

Operációs Rendszerek BSc

2. Gyak.

2022.02.15

Készítette:

Tóth Dániel Márk BSc

Mérnökinformatika

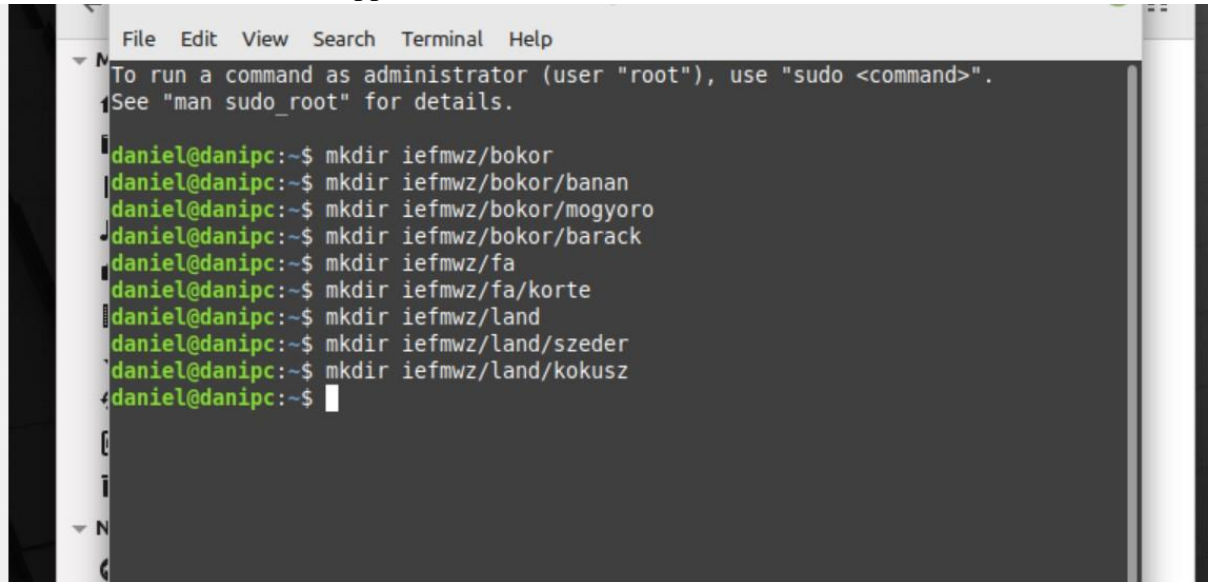
IEFMWZ

Miskolc, 2022

1. Feladat - Készítse el a következő feladatokat!

Az elvégzett feladatokról készítsen (a.)-j.)-ig.) képernyőképet, majd illessze be a jegyzőkönyvbe.

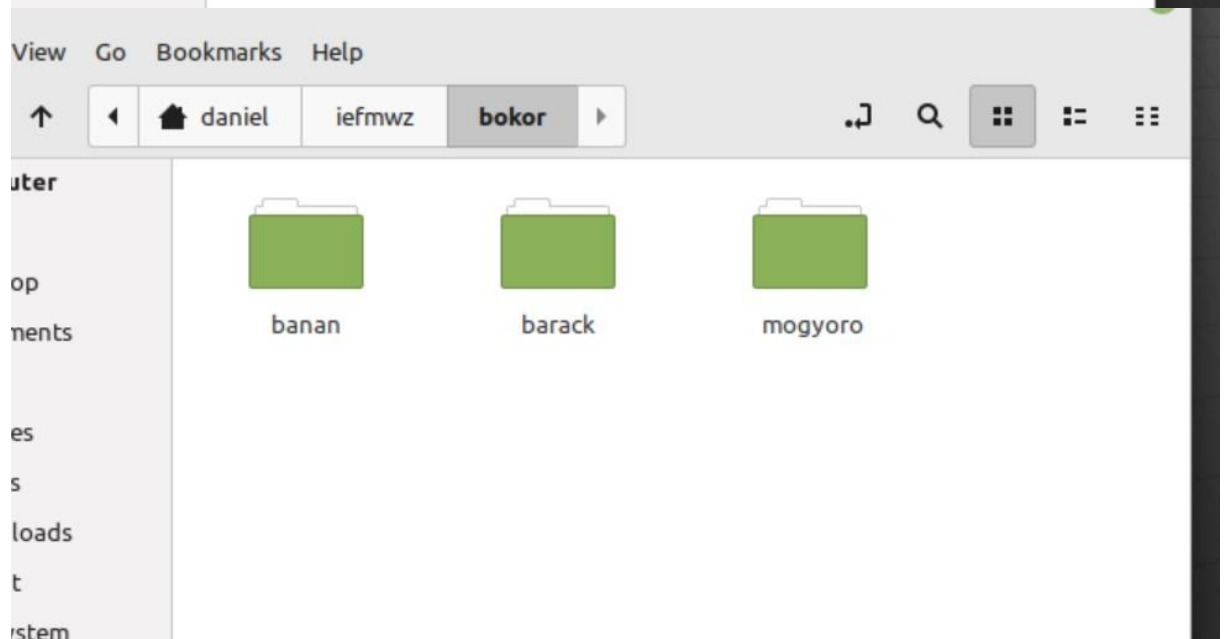
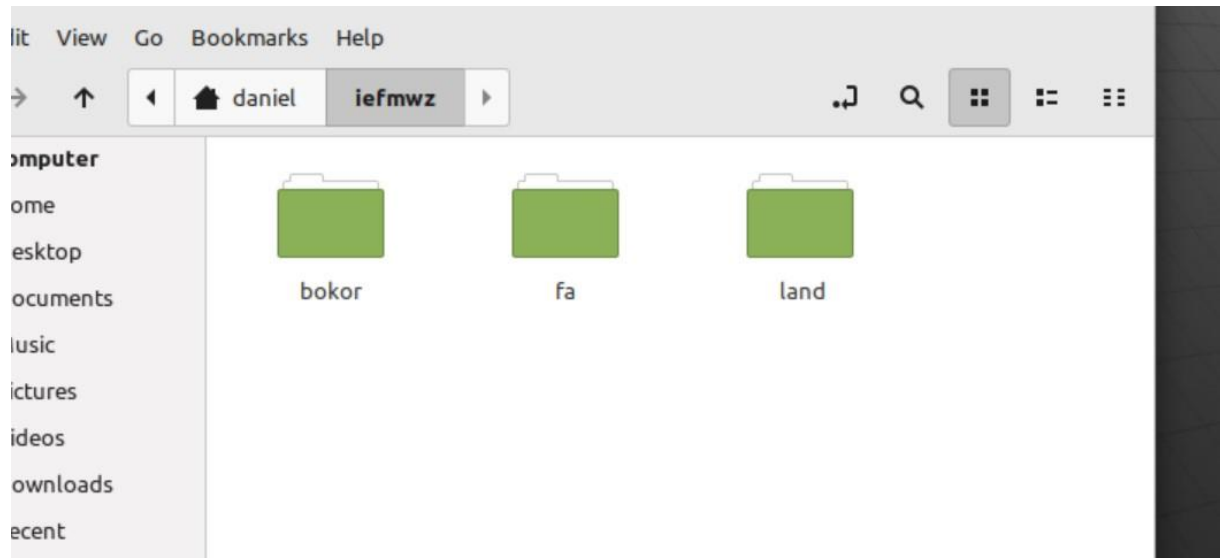
a.) Hozza létre a következő mappa szerkezetet!

