

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Durányik Bence Bsc

Mérnökinformatikus

TFOE75

Miskolc, 2022

1. Készítse el a következő feladatokat! Az elvégzett feladatokról készítsen (a.)-j.)-ig.) képernyőképet, majd illessze be a jegyzőkönyvbe.

a.) Hozza létre a megadott mappa szerkezetet!

```
D:\>md TFOE75

D:\>cd TFOE75

D:\TFOE75>md fa land bokor

D:\TFOE75>
D:\TFOE75>cd ..

D:\>md TFOE75

D:\>cd TFOE75

D:\TFOE75>md fa bokor land

D:\TFOE75>cd fa

D:\TFOE75\fa>md korte

D:\TFOE75\fa>cd ..

D:\TFOE75>cd bokor

D:\TFOE75\bokor>md banan mogyoro barack

D:\TFOE75\bokor>cd ..

D:\TFOE75>cd land

D:\TFOE75\land>md szeder kokusz

D:\TFOE75\land>_
```

b.) Készítsen másolatot:

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

```
D:\TFOE75>xcopy land fa /E
0 File(s) copied

D:\TFOE75> rd fa\kokusz

D:\TFOE75>xcopy bokor fa /E
0 File(s) copied

D:\TFOE75>rd fa\mogyoro fa\barack

D:\TFOE75>_
```

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

```
D:\TF0E75>move bokor/barack fa
1 dir(s) moved.

D:\TF0E75>move land/kokusz fa
1 dir(s) moved.
```

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

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

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

```
D:\TF0E75>rmdir land /S
land, Are you sure (Y/N)? y

D:\TF0E75>cd bokor\banan

D:\TF0E75\bokor\banan>copy con leiras.txt
sarga
oszi
kajszí
^Z
1 file(s) copied.

D:\TF0E75\bokor\banan>cd ..

D:\TF0E75\bokor>cd ..

D:\TF0E75>cd fa

D:\TF0E75\fa>attrib "felsorolas.txt" +R

D:\TF0E75\fa>attrib felsorolas.txt +R

D:\TF0E75\fa>copy con "felsorolas.txt"
banan
barack
kokusz
korte
szeder
^Z
1 file(s) copied.

D:\TF0E75\fa>_
```

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

```
D:\TF0E75>dir /S
Volume in drive D is Új kötet
Volume Serial Number is 82AE-56A2

Directory of D:\TF0E75

2022. 02. 19. 15:24 <DIR>      .
2022. 02. 19. 15:24 <DIR>      ..
2022. 02. 19. 15:02 <DIR>      bokor
2022. 02. 19. 15:25 <DIR>      fa
0 File(s)              0 bytes

Directory of D:\TF0E75\bokor

2022. 02. 19. 15:02 <DIR>      .
2022. 02. 19. 15:02 <DIR>      ..
2022. 02. 19. 14:52 <DIR>      banan
2022. 02. 19. 14:29 <DIR>      mogyoro
0 File(s)              0 bytes

Directory of D:\TF0E75\bokor\banan

2022. 02. 19. 14:52 <DIR>      .
2022. 02. 19. 14:52 <DIR>      ..
2022. 02. 19. 14:52                21 leiras.txt
1 File(s)              21 bytes

Directory of D:\TF0E75\bokor\mogyoro

2022. 02. 19. 14:29 <DIR>      .
2022. 02. 19. 14:29 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\TF0E75\fa

2022. 02. 19. 14:29 <DIR>      .
2022. 02. 19. 14:29 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\TF0E75\fa

2022. 02. 19. 15:25 <DIR>      .
2022. 02. 19. 15:25 <DIR>      ..
2022. 02. 19. 14:29 <DIR>      banan
2022. 02. 19. 15:01 <DIR>      barack
2022. 02. 19. 15:25                38 felsorolas.txt
2022. 02. 19. 15:00 <DIR>      kokusz
2022. 02. 19. 14:28 <DIR>      korte
2022. 02. 19. 14:30 <DIR>      szeder
1 File(s)              38 bytes

Directory of D:\TF0E75\fa\banan

2022. 02. 19. 14:29 <DIR>      .
2022. 02. 19. 14:29 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\TF0E75\fa\barack

2022. 02. 19. 15:01 <DIR>      .
2022. 02. 19. 15:01 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\TF0E75\fa\kokusz

2022. 02. 19. 15:00 <DIR>      .
2022. 02. 19. 15:00 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\TF0E75\fa\korte

2022. 02. 19. 14:28 <DIR>      .
2022. 02. 19. 14:28 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\TF0E75\fa\szeder

2022. 02. 19. 14:30 <DIR>      .
2022. 02. 19. 14:30 <DIR>      ..
0 File(s)              0 bytes

Total Files Listed:
2 File(s)              59 bytes
29 Dir(s)  570 007 552 000 bytes free
```

