

Operációs rendszerek

2. Gyakorlat

2025. 02. 26

Készítette:

Rác László

Szak: 1.PTI

CI880V

Sárospatak, 2025

1. feladat –

a.

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

```
C:\neptunkod
|
|- bokor
|   |- banan
|   |- mogyoro
|   |- barack
|
|- fa
|   |- korte
|
|-land
    |- szeder
    |- kokusz
```

Megvalósítás

```
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226>mkdir bokor
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226>cd bokor
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\bokor>mkdir banan
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\bokor>mkdir mogyoro
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\bokor>mkdir barack
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\bokor>cd..
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226>mkdir fa
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226>cd fa
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\fa>mkdir korte
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\fa>cd..
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226>mkdir land
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226>cd land
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\land>mkdir szeder
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\land>mkdir kokusz
```

b.

```
|- kokusz
```

b.) Karakteres felületen készítsen másolatot:

- a *neptunkod\land\szeder* katalógusról a *neptunkod\fa* katalógusba.
- a *neptunkod\bokor\banan* katalógusról a *neptunkod\fa* katalógusba.

Megvalósítás

xcopy

C:\Users\raczl\Desktop\CI880V_OS

Gyak\CI880V_0226\land\szeder

C:\Users\raczl\Desktop\CI880V_OS

Gyak\CI880V_0226\fa\szeder /E /I

xcopy

C:\Users\raczl\Desktop\CI880V_OS

Gyak\CI880V_0226\bokor\banan

C:\Users\raczl\Desktop\CI880V_OS

Gyak\CI880V_0226\fa\banan /E /I

c.

c.) Karakteres felületen 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

Megvalósítás

move C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\bokor\barack

C:\neptunkod\fa\

move C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\land\kokusz

C:\neptunkod\fa\

d.

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

- *neptunkod\bokor\banan\leiras.txt*

- *neptunkod\tree\felsorolas.txt*

Megvalósítás

```
rmdir /s /q C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\land
```

```
echo. >
```

```
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\bokor\banan\leiras.txt
```

```
echo. >
```

```
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\fa\felsorolas.txt
```

e.

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

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

Megvalósítás

```
( echo A barack egy finom gyümölcs.
```

```
echo Nyáron terem és lédús.
```

```
echo Sokféle fajtája létezik. ) >
```

```
C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\bokor\banan\leiras.txt
```

```
( echo Jakab Tibor
```

```
echo Batta István
```

```
echo Aros Damián
```

```
echo Orosz Kristóf
```

echo Ródé Martin) >

C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\fa\felsorolas.txt

f.

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

Megvalósítás

dir C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226 /s

g.

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

Megvalósítás

cd \

dir /s /b ?e*.*

h.

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

Megvalósítás

icacls C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\fa\felsorolas.txt
/grant Everyone:R

i.

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

Megvalósítás

du -sh /mnt/c/Users/raczl/Desktop/CI880V_OSGyak/CI880V_0226

j.