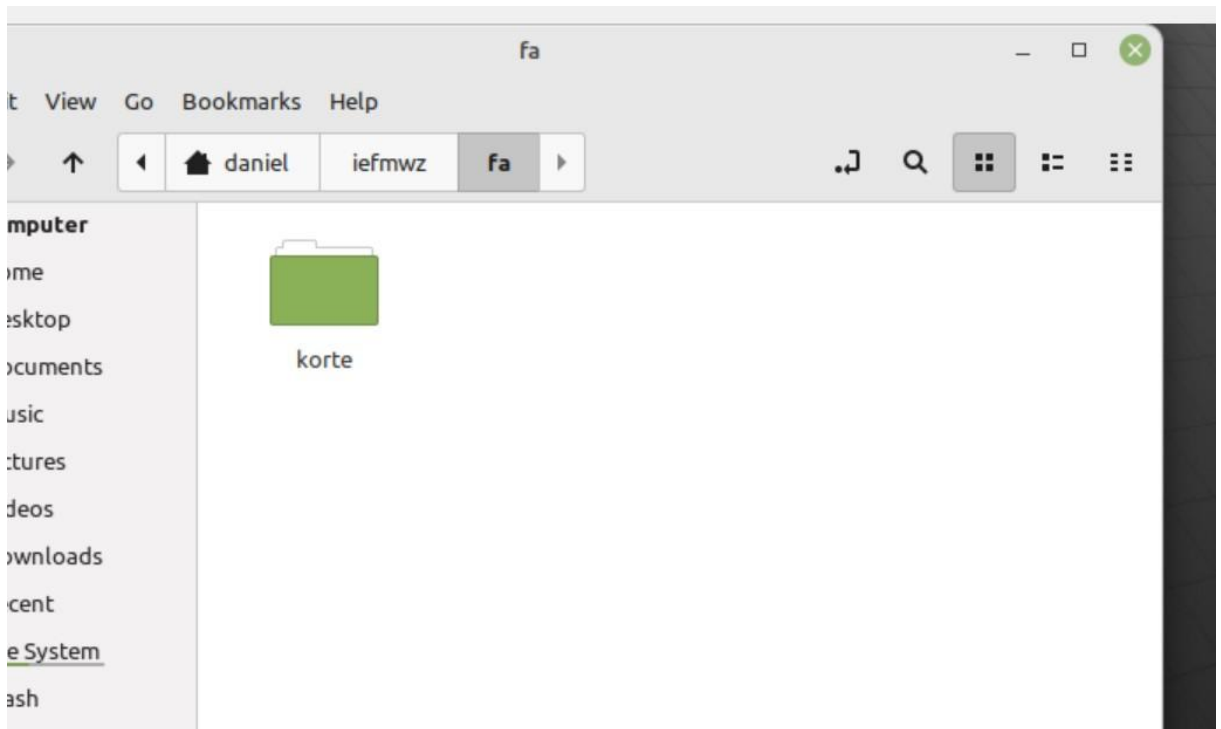
A screenshot of a Linux terminal window. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output shows a series of 'mkdir' commands being executed by a user named 'daniel' on a machine named 'danipc'. The commands create a hierarchical directory structure: 'iefmwz/bokor', 'iefmwz/bokor/banan', 'iefmwz/bokor/mogyoro', 'iefmwz/bokor/barack', 'iefmwz/fa', 'iefmwz/fa/korte', 'iefmwz/land', 'iefmwz/land/szeder', and 'iefmwz/land/kokusz'. The prompt 'daniel@danipc:~\$' is visible at the end of each command line. The terminal background is dark, and the text is light green.

```
File Edit View Search Terminal Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

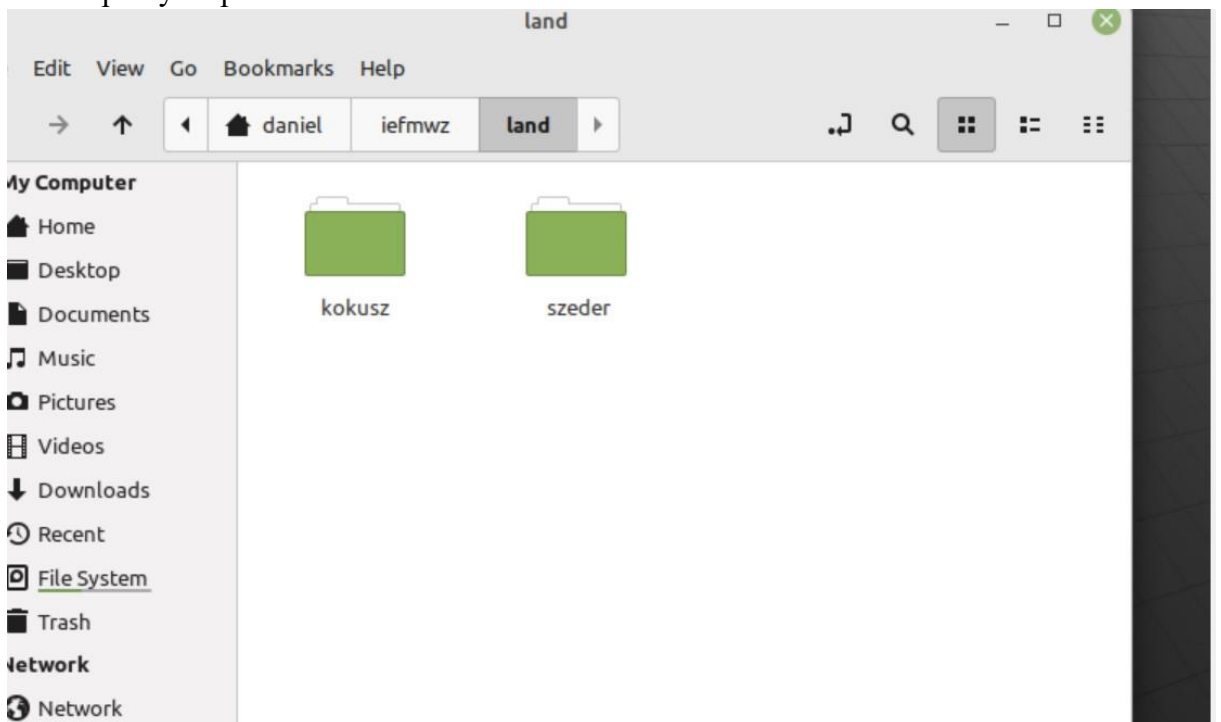
daniel@danipc:~$ mkdir iefmwz/bokor
daniel@danipc:~$ mkdir iefmwz/bokor/banan
daniel@danipc:~$ mkdir iefmwz/bokor/mogyoro
daniel@danipc:~$ mkdir iefmwz/bokor/barack
daniel@danipc:~$ mkdir iefmwz/fa
daniel@danipc:~$ mkdir iefmwz/fa/korte
daniel@danipc:~$ mkdir iefmwz/land
daniel@danipc:~$ mkdir iefmwz/land/szeder
daniel@danipc:~$ mkdir iefmwz/land/kokusz
daniel@danipc:~$
```

Itt látható a Linux parancs sorok, ahogyan létrehoztam a könyvtárakat. Alul pedig a végeredmények láthatóak a fájlkezelő programban.

