

# Operációs rendszerek BSc

2. Gyak.

2022. 02. 14.

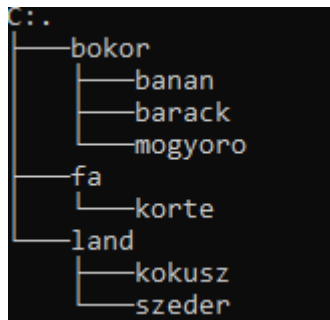
**Készítette:**

Bodnár László BSc  
MérnökInformatikus  
D1H8VP

**Miskolc, 2022**

**1. feladat** — ) Készítse el a következő feladatokat!

**A,** Hozza létre a következő mappa szerkezetet!



B, ) Készítsen másolatot:

```
C:\Users\Bodnár László\D1H8VP\land>xcopy /E szeder fa
Does fa specify a file name
or directory name on the target
(F = file, D = directory)? d
0 File(s) copied
```

```
C:\Users\Bodnár László\D1H8VP\bokor>xcopy /E banan fa
Does fa specify a file name
or directory name on the target
(F = file, D = directory)? d
```

c.) Végezze el a következő áthelyezéseket:

```
C:\Users\Bodnár László\D1H8VP\bokor>move barack fa
1 dir(s) moved.
```

```
C:\Users\Bodnár László\D1H8VP\land>move kokusz fa
1 dir(s) moved.
```

d.) Törölje a neptunkod/land katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:

```
C:\Users\Bodnár László\D1H8VP\bokor\banan>echo A barack egy nagyon finom gyümölcs, szép sárga színe miatt felismerhető m
inden boltban ezért sok család kevéncévé vált > leiras.txt
```

```
C:\Users\Bodnár László\D1H8VP\bokor\banan>
```

```
C:\Users\Bodnár László\D1H8VP>cd fa
```

```
C:\Users\Bodnár László\D1H8VP\fa>echo Bodnár László\n Csicsely Gábor\n > fels.txt
```

```
C:\Users\Bodnár László\D1H8VP\fa>copy con felsorolas.txt
```

```
Bodnar Laszlo
Csicsely Gabor
Danyi Krstof
Hauer Attila
Urban Oliver
```

```
C:\Users\Bodnár László\D1H8VP>rmdir /s land
land, Are you sure (Y/N)? Y
```

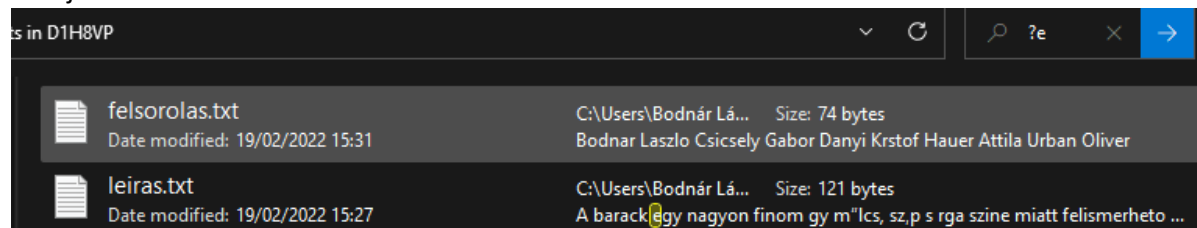
e.) A leiras.txt szöveges állományba írjon 3 sort a barackról. A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét:

Fentebb Látható, egy lépésben csináltam.

f.) Listázza a neptunkod mappa tartalmát úgy, hogy megjelenjen az almappák tartalma is.

```
C:\Users\Bodnár László\D1H8VP>tree
Folder PATH listing
Volume serial number is F22C-C0DE
C:..
|_ bokor
|   |_ banan
|   |_ mogyoro
|_ fa
|   |_ banan
|   |_ barack
|   |_ kokusz
|   |_ korte
|   |_ szeder
C:\Users\Bodnár László\D1H8VP>
```

g.) Térjen vissza a gyökérmappába és keresse meg az összes olyan file-t, amelyek nevének második betűje:

