.18% Commit Charge: 67.95% Processes: 224 Physical Usage: 70.28%

A segédprogramban a processzek állapotát követhetjük, erőforrás használat szerint, láthatjuk a CPU, memória használatot, a fenti grafikonok mutatják emellett az I/O és GPU használatot.

A jelenleg futó processzek közül a legtöbb memóriát a OneNote használta a képernyőfelvétel készítésekor.

3.2 Task Manager – Details nézet (belső segédprogram)



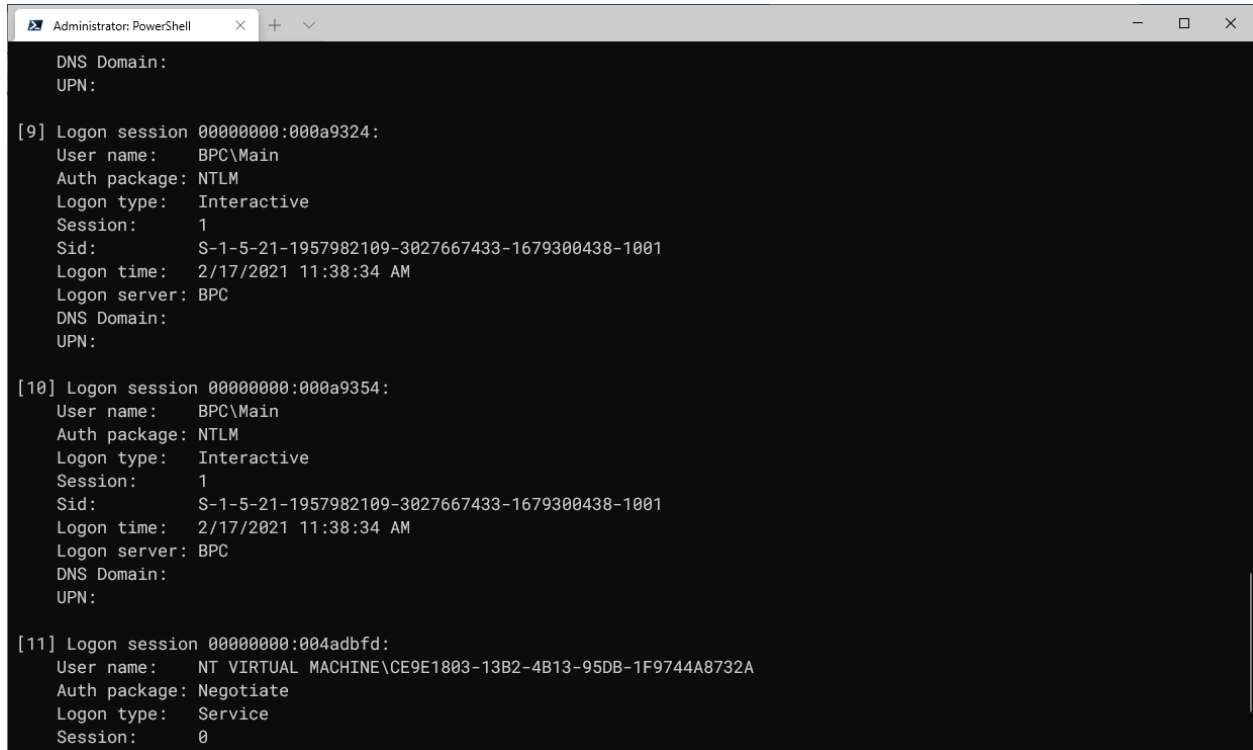
Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
AiChargerAP.exe	12788	Running	Main	00	1,436 K	Disabled
AnyDesk.exe	4388	Running	SYSTEM	00	18,164 K	Not allowed
AppleMobileDeviceS...	4212	Running	SYSTEM	00	2,720 K	Not allowed
armsvc.exe	4348	Running	SYSTEM	00	804 K	Not allowed
AsSysCtrlService.exe	4340	Running	SYSTEM	00	840 K	Not allowed
AsusUpdateCheck.exe	4112	Running	SYSTEM	00	1,612 K	Not allowed
atkexComSvc.exe	4368	Running	SYSTEM	00	5,656 K	Not allowed
audiodg.exe	15364	Running	LOCAL SE...	00	3,776 K	Not allowed
Autoruns.exe	1944	Running	Main	00	27,192 K	Disabled
CDASrv.exe	8508	Running	Main	00	1,632 K	Disabled
chrome.exe	9212	Running	Main	00	16,572 K	Disabled
chrome.exe	14944	Running	Main	00	5,520 K	Disabled
chrome.exe	8900	Running	Main	00	101,472 K	Disabled
chrome.exe	2896	Running	Main	00	1,460 K	Disabled
chrome.exe	11864	Running	Main	00	131,708 K	Disabled
chrome.exe	6548	Running	Main	00	31,816 K	Disabled
chrome.exe	12040	Running	Main	00	3,788 K	Disabled
chrome.exe	1428	Running	Main	00	38,348 K	Disabled
chrome.exe	1264	Running	Main	00	8,100 K	Disabled
chrome.exe	8528	Running	Main	00	37,664 K	Disabled
chrome.exe	13204	Running	Main	00	12,060 K	Disabled
chrome.exe	7860	Running	Main	00	34,904 K	Disabled
chrome.exe	13464	Running	Main	00	2,752 K	Disabled

^ Fewer details End task

A Details nézet hasonló információkat mutat a processzekről, a memória itt nincs Private Bytes és Working Set szerint részletezve, de látjuk a processzt indító felhasználó nevét.

