

Operációs rendszerek BSc

2. Gyak.

2022. 02. 14.

Készítette:

Kórád György Bsc

Programtervező informatikus

ZF440N

Miskolc, 2022

1. feladat –. Készítse el a következő feladatokat!

a.) Hozza létre a következő mappa szerkezetet!

```
└─mogyoro

E:\ZF440N>cd bokor

E:\ZF440N\bokor>mkdir banan mogyoro barack

E:\ZF440N\bokor>cd ..

E:\ZF440N>mkdir fa\korte

E:\ZF440N>mkdir land\szeder land\kokusz

E:\ZF440N>tree
Folder PATH listing
Volume serial number is 6E8C-3DF1
E:..
├─bokor
│   ├──banan
│   ├──barack
│   └─mogyoro
├─fa
│   └─korte
└─land
    ├──kokusz
    └─szeder
```

c.) Végezze el a következő áthelyezéseket:

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

```
E:\ZF440N>move
The syntax of the command is incorrect.

E:\ZF440N>move bokor\barack fa
1 dir(s) moved.

E:\ZF440N>tree
Folder PATH listing
Volume serial number is 6E8C-3DF1
E:..
├─bokor
│   ├──banan
│   └─mogyoro
├─fa
│   ├──barack
│   └─korte
└─land
    ├──kokusz
    └─szeder

E:\ZF440N>
```

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

```
E:\ZF440N>move land/kokusz fa
1 dir(s) moved.

E:\ZF440N>tree
Folder PATH listing
Volume serial number is 6E8C-3DF1
E:..
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── barack
│   ├── kokusz
│   └── korte
├── land
└── szeder

E:\ZF440N>
```

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

```
E:\ZF440N>rmdir land /s /q

E:\ZF440N>tree
Folder PATH listing
Volume serial number is 6E8C-3DF1
E:..
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── barack
│   ├── kokusz
│   └── korte
```

- neptunkod/bokor/banan/ leiras.txt

```
E:\ZF440N\bokor\banan>echo > leiras.txt

E:\ZF440N\bokor\banan>dir
Volume in drive E has no label.
Volume Serial Number is 6E8C-3DF1

Directory of E:\ZF440N\bokor\banan

2022. 02. 20.  14:45    <DIR>          .
2022. 02. 20.  14:07    <DIR>          ..
2022. 02. 20.  14:58               13 leiras.txt
                1 File(s)              13 bytes
                2 Dir(s)  780 917 321 728 bytes free
```

- neptunkod/tree/felsorolas.txt

```
E:\ZF440N\fa>echo > felsorolas.txt

E:\ZF440N\fa>dir
Volume in drive E has no label.
Volume Serial Number is 6E8C-3DF1

Directory of E:\ZF440N\fa

2022. 02. 20.  14:48    <DIR>        .
2022. 02. 20.  14:26    <DIR>        ..
2022. 02. 15.  17:14    <DIR>        barack
2022. 02. 20.  14:56             13 felsorolas.txt
2022. 02. 15.  17:15    <DIR>        kokusz
2022. 02. 15.  17:14    <DIR>        korte
                    1 File(s)          13 bytes
                    5 Dir(s)  780 917 350 400 bytes free

E:\ZF440N\fa>
```

e.) A leiras.txt szöveges állományba írjon 3 sort a barackról.

```
E:\ZF440N\bokor\banan>echo sarga >> leiras.txt

E:\ZF440N\bokor\banan>echo gombolyu >> leiras.txt

E:\ZF440N\bokor\banan>echo szoros >> leiras.txt
```

- A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét

```
E:\ZF440N\fa>echo Bencs Andras >> felsorolas.txt

E:\ZF440N\fa>echo Bereznai Benjamin >> felsorolas.txt
Bereznai Benjamin

E:\ZF440N\fa>echo Drig Dávid >> felsorolas.txt
Drig Dávid

E:\ZF440N\fa>echo Drig David >> felsorolas.txt

E:\ZF440N\fa>echo Bereznai Benjamin >> felsorolas.txt

E:\ZF440N\fa>echo Nagy Balazs >> felsorolas.txt
Nagy Balazs

E:\ZF440N\fa>echo Nagy Balazs >> felsorolas.txt

E:\ZF440N\fa>echo Trembeczki David >> felsorolas.txt

E:\ZF440N\fa>echo Nagy Balazs >> felsorolas.txt

E:\ZF440N\fa>
```