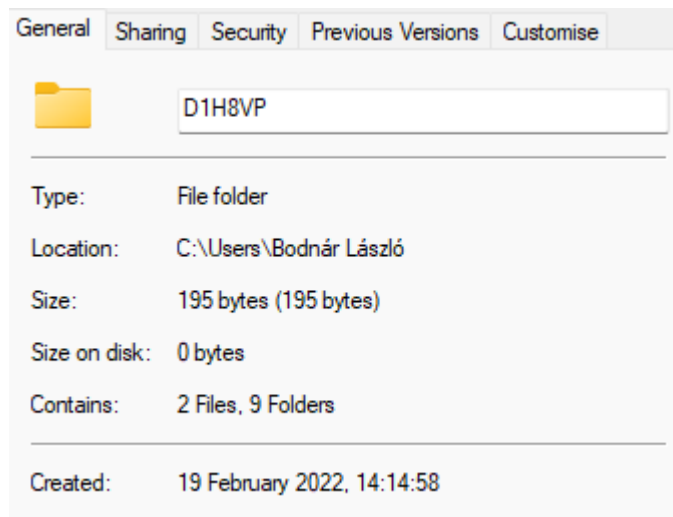


h.) Tegye mindenki számára olvashatóvá a felsorolas.txt file-t:

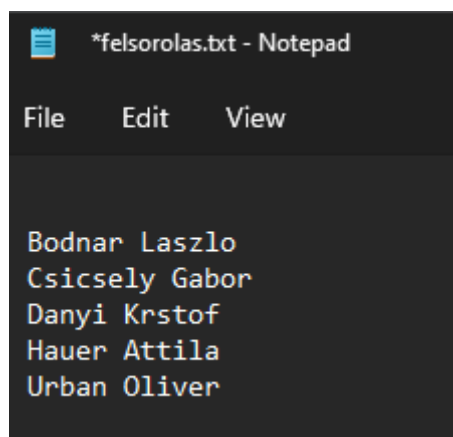
Permission entries:

Type	Principal	Access	Inherited from
Allow	SYSTEM	Full control	C:\Users\Bodnár László\
Allow	Administrators (BODNAR-LASZLO\Adminis...	Full control	C:\Users\Bodnár László\
Allow	Bodnár László (BODNAR-LASZLO\Bodnár L...	Full control	C:\Users\Bodnár László\

i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezén a neptunkod mappa az almappáival együtt



j.) Rendezze ABC-szerint a felsorolas.txt file tartalmát.



**2. feladat** Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.

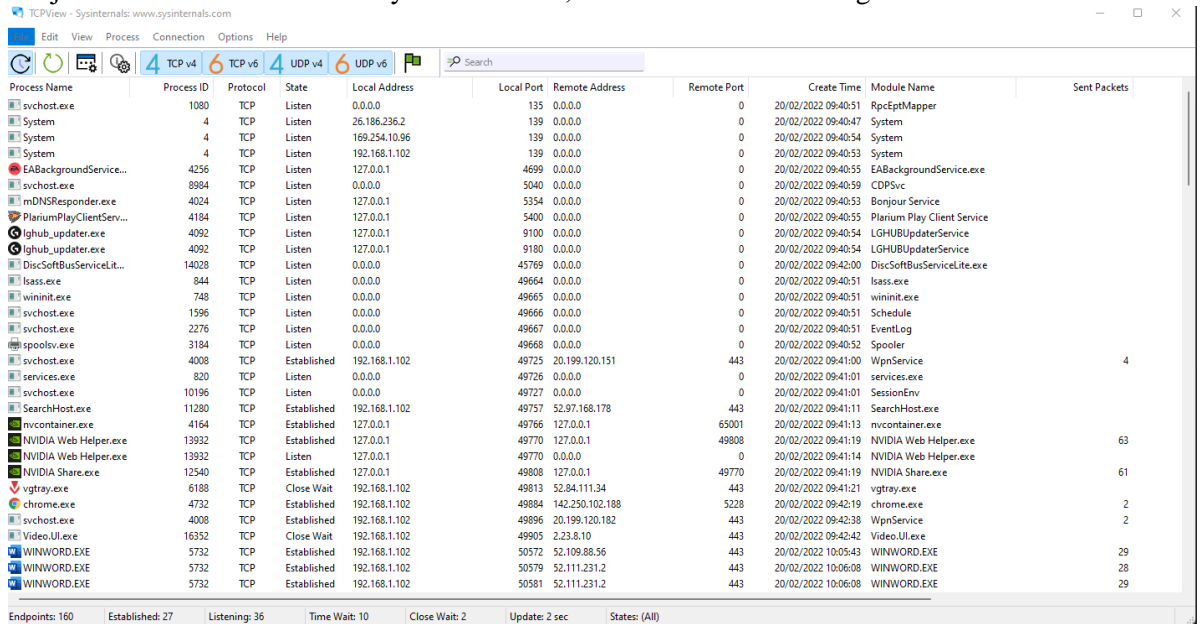
- a) File and Disk Utilities (Disk2vhd): A disk2vhd egy olyan segédprogram, amely létrehotta a fizikai lemezek VHD-verzióit. A Microsoft virtualis gépeken való használatra.



