

Operációs rendszerek BSc

2. Gyak.

2022. 02. 16.

Készítette:

Sikora Dávid Ádám Bsc

Mérnökinformatika

IRE699

Miskolc, 2022

1.Feladat

a.) Hozza létre a következő mappa szerkezetet!

```
Parancssor

C:\Users\sikor\Desktop\University\OS\IRE699>tree
Folder PATH listing
Volume serial number is CCCE-5DC3
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
└── land
    ├── kokusz
    └── szeder

C:\Users\sikor\Desktop\University\OS\IRE699>
```

b.) Készítsen másolatot:

- a neptunkod/ land/szeder katalógusról a neptunkod/fa katalógusba
- a neptunkod /bokor/banan katalógusról a neptunkod /fa katalógusba

```
C:\Users\sikor\Desktop\University\OS\IRE699>tree
Folder PATH listing
Volume serial number is CCCE-5DC3
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── banan
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder

C:\Users\sikor\Desktop\University\OS\IRE699>
```

c.) Végezze el a következő áthelyezéseket:

- a neptunkod /bokor/barack katalógust helyezze át a neptunkod /fa katalógusba
- a neptunkod /land /kokusz katalógust helyezze át a neptunkod/fa katalógusba

```
C:\Users\sikor\Desktop\University\OS\IRE699>tree
Folder PATH listing
Volume serial number is CCCE-5DC3
C:.\
|_ bokor
|   |_ banan
|   |_ mogyoro
|_ fa
|   |_ banan
|   |_ barack
|   |_ kokusz
|   |_ korte
|   |_ szeder
|_ land
|   |_ szeder

C:\Users\sikor\Desktop\University\OS\IRE699>
```



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

- neptunkod/bokor/banan/ leiras.txt
- neptunkod/tree/felsorolas.txt

```
C:\Users\sikor\Desktop\University\OS\IRE699>tree /F
Folder PATH listing
Volume serial number is CCCE-5DC3
C:.\
|_ bokor
|   |_ banan
|       leiras.txt
|   |_ mogyoro
|_ fa
|   |_ felsorolas.txt
|   |_ banan
|   |_ barack
|   |_ kokusz
|   |_ korte
|   |_ szeder
|_ land
|   |_ szeder

C:\Users\sikor\Desktop\University\OS\IRE699>
```

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

 felsorolas – J	 leiras – Jegyzet
Fájl Szerkesztés	Fájl Szerkesztés
András	A
Bence	barack
Gergő	finom.
Enikő	
Attila	

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

```
Directory of C:\Users\sikor\Desktop\University\OS\IRE699\fa\barack
02/16/2022  08:34 AM    <DIR>        .
02/16/2022  08:34 AM    <DIR>        ..
               0 File(s)                0 bytes

Directory of C:\Users\sikor\Desktop\University\OS\IRE699\fa\kokusz
02/16/2022  08:35 AM    <DIR>        .
02/16/2022  08:35 AM    <DIR>        ..
               0 File(s)                0 bytes

Directory of C:\Users\sikor\Desktop\University\OS\IRE699\fa\korte
02/16/2022  08:35 AM    <DIR>        .
02/16/2022  08:35 AM    <DIR>        ..
               0 File(s)                0 bytes

Directory of C:\Users\sikor\Desktop\University\OS\IRE699\fa\szeder
02/16/2022  08:35 AM    <DIR>        .
02/16/2022  08:35 AM    <DIR>        ..
               0 File(s)                0 bytes

Total Files Listed:
          2 File(s)                55 bytes
        29 Dir(s)  453,472,460,800 bytes free

C:\Users\sikor\Desktop\University\OS\IRE699>
```