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

```
D:\TF0E75>dir "?e*" /S
Volume in drive D is Új kötet
Volume Serial Number is 82AE-56A2

Directory of D:\TF0E75\bokor\banan

2022. 02. 19.  14:52                21 leiras.txt
                1 File(s)                21 bytes

Directory of D:\TF0E75\fa

2022. 02. 19.  14:56               45 felsorolas.txt
                1 File(s)               45 bytes

Total Files Listed:
                2 File(s)               66 bytes
                0 Dir(s)  570 007 552 000 bytes free

D:\TF0E75>_
```

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

```
D:\TF0E75\fa>attrib felsorolas.txt +R
```

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

```
Total Files Listed:
                2 File(s)               59 bytes
                29 Dir(s)  570 007 552 000 bytes free
```

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

```
D:\TF0E75>cd fa

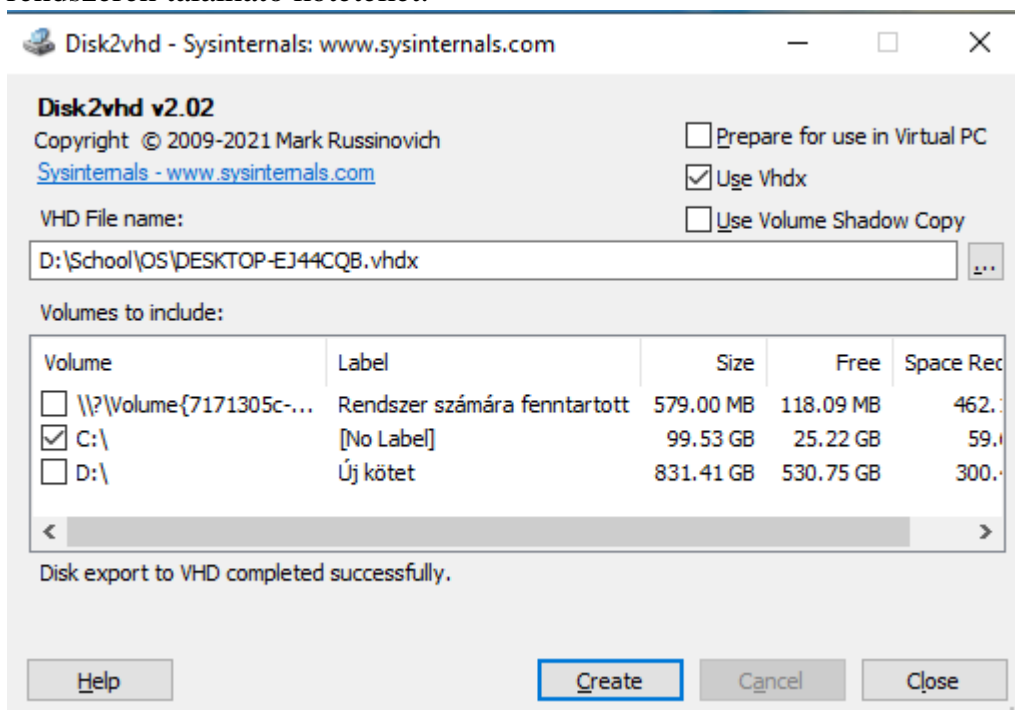
D:\TF0E75\fa>sort felsorolas.txt
banan
barack
kokusz
korte
szeder

D:\TF0E75\fa>_
```

2. Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít. A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el. A felsorolt eszközök közül minden eszköz esetén tölts le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét - majd mentse el a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

a) File and Disk Utilities (Disk2vhd)

A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-verzióit virtuális gépeken való használatra. A Disk2vhd felhasználói felület felsorolja a rendszeren található köteteket.