- b) Networking Utilities (TCPView):

A TCPView indítani fogja az összes aktív TCP- és UDP-végpont felsorolását, és feloldja az összes IP-címet a tartománynév-verziójukra. Eszköztárgomb vagy menüelem használatával válthat a feloldott nevek megjelenítésére. A TCPView megjeleníti az egyes végpontok

tulajdonában következő folyamat nevét, beleértve a szolgáltatás nevét is.

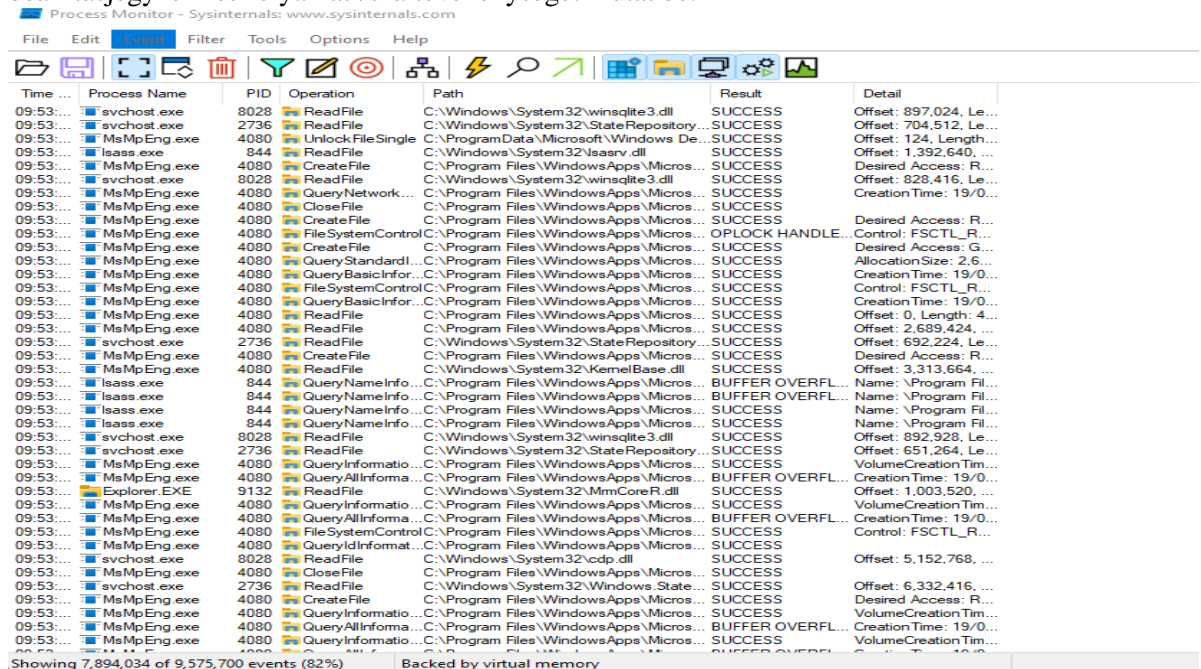


The screenshot shows the TCPView application window. The menu bar includes File, Edit, View, Process, Connection, Options, and Help. The toolbar has icons for refreshing, pausing, and other functions. The main window displays a table of active network connections. The columns are: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, Module Name, and Sent Packets. The table lists various processes such as svchost.exe, System, EABackgroundService..., mDNSResponder.exe, PlariumPlayClientServ..., lghub\_updater.exe, DiscSoftBusServiceLit..., lsass.exe, wininit.exe, services.exe, SearchHost.exe, nvcontainer.exe, NVIDIA Web Helper.exe, NVIDIA Share.exe, vgtay.exe, chrome.exe, Video.UI.exe, WINWORD.EXE, and WINWORD.EXE. The bottom status bar shows: Endpoints: 160, Established: 27, Listening: 36, Time Wait: 10, Close Wait: 2, Update: 2 sec, States: (All).

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	1080	TCP	Listen	0.0.0.0	135	0.0.0.0	0	20/02/2022 09:40:51	RpcCptMapper	
System	4	TCP	Listen	26.186.236.2	139	0.0.0.0	0	20/02/2022 09:40:47	System	
System	4	TCP	Listen	169.254.10.96	139	0.0.0.0	0	20/02/2022 09:40:54	System	
System	4	TCP	Listen	192.168.1.102	139	0.0.0.0	0	20/02/2022 09:40:53	System	
EABackgroundService...	4256	TCP	Listen	127.0.0.1	4699	0.0.0.0	0	20/02/2022 09:40:55	EABackgroundService.exe	
svchost.exe	8984	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	20/02/2022 09:40:59	CDPSvc	
mDNSResponder.exe	4024	TCP	Listen	127.0.0.1	5354	0.0.0.0	0	20/02/2022 09:40:53	Bonjour Service	
PlariumPlayClientServ...	4184	TCP	Listen	127.0.0.1	5400	0.0.0.0	0	20/02/2022 09:40:55	Plarium Play Client Service	
lghub_updater.exe	4092	TCP	Listen	127.0.0.1	9100	0.0.0.0	0	20/02/2022 09:40:54	LGHUBUpdaterService	
lghub_updater.exe	4092	TCP	Listen	127.0.0.1	9180	0.0.0.0	0	20/02/2022 09:40:54	LGHUBUpdaterService	