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

```
E:\ZF440N>tree
Folder PATH listing
Volume serial number is 6E8C-3DF1
E:..
|
+--- bokor
|    |
|    +--- banan
|    +--- mogyoro
|
+--- fa
     |
     +--- barack
     +--- kokusz
     +--- korte

E:\ZF440N>
```

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

```
E:\ZF440N>dir /S ?e*
Volume in drive E has no label.
Volume Serial Number is 6E8C-3DF1

Directory of E:\ZF440N\bokor\banan

2022. 02. 20.  15:02                41 leiras.txt
                1 File(s)              41 bytes

Directory of E:\ZF440N\fa

2022. 02. 20.  15:12                81 felsorolas.txt
                1 File(s)              81 bytes

Total Files Listed:
                2 File(s)              122 bytes
                0 Dir(s)  780 917 035 008 bytes free
```

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

```
E:\ZF440N\fa>attrib +R felsorolas.txt

E:\ZF440N\fa>attrib  felsorolas.txt
A      R                  E:\ZF440N\fa\felsorolas.txt

E:\ZF440N\fa>
```

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

```
E:\ZF440N>dir /s
Volume in drive E has no label.
Volume Serial Number is 6E8C-3DF1

Directory of E:\ZF440N

2022. 02. 20.  14:26    <DIR>        .
2022. 02. 20.  14:07    <DIR>        bokor
2022. 02. 20.  14:48    <DIR>        fa
                0 File(s)                0 bytes

Directory of E:\ZF440N\bokor

2022. 02. 20.  14:07    <DIR>        .
2022. 02. 20.  14:26    <DIR>        ..
2022. 02. 20.  14:45    <DIR>        banan
2022. 02. 15.  17:14    <DIR>        mogyoro
                0 File(s)                0 bytes

Directory of E:\ZF440N\bokor\banan

2022. 02. 20.  14:45    <DIR>        .
2022. 02. 20.  14:07    <DIR>        ..
2022. 02. 20.  15:02                41 leiras.txt
                1 File(s)                41 bytes

Directory of E:\ZF440N\bokor\mogyoro

2022. 02. 15.  17:14    <DIR>        .
2022. 02. 20.  14:07    <DIR>        ..
                0 File(s)                0 bytes

Directory of E:\ZF440N\fa

2022. 02. 20.  14:48    <DIR>        .
2022. 02. 20.  14:26    <DIR>        ..
2022. 02. 15.  17:14    <DIR>        barack
2022. 02. 20.  15:12                81 felsorolas.txt
2022. 02. 15.  17:15    <DIR>        kokusz
2022. 02. 15.  17:14    <DIR>        korte
                1 File(s)                81 bytes

Directory of E:\ZF440N\fa\barack

2022. 02. 15.  17:14    <DIR>        .
2022. 02. 20.  14:48    <DIR>        ..
                0 File(s)                0 bytes

Directory of E:\ZF440N\fa\barack

2022. 02. 15.  17:14    <DIR>        .
2022. 02. 20.  14:48    <DIR>        ..
                0 File(s)                0 bytes

Directory of E:\ZF440N\fa\kokusz

2022. 02. 15.  17:15    <DIR>        .
2022. 02. 20.  14:48    <DIR>        ..
                0 File(s)                0 bytes

Directory of E:\ZF440N\fa\korte

2022. 02. 15.  17:14    <DIR>        .
2022. 02. 20.  14:48    <DIR>        ..
                0 File(s)                0 bytes

Total Files Listed:
      2 File(s)                122 bytes
     22 Dir(s)  780 916 899 840 bytes free

E:\ZF440N>
```

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

```
E:\ZF440N>cd fa

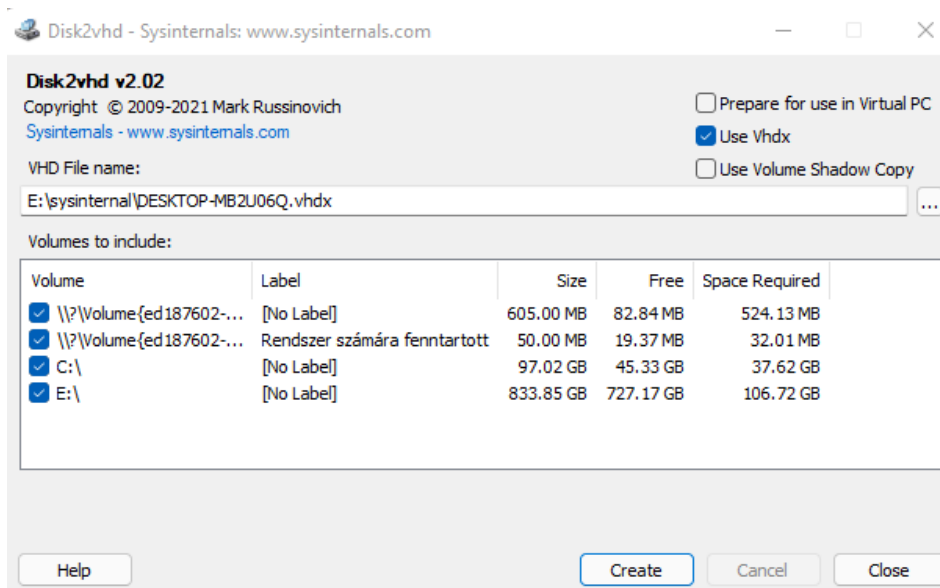
E:\ZF440N\fa>sort felsorolas.txt
Bencs Andras
Bereznai Benjamin
Drig David
Nagy Balazs
Trembeczki David

E:\ZF440N\fa>
```