4 Security Utilities

4.1 LogonSessions (külső segédprogram)

A screenshot of a Windows PowerShell window titled "Administrator: PowerShell". The window has a dark background and white text. It displays the output of the "LogonSessions" command, showing three active logon sessions. Each session entry includes details such as the user name, authentication package, logon type, session ID, SID, logon time, logon server, DNS domain, and UPN. The first two sessions are for "BPC\Main" using NTLM authentication, and the third is for "NT VIRTUAL MACHINE\CE9E1803-13B2-4B13-95DB-1F9744A8732A" using Negotiate authentication.

```
Administrator: PowerShell

DNS Domain:
UPN:

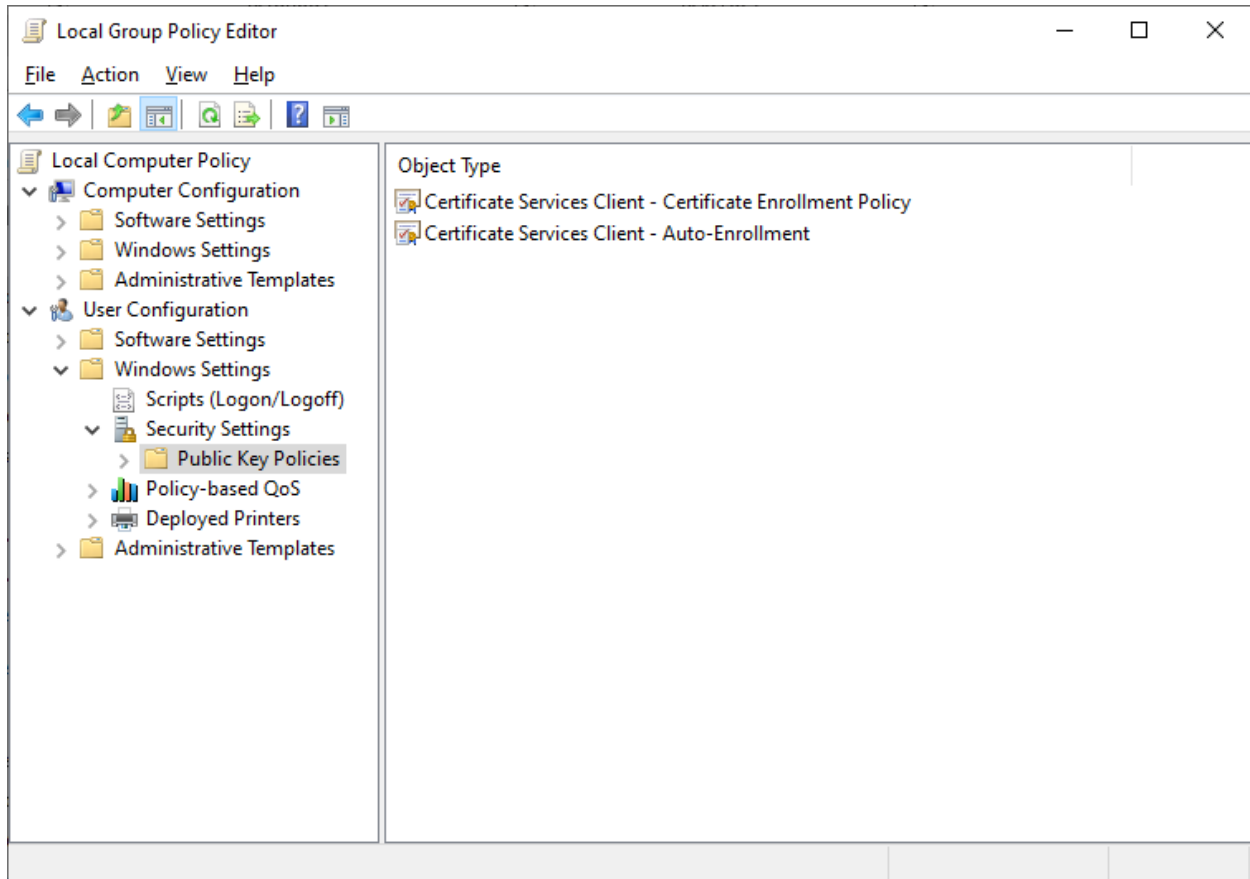
[9] Logon session 00000000:000a9324:
  User name: BPC\Main
  Auth package: NTLM
  Logon type: Interactive
  Session: 1
  Sid: S-1-5-21-1957982109-3027667433-1679300438-1001
  Logon time: 2/17/2021 11:38:34 AM
  Logon server: BPC
  DNS Domain:
  UPN:

[10] Logon session 00000000:000a9354:
  User name: BPC\Main
  Auth package: NTLM
  Logon type: Interactive
  Session: 1
  Sid: S-1-5-21-1957982109-3027667433-1679300438-1001
  Logon time: 2/17/2021 11:38:34 AM
  Logon server: BPC
  DNS Domain:
  UPN:

[11] Logon session 00000000:004adbfd:
  User name: NT VIRTUAL MACHINE\CE9E1803-13B2-4B13-95DB-1F9744A8732A
  Auth package: Negotiate
  Logon type: Service
  Session: 0
```

A LogonSessions-ben a beléptetett személyeket/entitásokat látjuk, melyekből meglepően sok van. Nem csak az aktuálisan használt felhasználói fiók van beléptetve, és az aktuális felhasználónak több logon session-je is van (a képen a [9]-es és a [10]-es).