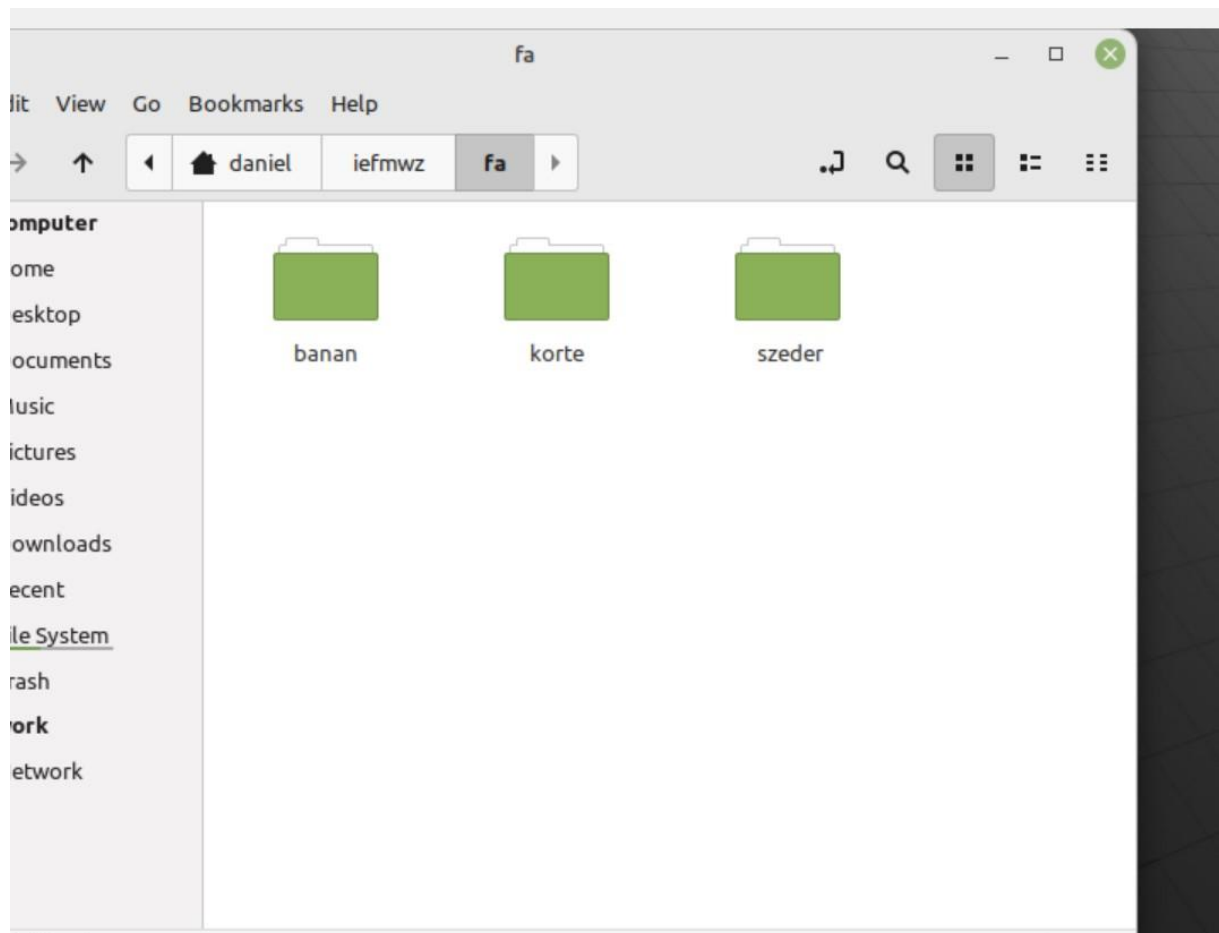




b.) A feladat leírása szerint másolatot kellett készítenem kettő almappáról. Az eredmény a lenti képernyőképen látható.



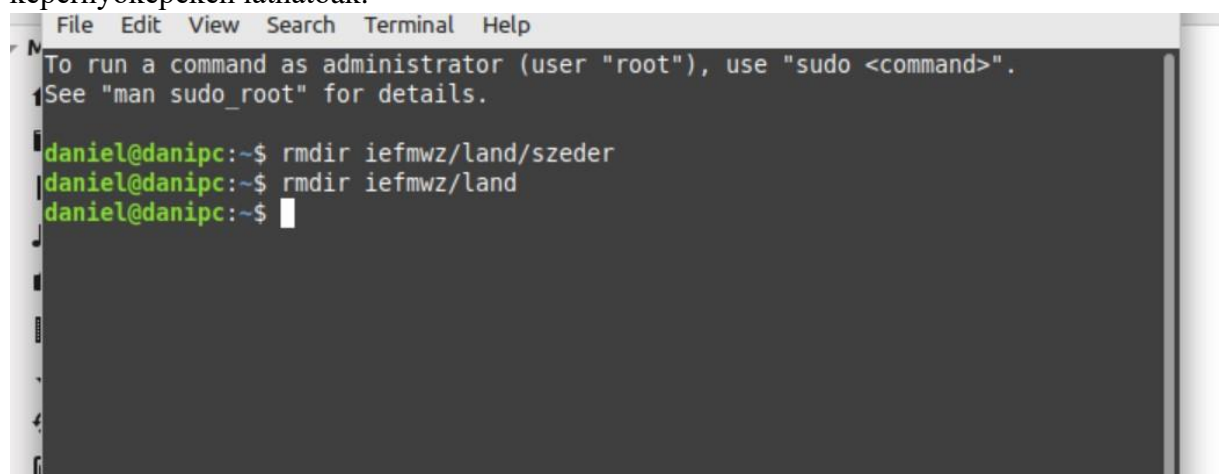
c.) A feladat leírása szerint 2 áthelyezést kellett végezni 2 almappán. Az eredmény a lenti képernyőképen látható.



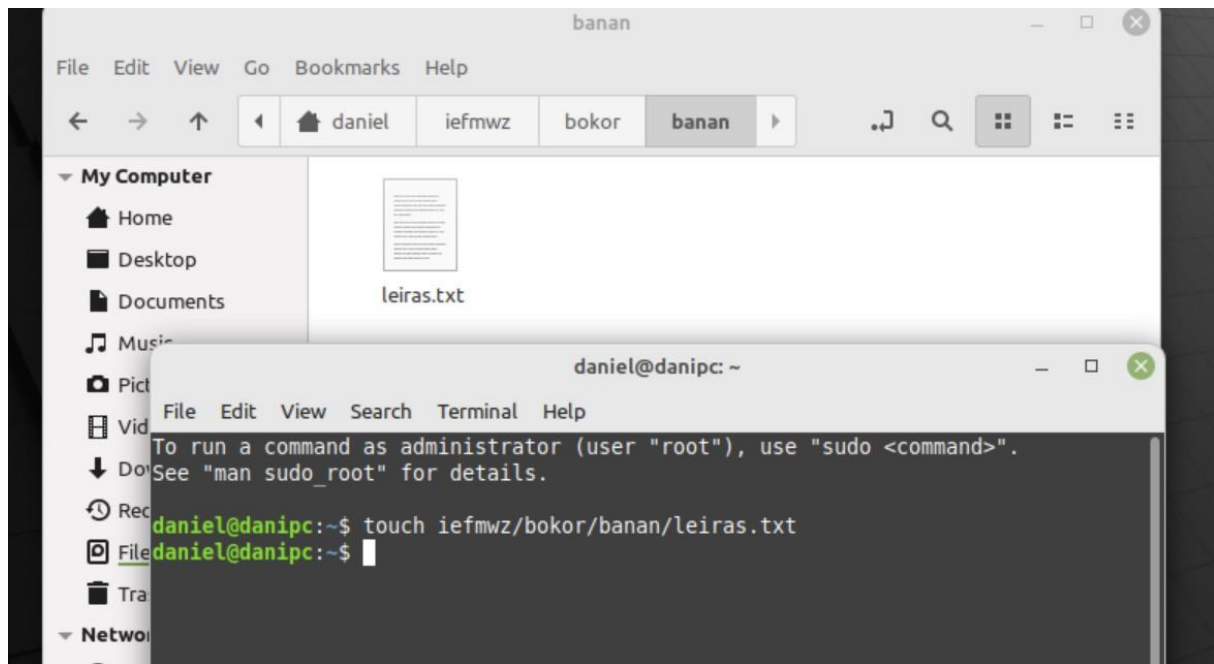
d.) A feladat leírása szerint törölnöm kellett a land mappa teljes tartalmát, majd a