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

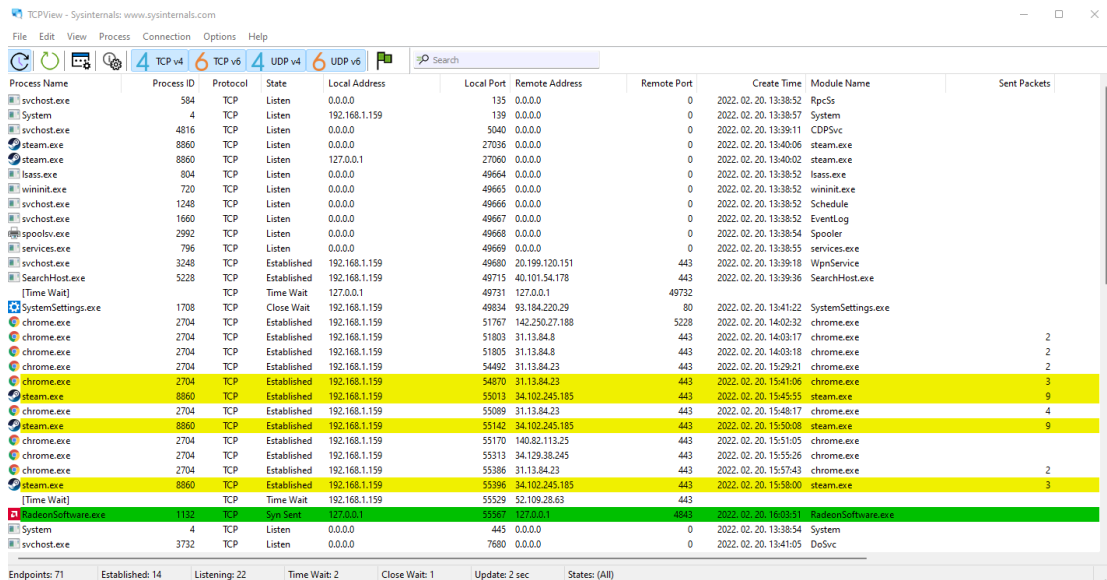
A felsorolt eszközök közül minden eszköz esetén tölts le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét - majd mentse el a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

a) File and Disk Utilities (Disk2vhd)



Leírás: Virtuális lemezeket lehet vele létrehozni.

b) Networking Utilities (TCPView)



The screenshot shows the TCPView utility window with a list of network connections. The columns include Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, Module Name, and Sent Packets. The list shows various processes like svchost.exe, System, steam.exe, chrome.exe, and SystemSettings.exe, along with their respective network activity.