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

```
C:\Users\sikor\Desktop\University\OS\IRE699>dir ?e* /S
Volume in drive C has no label.
Volume Serial Number is CCCE-5DC3

Directory of C:\Users\sikor\Desktop\University\OS\IRE699\bokor\banan
02/16/2022  08:57 AM                17 leiras.txt
               1 File(s)                17 bytes

Directory of C:\Users\sikor\Desktop\University\OS\IRE699\fa
02/16/2022  08:50 AM                38 felsorolas.txt
               1 File(s)                38 bytes

Total Files Listed:
               2 File(s)                55 bytes
               0 Dir(s) 453,469,368,320 bytes free
```

i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a neptunkod mappa az al-mappáival együtt.

```
Total Files Listed:
               2 File(s)                55 bytes
               29 Dir(s) 453,472,137,216 bytes free
```

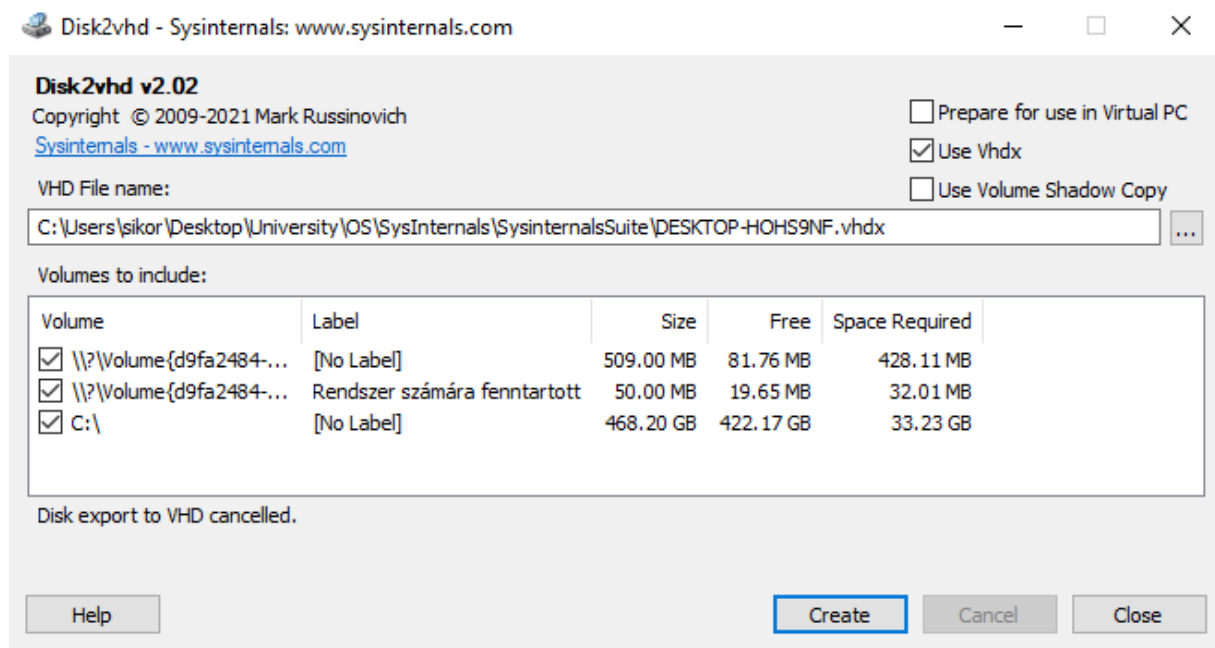
j.) Rendezze ABC-szerint a felsorolas.txt file tartalmát.

```
C:\Users\sikor\Desktop\University\OS\IRE699\fa>type felsorolas.txt
Andr|ís
Bence
Gerg|l
Enik|l
Attila
C:\Users\sikor\Desktop\University\OS\IRE699\fa>type felsorolas2.txt
Andr|ís
Attila
Bence
Enik|l
Gerg|l
```