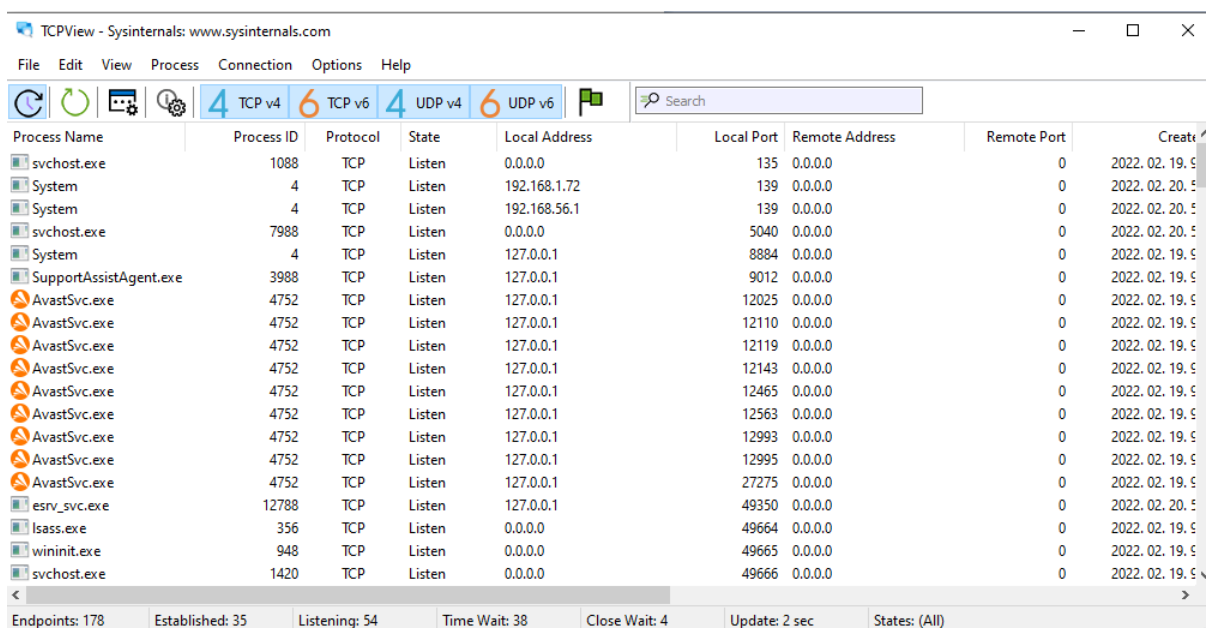


Minden olyan lemezhez létrehoz egy VHD-t, amelyen a kiválasztott kötetek találhatók. Megőrzi a lemez particionálási adatait, de csak a kiválasztott lemezen lévő kötetek adattartalmait másolja.

Név	Módosítás dátuma	Típus	Méret
DESKTOP-EJ44CQB	2022. 02. 19. 17:11	Merevlemezkép	71 115 777 ...
Zoomit	2022. 02. 16. 22:18	Alkalmazás	1 104 KB
Zoomit64	2022. 02. 16. 22:18	Alkalmazás	613 KB
Sysmon	2022. 02. 16. 22:18	Alkalmazás	7 119 KB
Sysmon64	2022. 02. 16. 22:18	Alkalmazás	3 834 KB
procmon	2022. 02. 16. 22:18	Lefordított HTML-...	63 KB
Procmon	2022. 02. 16. 22:18	Alkalmazás	5 091 KB
Procmon64	2022. 02. 16. 22:18	Alkalmazás	2 631 KB
autoruns	2022. 02. 16. 22:18	Lefordított HTML-...	25 KB
Autoruns	2022. 02. 16. 22:18	Alkalmazás	2 444 KB
Autoruns64	2022. 02. 16. 22:18	Alkalmazás	2 860 KB
autorunc	2022. 02. 16. 22:18	Alkalmazás	696 KB
autorunc64	2022. 02. 16. 22:18	Alkalmazás	770 KB

b) Networking Utilities (TCPView)

A TCPView egy Windows program, amely részletes listában mutatja be a rendszer összes TCP- és UDP-végpontját. 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 válthatunk a feloldott nevek megjelenítésére. A TCPView megjeleníti az egyes végpontok tulajdonában következő folyamat nevét, beleértve a szolgáltatás nevét is (ha van).