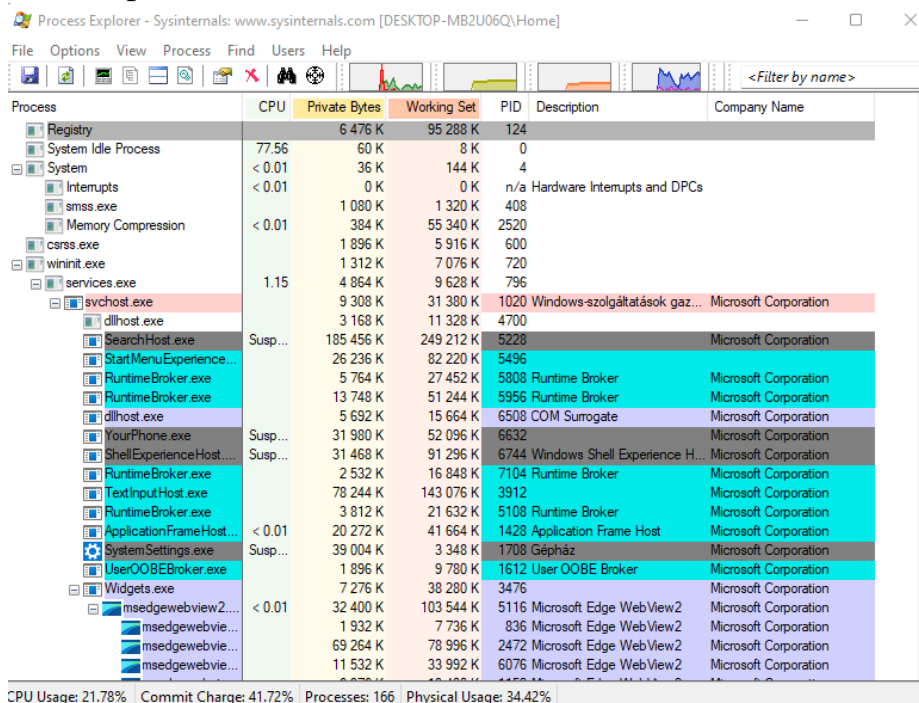
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	584	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.20.13:38:52	RpcSs	
System	4	TCP	Listen	192.168.1.159	139	0.0.0.0	0	2022.02.20.13:38:57	System	
svchost.exe	4816	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.20.13:39:11	CDPSvc	
steam.exe	8860	TCP	Listen	0.0.0.0	27036	0.0.0.0	0	2022.02.20.13:40:06	steam.exe	
steam.exe	8860	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	2022.02.20.13:40:02	steam.exe	
lsass.exe	804	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.20.13:38:52	lsass.exe	
wininit.exe	720	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.20.13:38:52	wininit.exe	
svchost.exe	1248	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.20.13:38:52	Schedule	
svchost.exe	1660	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.20.13:38:52	Eventlog	
spoolsv.exe	2992	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.20.13:38:54	Spooler	
services.exe	796	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2022.02.20.13:38:55	services.exe	
svchost.exe	3248	TCP	Established	192.168.1.159	49680	20.199.120.151	443	2022.02.20.13:39:18	WpnService	
SearchHost.exe	5228	TCP	Established	192.168.1.159	49715	40.101.54.178	443	2022.02.20.13:39:36	SearchHost.exe	
[Time Wait]		TCP	Time Wait	127.0.0.1	49731	127.0.0.1	49732			
SystemSettings.exe	1708	TCP	Close Wait	192.168.1.159	49834	93.184.220.29	80	2022.02.20.13:41:22	SystemSettings.exe	
chrome.exe	2704	TCP	Established	192.168.1.159	51767	142.250.27.188	5228	2022.02.20.14:02:32	chrome.exe	
chrome.exe	2704	TCP	Established	192.168.1.159	51803	31.13.84.8	443	2022.02.20.14:03:17	chrome.exe	2
chrome.exe	2704	TCP	Established	192.168.1.159	51805	31.13.84.8	443	2022.02.20.14:03:18	chrome.exe	2
chrome.exe	2704	TCP	Established	192.168.1.159	54492	31.13.84.23	443	2022.02.20.15:29:21	chrome.exe	2
chrome.exe	2704	TCP	Established	192.168.1.159	54970	31.13.84.23	443	2022.02.20.15:41:06	chrome.exe	3
steam.exe	8860	TCP	Established	192.168.1.159	55013	34.102.245.185	443	2022.02.20.15:45:55	steam.exe	9
chrome.exe	2704	TCP	Established	192.168.1.159	55089	31.13.84.23	443	2022.02.20.15:46:17	chrome.exe	4
steam.exe	8860	TCP	Established	192.168.1.159	55142	34.102.245.185	443	2022.02.20.15:50:08	steam.exe	9
chrome.exe	2704	TCP	Established	192.168.1.159	55170	140.82.113.25	443	2022.02.20.15:51:05	chrome.exe	
chrome.exe	2704	TCP	Established	192.168.1.159	55313	34.129.38.245	443	2022.02.20.15:55:26	chrome.exe	
chrome.exe	2704	TCP	Established	192.168.1.159	55386	31.13.84.23	443	2022.02.20.15:57:43	chrome.exe	2
steam.exe	8860	TCP	Established	192.168.1.159	55396	34.102.245.185	443	2022.02.20.15:58:00	steam.exe	3
[Time Wait]		TCP	Time Wait	127.0.0.1	55529	52.109.28.63	443			
RadeonSoftware.exe	1132	TCP	Syn Sent	127.0.0.1	55567	127.0.0.1	4843	2022.02.20.16:03:51	RadeonSoftware.exe	
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2022.02.20.13:38:54	System	
svchost.exe	3732	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	2022.02.20.13:41:05	DoSvc	

Endpoints: 71 Established: 14 Listening: 22 Time Wait: 2 Close Wait: 1 Update: 2 sec States: (All)

Leírás: Ezzel különböző programok hálózati forgalmát lehet megjeleníteni valamint, a küldött és fogadott csomagok adatmennyiségét.

