

Operációs rendszerek BSc

2.Gyak.

2022. 02. 15.

Készítette:

Ónodi Bence BSC

Programtervező
informatikus

RYSNLC

Miskolc, 2022

1. feladat a.) Hozza létre a következő mappa szerkezetet!

```
C:\>tree rysnlc
Folder PATH listing
Volume serial number is 0000009E 22C8:FA62
C:\RYSNLC
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
└── land
    ├── kokusz
    └── szeder
```

b.) Készítsen másolatot:

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

```
C:\rysnlc>tree fa
Folder PATH listing
Volume serial number is 00000001 22C8:FA62
C:\RYSNLC\FA
├── banan
├── korte
└── szeder
```

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:\rysnlc>tree fa
Folder PATH listing
Volume serial number is 00000076 22C8:FA62
C:\RYSNLC\FA
├── banan
├── barack
├── kokusz
├── korte
└── szeder
```

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:\rysnlc>rmdir /s land
land, Are you sure (Y/N)? y
C:\rysnlc>cd C:\
C:\>tree rysnlc
Folder PATH listing
Volume serial number is 000000A2 22C8:FA62
C:\RYSNLC
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder
C:\>cd C:\rysnlc\bokor\banan
C:\rysnlc\bokor\banan>type nul > leiras.txt
C:\rysnlc\bokor\banan>cd C:\rysnlc\fa
C:\rysnlc\fa>type nul > felsorolas.txt
C:\>tree rysnlc /f
Folder PATH listing
Volume serial number is 0000004C 22C8:FA62
C:\RYSNLC
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   ├── barack
│   └── mogyoro
└── fa
    ├── felsorolas.txt
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder
```

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

```
C:\rysnlc\fa>echo BerkiViktor HajduAdrian CsonkaPatrik KormosBalazs SzaboAlen >felsorolas.txt
C:\rysnlc\fa>cd C:\rysnlc\bokor\banan
C:\rysnlc\bokor\banan>echo A faj Prunus persica K'n ban <shonos. Az <szibarackfa lombhullat' fafaj. L ndzsa alakt, el
lipszis alakt vagy hossztk s levelei vannak
A faj Prunus persica K'n ban <shonos. Az <szibarackfa lombhullat' fafaj. L ndzsa alakt, ellipszis alakt vagy hossztk
s levelei vannak
C:\rysnlc\bokor\banan>echo Az oszibarackfa lombhullato fafaj. Akar 6-8 m magassagot is elerhet. Landzsa alaku, enyhen
hegyes levelei vannak > leiras.txt
C:\rysnlc\bokor\banan>cd C:\rysnlc
C:\rysnlc>sort leiras.txt
leiras.txtA rendszer nem tal lja a megadott f jlt.
C:\rysnlc>cd C:\rysnlc\bokor\banan
C:\rysnlc\bokor\banan>sort leiras.txt
Az oszibarackfa lombhullato fafaj. Akar 6-8 m magassagot is elerhet. Landzsa alaku, enyhen hegyes levelei vannak
C:\rysnlc\bokor\banan>cd C:\rysnlc\fa
C:\rysnlc\fa>sort felsorolas.txt
BerkiViktor HajduAdrian CsonkaPatrik KormosBalazs SzaboAlen
```

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

```
C:\>tree rysnlc /f
Folder PATH listing
Volume serial number is 000000CC 22C8:FA62
C:\RYSNLC
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   ├── barack
│   └── mogyoro
└── fa
    ├── felsorolas.txt
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder
```

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

```

Directory of C:\Windows\WinSxS\x86_wcf-m_svc_mon_sup_dll_31bf3856ad364e35_10.0.19200.110_none_756ba0685b6c3f32
2021. 10. 06. 14:40 11 152 ServiceMonikerSupport.dll
1 File(s) 11 152 bytes

Directory of C:\Windows\WinSxS\x86_windows-defender-management-powershell_31bf3856ad364e35_10.0.19041.1_none_3d95cd0a88523a81
2019. 12. 07. 10:29 7 674 Defender.psd1
1 File(s) 7 674 bytes

Directory of C:\Windows\WinSxS\x86_wpf-penimc_31bf3856ad364e35_10.0.19200.250_none_7b137039149c1529
2021. 10. 06. 14:40 35 108 PenIMC.dll
1 File(s) 35 108 bytes

Directory of C:\Windows\WinSxS\x86_wpf-reachframework_31bf3856ad364e35_10.0.19200.250_none_cf8c888138a7c1a4
2021. 10. 06. 14:40 166 900 ReachFramework.dll
1 File(s) 166 900 bytes

Total Files Listed:
14310 File(s) 2 444 666 096 bytes
1476 Dir(s) 382 672 588 800 bytes free