DiscSoftBusServiceLit...	14028	TCP	Listen	0.0.0.0	45769	0.0.0.0	0	20/02/2022 09:42:00	DiscSoftBusServiceLite.exe	
lsass.exe	844	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	20/02/2022 09:40:51	lsass.exe	
wininit.exe	748	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	20/02/2022 09:40:51	wininit.exe	
services.exe	1596	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	20/02/2022 09:40:51	Schedule	
svchost.exe	2276	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	20/02/2022 09:40:51	EventLog	
spoolsv.exe	3184	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	20/02/2022 09:40:52	Spooler	
svchost.exe	4008	TCP	Established	192.168.1.102	49725	20.199.120.151	443	20/02/2022 09:41:00	WpnService	4
services.exe	820	TCP	Listen	0.0.0.0	49726	0.0.0.0	0	20/02/2022 09:41:01	services.exe	
svchost.exe	10196	TCP	Listen	0.0.0.0	49727	0.0.0.0	0	20/02/2022 09:41:01	SessionEnv	
SearchHost.exe	11280	TCP	Established	192.168.1.102	49757	52.97.168.178	443	20/02/2022 09:41:11	SearchHost.exe	
nvcontainer.exe	4164	TCP	Established	127.0.0.1	49766	127.0.0.1	65001	20/02/2022 09:41:13	nvcontainer.exe	
NVIDIA Web Helper.exe	13932	TCP	Established	127.0.0.1	49770	127.0.0.1	49808	20/02/2022 09:41:19	NVIDIA Web Helper.exe	63
NVIDIA Web Helper.exe	13932	TCP	Listen	127.0.0.1	49770	0.0.0.0	0	20/02/2022 09:41:14	NVIDIA Web Helper.exe	
NVIDIA Share.exe	12540	TCP	Established	127.0.0.1	49808	127.0.0.1	49770	20/02/2022 09:41:19	NVIDIA Share.exe	61
vgtay.exe	6188	TCP	Close Wait	192.168.1.102	49813	52.84.111.34	443	20/02/2022 09:41:21	vgtay.exe	
chrome.exe	4732	TCP	Established	192.168.1.102	49884	142.250.102.188	5228	20/02/2022 09:42:19	chrome.exe	2
svchost.exe	4008	TCP	Established	192.168.1.102	49896	20.199.120.182	443	20/02/2022 09:42:38	WpnService	2
Video.UI.exe	16352	TCP	Close Wait	192.168.1.102	49905	2.23.8.10	443	20/02/2022 09:42:42	Video.UI.exe	
WINWORD.EXE	5732	TCP	Established	192.168.1.102	50572	52.109.88.56	443	20/02/2022 10:05:43	WINWORD.EXE	28
WINWORD.EXE	5732	TCP	Established	192.168.1.102	50579	52.111.231.2	443	20/02/2022 10:06:08	WINWORD.EXE	29
WINWORD.EXE	5732	TCP	Established	192.168.1.102	50581	52.111.231.2	443	20/02/2022 10:06:08	WINWORD.EXE	29