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

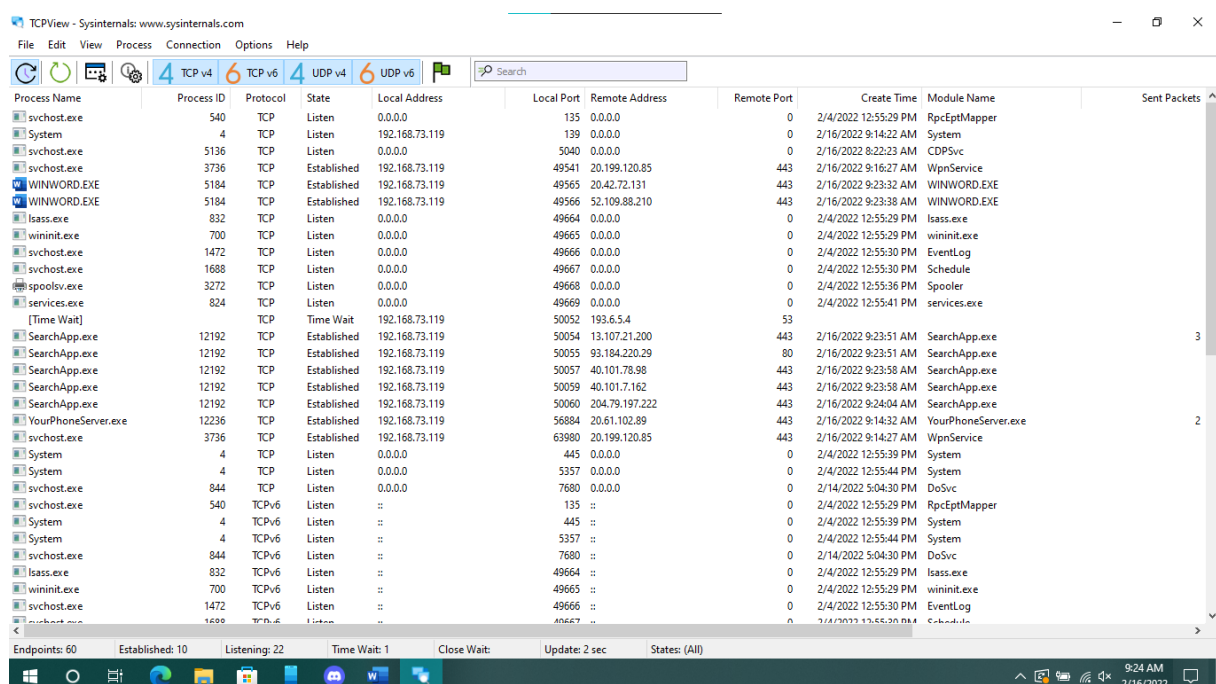
a) File and Disk Utilities (Disk2vhd)

Ez a segédprogram a meghajtó(ink)ról tud lemezképfájlt készíteni, amivel később vissza tudjuk állítani számítógépünket ha szükséges lenne.



b) Networking Utilities (TCPView)

A különböző hálózatokat aktuálisan használó programokat listázza ki a TPCView.



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

Ezen segédprogramok az aktuálisan futó programok figyelését, erőforrás igényének megfigyelését teszi lehetővé. Az AutoRuns pedig a számítógép indításakor, vagy más pillanatokban automatikusan elinduló alkalmazásokat listázza ki.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
9:25.5...	MsMpEng.exe	11796	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15,757,312...
9:25.5...	lsass.exe	832	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1,607,680...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\Software\Microsoft\SystemCertifi...	NAME NOT FOUND	Desired Access: R...
9:25.5...	Explorer.EXE	8204	ReadFile	C:\Windows\System32\ehhlpapi.dll	SUCCESS	Offset: 312,832, Le...
9:25.5...	Autounst64.exe	14936	RegCloseKey	HKCU	SUCCESS	
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegCreateKey	HKCU\Software\Microsoft\SystemCertifi...	SUCCESS	Desired Access: R...
9:25.5...	Autounst64.exe	14936	RegCloseKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKLM\Software\Policies\Microsoft\Syst...	NAME NOT FOUND	Desired Access: R...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\Software\Policies\Microsoft\Syst...	NAME NOT FOUND	Desired Access: R...
9:25.5...	Autounst64.exe	14936	RegCloseKey	HKCU	SUCCESS	
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKLM\Software\Microsoft\SystemCertifi...	NAME NOT FOUND	Desired Access: R...
9:25.5...	Explorer.EXE	8204	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 3,470,848...
9:25.5...	svchost.exe	2764	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690,880, Le...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegCreateKey	HKCU\Software\Microsoft\SystemCertifi...	SUCCESS	Desired Access: R...
9:25.5...	Autounst64.exe	14936	RegCloseKey	HKCU	SUCCESS	
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Desired Access: R...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegCreateKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Desired Access: R...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Query: Cached, Su...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Query: Cached, Su...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Query: HandleTag...
9:25.5...	Autounst64.exe	14936	RegCreateKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Desired Access: R...
9:25.5...	Autounst64.exe	14936	RegOpenKey	HKCU\SOFTWARE\Microsoft\SystemC...	SUCCESS	Query: Cached, Su...