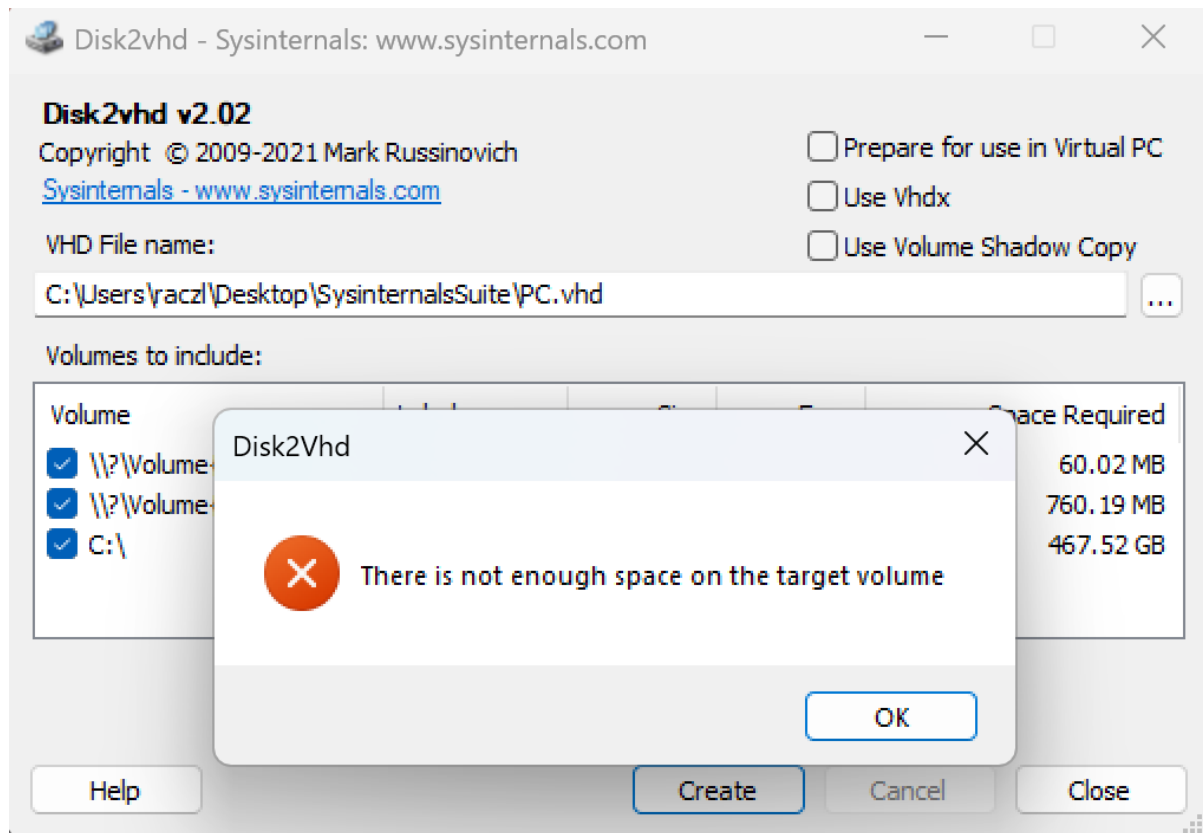
j.) Rendezze ABC-szerint a *felsorolas.txt* file tartalmát.

Megvalósítás

sort C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\fa\felsorolas.txt