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

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create
svchost.exe	1088	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.19.9
System	4	TCP	Listen	192.168.1.72	139	0.0.0.0	0	2022.02.20.5
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.20.5
svchost.exe	7988	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.20.5
System	4	TCP	Listen	127.0.0.1	8884	0.0.0.0	0	2022.02.19.9
SupportAssistAgent.exe	3988	TCP	Listen	127.0.0.1	9012	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12025	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12110	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12119	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12143	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12465	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12563	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12993	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	12995	0.0.0.0	0	2022.02.19.9
AvastSvc.exe	4752	TCP	Listen	127.0.0.1	27275	0.0.0.0	0	2022.02.19.9
esrv_svc.exe	12788	TCP	Listen	127.0.0.1	49350	0.0.0.0	0	2022.02.20.5
lsass.exe	356	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.19.9
wininit.exe	948	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.19.9
svchost.exe	1420	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.19.9

Summary statistics at the bottom: Endpoints: 178, Established: 35, Listening: 54, Time Wait: 38, Close Wait: 4, Update: 2 sec, States: (All)

Azok a végpontok, amelyek az egyik frissítésről a következőre váltják az állapotot, sárga színnel vannak kiemelve; A törölt végpontok piros színnel jelennek meg, az új végpontok pedig zöld színnel jelennek meg. A TCPView kimeneti ablakát a Mentés menüelem használatával menthetjük fájlba.

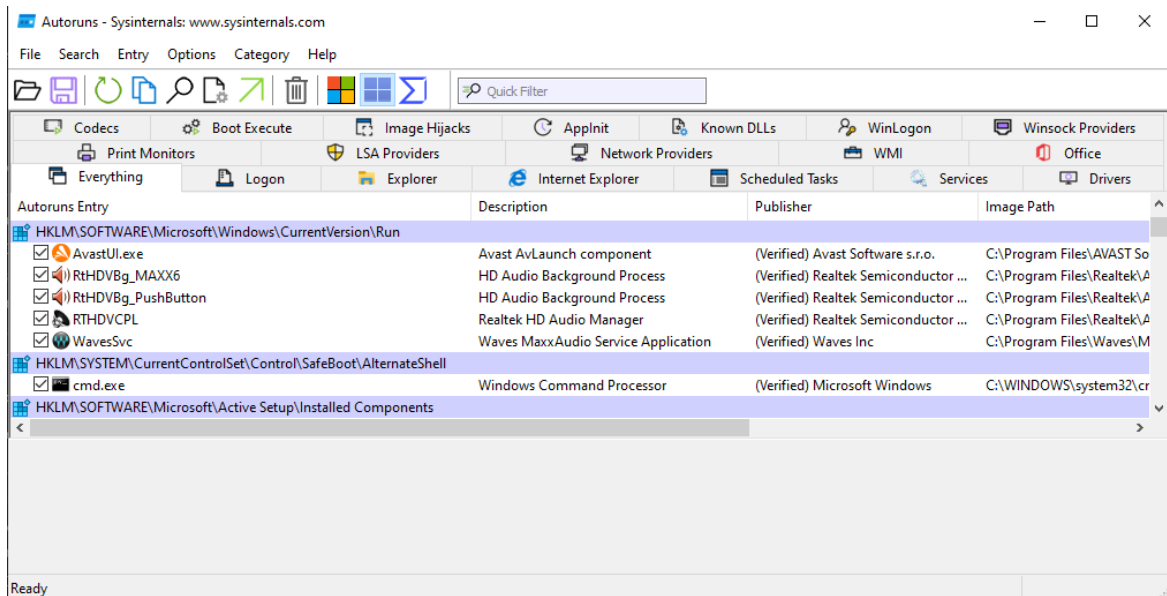
c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)