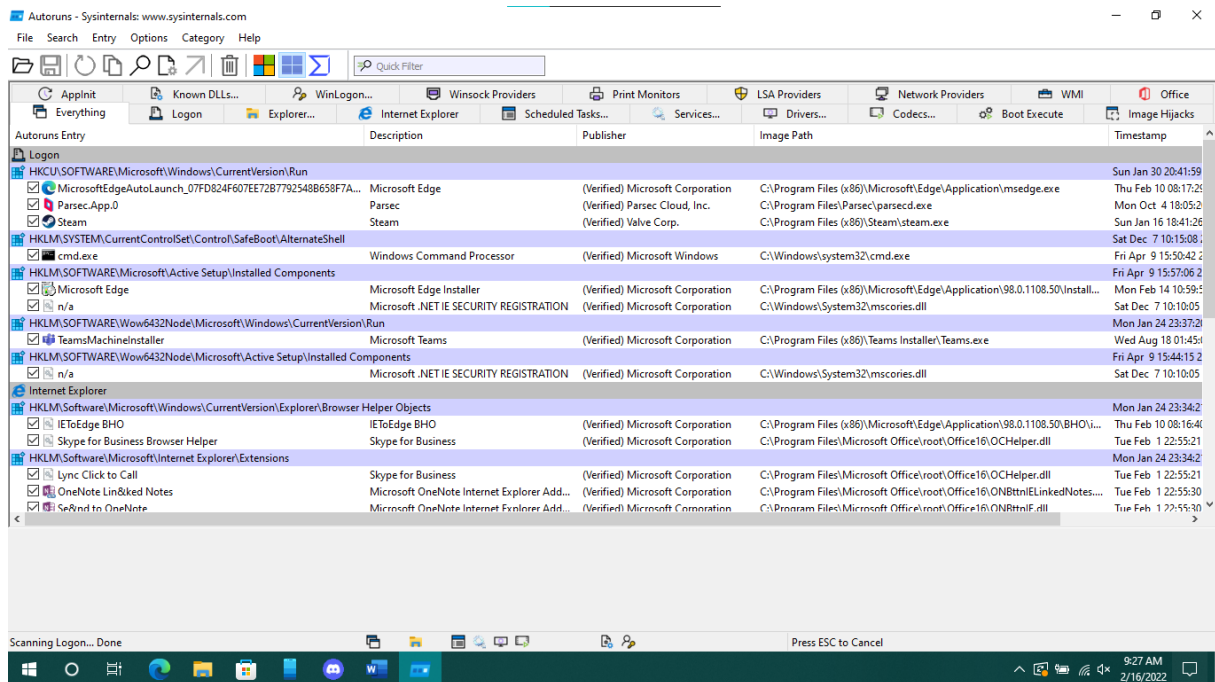
Showing 329,974 of 527,034 events (62%) Backed by virtual memory