/o C:\Users\raczl\Desktop\CI880V_OSGyak\CI880V_0226\fa\felsorolas.txt

2. feladat –

a) File and Disk Utilities (Disk2vhd)



Nem futtatható tárhely hiánya miatt

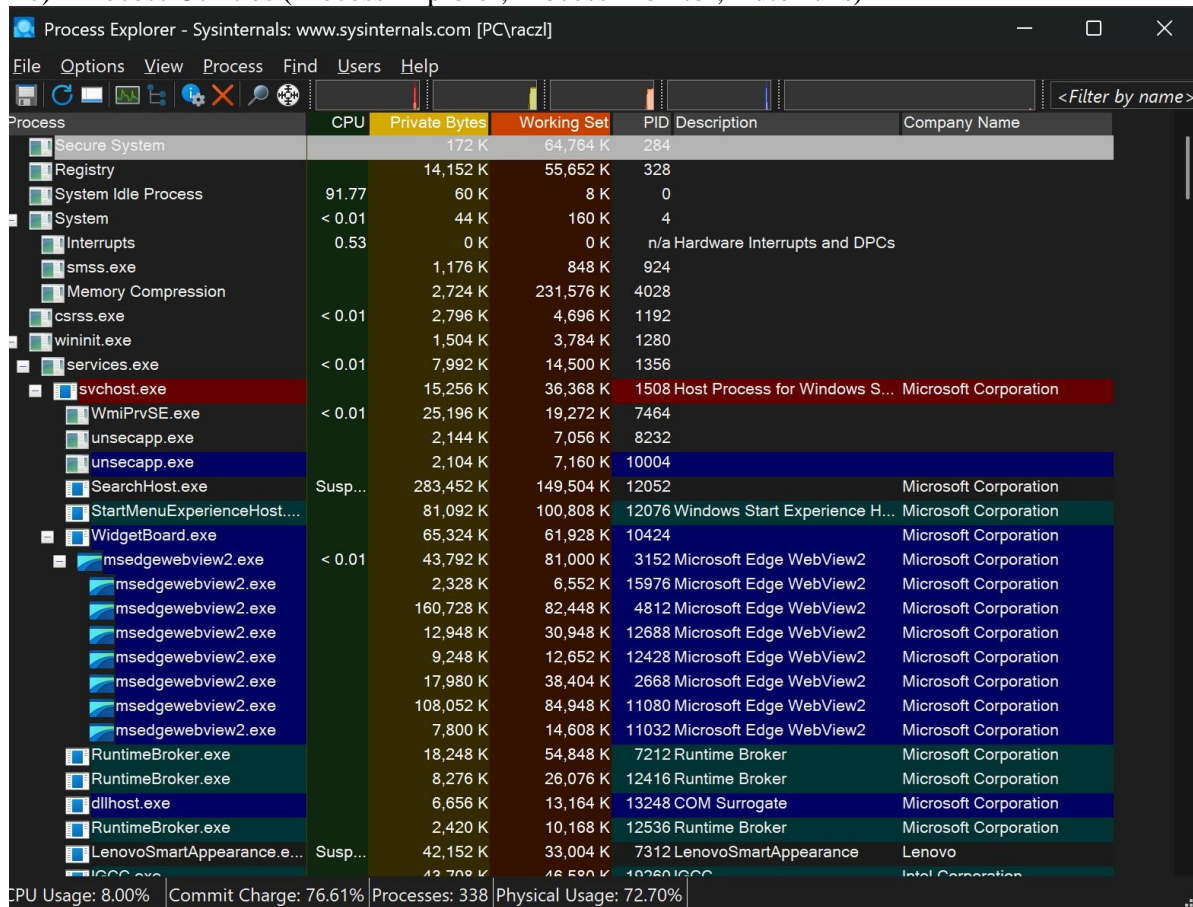
b) Networking Utilities (TCPView)