AutoRuns

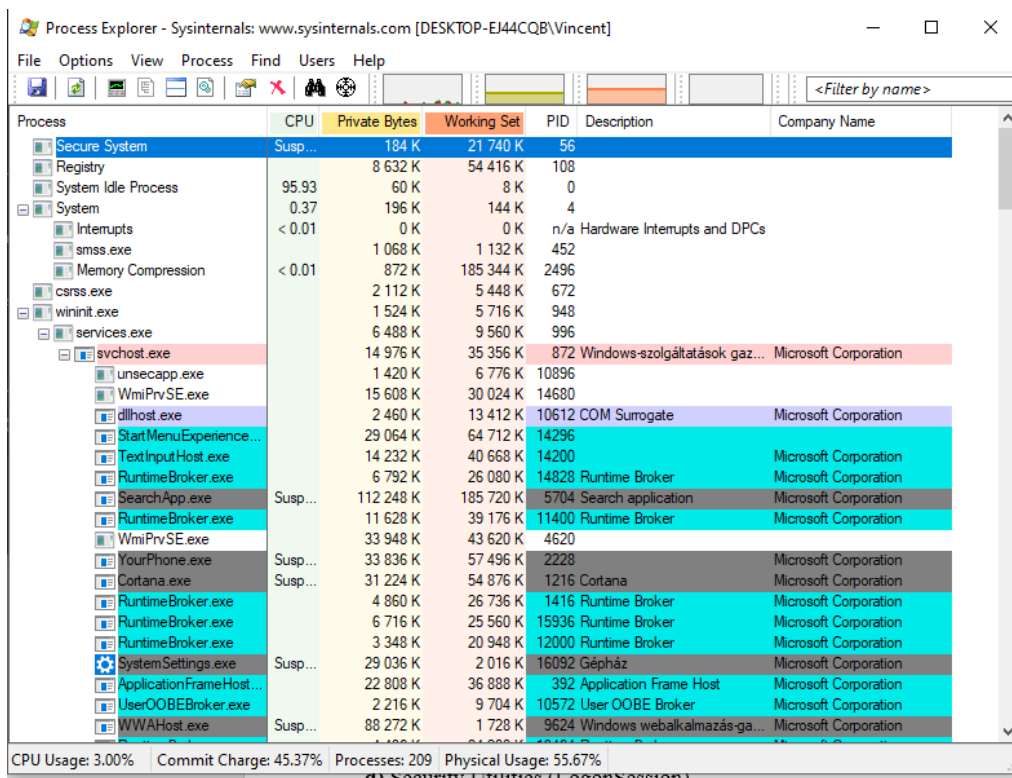
Ez a segédprogram megmutatja, milyen programok futtatására van konfigurálva a rendszerindítás vagy a bejelentkezés során, és mikor indít el különböző beépített Windows-alkalmazásokat. Az Autoruns Aláírt Microsoft-bejegyzések elrejtése beállítással nagyíthatjuk a rendszerhez hozzáadott, harmadik féltől származó automatikus indítási képeket, és támogatja a rendszeren konfigurált egyéb fiókokhoz konfigurált automatikus indítási képek használatát.

Az automatikus indítási bejegyzés letiltásához töröljük a jelölőnégyzet jelölését. Az automatikus indítási konfiguráció bejegyzésének törléséhez használjuk a Törölés menüelemet vagy eszköztárgombot.

A Felhasználói menü bejegyzéseinek kiválasztásával megtekinthetjük a különböző felhasználói fiókok automatikus indítási képeit.



Process Explorer



A Folyamatkezelő megmutatja, hogy mely leírókat és DLL-folyamatokat nyitották meg vagy töltötték be. A Folyamatkezelő megjelenítése két ablakból áll. A felső ablakban mindig megjelenik a jelenleg aktív folyamatok listája, beleértve a saját fiókjuk nevét, míg az alsó ablakban megjelenő információk a Folyamatkezelő módtól

függnek: ha leíró módban van, a felső ablakban kiválasztott folyamat leírói jelennek meg; Ha a Folyamatkezelő DLL módban van, látni fogjuk a folyamat által betöltött DLL-eket és memória leképezett fájlokat. A Folyamatkezelő egyedi képességei hasznosak a DLL-verzióproblémák nyomon követéséhez vagy a szivárgások kezeléséhez, és betekintést nyújtanak a Windows és alkalmazásokba.