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

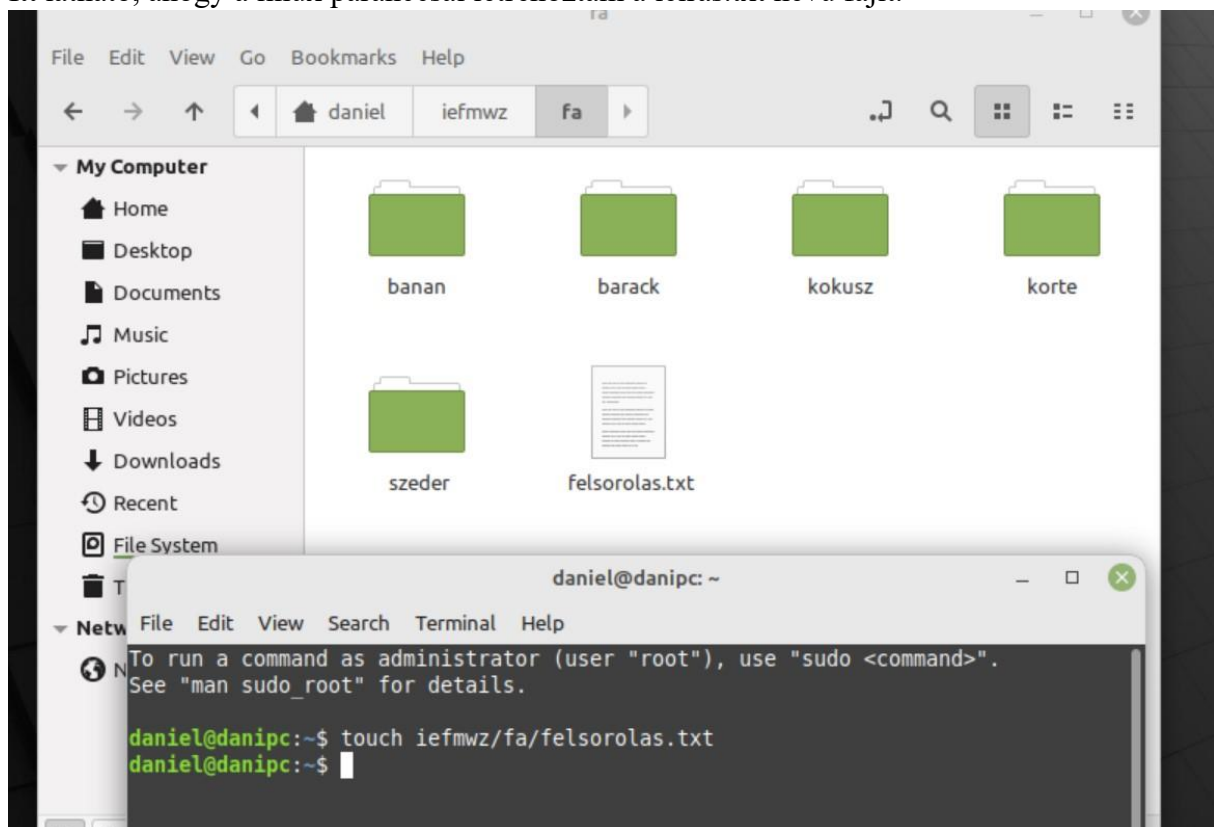
fájlokat kellett létrehoznom. A parancs sorok és az eredmények a lenti képernyőképeken láthatóak.



Itt látható, ahogyan ezekkel a parancsokkal töröltem a land mappát a benne lévő almappákkal.



Itt látható, ahogy a linux paranccsal létrehoztam a leiras.txt nevű fájlt.

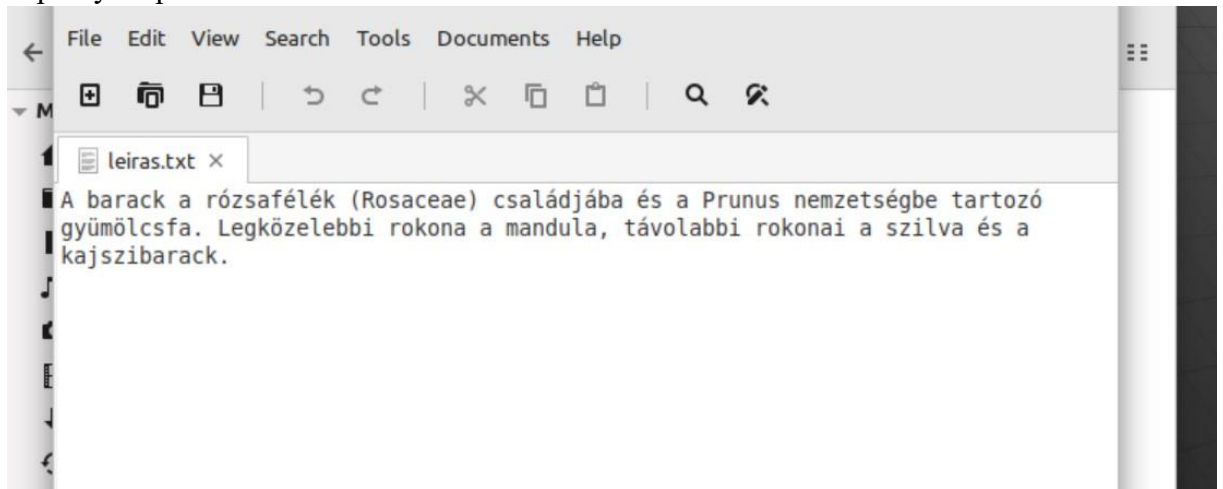


Itt pedig látható, ahogyan létrehoztam a felsorolas.txt-t Linux parancsokkal.