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-HOHS9NF\sikor]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		5,396 K	37,464 K	100		
System Idle Process	61.94	60 K	8 K	0		
System	0.37	216 K	3,032 K	4		
Interrupts	0.75	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,084 K	512 K	408		
Memory Compression	< 0.01	728 K	225,100 K	1396		
csrss.exe	< 0.01	2,148 K	3,024 K	588		
wininit.exe		1,660 K	3,332 K	700		
services.exe	< 0.37	6,316 K	6,820 K	824		
svchost.exe	< 0.01	18,200 K	26,832 K	960	Windows-szolgáltatások gaz...	Microsoft Corporation
MoUsoCoreWorker.exe		30,840 K	31,672 K	11908		
dhost.exe		3,540 K	4,468 K	8168		
Eap3Host.exe		2,852 K	5,576 K	9988		
StartMenuExperience...		19,412 K	55,492 K	7156		
TextInputHost.exe		14,140 K	39,008 K	6504		Microsoft Corporation
RuntimeBroker.exe		6,308 K	25,144 K	6748	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		15,184 K	41,296 K	5668	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3,508 K	16,656 K	3076	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		7,524 K	6,756 K	6340	Host Process for Setting Syn...	Microsoft Corporation
SearchIndexing.exe	Susp...	97,376 K	95,512 K	8882	Search application	Microsoft Corporation
YouPhoneServer.exe	< 0.01	58,044 K	88,468 K	12236		
dllhost.exe		5,604 K	13,284 K	2156	COM Surrogate	Microsoft Corporation
ShellExperienceHost...	Susp...	42,472 K	58,812 K	9572	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		7,136 K	33,860 K	9654	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		9,928 K	25,848 K	15180	Application Frame Host	Microsoft Corporation
SystemSettings.exe	Susp...	28,448 K	2,044 K	14500	Gépház	Microsoft Corporation
UserOOBEBroker.exe		1,868 K	8,872 K	5504	User OOBEBroker	Microsoft Corporation
SystemSettingsBroker...		7,168 K	28,464 K	4692	System Settings Broker	Microsoft Corporation
YouPhone.exe	Susp...	34,560 K	3,932 K	13680		Microsoft Corporation
RuntimeBroker.exe		2,136 K	12,264 K	8852	Runtime Broker	Microsoft Corporation
SearchApp.exe		127,492 K	198,384 K	12192	Search application	Microsoft Corporation
WmiPrivSE.exe		2,500 K	9,280 K	13984		
ScreenClippingHost.exe	4.48	17,964 K	50,980 K	15288		Microsoft Corporation
svchost.exe	0.37	13,776 K	15,712 K	540	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2,992 K	5,348 K	572	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2,888 K	6,332 K	1192	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		1,728 K	2,780 K	1236	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	< 0.01	2,060 K	2,552 K	1244	Windows-szolgáltatások gaz...	Microsoft Corporation