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

- Process Explorer



The screenshot shows the Process Explorer utility window with a list of running processes. The columns include CPU, Private Bytes, Working Set, PID, Description, and Company Name. The list shows various processes like Registry, System Idle Process, System, Interrupts, smss.exe, Memory Compression, csrss.exe, wininit.exe, services.exe, svchost.exe, dlh.exe, SearchHost.exe, StartMenuExperienceHost.exe, RuntimeBroker.exe, dlihost.exe, YourPhone.exe, ShellExperienceHost.exe, RuntimeBroker.exe, TextInputHost.exe, ApplicationFrameHost.exe, SystemSettings.exe, UserOOBEBroker.exe, Widgets.exe, msedge.exe, and msedge.exe.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		6 476 K	95 288 K	124		
System Idle Process	77.56	60 K	8 K	0		
System	< 0.01	36 K	144 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 080 K	1 320 K	408		
Memory Compression	< 0.01	384 K	55 340 K	2520		
csrss.exe		1 896 K	5 916 K	600		
wininit.exe		1 312 K	7 076 K	720		
services.exe	1.15	4 864 K	9 628 K	796		
svchost.exe		9 308 K	31 380 K	1020	Windows-szolgáltatások gaz...	Microsoft Corporation
dlh.exe		3 168 K	11 328 K	4700		
SearchHost.exe	Susp...	185 456 K	249 212 K	5228		Microsoft Corporation
StartMenuExperienceHost.exe		26 236 K	82 220 K	5496		
RuntimeBroker.exe		5 764 K	27 452 K	5808	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		13 748 K	51 244 K	5956	Runtime Broker	Microsoft Corporation
dlihost.exe		5 692 K	15 664 K	6508	COM Surrogate	Microsoft Corporation
YourPhone.exe	Susp...	31 980 K	52 096 K	6632		Microsoft Corporation
ShellExperienceHost.exe	Susp...	31 468 K	91 296 K	6744	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2 532 K	16 848 K	7104	Runtime Broker	Microsoft Corporation
TextInputHost.exe		78 244 K	143 076 K	3912		Microsoft Corporation
RuntimeBroker.exe		3 812 K	21 632 K	5108	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe	< 0.01	20 272 K	41 664 K	1428	Application Frame Host	Microsoft Corporation
SystemSettings.exe	Susp...	39 004 K	3 348 K	1708	Gépház	Microsoft Corporation
UserOOBEBroker.exe		1 896 K	9 780 K	1612	User OOBEBroker	Microsoft Corporation
Widgets.exe		7 276 K	38 280 K	3476		Microsoft Corporation
msedge.exe	< 0.01	32 400 K	103 544 K	5116	Microsoft Edge WebView2	Microsoft Corporation
msedge.exe		1 932 K	7 736 K	836	Microsoft Edge WebView2	Microsoft Corporation
msedge.exe		69 264 K	78 996 K	2472	Microsoft Edge WebView2	Microsoft Corporation
msedge.exe		11 532 K	33 992 K	6076	Microsoft Edge WebView2	Microsoft Corporation

CPU Usage: 21.78% Commit Charge: 41.72% Processes: 166 Physical Usage: 34.42%

Leírás: A futó folyamatokat listázza, megjeleníti az erőforrások kihasználtságát, hasonlóan a Windows beépített feladatkezelőjéhez.

- Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	lsass.exe	804	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 392 640, ...
16:17:...	Explorer.EXE	5144	ReadFile	C:\Windows\System32\SHCore.dll	SUCCESS	Offset: 802 816, Le...
16:17:...	ctfmon.exe	2636	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4 186 112, ...
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	steam.exe	8860	CreateFile	E:\sysinternal\Procmon64.exe	SUCCESS	Desired Access: R...
16:17:...	steam.exe	8860	QueryInformati...	E:\sysinternal\Procmon64.exe	SUCCESS	VolumeCreationTim...
16:17:...	steam.exe	8860	QueryAllInforma...	E:\sysinternal\Procmon64.exe	BUFFER OVERFL...	CreationTime: 202...
16:17:...	steam.exe	8860	CloseFile	E:\sysinternal\Procmon64.exe	SUCCESS	
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	MsMpEng.exe	3264	Lock File	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	MsMpEng.exe	3264	Unlock File Single	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124, Length...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	MsMpEng.exe	3264	Lock File	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
16:17:...	MsMpEng.exe	3264	Unlock File Single	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124, Length...
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...
16:17:...	svchost.exe	2260	Unlock File Single	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
16:17:...	svchost.exe	2260	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:17:...	svchost.exe	2260	QueryStandar...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 4 1...