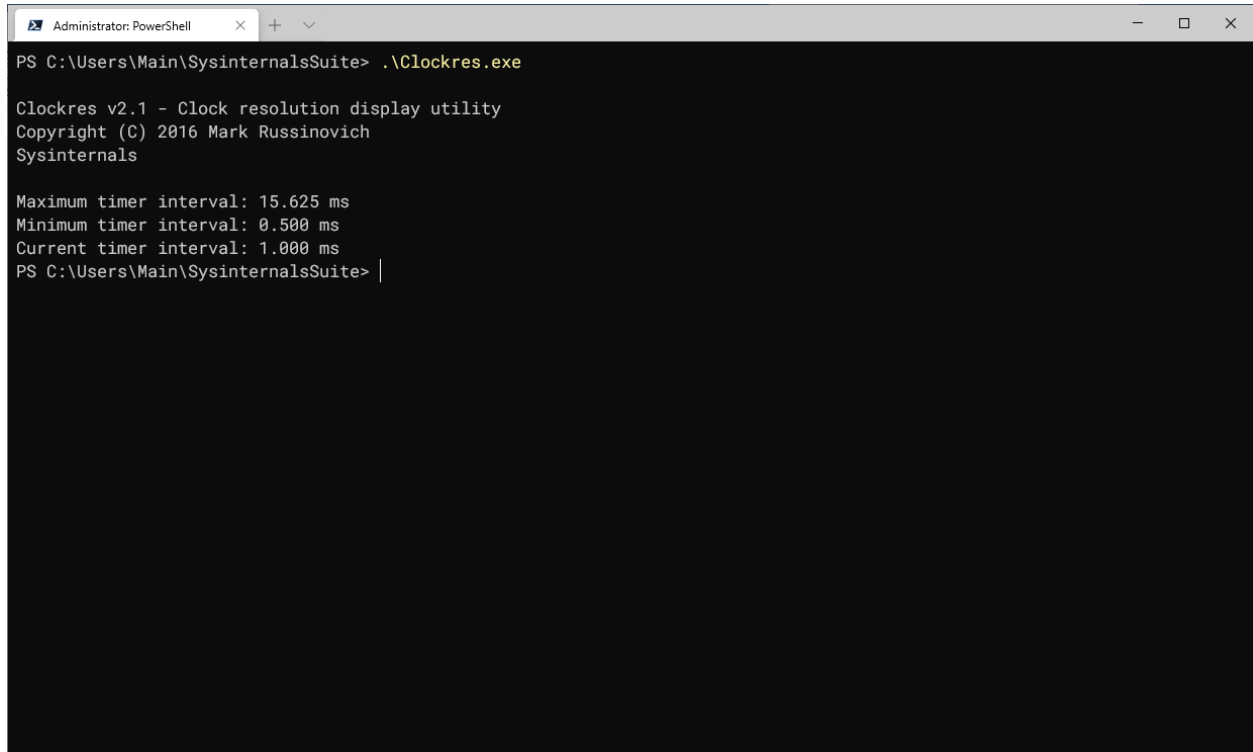
4.2 Local Group Policy Editor (belső segédprogram)



A Group Policy Editor-ben a felhasználók és a számítógép (biztonsági) beállításait kezelhetjük, engedélyezhetünk, letilthatunk, konfigurálhatunk funkciókat.

5 System Utilities

5.1 ClockRes (külső segédprogram)

A screenshot of a Windows PowerShell window titled "Administrator: PowerShell". The window has a dark background and a light gray title bar. The command prompt shows the execution of the command ".\Clockres.exe" in the directory "C:\Users\Main\SysinternalsSuite". The output of the command is displayed in white text. The output includes the version "v2.1", the description "Clock resolution display utility", the copyright "Copyright (C) 2016 Mark Russinovich", and the organization "Sysinternals". It also shows three timer intervals: "Maximum timer interval: 15.625 ms", "Minimum timer interval: 0.500 ms", and "Current timer interval: 1.000 ms". The prompt returns to "PS C:\Users\Main\SysinternalsSuite>".

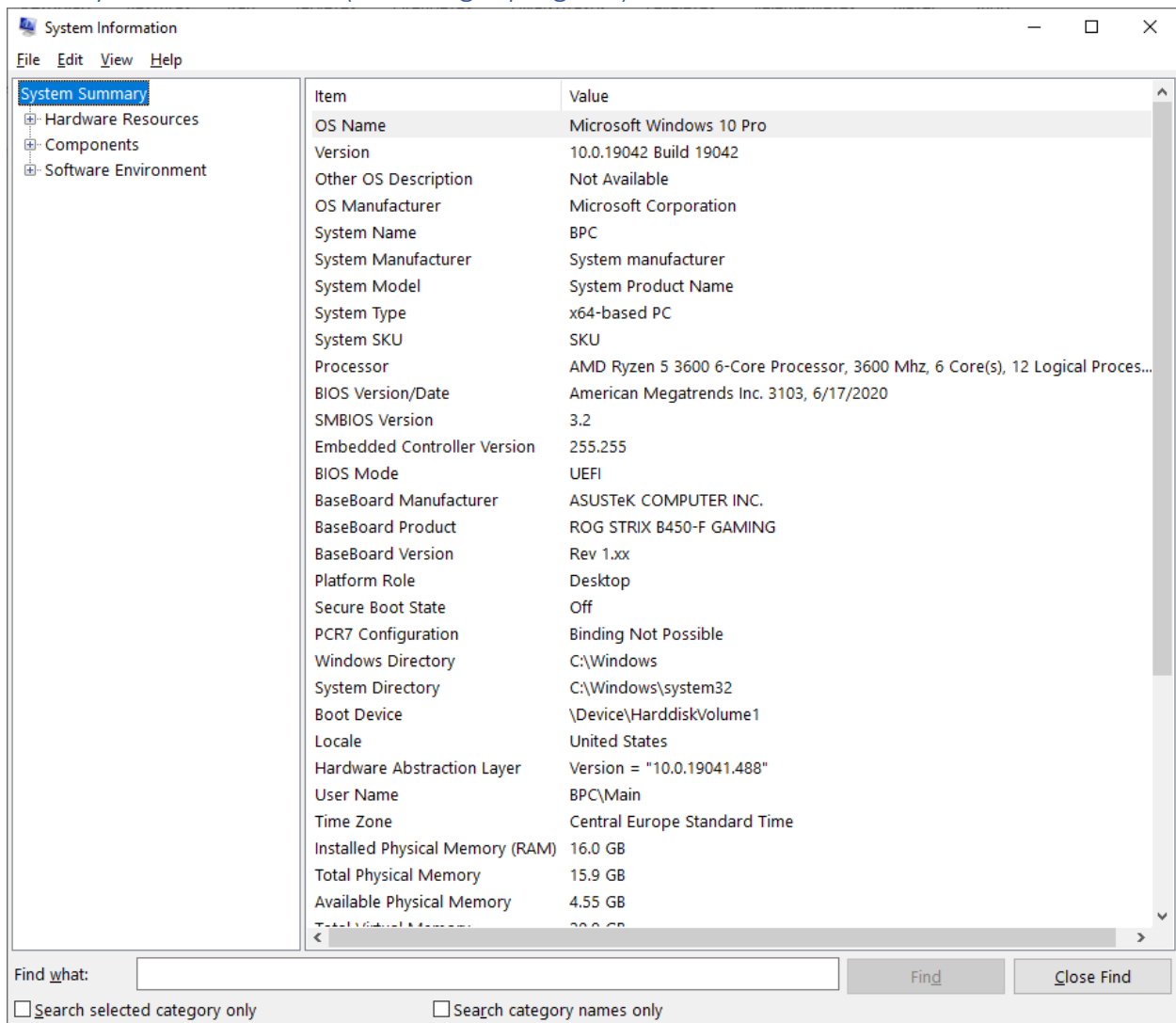
```
PS C:\Users\Main\SysinternalsSuite> .\Clockres.exe

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
PS C:\Users\Main\SysinternalsSuite> |
```

