

Operációs rendszerek

2.Gyakorlat

2025.02.26.

Készítette:

Orosz Kristóf Bsc

Szak: Programtervező Informatikus

Neptunkód: EYZWG9

Sárospatak, 2025

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

a.) Hozza létre a következő mappa szerkezetet! Karakteres felületen végezze el a következő műveleteket!

```
C:\eyzwg9> TREE
Folder PATH listing for volume OS
Volume serial number is B219-AE2C
C:..
|_bokor
|   |_banan
|   |_barack
|   |_mogyoro
|_fa
|   |_korte
|_land
|   |_kokusz
|   |_szeder
```

b.) Karakteres felületen készítsen másolatot:

- a neptunkod\land\szeder katalógusról a neptunkod\fa katalógusba.

```
C:\eyzwg9>robocopy "C:\eyzwg9\land\szeder" "C:\eyzwg9\fa\szeder" /E
```

```
C:\eyzwg9>TREE
Folder PATH listing for volume OS
Volume serial number is B219-AE2C
C:..
|_bokor
|   |_banan
|   |_barack
|   |_mogyoro
|_fa
|   |_korte
|   |_szeder
|_land
|   |_kokusz
|   |_szeder
```

A mappa másolást a **szeder** katalógusról a **fa** katalógusba a **robocopy** paranccsal valósítottam meg, mivel üres mappákat másoltam.

- a neptunkod \bokor\banan katalógusról a neptunkod \fa katalógusba.

```
C:\eyzwg9>robocopy "C:\eyzwg9\bokor\banan" "C:\eyzwg9\fa\banan" /E
```

```
C:\eyzwg9>tree
Folder PATH listing for volume OS
Volume serial number is B219-AE2C
C:..
|_ bokor
|   |_ banan
|   |_ barack
|   |_ mogyoro
|_ fa
|   |_ banan
|   |_ korte
|   |_ szeder
|_ land
|   |_ kokusz
|   |_ szeder
```

A mappa másolást a **banan** katalógusról a **fa** katalógusba a **robocopy** paranccsal valósítottam meg, mivel üres mappákat másoltam.

c.) Karakteres felületen végezze el a következő áthelyezéseket:

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

```
C:\eyzwg9>move "C:\eyzwg9\bokor\barack" "C:\eyzwg9\fa\"
1 dir(s) moved.
```

```
C:\eyzwg9>TREE
Folder PATH listing for volume OS
Volume serial number is B219-AE2C
C:..
|_ bokor
|   |_ banan
|   |_ mogyoro
|_ fa
|   |_ banan
|   |_ barack
|   |_ korte
|   |_ szeder
|_ land
|   |_ kokusz
|   |_ szeder
```

A **barack** katalógus áthelyezését a **fa** katalógusba a **move** paranccsal valósítottam meg.

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

```
C:\eyzwg9>move "C:\eyzwg9\land\kokusz" "C:\eyzwg9\fa\  
1 dir(s) moved.
```

```
C:\eyzwg9>TREE  
Folder PATH listing for volume OS  
Volume serial number is B219-AE2C  
C:.  
├── bokor  
│   ├── banan  
│   └── mogyoro  
├── fa  
│   ├── banan  
│   ├── barack  
│   ├── kokusz  
│   ├── korte  
│   └── szeder  
└── land  
    └── szeder
```

A **kokusz** katalógus áthelyezését a **fa** katalógusba a **move** paranccsal valósítottam meg.

d.) Karakteres felületen törölje a neptunkod\land katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:

```
C:\eyzwg9>rmdir land
```

```
C:\eyzwg9>TREE  
Folder PATH listing for volume OS  
Volume serial number is B219-AE2C  
C:.  
├── bokor  
│   ├── banan  
│   └── mogyoro  
├── fa  
│   ├── banan  
│   ├── barack  
│   ├── kokusz  
│   ├── korte  
│   └── szeder
```

A **land** katalógust a teljes tartalmával együtt a **rmdir** paranccsal töröltem ki.

- neptunkod\bokor\banan\leiras.txt

```
C:\eyzwg9\bokor\banan> copy con leiras.txt
^Z
1 file(s) copied.
```

```
C:\eyzwg9>TREE /F
Folder PATH listing for volume OS
Volume serial number is B219-AE2C
C:.
|
|-- bokor
|   |-- banan
|       leiras.txt
|   |-- mogyoro
|
|-- fa
|   |-- banan
|   |-- barack
|   |-- kokusz
|   |-- korte
|   |-- szeder
|
|-- tree
```

A **leiras.txt** fájlt a **copy con** paranccsal tudtam létrehozni.