```

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

```

C:\>cd C:\rysnlc\fa
C:\rysnlc\fa>attrib
A C:\rysnlc\fa\felsorolas.txt
C:\rysnlc\fa>attrib +r felsorolas.txt
C:\rysnlc\fa>attrib
A R C:\rysnlc\fa\felsorolas.txt

```

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

```

Directory of C:\rysnlc\fa\korte
2022. 02. 16. 20:50 <DIR> .
2022. 02. 16. 20:50 <DIR> ..
0 File(s) 0 bytes

Directory of C:\rysnlc\fa\szeder
2022. 02. 17. 17:13 <DIR> .
2022. 02. 17. 17:13 <DIR> ..
0 File(s) 0 bytes

Total Files Listed:
2 File(s) 220 bytes
32 Dir(s) 382 642 536 448 bytes free

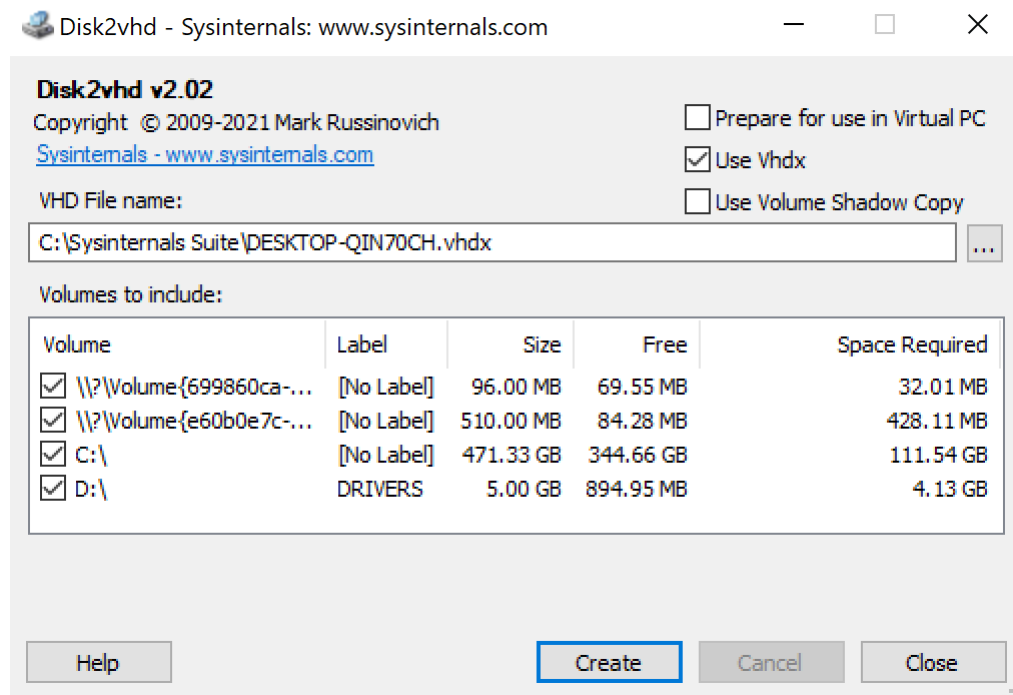
```

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 a fizikai lemezek VHD (Virtual Hard Disk) változatát Microsoft Virtual PC-ben vagy Hyper-V virtuális gépekben való használatra. A Disk2vhd előnye, hogy online rendszereken is futtatható. A Disk2vhd felhasználói felületén felsorolja a rendszeren lévő partíciókat:



Minden kijelölt lemezhez egy VHD-t lehet létrehozni. Ez a VHD megőrzi a lemez partícionálási információit, de csak a kiválasztott lemezen levő köteteknek az adattartalmát másolja.