Process Monitor

Time	Process Name	PID	Operation	Path	Result	Detail
11:41:...	AvastSvc.exe	4752	ReadFile	C:\Program Files\AVAST Software\Ava...	SUCCESS	Offset: 812 544, Le...
11:41:...	ServiceHost.exe	5344	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
11:41:...	ServiceHost.exe	5344	RegOpenKey	HKLM\SOFTWARE\McAfee\WebAdvi...	SUCCESS	Desired Access: Q...
11:41:...	ServiceHost.exe	5344	RegSetInfoKey	HKLM\SOFTWARE\McAfee\WebAdvi...	SUCCESS	KeySetInformation...
11:41:...	ServiceHost.exe	5344	RegQueryValue	HKLM\SOFTWARE\McAfee\WebAdvi...	SUCCESS	Type: REG_BINARY...
11:41:...	ServiceHost.exe	5344	RegQueryValue	HKLM\SOFTWARE\McAfee\WebAdvi...	SUCCESS	Type: REG_BINARY...
11:41:...	ServiceHost.exe	5344	RegCloseKey	HKLM\SOFTWARE\McAfee\WebAdvi...	SUCCESS	
11:41:...	Explorer.EXE	13600	QueryOpen	D:\School\OS\Procmon64.exe	SUCCESS	CreationTime: 202...
11:41:...	svchost.exe	15468	ReadFile	C:\Windows\System32\winsqlite3.dll	SUCCESS	Offset: 864 256, Le...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCU\Software\Classes\CLSID\{F0AE...	NAME NOT FOUND	Desired Access: R...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-A...	SUCCESS	Desired Access: R...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-a1...	SUCCESS	Query: Name
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-a1...	SUCCESS	Query: HandleTag...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCU\Software\Classes\CLSID\{F0AE1...	NAME NOT FOUND	Desired Access: Q...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-a1...	SUCCESS	Query: HandleTag...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-a1...	NAME NOT FOUND	Desired Access: Q...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-a1...	SUCCESS	Query: Name
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-a1...	SUCCESS	Query: Name
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCR\CLSID\{F0AE1542-F497-484B-a1...	SUCCESS	Query: HandleTag...
11:41:...	Explorer.EXE	13600	RegOpenKey	HKCU\Software\Classes\CLSID\{F0AE1...	NAME NOT FOUND	Desired Access: M...
11:41:...	svchost.exe	2612	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
11:41:...	Explorer.EXE	13600	RegQueryValue	HKCR\CLSID\{F0AE1542-F497-484B-a1...	NAME NOT FOUND	Length: 16

Showing 415 080 of 997 235 events (41%) Backed by virtual memory

A Folyamatfigyelő egy fejlett monitorozási eszköz Windows, amely valós idejű fájlrendszer-, beállításjegyzék- és folyamat-/száltevékenységet mutat be. A nem kipusztító szűrők lehetővé teszik, hogy adatvesztés nélkül állítsunk be szűrőket. Az egyes műveletek számkészletének rögzítése számos esetben lehetővé teszi a művelet kiváltó okának azonosítását. Szűrők bármely adatmezőhöz beállíthatók, beleértve a nem oszlopként konfigurált mezőket is. A natív naplóformátum minden adatot megőriz egy másik Folyamatfigyelő-példányba való betöltéshez.

d) Security Utilities (LogonSession)