- neptunkod\tree\felsorolas.txt

```
C:\eyzwg9\tree> copy con felsorolas.txt
^Z
1 file(s) copied.
```

```
C:\eyzwg9>TREE /F
Folder PATH listing for volume OS
Volume serial number is B219-AE2C
C:.
|
|-- bokor
|   |-- banan
|       leiras.txt
|   |-- mogyoro
|
|-- fa
|   |-- banan
|   |-- barack
|   |-- kokusz
|   |-- korte
|   |-- szeder
|
|-- tree
    felsorolas.txt
```

A **felsorolas.txt** fájlt a **copy con** paranccsal tudtam létrehozni.

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

A **felsorolas** szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
C:\eyzwg9\bokor\banan> notepad leiras.txt

C:\eyzwg9\bokor\banan>type C:\eyzwg9\bokor\banan\leiras.txt
Barack
Barack
Barack
```

Ezt a feladatot a **notepad** paranccsal valósítottam meg.

```
C:\eyzwg9\tree>notepad felsorolas.txt

C:\eyzwg9\tree>type C:\eyzwg9\tree\felsorolas.txt
Adam
Gergo
Damjan
```

Ezt a feladatot a **notepad** paranccsal valósítottam meg.

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

```
C:\eyzwg9>TREE /F
Folder PATH listing for volume OS
Volume serial number is B219-AE2C
C:
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── tree
    └── felsorolas.txt
```

Ezt a feladatot a **TREE /F** paranccsal valósítottam meg. A **/F** részre azért volt szükség, mert így a teljes mappaszerkezetet kilistázta.

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

```
C:\eyzwg9> dir /S /B "C:\eyzwg9\?e*.txt"
C:\eyzwg9\bokor\banan\leiras.txt
C:\eyzwg9\tree\felsorolas.txt
```

Ezt a feladatot a **dir /S /B „C:\eyzwg9\?e*.txt”** paranccsal tudtam megvalósítani.

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



Ebben az esetben a **felsorolas.txt** fájl elérési útvonalának megadása után egy **/grant Everyone :R** paranccsal lehet mindenki számára elérhetővé tenni a fájlt.

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

```
C:\eyzwg9> dir "C:\eyzwg9" /S
Volume in drive C is OS
Volume Serial Number is B219-AE2C
```

```
Total Files Listed:
      2 File(s)           50 bytes
     37 Dir(s)  273 076 486 144 bytes free
```

Ezt a **dir** paranccsal lehet megoldani, amely során az elérési útvonal megadása után „**C:\eyzwg9**” **/S** parancsot adtam meg, ahol a **/S** azt a célt szolgálja, hogy minden mappa, almappa, és a benne lévő fájlok megjelenjenek.

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