Futtatás eredménye: Kijelölt lemezek másolat készítése VHD-re.

b) Networking Utilities (TCPView)

A TCPView megmutatja a rendszer összes TCP- és UDP-végpontjának részletes listáját, beleértve a helyi és távoli címeket is. A TCPView elindításakor az összes aktív TCP- és UDP-végpontot felsorolja, majd jellemzi Processz névvel, Processz ID-vel, protokollal, állapottal, IP-címmel, távoli címmel, kezdeti időponttal, modul névvel etc. Alapértelmezettként másodpercenként frissül. Azok a végpontok, amelyek állapotát egyik frissítésről a másikra változtatják, sárga színnel jelölik, törölteket pirossal, új végpontokat zölddel.

Futtatás eredménye: Oprendszeremen zajló összes processz adatainak láthatósága

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6

Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	1208	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.17.15:48:00	RpcSs	
System	4	TCP	Listen	192.168.0.81	139	0.0.0.0	0	2022.02.18.19:42:36	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.18.17:49:19	System	
svchost.exe	7776	TCP	Listen	0.0.0.0	5940	0.0.0.0	0	2022.02.18.17:49:16	CDPSvc	
svchost.exe	5804	TCP	Established	192.168.0.81	49429	20.199.120.182	443	2022.02.18.19:42:35	WynrService	11
lsass.exe	1016	TCP	Listen	0.0.0.0	49654	0.0.0.0	0	2022.02.17.15:48:00	lsass.exe	
wininit.exe	952	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.17.15:48:00	wininit.exe	
svchost.exe	1100	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.17.15:48:01	EventLog	
svchost.exe	2436	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.17.15:48:01	Schedule	
spoolsv.exe	4812	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2022.02.17.15:48:02	Spooler	
services.exe	1000	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	2022.02.17.15:48:03	services.exe	
AsusLinkNear.exe	5080	TCP	Listen	0.0.0.0	49674	0.0.0.0	0	2022.02.17.15:48:03	ASUSLinkNear	
AsusLinkNear.exe	5080	TCP	Listen	0.0.0.0	49675	0.0.0.0	0	2022.02.17.15:48:03	ASUSLinkNear	
chrome.exe	15008	TCP	Established	192.168.0.81	51033	31.13.84.23	443	2022.02.18.19:42:33	chrome.exe	357
chrome.exe	15008	TCP	Established	192.168.0.81	51035	31.13.84.23	443	2022.02.18.19:42:33	chrome.exe	106
svchost.exe	5804	TCP	Established	192.168.0.81	51036	20.199.120.182	443	2022.02.18.19:42:34	WynrService	4
chrome.exe	15008	TCP	Established	192.168.0.81	51038	31.13.84.8	443	2022.02.18.19:42:34	chrome.exe	703
chrome.exe	15008	TCP	Established	192.168.0.81	51039	31.13.84.8	443	2022.02.18.19:42:34	chrome.exe	151
chrome.exe	15008	TCP	Established	192.168.0.81	51082	142.250.27.188	443	2022.02.18.19:42:38	chrome.exe	3
[Time Wait]		TCP	Time Wait	192.168.0.81	51113	172.217.20.14	443			
SearchApp.exe	2280	TCP	Established	192.168.0.81	51115	13.107.21.200	443	2022.02.18.20:01:37	SearchApp.exe	1
SearchApp.exe	2280	TCP	Established	192.168.0.81	51116	13.107.21.200	443	2022.02.18.20:01:37	SearchApp.exe	1
SearchApp.exe	2280	TCP	Established	192.168.0.81	51117	40.101.71.96	443	2022.02.18.20:01:37	SearchApp.exe	
smartScreen.exe	7784	TCP	Ask	192.168.0.81	51119	20.67.219.152	443	2022.02.18.20:01:38	smartScreen.exe	
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2022.02.17.15:48:03	System	
svchost.exe	1208	TCPv6	Listen	:	135	:	0	2022.02.17.15:48:00	RpcSs	
System	4	TCPv6	Listen	:	445	:	0	2022.02.17.15:48:03	System	
lsass.exe	1016	TCPv6	Listen	:	49654	:	0	2022.02.17.15:48:00	lsass.exe	
wininit.exe	952	TCPv6	Listen	:	49665	:	0	2022.02.17.15:48:00	wininit.exe	
svchost.exe	1100	TCPv6	Listen	:	49666	:	0	2022.02.17.15:48:01	EventLog	
svchost.exe	2436	TCPv6	Listen	:	49667	:	0	2022.02.17.15:48:01	Schedule	
spoolsv.exe	4812	TCPv6	Listen	:	49669	:	0	2022.02.17.15:48:02	Spooler	
jhl_service.exe	6088	TCPv6	Listen	:	49670	:	0	2022.02.17.15:48:03	jhl_service	
services.exe	1000	TCPv6	Listen	:	49671	:	0	2022.02.17.15:48:03	services.exe	
System	4	UDP		192.168.0.81	137	*		2022.02.18.19:42:36	System	
System	4	UDP		192.168.56.1	137	*		2022.02.18.17:49:19	System	
System	4	UDP		192.168.0.81	138	*		2022.02.18.19:42:36	System	
System	4	UDP		192.168.56.1	138	*		2022.02.18.17:49:19	System	