Showing 257 050 of 355 579 events (72%) Backed by virtual memory

Leírás: Hasonló a Process explorerhez annyi különbséggel, hogy egyes processek aktuális műveletét is megmutatja (read, write) és néhány részletet is elárul a processzről.

- AutoRuns

AutoRuns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

Autonuns Entry	Description	Publisher	Image Path	Timestamp
Logon				
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Microsoft Teams	(Verified) Microsoft 3rd Party Appl...	C:\Users\Home\AppData\Local\Microsoft\Teams\Update.exe	Thu Feb 17 17:50:19 2022
com.apple.Teams.Teams	Update	(Verified) Discord Inc.	C:\Users\Home\AppData\Local\Discord\Update.exe	Sun Feb 13 12:05:12 2022
Discord	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\OneDrive.exe	Tue Sep 21 19:16:42 2021
OneDrive	qBittorrent - A BitTorrent Client	(Not Verified) The qBittorrent Proj...	C:\Program Files\qBittorrent\qBittorrent.exe	Thu Feb 17 17:04:04 2022
qBittorrent	Steam	(Verified) Valve Corp.	C:\Program Files (x86)\Steam\steam.exe	Thu Jan 6 20:07:20 2022
Steam	Realtek HD Audio Manager	(Verified) Realtek Semiconductor ...	C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe	Sun Jan 16 18:41:26 2022
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Realtek HD Audio Manager	(Verified) Realtek Semiconductor ...	C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe	Sun Feb 13 12:42:55 2022
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Thu Jan 20 20:12:26 2022
cmd.exe	Google Chrome	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\98.0.4758.102\Install...	Sat Jun 5 14:10:40 2021
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.56\Install...	Sat Jun 5 14:04:59 2021
Google Chrome	Microsoft .NET 4.5.2 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscorres.dll	Sun Feb 6 19:40:17 2022
Microsoft Edge	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Thu Feb 17 17:49:24 2022
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	Microsoft Teams	(Verified) Microsoft Corporation	C:\Program Files (x86)\Teams\Installer\Teams.exe	Sun Feb 13 14:52:22 2022
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	Microsoft Teams	(Verified) Microsoft Corporation	C:\Program Files (x86)\Teams\Installer\Teams.exe	Sat Jun 5 19:53:36 2021
TeamsMachineInstaller	Microsoft .NET 4.5.2 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscorres.dll	Sat Feb 12 19:06:35 2022
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	Microsoft .NET 4.5.2 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscorres.dll	Wed Dec 15 12:36:42 2021
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	Microsoft .NET 4.5.2 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscorres.dll	Wed Aug 18 01:45:00 2021
Explorer	Microsoft .NET 4.5.2 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscorres.dll	Sat Jun 5 19:53:36 2021
HKLM\SOFTWARE\Classes\Protocols\Filter	Microsoft .NET 4.5.2 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscorres.dll	Sat Feb 12 17:36:50 2022

Scanning Codes... Done Press ESC to Cancel

Leírás: A Windows által automatikusan indított alkalmazásokat mutatja meg kategorizálva.