The screenshot shows the TCPView application window. The title bar reads "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, View, Process, Connection, Options, and Help. The toolbar shows icons for TCP v4, TCP v6, UDP v4, and UDP v6. The main window displays a table of network connections.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1612	TCP	Listen	0.0.0.0	135	0.0.0.0	0	3/24/2025 2:28:10 PM	RpcSs
System	4	TCP	Listen	26.151.143.43	139	0.0.0.0	0	3/24/2025 2:28:21 PM	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	3/24/2025 2:28:03 PM	System
System	4	TCP	Listen	192.168.221.162	139	0.0.0.0	0	3/25/2025 3:12:43 PM	System
svchost.exe	10644	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	3/25/2025 3:55:53 PM	CDPSvc
msedgewebview2.exe	11228	TCP	Listen	127.0.0.1	9222	0.0.0.0	0	3/24/2025 2:28:20 PM	msedgewebview
System	4	TCP	Listen	127.0.0.1	28385	0.0.0.0	0	3/24/2025 2:28:13 PM	System
System	4	TCP	Listen	127.0.0.1	28390	0.0.0.0	0	3/24/2025 2:28:13 PM	System
esrv.exe	19200	TCP	Listen	127.0.0.1	49351	0.0.0.0	0	3/24/2025 2:32:15 PM	esrv.exe
svchost.exe	5336	TCP	Established	192.168.221.162	49422	20.199.120.182	443	3/25/2025 3:12:40 PM	WpnService
lsass.exe	1384	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	3/24/2025 2:28:10 PM	lsass.exe
wininit.exe	1280	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	3/24/2025 2:28:10 PM	wininit.exe
svchost.exe	2468	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	3/24/2025 2:28:11 PM	Schedule
svchost.exe	3872	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	3/24/2025 2:28:11 PM	EventLog
spoolsv.exe	4616	TCP	Listen	0.0.0.0	49672	0.0.0.0	0	3/24/2025 2:28:12 PM	Spooler
services.exe	1356	TCP	Listen	0.0.0.0	49676	0.0.0.0	0	3/24/2025 2:28:12 PM	services.exe
WUDFHost.exe	1664	TCP	Established	127.0.0.1	49679	127.0.0.1	49680	3/24/2025 2:28:14 PM	WUDFHost.exe
WUDFHost.exe	1664	TCP	Established	127.0.0.1	49680	127.0.0.1	49679	3/24/2025 2:28:14 PM	WUDFHost.exe
WUDFHost.exe	1740	TCP	Established	127.0.0.1	49681	127.0.0.1	49682	3/24/2025 2:28:14 PM	WUDFHost.exe
WUDFHost.exe	1740	TCP	Established	127.0.0.1	49682	127.0.0.1	49681	3/24/2025 2:28:14 PM	WUDFHost.exe
firefox.exe	16324	TCP	Established	127.0.0.1	49685	127.0.0.1	49686	3/24/2025 2:28:21 PM	firefox.exe
firefox.exe	16324	TCP	Established	127.0.0.1	49686	127.0.0.1	49685	3/24/2025 2:28:21 PM	firefox.exe
firefox.exe	15820	TCP	Established	127.0.0.1	49688	127.0.0.1	49689	3/24/2025 2:28:21 PM	firefox.exe
firefox.exe	15820	TCP	Established	127.0.0.1	49689	127.0.0.1	49688	3/24/2025 2:28:21 PM	firefox.exe
RiotClientServices.exe	15688	TCP	Listen	127.0.0.1	49769	0.0.0.0	0	3/24/2025 2:28:29 PM	RiotClientService