Endpoints: 72 Established: 10 Listening: 22 Time Wait: 1 Close Wait: Update: 2 sec States: (All)

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

Átfogó képet ad az indítási monitorok automatikus indítási helyeiről, megmutatja milyen programok vannak beállítva a rendszerindítás vagy bejelentkezés során. Használata egyszerű, futtatás után megmutatja az indítási alkalmazásokat, valamint az automatikus indítási konfigurációhoz elérhető rendszerleíró adatbázis és fájlrendszer helyek teljes listáját.

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

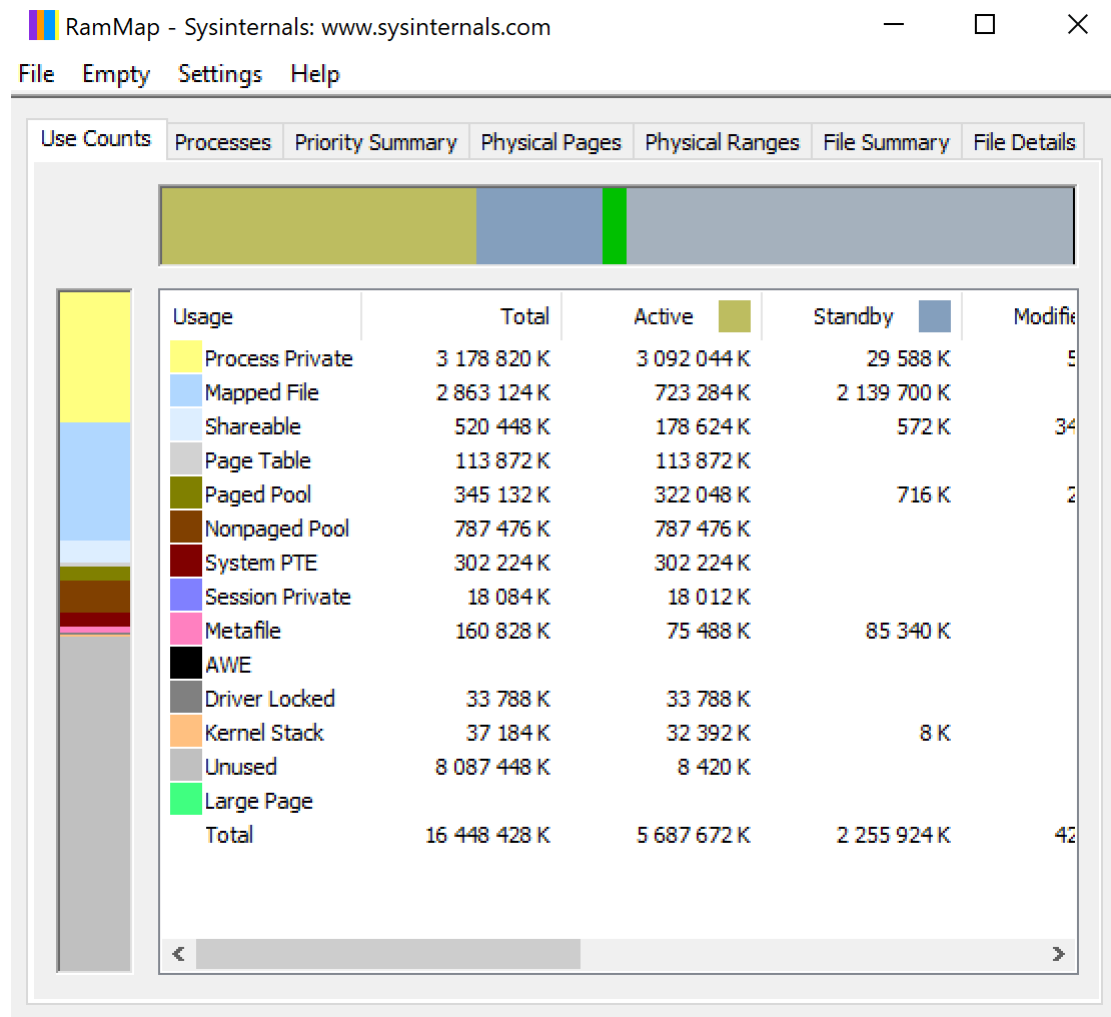
Quick Filter

Autoruns Entry	Description	Publisher	Image Path
Logon			
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> Discord	Update	(Verified) Discord Inc.	C:\Users\onodi\AppData\Local\Discord
<input checked="" type="checkbox"/> EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	C:\Program Files (x86)\Epic Games\Laur
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\onodi\AppData\Local\Microso
<input checked="" type="checkbox"/> Spotify	Spotify	(Verified) Spotify AB	C:\Users\onodi\AppData\Roaming\Spc