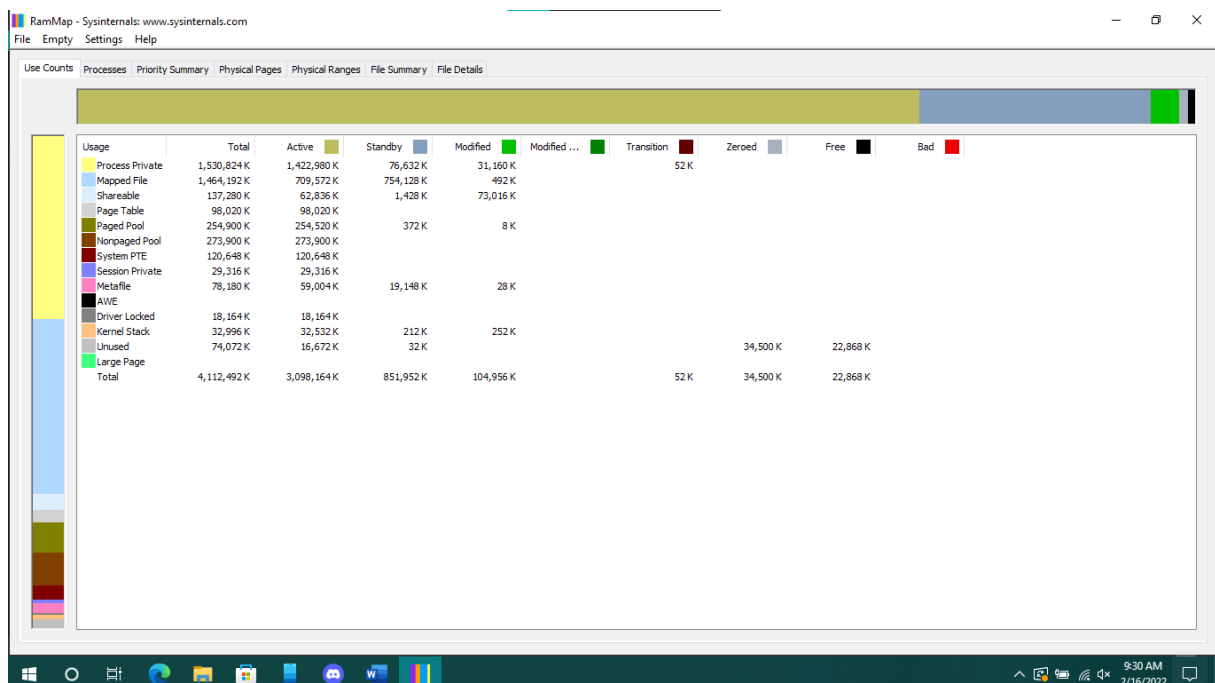
CPU Usage: 38.06% Commit Charge: 75.11% Processes: 164 Physical Usage: 80.25%



d) Security Utilities (LogonSession) – A Program Nem futott le!

e) Information Utilities (RAMMap)

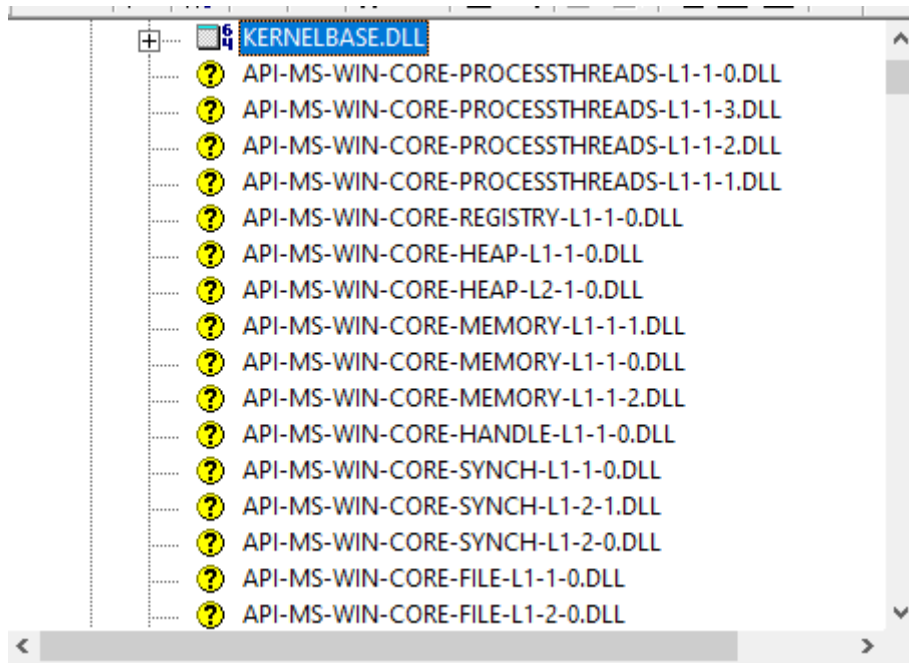
A rendszermemória felhasználtságtát kijelző program, mely részletesen megmutatja a ram mekkora területei milyen célra vannak éppen hasznosítva.



3.Feladat - Töltse le a következő programot: Dependency Walker

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

Az NTDLL.DLL egy dinamikusan csatolt könyvtár mely alap NT kernel funkciókat tartalmaz, mely az operációs rendszer és a legtöbb program számára szükséges.