```
C:\eyzwg9\tree> sort felsorolas.txt
Adam
Damjan
Gergo
```

Ezt a feladatot a **sort** paranccsal egyszerűen meglehet valósítani, amely során a fájlban lévő szövegek **ABC** sorrendbe rendeződnek.

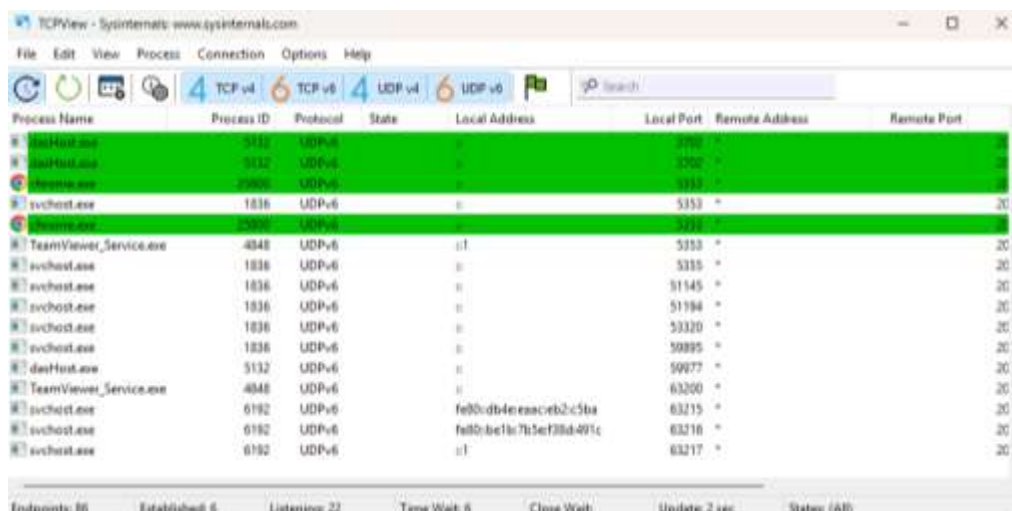
2.feladat

Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít. <https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite>

A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

a) **File and Disk Utilities (Disk2vhd)**

b) **Networking Utilities (TCPView)**

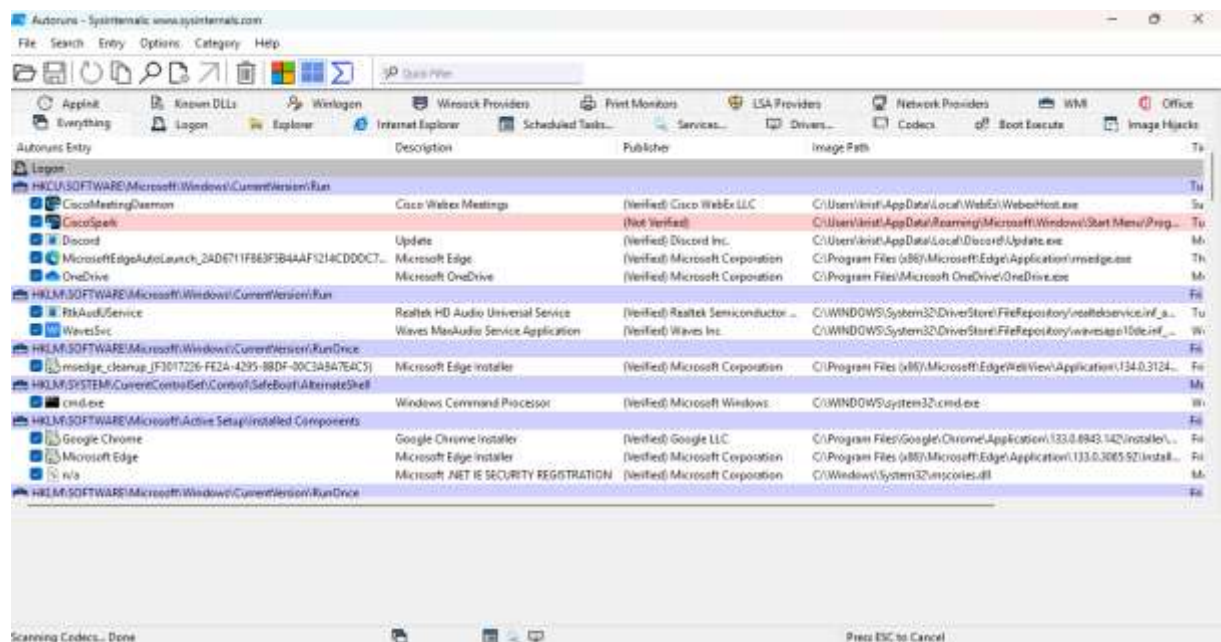


The screenshot shows the TCPView application window from Sysinternals. The window title is 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes File, Edit, View, Process, Connection, Options, and Help. The toolbar has icons for refreshing, pausing, and searching, along with filters for TCP v4, TCP v6, UDP v4, and UDP v6. A search bar is also present. The main table displays network connections with columns: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, and Remote Port. Several rows are highlighted in green, indicating new connections. The status bar at the bottom shows: Endpoints: 88, Established: 6, Listening: 22, Time Wait: 6, Close Wait: 0, Update: 2 sec, Status: (All).

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
svchost.exe	5112	UDPv6		*	3760	*	20
svchost.exe	5112	UDPv6		*	3760	*	20