Endpoints: 125 Established: 32 Listening: 36 Time Wait: 5 Close Wait: Update: 2 sec States: (All)

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



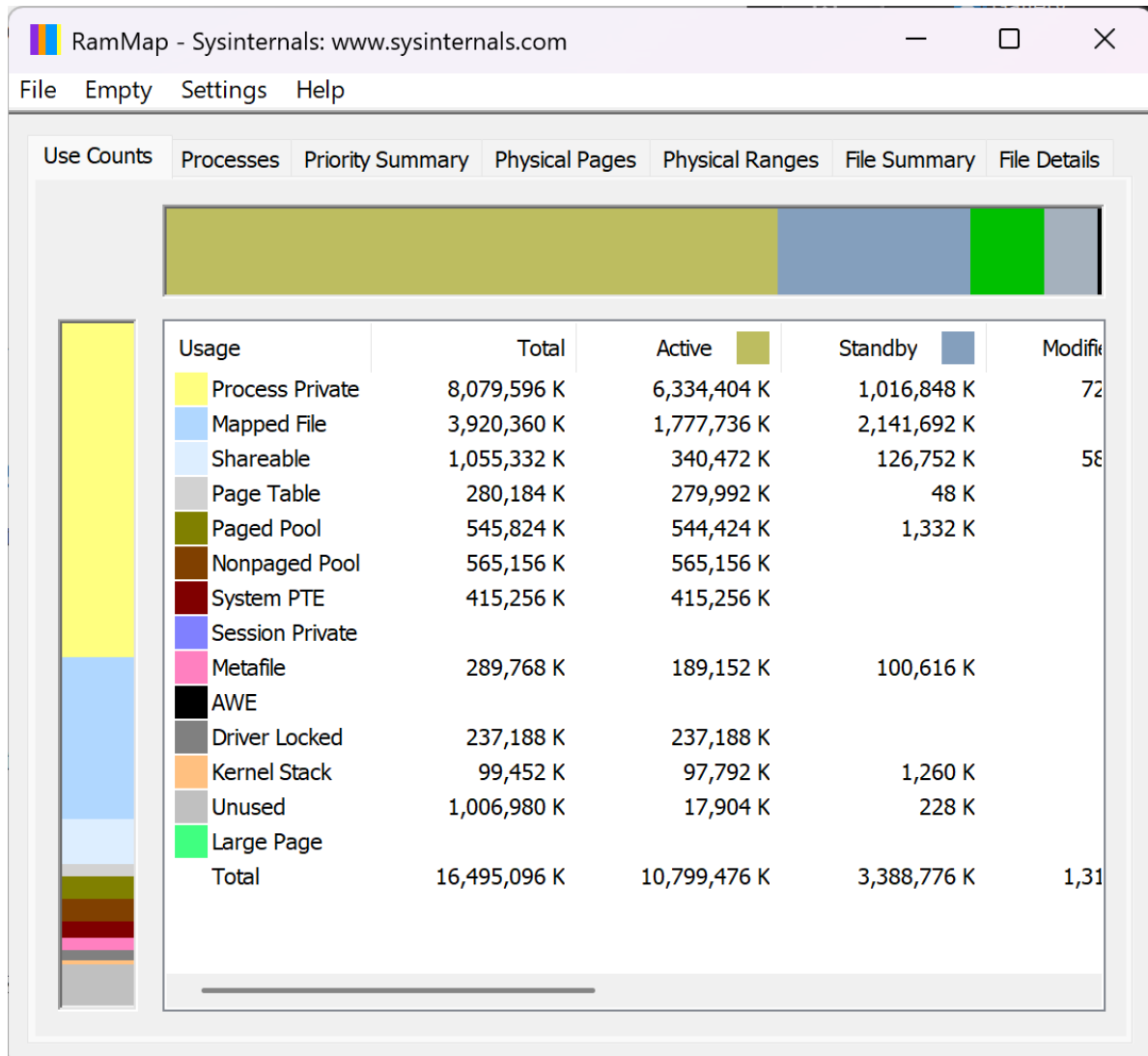
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System		172 K	64,764 K	284		
Registry		14,152 K	55,652 K	328		
System Idle Process	91.77	60 K	8 K	0		
System	< 0.01	44 K	160 K	4		
Interrupts	0.53	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,176 K	848 K	924		
Memory Compression		2,724 K	231,576 K	4028		
csrss.exe	< 0.01	2,796 K	4,696 K	1192		
wininit.exe		1,504 K	3,784 K	1280		
services.exe	< 0.01	7,992 K	14,500 K	1356		
svchost.exe		15,256 K	36,368 K	1508	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	< 0.01	25,196 K	19,272 K	7464		
unsecapp.exe		2,144 K	7,056 K	8232		
unsecapp.exe		2,104 K	7,160 K	10004		
SearchHost.exe	Susp...	283,452 K	149,504 K	12052		Microsoft Corporation
StartMenuExperienceHost...		81,092 K	100,808 K	12076	Windows Start Experience H...	Microsoft Corporation
WidgetBoard.exe		65,324 K	61,928 K	10424		Microsoft Corporation
msedgewebview2.exe	< 0.01	43,792 K	81,000 K	3152	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,328 K	6,552 K	15976	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		160,728 K	82,448 K	4812	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		12,948 K	30,948 K	12688	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		9,248 K	12,652 K	12428	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		17,980 K	38,404 K	2668	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		108,052 K	84,948 K	11080	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		7,800 K	14,608 K	11032	Microsoft Edge WebView2	Microsoft Corporation
RuntimeBroker.exe		18,248 K	54,848 K	7212	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		8,276 K	26,076 K	12416	Runtime Broker	Microsoft Corporation
dllhost.exe		6,656 K	13,164 K	13248	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		2,420 K	10,168 K	12536	Runtime Broker	Microsoft Corporation
LenovoSmartAppearance.e...	Susp...	42,152 K	33,004 K	7312	LenovoSmartAppearance	Lenovo
igcc.exe		43,708 K	46,580 K	10260	igcc	Intel Corporation