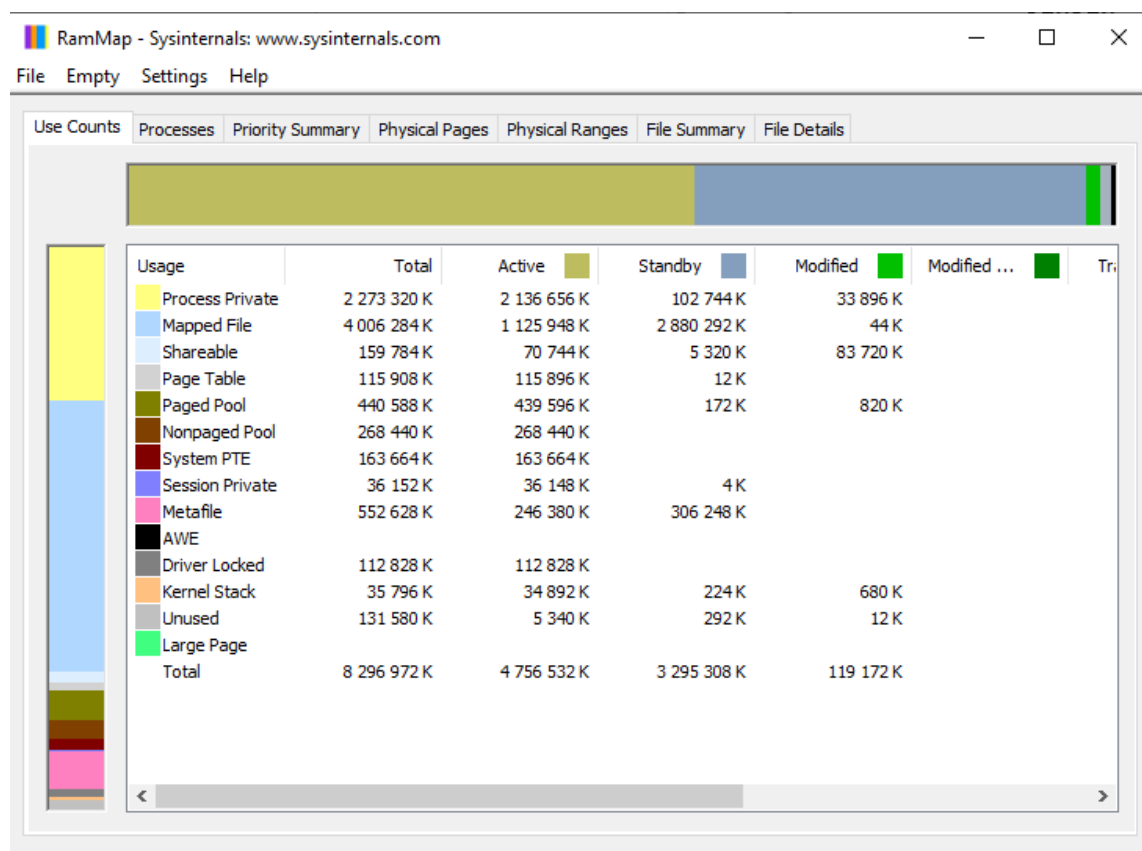
Ez a segédprogram felsorolja a jelenleg aktív bejelentkezési munkameneteket, és az egyes munkamenetekben futó folyamatokat.

```
C:\>logonsessions -p

[13] Logon session 00000000:6a6d6160:
  User name:      NTDEV\markruss
  Auth package:   Kerberos
  Logon type:     RemoteInteractive
  Session:       1
  Sid:           S-1-5-21-397955417-626881126-188441444-3615555
  Logon time:     7/2/2015 6:05:31 PM
  Logon server:   NTDEV-99
  DNS Domain:    NTDEV.CORP.MICROSOFT.COM
  UPN:            markruss@ntdev.microsoft.com
  15368: ProcExp.exe
  17528: ProcExp64.exe
  13116: cmd.exe
  17100: conhost.exe
  6716: logonsessions.exe
```

e) Information Utilities (RAMMap)

A RAMMap egy speciális fizikai memóriahasználat-elemzési segédprogram amely, különböző módokon mutatja be a használati adatokat a különböző lapjain.



A RAMMap használatával megérthetjük, hogyan kezeli Windows a memóriahasználatot, elemezheti az alkalmazás memóriahasználatát, vagy választ ad a RAM kiosztásával kapcsolatos konkrét kérdésekre. A RAMMap frissítési funkciója lehetővé teszi a megjelenítés frissítését, és támogatja a memória-pillanatképek mentését és betöltését.

3. Töltse le a következő programot: Dependency Walker! Feladata: a segédprogram megvizsgálja milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program. „ Készítsen egy neptunkod.c nevű forráskódot, amely egy vezeteknev.txt fájl létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc. Fordítsa le kódot a C fordító, majd tegye futtathatóvá az állományt: neptunkod.exe 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.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról! „ Mentés: Írja le a program

szolgáltatásait és a futtatás eredményét a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).