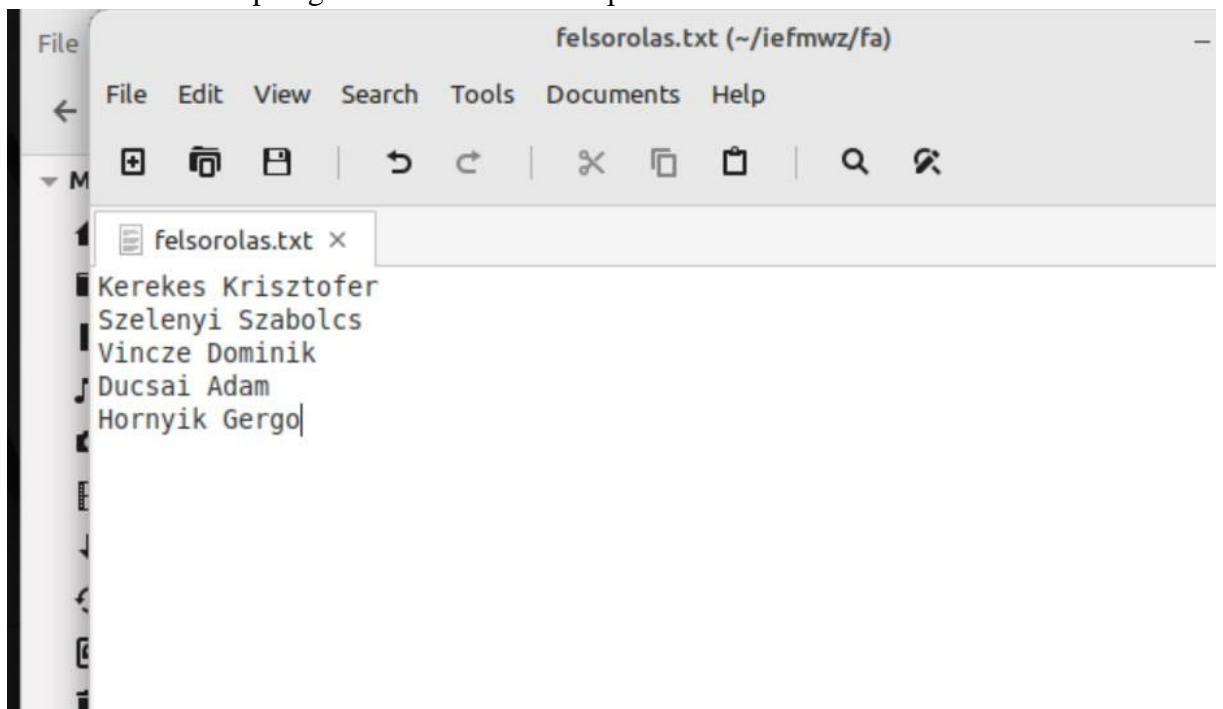
e.) A leiras.txt szöveges állományba írjon 3 sort a barackról.

A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

A leiras.txt fájlba beleillesztettem 3 sornyi adatot a barackról. Az eredmény a képernyőképen látható.



A felsorolas.txt-be pedig beleillesztettem 5 csoport társam nevét.



f.) Listázza a neptunkod mappa tartalmát úgy, hogy megjelenjen az almappák tartalma. Miután beírtam az adott parancsot, ez az eredmény fogadott, ami a lenti képernyőképen látható. Látszik a minden egyes mappa, és a benne lévő almappák, esetleg fájlok nevei, elhelyezései.

```
daniel@danipc:~$ ls -R iefmwz
iefmwz:
bokor fa

iefmwz/bokor:
banan mogyoro

iefmwz/bokor/banan:
leiras.txt

iefmwz/bokor/mogyoro:

iefmwz/fa:
banan barack felsorolas.txt kokusz korte szeder

iefmwz/fa/banan:
iefmwz/fa/barack:
iefmwz/fa/kokusz:
iefmwz/fa/korte:
iefmwz/fa/szeder:
daniel@danipc:~$
```

"bokor" selected (containing 2 items), Free space: 11,3 GB

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

Miután a feladat megoldásához szükséges Linux parancsot beírtam, sikeresen olvashatóvá tettem a felsorolas.txt fájlt az összes felhasználó számára. A kód, amit használtam itt van a lenti képernyőképen.

```
iefmwz/fa/korte:
iefmwz/fa/szeder:
daniel@danipc:~$ chmod +r iefmwz/fa/felsorolas.txt
daniel@danipc:~$
```

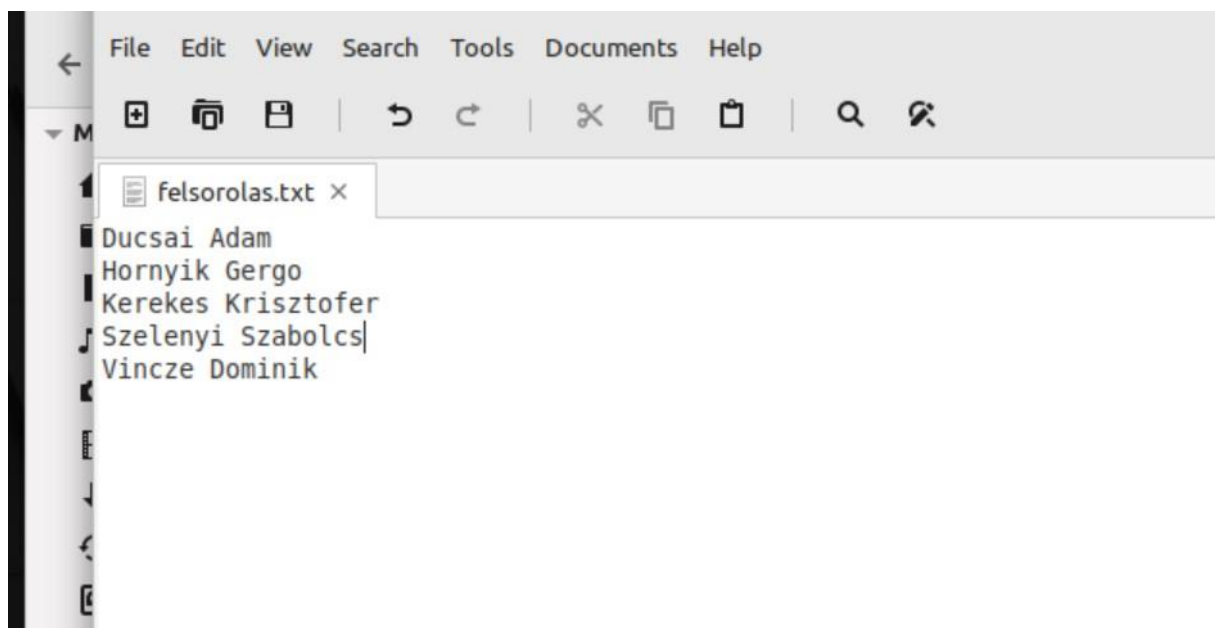
i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezén a neptunkod mappa az almappjaival együtt.

A Linux parancs beírása után ez az eredmény fogadott. Látható, hogy bal oldalt kiírja minden egyes almappjának a tárhely igényét, továbbá legalul, pontosabban az utolsó sorban pedig maga az iefmwz mappa mennyi helyet foglal el.


```
98M
daniel@danipc:~$ du -h iefmwz
4,0K    iefmwz/fa/banan
4,0K    iefmwz/fa/korte
4,0K    iefmwz/fa/kokusz
4,0K    iefmwz/fa/szeder
4,0K    iefmwz/fa/barack
28K     iefmwz/fa
8,0K    iefmwz/bokor/banan
4,0K    iefmwz/bokor/mogyoro
16K     iefmwz/bokor
48K     iefmwz
daniel@danipc:~$
```

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

Ehhez már nem a Terminált használtam a feladat komplexitása miatt, hanem írtam egy bash script file-t, amit végül lefuttattam a terminálban. A végeredmény a lenti képen látható.



Úgy állítottam be a script file-t hogy tulajdonnév szerint rendezze sorba.

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

a) File and Disk Utilities:

Ez a program (Disk2vhd) .vhd fájlokat készít különféle partíciókról. Ez lehet akár egy biztonsági mentés is, ha arra szeretné a felhasználó használni a készített. Vdh fájlokat. A felület, ami fogadott a lenti képen látható.