<input checked="" type="checkbox"/> Windscribe	Windscribe GUI	(Verified) Windscribe Limited	C:\Program Files (x86)\Windscribe\Win
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> Riot Vanguard	Vanguard tray notification.	(Verified) Riot Games, Inc.	C:\Program Files\Riot Vanguard\vgtray
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chrome\Appl
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge
<input checked="" type="checkbox"/> Microsoft .NET Framework 4.8.1	Microsoft .NET Framework 4.8.1	(Verified) Microsoft Corporation	C:\Windows\System32\Microsoft.NET

d) Security Utilities (LogonSession) e) Information Utilities (RAMMap)

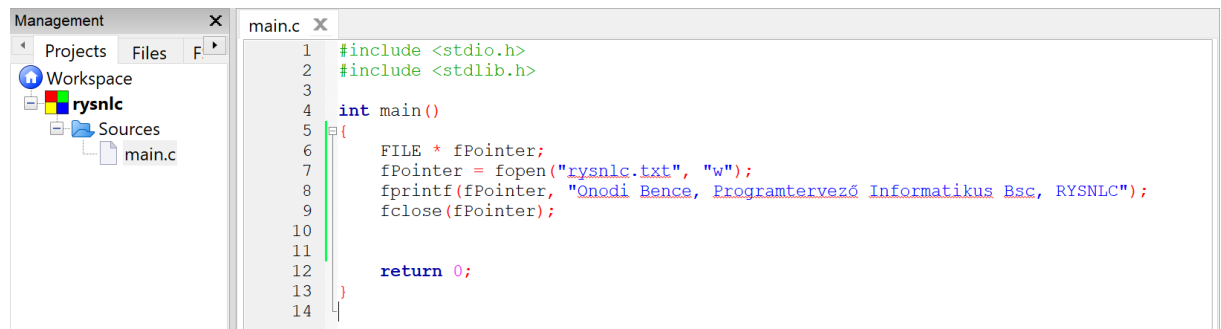
A RAMMap egy fejlett memóriahasználat-elemző segédprogram. Különböző módokon jeleníti meg a használati információkat mint például processzek, fájlként, fizikai oldalakként etc.

A program segítségével megérthetjük azt, hogy a Windows hogyan kezeli a memóriát.



3.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.



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! „