svchost.exe	25800	UDPv6		*	5353	*	20
svchost.exe	1836	UDPv6		*	5353	*	20
svchost.exe	25800	UDPv6		*	5353	*	20
TeamViewer_Service.exe	4048	UDPv6		*	5353	*	20
svchost.exe	1836	UDPv6		*	5353	*	20
svchost.exe	1836	UDPv6		*	51545	*	20
svchost.exe	1836	UDPv6		*	51794	*	20
svchost.exe	1836	UDPv6		*	53320	*	20
svchost.exe	1836	UDPv6		*	59895	*	20
svchost.exe	1836	UDPv6		*	59895	*	20
svchost.exe	5132	UDPv6		*	59877	*	20
TeamViewer_Service.exe	4048	UDPv6		*	63200	*	20
svchost.exe	6192	UDPv6		fe80::db4e::eac::eb2::c5ba	63215	*	20
svchost.exe	6192	UDPv6		fe80::db4e::eac::eb2::c5ba	63216	*	20
svchost.exe	6192	UDPv6		*	63217	*	20

Ez a **TCPView** ablak, amely a Windows rendszeren futó folyamatok hálózati kapcsolatainak listáját mutatja. A listában szerepel a folyamat neve, azonosítója, a használt protokoll, valamint a helyi és távoli IP-címek és portok. A zöld szín azt jelzi, hogy az adott kapcsolat vagy folyamat újonnan jelent meg a listában. Így könnyen nyomon követhető, hogy mely alkalmazások kapcsolódnak az internetre, illetve milyen portokat használnak azok.

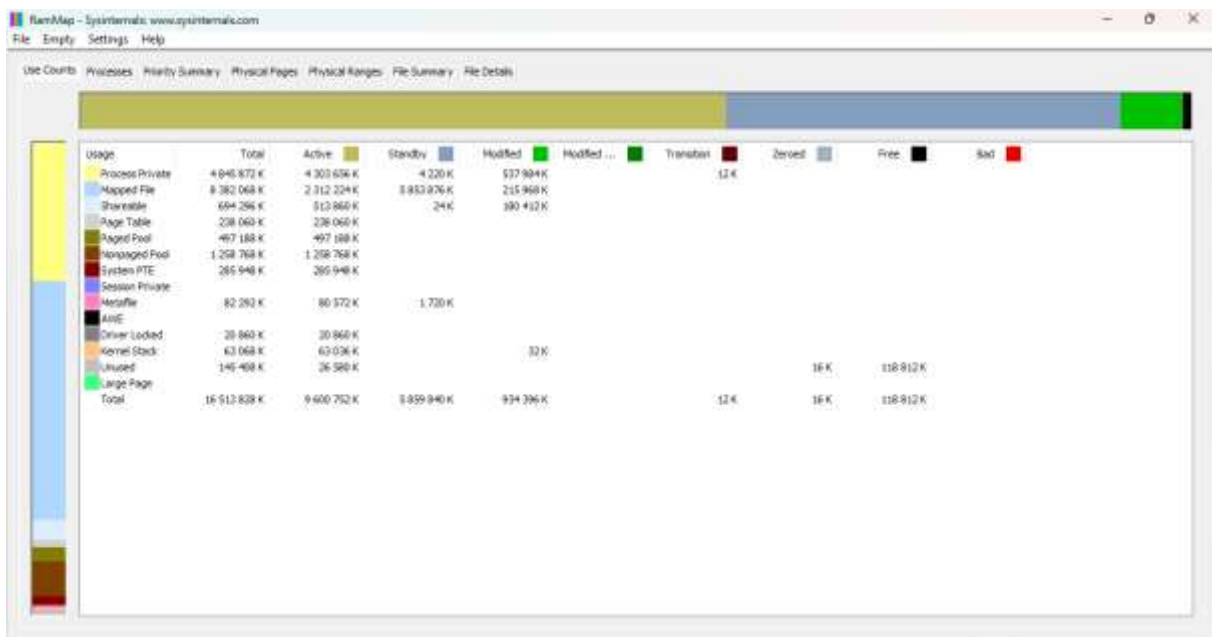
AutoRuns



Ez az **Autoruns** alkalmazás, amely megmutatja a Windows rendszer indulásakor automatikusan futó programokat, szolgáltatásokat és bejegyzéseket. A listában látható, hogy melyik elem honnan illetve ki a kiadója, és pontosan hol található a futtatható fájl.

d) Security Utilities (LogonSession)