Autoruns - Sysinternals www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

Everything Logon LSA Providers Internet Explorer Scheduled Tasks Services... Drivers... Codecs Boot Execute Image Hijacks WMI AppInit Known DLLs WinLogon Winsock Providers Office

Logon	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Thu Feb 3 08:03:14 2022	
CiscoMeetingDaemon	Cisco Webex Meetings	(Verified) Cisco WebEx, LLC	C:\Users\javor\AppData\Local\WebEx\WebexHost.exe	Thu Feb 17 09:25:45 2022	
CiscoSpark		(Not Verified)	C:\Users\javor\AppData\Local\Microsoft\Teams\Start Menu\Pro...	Sat Jul 10 19:00:22 2021	
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Appl...	C:\Users\javor\AppData\Local\Microsoft\Teams\Update.exe	Sun Jan 9 17:12:34 2022	
Discord	Update	(Verified) Discord Inc.	C:\Users\javor\AppData\Local\Discord\Update.exe	Thu Dec 2 22:40:28 2020	
EADM	Origin	(Verified) Electronic Arts, Inc.	C:\Program Files (x86)\Origin\Origin.exe	Tue Jan 18 11:09:30 2022	
EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games, Inc.	C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\Epi...	Tue Oct 19 20:27:58 2021	
GoogleDriveFS	Google Drive	(Verified) Google LLC	C:\Program Files (Google Drive File Stream)\55.0.3.0\GoogleDriveFS.exe	Tue Jan 25 13:27:10 2022	
LOHUB	LOHUB	(Verified) Logitech Inc.	C:\Program Files\LOHUB\lghub.exe	Wed Feb 16 21:10:05 2022	
lync	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\lync.exe	Sat Feb 19 18:07:06 2022	
PreMD	PreMD	(Not Verified) GitHub, Inc.	C:\Users\javor\AppData\Local\Microsoft\Windows\CurrentVersion\Run	Sun Feb 21 01:34:08 2021	
Steam	Steam	(Verified) Valve Corp.	C:\Program Files (x86)\Steam\steam.exe	Sun Jan 16 18:41:26 2022	
Wargaming.net Game Center	Wargaming.net Game Center	(Verified) Wargaming.net Limited	C:\ProgramData\Wargaming.net\GameCenter\lgwc.exe	Sat Feb 5 18:03:14 2022	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Sat Feb 5 18:03:14 2022	
Adobe GC Invoker Utility	Adobe GC Invoker Utility	(Verified) Adobe Inc.	C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGCInv...	Tue Nov 23 02:31:46 2021	
Realtek HD Audio Manager	Realtek HD Audio Manager	(Verified) Realtek Semiconductor ...	C:\Program Files\Realtek\Audio\HDA\RAudioM4.exe	Fri Sep 4 08:36:40 2020	
Sonic Suite 3	Sonic Suite 3	(Not Verified) ASUSTek COMPUTE...	C:\Program Files\ASUSTekComputer Inc\Sonic Suite 3\Foundation\SS3...	Wed Jun 20 14:56:14 2018	
Wondershare Helper Compact.exe	Wondershare Studio	(Verified) Wondershare Technology...	C:\Program Files (x86)\Common Files\Wondershare\Wondershare Help...	Thu Mar 23 09:52:20 2017	
Wondershare Helper Compact.exe	Wondershare Studio	(Verified) Wondershare Technology...	C:\Program Files\Wondershare\Wondershare UsConverter 13 For Wind...	Mon Dec 27 15:53:00 2021	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Sat Jun 5 14:11:09 2021	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sat Jun 5 14:05:12 2021	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Wed Oct 6 16:00:11 2021	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files (Google Chrome\Application)\98.0.4758.102\Installer\c...	Tue Feb 15 18:16:49 2022	
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.50\Instal...	Fri Feb 18 16:51:21 2022	
n/a	Microsoft .NET 10 SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscorres.dll	Sat Jun 5 14:06:26 2021	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Sat Feb 5 18:03:20 2022	
ASUS Ai Charger	AICharger Application	(Verified) ASUSTek Computer Inc.	C:\Program Files (x86)\ASUS\ASUS Ai Charger\AiChargerAP.exe	Wed Mar 5 10:29:44 2014	
Brave			C:\Program Files (x86)\Brave\Brave.exe	Wed Mar 4 07:37:29 2020	
Cisco AnyConnect Secure Mobility Agent for Windows	Cisco AnyConnect User Interface	(Verified) Cisco Systems, Inc.	C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\...	Wed Apr 2 15:04:16 2019	
LogMeIn Hamachi UI	Hamachi Client Application	(Verified) LogMeIn, Inc.	C:\Program Files (x86)\LogMeIn\Hamachi\hamachi-2-ui.exe	Tue Jan 18 08:36:34 2020	
JavaUpdateScheduler	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Fri May 15 00:46:10 2020	
TeamsMachineInstaller	Microsoft Teams	(Verified) Microsoft Corporation	C:\Program Files (x86)\Teams\Installer\Teams.exe	Tue Nov 17 22:01:16 2020	
vmware-tray.exe	VMware Tray Process	(Verified) VMware, Inc.	C:\Program Files (x86)\VMware\VMware Workstation\vmware-tray.exe	Thu Mar 23 09:52:20 2017	
Wondershare Helper Compact.exe	Wondershare Studio	(Verified) Wondershare Technology...	C:\Program Files (x86)\Common Files\Wondershare\Wondershare Help...	Fri May 3 17:34:16 2019	
Wrath Prism	Wrath Prism HID	(Not Verified) Cooler Master	C:\Program Files (x86)\AMD\Wrath\Wrath Prism\Wrath Prism HID.exe	Wed Oct 6 16:04:36 2021	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Wed Oct 6 16:04:36 2021	

d) Security Utilites:

Ezt a programot sajnos nem tudtam futtatni valamilyen hiba miatt, így nem tudtam megnézni, hogy mit tud, hogy néz ki és mik a funkciói. A programot futtattam adminisztrációs jogokkal, és sajnos szinte azonnal összeomlott a program, ha pedig nem adminisztrációs jogokkal indítottam, ez a felület fogadott.

```

C:\Users\javor\Downloads\Sysir x + v -
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

Initialization error:
Make sure that you are an administrator and run from an administrative command prompt.

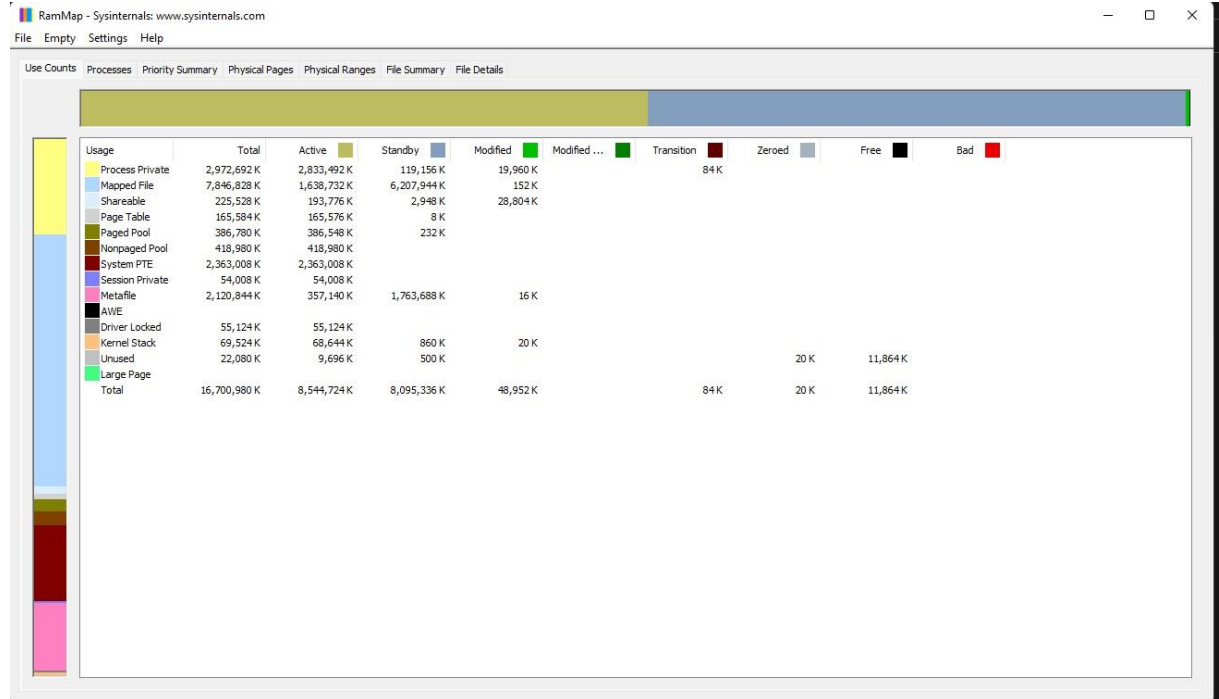
[process exited with code 1]