c) Process Utilities (Process Explorer, Process Monitor, AutoRuns):

A Folyamatfigyelő egy fejlett monitorozási eszköz Windows, amely valós idejű fájlrendszer-, beállításjegyzék- és folyamat-/száltevékenységet mutat be.



The screenshot shows the Process Monitor application window. The menu bar includes File, Edit, Events, Filter, Tools, Options, and Help. The toolbar has icons for file operations, filters, and other functions. The main window displays a table of system events. The columns are: Time, Process Name, PID, Operation, Path, Result, and Detail. The table lists various events such as ReadFile, CreateFile, QueryNetwork..., CloseFile, CreateFile, File System Control..., QueryStandard..., QueryBasicInfo..., File System Control..., ReadFile, QueryInfo..., QueryAllInfo..., Explorer.EXE, QueryInfo..., QueryAllInfo..., File System Control..., QueryIdInfo..., ReadFile, CloseFile, ReadFile, CreateFile, QueryInfo..., QueryAllInfo..., and QueryInfo.... The bottom status bar shows: Showing 7,894,034 of 9,575,700 events (82%) and Backed by virtual memory.

Time	Process Name	PID	Operation	Path	Result	Detail
09:53:...	svchost.exe	8028	ReadFile	C:\Windows\System32\winsqlite3.dll	SUCCESS	Offset: 897,024, Le...
09:53:...	svchost.exe	2736	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 704,512, Le...
09:53:...	MsMpEng.exe	4080	Unlock File Single	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124, Lengh...
09:53:...	lsass.exe	844	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1,392,640, ...
09:53:...	MsMpEng.exe	4080	CreateFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Desired Access: R...
09:53:...	svchost.exe	8028	ReadFile	C:\Windows\System32\winsqlite3.dll	SUCCESS	Offset: 828,416, Le...
09:53:...	MsMpEng.exe	4080	QueryNetwork...	C:\Program Files\WindowsApps\Micros...	SUCCESS	Creation Time: 19/0...
09:53:...	MsMpEng.exe	4080	CloseFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	
09:53:...	MsMpEng.exe	4080	CreateFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	
09:53:...	MsMpEng.exe	4080	File System Control	C:\Program Files\WindowsApps\Micros...	OPLOCK HANDLE...	Control: FSCTL_R...
09:53:...	MsMpEng.exe	4080	CreateFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Desired Access: G...
09:53:...	MsMpEng.exe	4080	QueryStandard...	C:\Program Files\WindowsApps\Micros...	SUCCESS	Allocation Size: 2.6...
09:53:...	MsMpEng.exe	4080	QueryBasicInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	Creation Time: 19/0...
09:53:...	MsMpEng.exe	4080	File System Control	C:\Program Files\WindowsApps\Micros...	SUCCESS	Control: FSCTL_R...