d) Security Utilities (LogonSession)

```
E:\sysinternal>logonsessions.exe

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

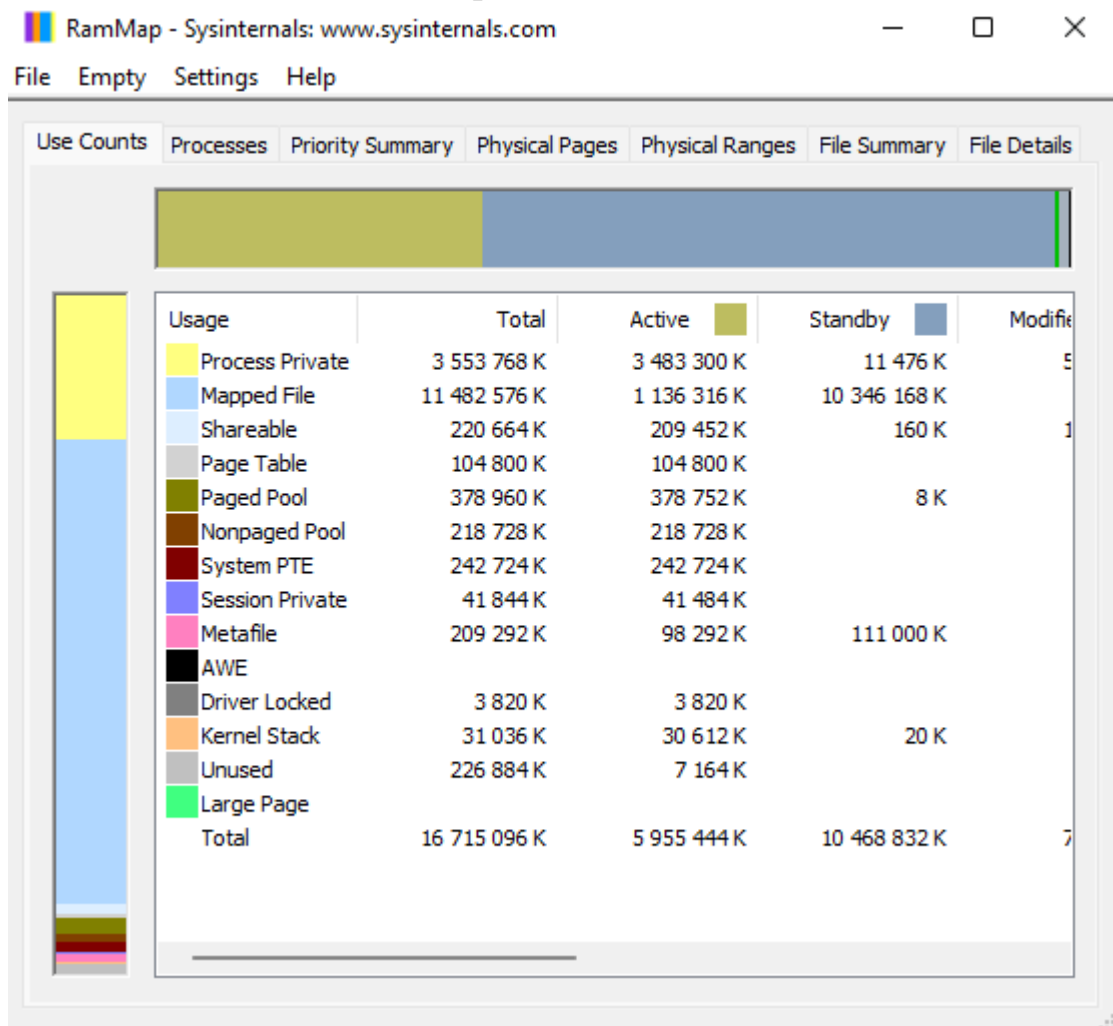
[0] Logon session 00000000:000003e7:
    User name:      WORKGROUP\DESKTOP-MB2U06Q$
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            S-1-5-18
    Logon time:     2022. 02. 20. 13:38:52
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000aa43:
    User name:
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            (none)
    Logon time:     2022. 02. 20. 13:38:52
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:0000b200:
    User name:      Font Driver Host\UMFD-1
    Auth package:   Negotiate
    Logon type:     Interactive
    Session:        1
    Sid:            S-1-5-96-0-1
    Logon time:     2022. 02. 20. 13:38:52
    Logon server:
    DNS Domain:
    UPN:
```

Leírás: A windowsba való belépés időpontját jeleníti meg.

e) Information Utilities (RAMMap)



Leírás: Megvizsgálja, hogy a felhasznált memóriamennyiség hogyan oszlik el. Megjeleníthető vele hogy, egyes folyamatok mennyi memóriát használnak fel.