```

e) Information Utilites:

Ebben a feladatban a RAMMap programot használtam. Ebben a programban pontosan leírja, hogy például a processek mekkora RAM memóriát foglalnak le és használnak fel. Továbbá leírja azokról a pontos adatokat további vizsgálatokhoz. A

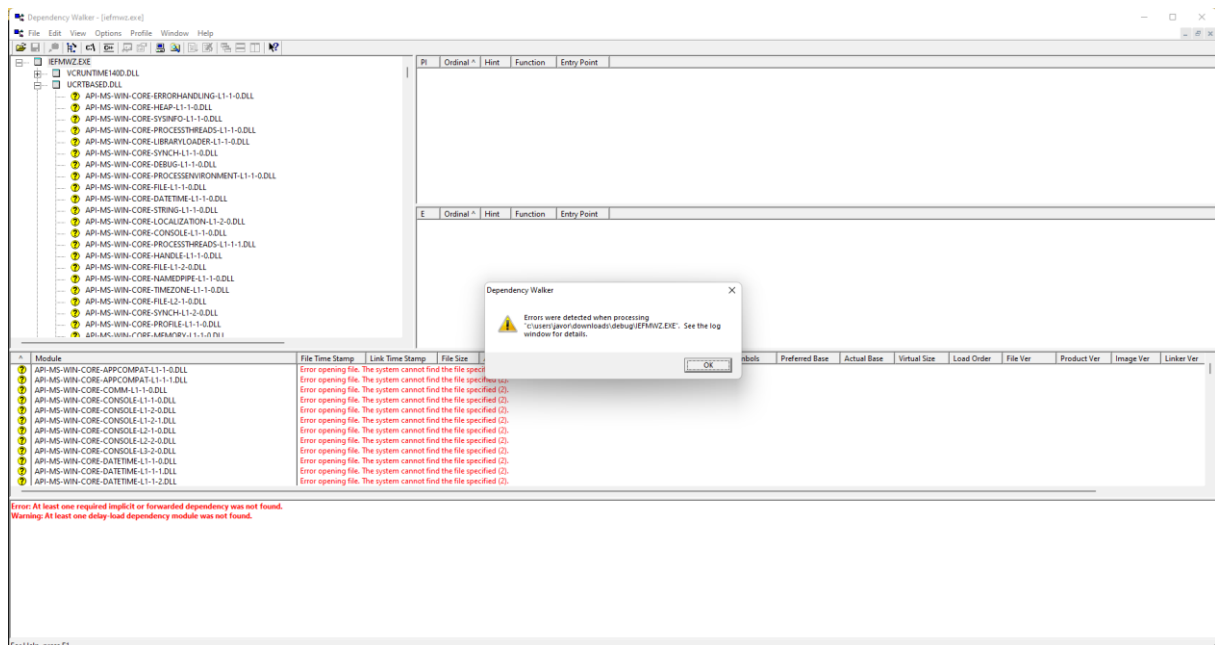
képen látható felület fogadott, mikor elindítottam a programot.



3. Töltse le a következő programot: Dependency Walker

a) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből

Miután készítettem egy iefmwz.c programot, ezzel a programmal megvizsgálva ezt a hibaüzenetet dobta ki, ami a lenti képen látható.



Az interneten sajnos nem találtam hozzá megoldást, így csak így tudom megmutatni, hogy mit mutat a program.

A programkód és a végeredményt is szívesen megmutatom.

```
iefmwz.c
iefmwz (Global Scope)

1  #include <stdio.h>
2  #pragma warning(disable:4996)
3
4  int main()
5  {
6      char str[] = "Toth Daniel Mark MERNOKINFORMATIKA IEFMWZ\n";
7      char filename[] = "vezeteknev.txt";
8
9      WriteFile(str, filename);
10     ReadFile(filename);
11 }
12
13 int WriteFile(char str[], char filename[])
14 {
15     int i;
16     FILE * fptr;
17     fptr = fopen(filename, "w");
18     for (i = 0; str[i] != '\n'; i++) {
19         fputc(str[i], fptr);
20     }
21     fclose(fptr);
22 }
23
24 int ReadFile(char filename[])
25 {
26     FILE * fp;
27     char texts[255];
28     fp = fopen(filename, "r");
29     fgets(texts, 255, (FILE*)fp);
30     printf("%s\n", texts);
31     fclose(fp);
32 }
```

Ez itt a programkód. A lenti kép pedig a végeredményt mutatja egy konzol ablakban.

```
Microsoft Visual Studio Debug (
+
-

Toth Daniel Mark MERNOKINFORMATIKA IEFMWZ

C:\Users\javor\source\repos\iefmwz\Debug\iefmwz.exe (process 15468) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging
le when debugging stops.
```

Tehát összegezve, a program sikeresen lefut, mégis hibába ütközök, amit sajnos nem tudok orvosolni.

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 olyan modul, ami NT funkciókat, függvényeket tartalmaz. Rövid tény róla, hogy régebben a Microsoft egy súlyos biztonsági résznek tartotta, amit később természetesen kijavítottak.

Miután ebben a programban megkerestem és megvizsgáltam az NTDLL.DLL fájlt, ez a felület fogadott.