A ClockRes segédprogram segítségével lekérhetjük a rendszeróránk felbontását. Erre akkor lehet például szükségünk, ha pontosan szeretnénk mérni egy algoritmus végrehajtási idejét, ekkor a programunk maximum ekkora felbontással mérhet.

5.2 System Information (belső segédprogram)



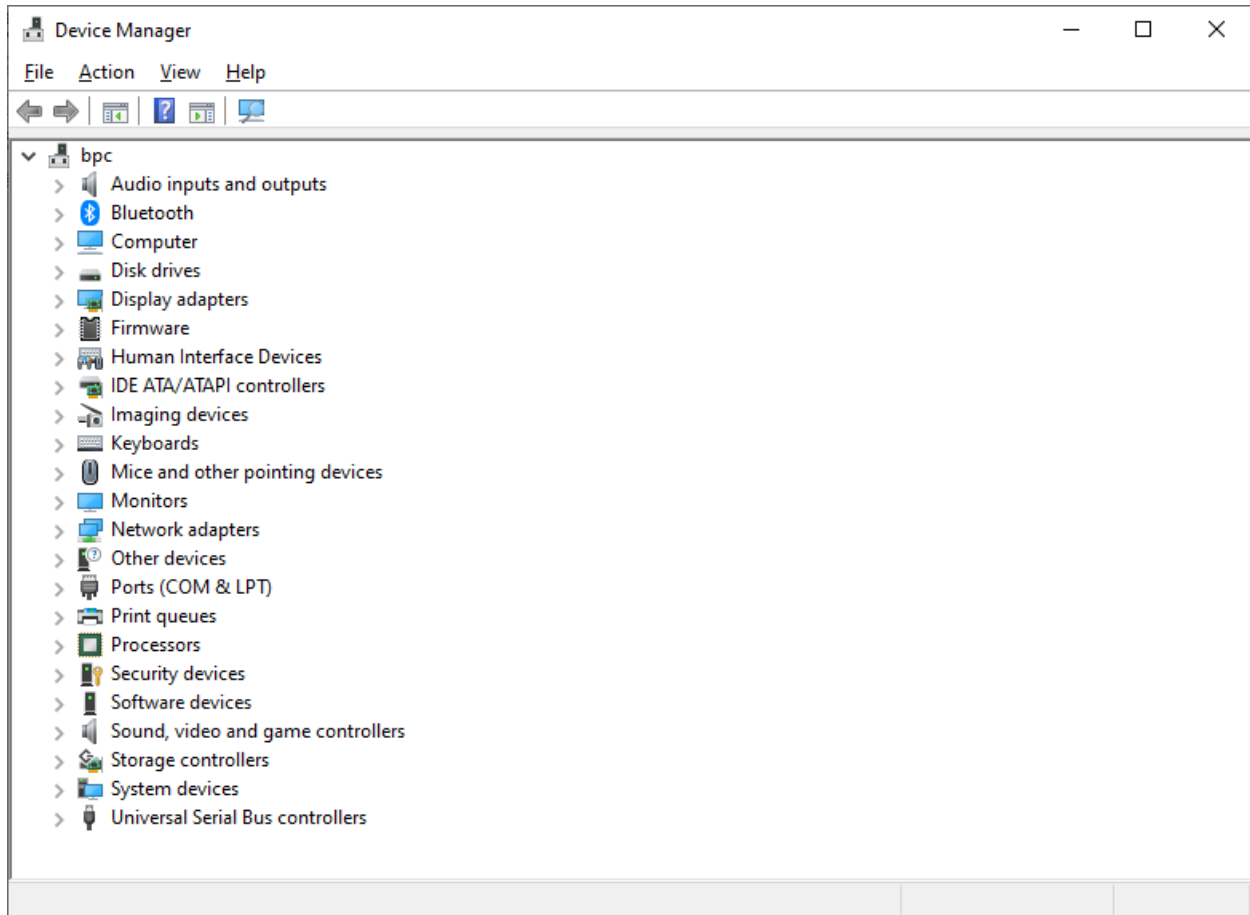
The screenshot shows the Windows System Information application. The left sidebar has a tree view with 'System Summary' selected, and other categories like 'Hardware Resources', 'Components', and 'Software Environment'. The main area displays a table of system information.

Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.19042 Build 19042
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	BPC
System Manufacturer	System manufacturer
System Model	System Product Name
System Type	x64-based PC
System SKU	SKU
Processor	AMD Ryzen 5 3600 6-Core Processor, 3600 Mhz, 6 Core(s), 12 Logical Proces...
BIOS Version/Date	American Megatrends Inc. 3103, 6/17/2020
SMBIOS Version	3.2
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	ASUSTeK COMPUTER INC.
BaseBoard Product	ROG STRIX B450-F GAMING
BaseBoard Version	Rev 1.xx
Platform Role	Desktop
Secure Boot State	Off
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.19041.488"
User Name	BPC\Main
Time Zone	Central Europe Standard Time
Installed Physical Memory (RAM)	16.0 GB
Total Physical Memory	15.9 GB
Available Physical Memory	4.55 GB
Total Virtual Memory	32.0 GB

At the bottom, there is a search bar labeled 'Find what:' with a 'Find' button and a 'Close Find' button. Below the search bar are two checkboxes: 'Search selected category only' and 'Search category names only'.

A System Information programmal a rendszerünk alapadatait tekinthetjük meg.

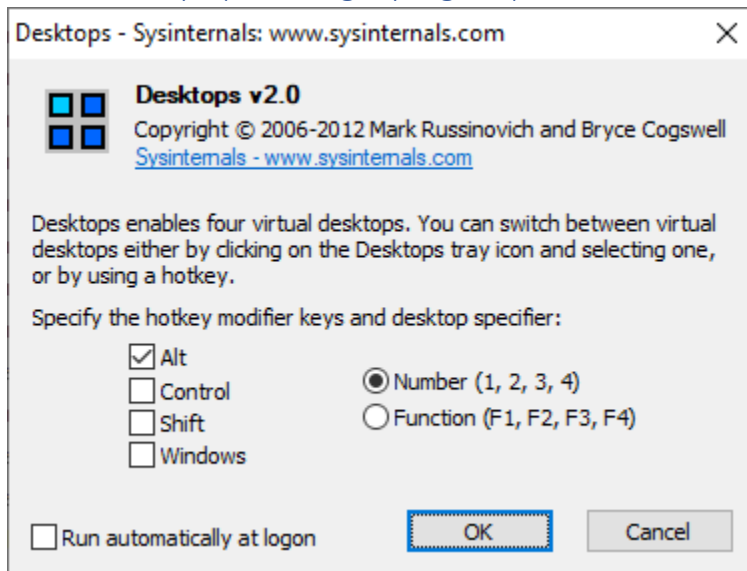
5.3 Device Manager (belső segédprogram)



A Device Manager megjeleníti a gépünkben található hardware eszközöket, ezek tulajdonságait, lehetőséget ad az illesztőprogram ellenőrzésére, frissítésére.

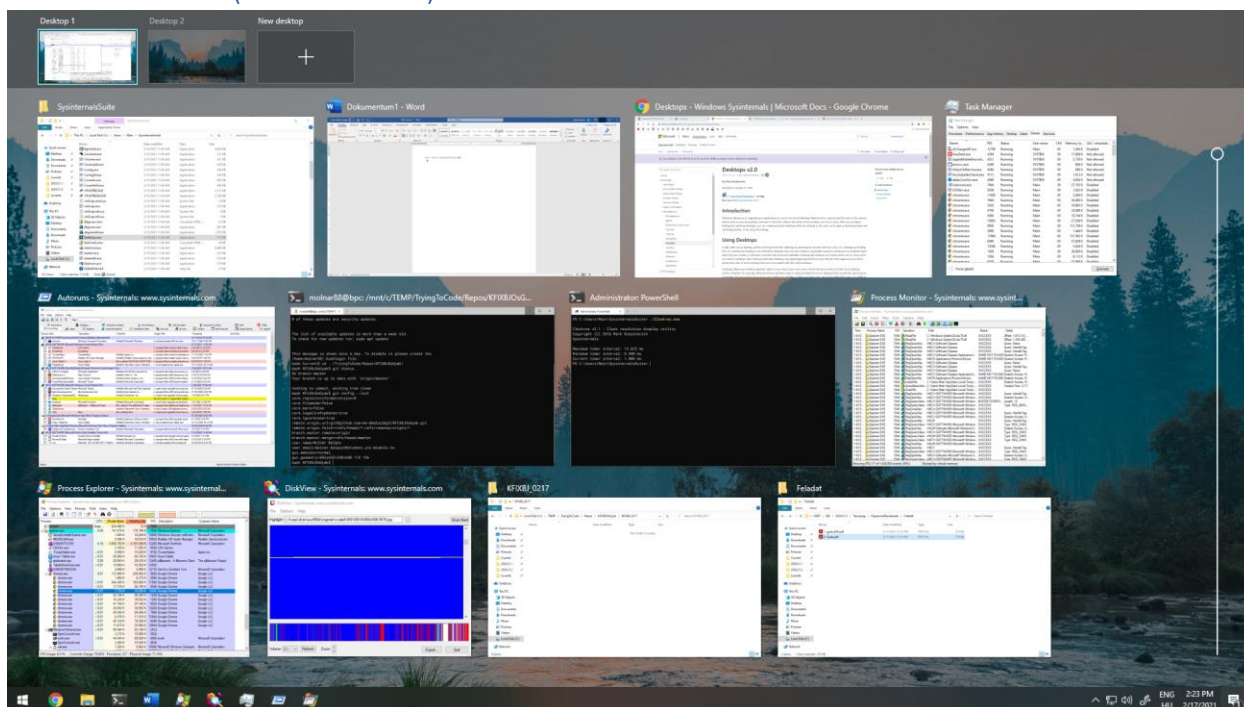
6 Egyéb segédprogramok

6.1 Desktops (külső segédprogram)



A Desktops virtuális asztalok létrehozását teszi lehetővé, ez manapság a Desktop OS-ekben alapértelmezetten megtalálható. Beleértve a Windowst is (Win 10-től kezdve).