09:53:...	MsMpEng.exe	4080	QueryBasicInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	Creation Time: 19/0...
09:53:...	MsMpEng.exe	4080	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 0, Length: 4...
09:53:...	MsMpEng.exe	4080	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,689,424, ...
09:53:...	svchost.exe	2736	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 692,224, Le...
09:53:...	MsMpEng.exe	4080	CreateFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Desired Access: R...
09:53:...	MsMpEng.exe	4080	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,313,664, ...
09:53:...	lsass.exe	844	QueryNameInfo...	C:\Program Files\WindowsApps\Micros...	BUFFER OVERFL...	Name: \Program Fil...
09:53:...	lsass.exe	844	QueryNameInfo...	C:\Program Files\WindowsApps\Micros...	BUFFER OVERFL...	Name: \Program Fil...
09:53:...	lsass.exe	844	QueryNameInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	Name: \Program Fil...
09:53:...	svchost.exe	8028	ReadFile	C:\Windows\System32\winsqlite3.dll	SUCCESS	Offset: 892,928, Le...
09:53:...	svchost.exe	2736	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 651,264, Le...
09:53:...	MsMpEng.exe	4080	QueryInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	VolumeCreationTim...
09:53:...	MsMpEng.exe	4080	QueryAllInfo...	C:\Program Files\WindowsApps\Micros...	BUFFER OVERFL...	Creation Time: 19/0...
09:53:...	Explorer.EXE	9132	ReadFile	C:\Windows\System32\MmCoreR.dll	SUCCESS	Offset: 1,003,520, ...
09:53:...	MsMpEng.exe	4080	QueryInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	VolumeCreationTim...
09:53:...	MsMpEng.exe	4080	QueryAllInfo...	C:\Program Files\WindowsApps\Micros...	BUFFER OVERFL...	Creation Time: 19/0...
09:53:...	svchost.exe	4080	File System Control	C:\Program Files\WindowsApps\Micros...	SUCCESS	Control: FSCTL_R...
09:53:...	svchost.exe	4080	QueryIdInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	
09:53:...	svchost.exe	8028	ReadFile	C:\Windows\System32\cdp.dll	SUCCESS	Offset: 5,152,768, ...
09:53:...	MsMpEng.exe	4080	CloseFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	
09:53:...	svchost.exe	2736	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6,332,416, ...
09:53:...	MsMpEng.exe	4080	CreateFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Desired Access: R...
09:53:...	MsMpEng.exe	4080	QueryInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	VolumeCreationTim...
09:53:...	MsMpEng.exe	4080	QueryAllInfo...	C:\Program Files\WindowsApps\Micros...	BUFFER OVERFL...	Creation Time: 19/0...
09:53:...	MsMpEng.exe	4080	QueryInfo...	C:\Program Files\WindowsApps\Micros...	SUCCESS	VolumeCreationTim...

d) Security Utilities (LogonSession):