d) Information Utilities (RAMMap)



Ez a **RAMMap** alkalmazás, amely a rendszerben lévő fizikai memória (RAM) felhasználását mutatja részletesen. A felső sáv színekkel jelöli a memória különböző állapotait a táblázatban pedig látható, hogy pontosan mennyi RAM-ot használ el a rendszer és a különböző folyamatok.

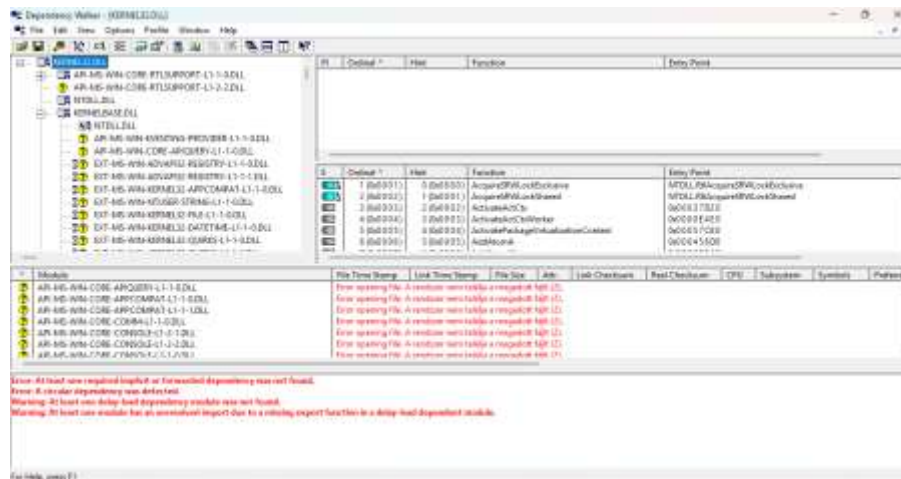
3.feladat

3. Töltse le a következő programot: Dependency Walker URL: <http://www.dependencywalker.com/>
Feladata: a segédprogram megvizsgálja milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program. „Készítsen egy neptunkod.c nevű forráskódot, amely egy neptunkod.txt fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc. -sortörés.Fordítsa le kódot, majd tegye futtathatóvá az állományt: neptunkod.exe

A Dependency Walker segítségével végezze el a következő feladatokat.

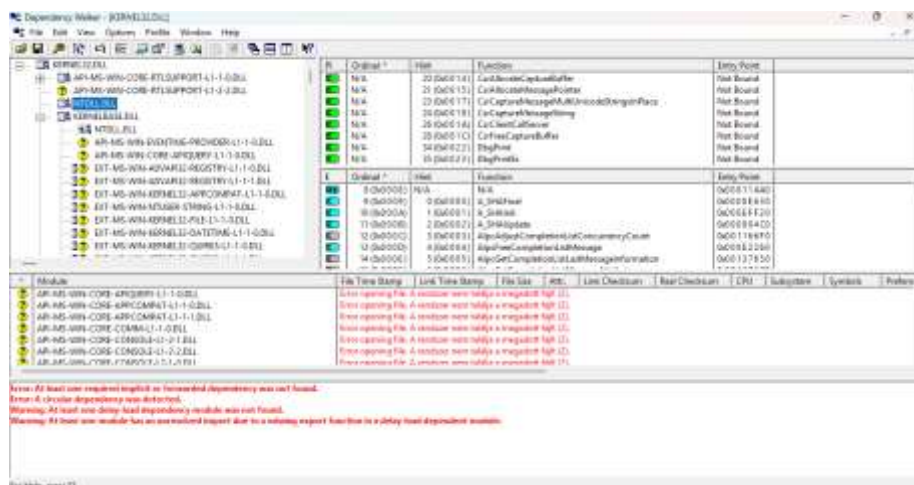
Nyissa meg a neptunkod.exe fájlt!

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



AZ eyzwg9.exe sokfajta API hívásokat használ a kernel32.dll-ből. Ezek a képernyő jobb oldalán látszódnak. Ilyen például a DeactivateActCtxA, vagy a ActivateActCtx.

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** a Windows NT-alapú rendszerek legalacsonyabb szintű könyvtára, amely az úgynevezett Native API függvényeit tartalmazza. Ezek a függvények például NtCreateFile, vagy a NtQuerySystemInformation.