6.2 Win + Tab (belső funkció)



A Windows-ban a Win + Tab billentyűkombináció segítségével virtuális asztalokat hozhatunk létre, ill. nyitott ablakokat vihetünk egyik asztalról a másikra.

4. feladat - A Dependency Walker segítségével végezze el a következő feladatokat.

Nyissa meg a neptunkod.exe fájlt!

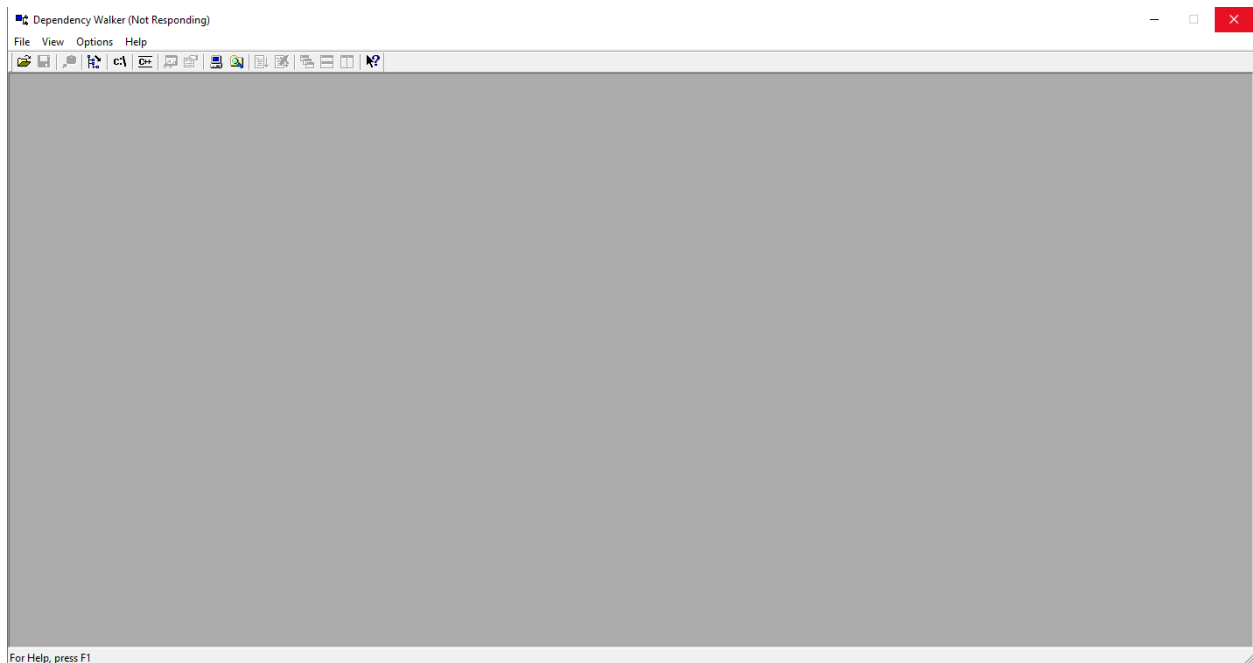
a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!

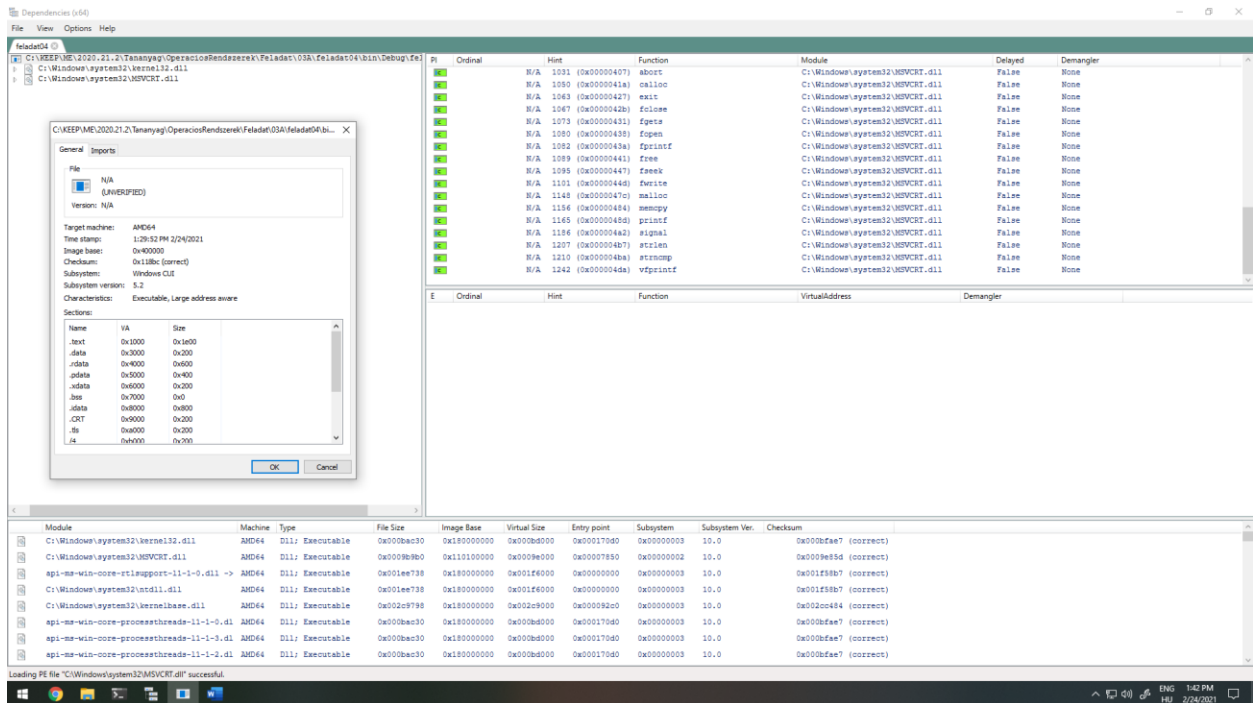
b.) Milyen függőségei vannak a kernel32.dll-nek!