Felsorolja a jelenleg aktív bejelentkezési munkameneteket, és ha megadja a -p beállítást, az egyes munkamenetekben futó folyamatokat.

```

C:\WINDOWS\system32>logonsessions -p

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

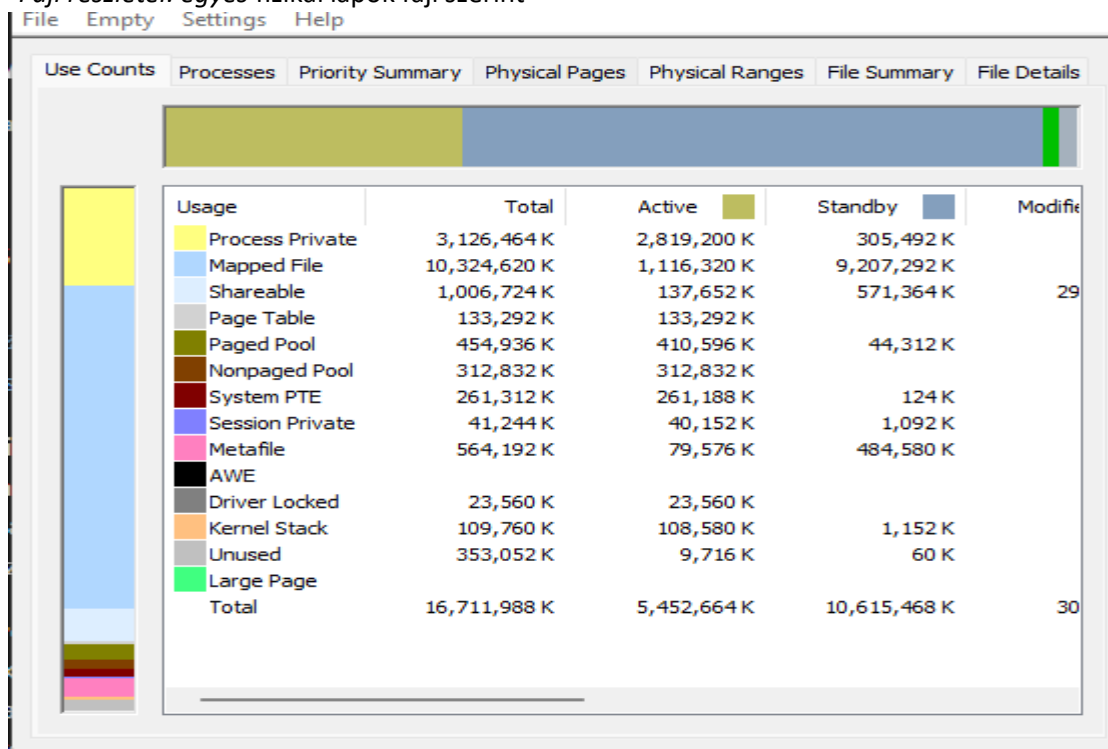
[0] Logon session 00000000:000003e7:
  User name:      WORKGROUP\BODNAR-LASZLO$
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            S-1-5-18
  Logon time:     20/02/2022 09:40:50
  Logon server:
  DNS Domain:
  UPN:
    844: lsass.exe
    1000: winlogon.exe
    1008: svchost.exe

```

e) Information Utilities (RAMMap):

A RAMMap egy speciális fizikai memóriahasználat-elemzési segédprogram a Windows Vista és újabb verziókhoz: *Folyamatok*: a munkakészletek méretének feldolgozása

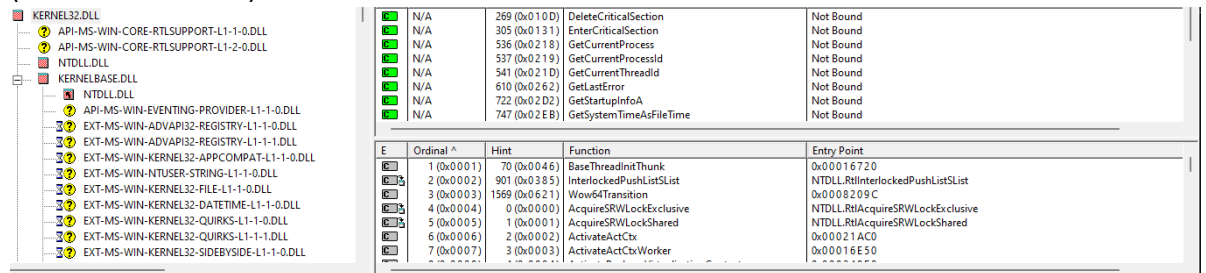
- *Prioritás összegzése*: rangsorolósó készenléti listaméretetek
- *Fizikai lapok*: oldalankénti használat az összes fizikai memóriához
- *Fizikai tartományok*: fizikai memóriacímek
- *Fájl összegzése*: fájl adatok a RAM-ban fájl szerint
- *Fájl részletei*: egyes fizikai lapok fájl szerint



### 3.feladat: Töltse le a következő programot: Dependency Walker

A, Dependency walker: Egy ingyenes windows segédprogram, amely megvizsgálja milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program.