Dependency Walker - (NTDLL.dll)																			
File Edit View Options Profile Windows Help																			
NTDLL.dll																			
		B	Ordinal ^	Hint	Function	Entry Point													
		E	Ordinal ^	Hint	Function	Entry Point													
		400 (0x0199)	394 (0x018A)		NtLsLanguageComitted	0x0075AB0													
		401 (0x019A)	395 (0x018B)		NtListenPort	0x0075AC0													
		411 (0x019B)	396 (0x018C)		NtLoadDriver	0x0075AD0													
		412 (0x019C)	397 (0x018D)		NtLoadEnclaveData	0x0075AE0													
		413 (0x019D)	399 (0x018F)		NtLoadKey2	0x0075B00													
		414 (0x019E)	400 (0x0190)		NtLoadKey3	0x0075B10													
		415 (0x019F)	398 (0x018E)		NtLoadKey	0x0075AF0													
		416 (0x01A0)	401 (0x0191)		NtLoadKeyEx	0x0075B20													
		417 (0x01A1)	402 (0x0192)		NtLockFile	0x0075B30													
		418 (0x01A2)	403 (0x0193)		NtLockProductActivationKeys	0x0075B40													
		419 (0x01A3)	404 (0x0194)		NtLockRegistryKey	0x0075B50													
		420 (0x01A4)	405 (0x0195)		NtLockVirtualMemory	0x0075B60													
		421 (0x01A5)	406 (0x0196)		NtMakePermanentObject	0x0075B70													
		422 (0x01A6)	407 (0x0197)		NtMakeTemporaryObject	0x0075B80													
		423 (0x01A7)	408 (0x0198)		NtManageHotPatch	0x0075B90													
		424 (0x01A8)	409 (0x0199)		NtManagePartition	0x0075BA0													
		425 (0x01A9)	410 (0x019A)		NtMapCMFModule	0x0075BB0													
		426 (0x01AA)	411 (0x019B)		NtMapUserPhysicalPages	0x0075BC0													
		427 (0x01AB)	412 (0x019C)		NtMapUserPhysicalPagesScatter	0x0075BD0													
		428 (0x01AC)	413 (0x019D)		NtMapViewOfSection	0x0075BE0													
		429 (0x01AD)	414 (0x019E)		NtMapViewOfSectionEx	0x0075BF0													
		430 (0x01AE)	415 (0x019F)		NtModifyBootEntry	0x0075C00													
		431 (0x01AF)	416 (0x01A0)		NtModifyDriverEntry	0x0075C10													
		432 (0x01B0)	417 (0x01A1)		NtNotifyChangeDirectoryFile	0x0075C20													
		433 (0x01B1)	418 (0x01A2)		NtNotifyChangeDirectoryFileEx	0x0075C30													
		434 (0x01B2)	419 (0x01A3)		NtNotifyChangeKey	0x0075C40													
		435 (0x01B3)	420 (0x01A4)		NtNotifyChangeMultipleKeys	0x0075C50													
		436 (0x01B4)	421 (0x01A5)		NtNotifyChangeSession	0x0075C60													
		437 (0x01B5)	422 (0x01A6)		NtOpenDirectoryObject	0x0075C70													
		438 (0x01B6)	423 (0x01A7)		NtOpenEnlistment	0x0075C80													
		439 (0x01B7)	424 (0x01A8)		NtOpenEvent	0x0075C90													
		440 (0x01B8)	425 (0x01A9)		NtOpenEventPair	0x0075CA0													
		441 (0x01B9)	426 (0x01AA)		NtOpenFile	0x0075CB0													
		442 (0x01BA)	427 (0x01AB)		NtOpenIoCompletion	0x0075CC0													
		443 (0x01BB)	428 (0x01AC)		NtOpenJobObject	0x0075CD0													
		444 (0x01BC)	429 (0x01AD)		NtOpenKey	0x0075CE0													
		445 (0x01BD)	430 (0x01AE)		NtOpenKeyEx	0x0075CF0													
		446 (0x01BE)	431 (0x01AF)		NtOpenKeyTransacted	0x0075D00													
		447 (0x01BF)	432 (0x01B0)		NtOpenKeyTransactedEx	0x0075D10													
		448 (0x01C0)	433 (0x01B1)		NtOpenKeyedEvent	0x0075D20													
Module	File Name	Link Time Stamp	File Size	Alt.	Link Checksum	Base Checksum	CPU	Subsystem	Symbolic	Preferred Name	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver	Linker Ver	OS Ver	Subsystem Ver
NTDLL.dll	C:\Windows\System32\NTDLL.dll	10/20/2009 15:06	1,352,194 B		0x01ACCEB	0x01ACCEB	x64	Console	(Unknown)	0x01A0000	0x01A0000	16,384	1	6.0.6002.18005	6.0.6002.18005	6.0.6002.18005	6.0.6002.18005	6.0.6002.18005	6.0.6002.18005

Ott középen látható pár függvény, vagy modul, amit ez a .DLL fájl felhasznál, vagy meghív. A lenti képen található még pár függvény ráközelítve.

E	Ordinal ^	Hint	Function	Entry Point
400	(0x0199)	394 (0x018A)	NtLsLanguageComitted	0x0075AB0
401	(0x019A)	395 (0x018B)	NtListenPort	0x0075AC0
411	(0x019B)	396 (0x018C)	NtLoadDriver	0x0075AD0
412	(0x019C)	397 (0x018D)	NtLoadEnclaveData	0x0075AE0
413	(0x019D)	399 (0x018F)	NtLoadKey2	0x0075B00
414	(0x019E)	400 (0x0190)	NtLoadKey3	0x0075B10
415	(0x019F)	398 (0x018E)	NtLoadKey	0x0075AF0
416	(0x01A0)	401 (0x0191)	NtLoadKeyEx	0x0075B20
417	(0x01A1)	402 (0x0192)	NtLockFile	0x0075B30
418	(0x01A2)	403 (0x0193)	NtLockProductActivationKeys	0x0075B40
419	(0x01A3)	404 (0x0194)	NtLockRegistryKey	0x0075B50
420	(0x01A4)	405 (0x0195)	NtLockVirtualMemory	0x0075B60
421	(0x01A5)	406 (0x0196)	NtMakePermanentObject	0x0075B70
422	(0x01A6)	407 (0x0197)	NtMakeTemporaryObject	0x0075B80
423	(0x01A7)	408 (0x0198)	NtManageHotPatch	0x0075B90
424	(0x01A8)	409 (0x0199)	NtManagePartition	0x0075BA0
425	(0x01A9)	410 (0x019A)	NtMapCMFModule	0x0075BB0
426	(0x01AA)	411 (0x019B)	NtMapUserPhysicalPages	0x0075BC0
427	(0x01AB)	412 (0x019C)	NtMapUserPhysicalPagesScatter	0x0075BD0
428	(0x01AC)	413 (0x019D)	NtMapViewOfSection	0x0075BE0
429	(0x01AD)	414 (0x019E)	NtMapViewOfSectionEx	0x0075BF0
430	(0x01AE)	415 (0x019F)	NtModifyBootEntry	0x0075C00
431	(0x01AF)	416 (0x01A0)	NtModifyDriverEntry	0x0075C10
432	(0x01B0)	417 (0x01A1)	NtNotifyChangeDirectoryFile	0x0075C20
433	(0x01B1)	418 (0x01A2)	NtNotifyChangeDirectoryFileEx	0x0075C30
434	(0x01B2)	419 (0x01A3)	NtNotifyChangeKey	0x0075C40
435	(0x01B3)	420 (0x01A4)	NtNotifyChangeMultipleKeys	0x0075C50
436	(0x01B4)	421 (0x01A5)	NtNotifyChangeSession	0x0075C60
437	(0x01B5)	422 (0x01A6)	NtOpenDirectoryObject	0x0075C70
438	(0x01B6)	423 (0x01A7)	NtOpenEnlistment	0x0075C80
439	(0x01B7)	424 (0x01A8)	NtOpenEvent	0x0075C90
440	(0x01B8)	425 (0x01A9)	NtOpenEventPair	0x0075CA0
441	(0x01B9)	426 (0x01AA)	NtOpenFile	0x0075CB0
442	(0x01BA)	427 (0x01AB)	NtOpenIoCompletion	0x0075CC0
443	(0x01BB)	428 (0x01AC)	NtOpenJobObject	0x0075CD0
444	(0x01BC)	429 (0x01AD)	NtOpenKey	0x0075CE0
445	(0x01BD)	430 (0x01AE)	NtOpenKeyEx	0x0075CF0
446	(0x01BE)	431 (0x01AF)	NtOpenKeyTransacted	0x0075D00
447	(0x01BF)	432 (0x01B0)	NtOpenKeyTransactedEx	0x0075D10
448	(0x01C0)	433 (0x01B1)	NtOpenKeyedEvent	0x0075D20

Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver	Linker Ver	OS Ver	Sub
----------------	-------------	--------------	------------	----------	-------------	-----------	------------	--------	-----