3. Töltse le a következő programot: Dependency Walker.

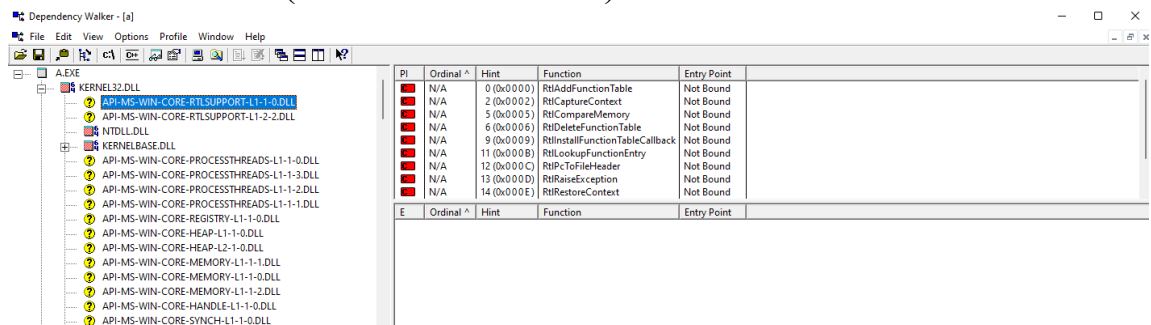
Feladata: a segédprogram megvizsgálja milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program. Készítsen egy neptunkod.c nevű forráskódot, amely egy vezeteknev.txt fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc. Fordítsa le a kódot a C fordító, majd tegye futtathatóvá az állományt: neptunkod.exe A Dependency Walker segítségével végezze el a következő feladatokat.

Nyissa meg a neptunkod.exe fájlt!

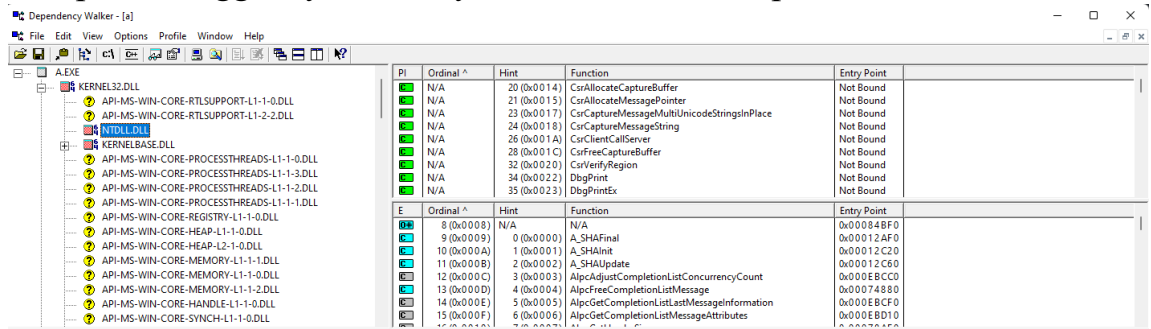
ZF440N.C file

```
C ZF440N.c • korad.txt
C > C ZF440N.c
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main()
5  {
6
7      FILE *fp;
8      fp = fopen("korad.txt", "w");
9      fprintf(fp, "Kórád György, Programtervező Informatikus, ZF440N");
10     fclose(fp);
11     system("pause");
12
13     return 0;
14 }
```

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



Name	Ordinal	Hint	Function	Entry Point
CsrAllocateCaptureBuffer	20 (0x0014)		CsrAllocateCaptureBuffer	Not Bound
CsrAllocateMessagePointer	21 (0x0015)		CsrAllocateMessagePointer	Not Bound
CsrCaptureMessageMultiUnicodeStringsInPlace	23 (0x0017)		CsrCaptureMessageMultiUnicodeStringsInPlace	Not Bound
CsrCaptureMessageString	24 (0x0018)		CsrCaptureMessageString	Not Bound
CsrClientCallServer	26 (0x001A)		CsrClientCallServer	Not Bound
CsrFreeCaptureBuffer	28 (0x001C)		CsrFreeCaptureBuffer	Not Bound
CsrVerifyRegion	32 (0x0020)		CsrVerifyRegion	Not Bound
DbgPrint	34 (0x0022)		DbgPrint	Not Bound
DbgPrintEx	35 (0x0023)		DbgPrintEx	Not Bound
A_SHAFinal	8 (0x0008)	N/A	A_SHAFinal	0x00084BF0
A_SHALink	9 (0x0009)	0 (0x0000)	A_SHALink	0x00012AF0
A_SHALink	10 (0x000A)	1 (0x0001)	A_SHALink	0x00012C20
A_SHALink	11 (0x000B)	2 (0x0002)	A_SHALink	0x00012C60
AlpcAdjustCompletionListConcurrencyCount	12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000EBC00
AlpcFreeCompletionListMessage	13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage	0x00074880
AlpcGetCompletionListLastMessageInformation	14 (0x000E)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation	0x000EBCF0
AlpcGetCompletionListMessageAttributes	15 (0x000F)	6 (0x0006)	AlpcGetCompletionListMessageAttributes	0x000EBD10

A windows telépitésekor jön létre, kernel funkciókat tartalmaz, így elengedhetetlen a rendszer helyes működéséhez.