CPU Usage: 8.00% | Commit Charge: 76.61% | Processes: 338 | Physical Usage: 72.70%

d) Security Utilities (LogonSession)

Nem futtatható

e) Information Utilities (RAMMap)

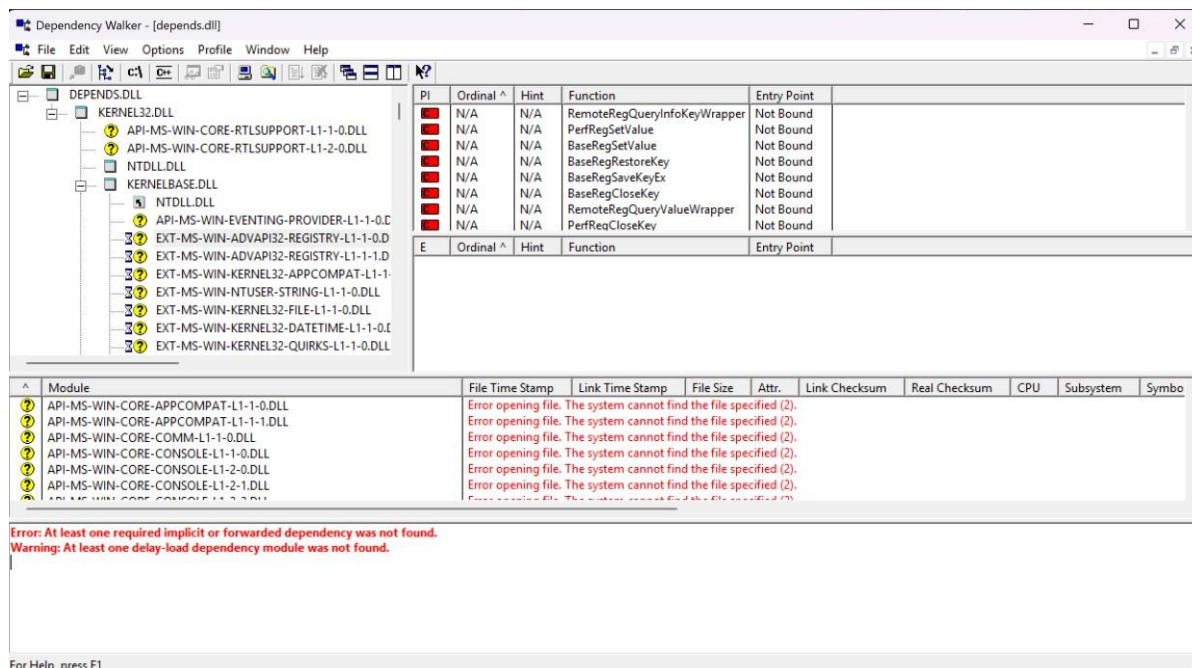


3. Feladat

Töltse le a következő programot:

Dependency Walker

Megvalósítás:



Feltelepítettem a dependency walkert aminek feladata, hogy *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)!

a) Megvalósítás:

Kernel32.dll API hívások:

A program a következő kernel32.dll
függvényeket használja:

- CreateFileW - Fájl
létrehozása/megnyitása
- WriteFile - Fájlba írás
- ReadFile - Fájl olvasása
- CloseHandle - Fájl lezárása
- GetStdHandle - Standard input/output
kezelése
- SetFilePointer - Fájlmutató
pozicionálása
- GetFileType - Fájl típus lekérdezése
- GetConsoleMode - Konzol mód
lekérdezése
- SetConsoleMode - Konzol mód
beállítása
- GetLastError - Utolsó hiba lekérdezése

Dependency Walker - [C:\880V]

File Edit View Options Profile Window Help

CI880V.EXE

Kernel32.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL

NTDLL.DLL

KERNELBASE.DLL

NTDLL.DLL

API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-2-0.DLL

EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL

EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	281 (0x0119)	DeleteCriticalSection	Not Bound
	N/A	317 (0x013D)	EnterCriticalSection	Not Bound
	N/A	441 (0x01B9)	FreeLibrary	Not Bound
	N/A	628 (0x0274)	GetLastError	Not Bound
	N/A	649 (0x0289)	GetModuleHandleA	Not Bound
	N/A	708 (0x02C4)	GetProcAddress	Not Bound
	N/A	890 (0x037A)	InitializeCriticalSection	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
	1 (0x0001)	73 (0x0049)	BaseThreadInitThunk	0x00015D30
	2 (0x0002)	920 (0x0398)	InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList
	3 (0x0003)	1596 (0x063C)	Wow64Transition	0x000822DC
	4 (0x0004)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
	5 (0x0005)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
	6 (0x0006)	2 (0x0002)	ActivateActCtx	0x0002F240

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Σ
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL								
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL								
API-MS-WIN-CORE-COMM-L1-1-0.DLL								
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL								
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL								
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL								
API-MS-WIN-CORE-CONSOLE-L1-2-2.DLL								

Error: At least one required implicit or forwarded dependency was not found.

Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.

Error: Modules with different CPU types were found.

Warning: At least one delay-load dependency module was not found.

For Help, press F1

b.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az

Az NTDLL.DLL a Windows NT kernel alrendszerének felhasználói módú része. Főbb szerepei:

- Alacsony szintű rendszerhívások (system calls) megvalósítása
- A kernel és a felhasználói módú programok közötti interfész biztosítása
- Memóriakezelés, szálkezelés, I/O műveletek alacsony szintű implementációi

Az NT API szerepe:

- Biztosítja az alapvető operációs rendszer szolgáltatásokat (memória, processz, fájlrendszer)
- Több rétegű biztonsági mechanizmusokat implementál
- Hardver absztrakciós réteget biztosít
- Hibakezelést és hibakeresési támogatást nyújt

For Help, press F1