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

Forrásfájl: KFIXBJ.c

A Dependency Walker segítségével nem sikerült elemeznem a KFIXBJ.exe fájlt, mivel többszöri próbálkozás után is leáll a program, mikor megpróbálom megnyitni a .exe fájlt.





Mivel a Dependency Walker nem működött, letöltöttem egy alternatív Dependencies programot (<https://github.com/lucasg/Dependencies>), melyben a fenti eredményt kaptam. A függőségek között a kernel32.dll és az MSVCRT.dll szerepel.

a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!

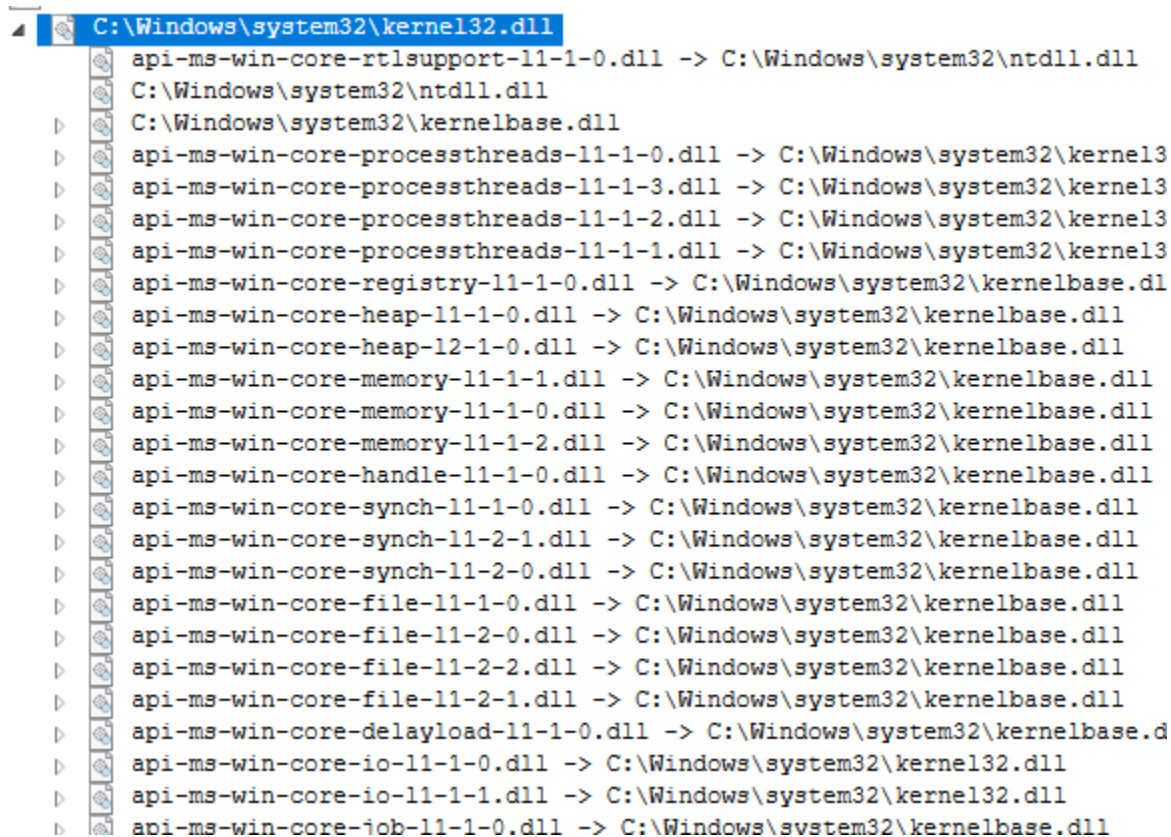
PI	Ordinal	Hint	Function	Module	Delayed	Demangler
		N/A	269 (0x0000010d) DeleteCriticalSection	C:\Windows\system32\kernel32.dll	False	None
		N/A	305 (0x00000131) EnterCriticalSection	C:\Windows\system32\kernel32.dll	False	None
		N/A	536 (0x00000218) GetCurrentProcess	C:\Windows\system32\kernel32.dll	False	None
		N/A	537 (0x00000219) GetCurrentProcessId	C:\Windows\system32\kernel32.dll	False	None
		N/A	541 (0x0000021d) GetCurrentThreadId	C:\Windows\system32\kernel32.dll	False	None
		N/A	610 (0x00000262) GetLastError	C:\Windows\system32\kernel32.dll	False	None
		N/A	722 (0x000002d2) GetStartupInfoA	C:\Windows\system32\kernel32.dll	False	None
		N/A	747 (0x000002eb) GetSystemTimeAsFileTime	C:\Windows\system32\kernel32.dll	False	None
		N/A	775 (0x00000307) GetTickCount	C:\Windows\system32\kernel32.dll	False	None
		N/A	864 (0x00000360) InitializeCriticalSection	C:\Windows\system32\kernel32.dll	False	None
		N/A	952 (0x000003b8) LeaveCriticalSection	C:\Windows\system32\kernel32.dll	False	None
		N/A	1094 (0x00000446) QueryPerformanceCounter	C:\Windows\system32\kernel32.dll	False	None
		N/A	1180 (0x0000049c) RtlAddFunctionTable	C:\Windows\system32\kernel32.dll	False	None
		N/A	1181 (0x0000049d) RtlCaptureContext	C:\Windows\system32\kernel32.dll	False	None
		N/A	1188 (0x000004a4) RtlLookupFunctionEntry	C:\Windows\system32\kernel32.dll	False	None
		N/A	1195 (0x000004ab) RtlVirtualUnwind	C:\Windows\system32\kernel32.dll	False	None
		N/A	1347 (0x00000543) SetUnhandledExceptionFilter	C:\Windows\system32\kernel32.dll	False	None
		N/A	1361 (0x00000551) Sleep	C:\Windows\system32\kernel32.dll	False	None
		N/A	1376 (0x00000560) TerminateProcess	C:\Windows\system32\kernel32.dll	False	None
		N/A	1396 (0x00000574) TlsGetValue	C:\Windows\system32\kernel32.dll	False	None
		N/A	1410 (0x00000582) UnhandledExceptionFilter	C:\Windows\system32\kernel32.dll	False	None
		N/A	1444 (0x000005a4) VirtualProtect	C:\Windows\system32\kernel32.dll	False	None
		N/A	1446 (0x000005a6) VirtualQuery	C:\Windows\system32\kernel32.dll	False	None