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



The screenshot shows the Dependency Walker interface. On the left, a tree view lists the loaded DLLs, including kernel32.dll, API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL, API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL, NTDLL.DLL, KERNELBASE.DLL, and NTDLL.DLL. On the right, a table lists the functions used by neptunkod.exe from kernel32.dll. The table has columns for Ordinal, Hint, Function, and Entry Point.

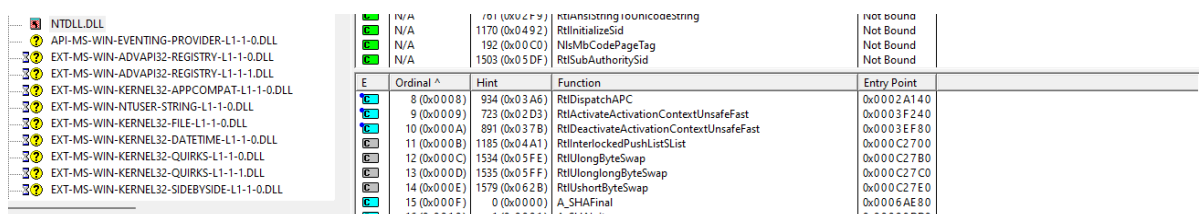
Ordinal	Hint	Function	Entry Point
1 (0x0001)	70 (0x0046)	BaseThreadInitThunk	0x00016720
2 (0x0002)	901 (0x0385)	InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList
3 (0x0003)	1569 (0x0621)	Wow64Transition	0x0008209C
4 (0x0004)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
5 (0x0005)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
6 (0x0006)	2 (0x0002)	ActivateActCtx	0x00021AC0
7 (0x0007)	3 (0x0003)	ActivateActCtxWorker	0x00016E50

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 NT Layer DLL fájlként is ismert. A Microsoft készítette Microsoft Windows Operating System fejlesztéséhez. DLL fájlok Win32 DLL fájl típus kategóriába sorolandók.

Dynamic Link Library fájlok, mint ntdll.dll, alapvetően útmutató könyvek, amelyek információkat és útmutatásokat tartalmaznak a végrehajtható (EXE) a követéshez. Ezeket a fájlokat úgy hozták létre, hogy több program megoszthat azonos ntdll.dll fájlt, ezáltal értékes memória-allokációt takarít meg, így a számítógép hatékonyabban működik.

NT Api: Szükség van rá a c programok futtatásához és hívásaihoz.



The screenshot shows the Dependency Walker interface. On the left, a tree view lists the loaded DLLs, including NTDLL.DLL, API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL, EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1-0.DLL, EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-1-0.DLL, EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL, EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL, EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1-0.DLL, and EXT-MS-WIN-KERNEL32-SIDEWAYSIDE-L1-1-0.DLL. On the right, a table lists the functions used by neptunkod.exe from ntdll.dll. The table has columns for Ordinal, Hint, Function, and Entry Point.

Ordinal	Hint	Function	Entry Point
8 (0x0008)	934 (0x03A6)	RtlDispatchAPC	0x0002A140
9 (0x0009)	723 (0x02D3)	RtlActivateActivationContextUnsafeFast	0x0003F240
10 (0x000A)	891 (0x037B)	RtlDeactivateActivationContextUnsafeFast	0x0003FE80
11 (0x000B)	1185 (0x04A1)	RtlInterlockedPushListSList	0x000C2700
12 (0x000C)	1534 (0x05FE)	RtlUlongByteSwap	0x000C27B0
13 (0x000D)	1535 (0x05FF)	RtlUlonglongByteSwap	0x000C27C0
14 (0x000E)	1579 (0x062B)	RtlUshortByteSwap	0x000C27E0
15 (0x000F)	0 (0x0000)	A_SHAFinal	0x0006AE80