A hívások között vannak a processzel kapcsolatosak. A program elindításakor a felhasználó létrehoz egy processzt, a különböző API hívásokban pedig lekérésre kerül a processz objektum és az azonosítója (GetCurrentProcess, GetCurrentProcessId). A program futásának végén a processzt meg kell szüntetni, erre szolgál a TerminateProcess hívás.

A hívások között sokszor szerepel a Critical Section (pl. InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection). A Critical Section a közös erőforrásokhoz (pl. lemez) való hozzáférés kizárólagosságát biztosítja, azaz, hogy egyszerre csak egy processz és (párhuzamos program esetén) annak csak egy szála használhassa az erőforrást.

A Sleep hívás biztosítja, hogy a program tudjon várakozni.

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


















```
C:\Windows\system32\kernel32.dll
api-ms-win-core-rtlsupport-l1-1-0.dll -> C:\Windows\system32\ntdll.dll
C:\Windows\system32\ntdll.dll
C:\Windows\system32\kernelbase.dll
api-ms-win-core-processthreads-l1-1-0.dll -> C:\Windows\system32\kernel32.dll
api-ms-win-core-processthreads-l1-1-3.dll -> C:\Windows\system32\kernel32.dll
api-ms-win-core-processthreads-l1-1-2.dll -> C:\Windows\system32\kernel32.dll
api-ms-win-core-processthreads-l1-1-1.dll -> C:\Windows\system32\kernel32.dll
api-ms-win-core-registry-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-heap-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-heap-l2-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-memory-l1-1-1.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-memory-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-memory-l1-1-2.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-handle-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-synch-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-synch-l1-2-1.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-synch-l1-2-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-file-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-file-l1-2-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-file-l1-2-2.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-file-l1-2-1.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-delayload-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
api-ms-win-core-io-l1-1-0.dll -> C:\Windows\system32\kernel32.dll
api-ms-win-core-io-l1-1-1.dll -> C:\Windows\system32\kernel32.dll
api-ms-win-core-job-l1-1-0.dll -> C:\Windows\system32\kernelbase.dll
```

A kernel32.dll-nek függősége az ntdll.dll, a kernelbase.dll, és különböző Windows Core API-k (pl. memória, fájl- és I/O-kezeléshez).

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 tartalmazza a Windows Native API-t. Ezek a hívások hajtják végre konkrétan a különböző kernel feladatokat, a Win32 API hívások valójában belül ezeket az NT hívásokat használják.

PI	Ordinal	Hint	Function	Module	Delayed	Demangle
		N/A 914 (0x00000392)	RtlDoesFileExists_U	C:\Windows\system32\ntdll.dll	False	None
		N/A 512 (0x00000200)	NtQueryVolumeInformationFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 361 (0x00000169)	NtFsControlFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 416 (0x000001a0)	NtOpenFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 474 (0x000001da)	NtQueryInformationFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 580 (0x00000244)	NtSetInformationFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 278 (0x00000116)	NtCreateFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 572 (0x0000023c)	NtSetEaFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 468 (0x000001d4)	NtQueryEaFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 146 (0x00000092)	LdrQueryImageFileKeyOption	C:\Windows\system32\ntdll.dll	False	None
		N/A 140 (0x0000008c)	LdrOpenImageFileOptionsKey	C:\Windows\system32\ntdll.dll	False	None
		N/A 657 (0x00000291)	NtWriteFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 640 (0x00000280)	NtUnlockFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 519 (0x00000207)	NtReadFile	C:\Windows\system32\ntdll.dll	False	None
		N/A 392 (0x00000188)	NtLockFile	C:\Windows\system32\ntdll.dll	False	None

A Native API-nak sok exportált függvénye van, vannak amelyek fájlkezelésre használhatók (NtCreateFile, NtOpenFile, NtWriteFile, NtReadFile, NtLockFile stb.).

Vannak alapfüggvények is, amelyek számokon (sin, cos, floor) vagy karaktereken (toupper, tolower) dolgoznak.