

Operációs rendszerek BSc

2. Gyak.

2022. 02. 16.

Készítette:

Türk Viktor Bsc

Programtervező informatikus

F5HV4G

Miskolc, 2022

1.feladat – Készítse el a következő feladatokat!

a.) Hozza létre a következő mappa szerkezetet:

Az md paranccsal létrehoztam mappákat, de még használhattam volna az mkdir parancsot is, cd paranccsal pedig a könyvtárakba ki-be lépegettem, hogy a megfelelő helyen létrehozhassam a mappa szerkezetet.

```
Command Prompt
C:\Users\TEMP.IIT.000.001>cd desktop
C:\Users\TEMP.IIT.000.001\Desktop>cd gyak
C:\Users\TEMP.IIT.000.001\Desktop\gyak>md bokor
C:\Users\TEMP.IIT.000.001\Desktop\gyak>md fa
C:\Users\TEMP.IIT.000.001\Desktop\gyak>md land
C:\Users\TEMP.IIT.000.001\Desktop\gyak>cd bokor
C:\Users\TEMP.IIT.000.001\Desktop\gyak\bokor>md banan
C:\Users\TEMP.IIT.000.001\Desktop\gyak\bokor>md mogyoro
C:\Users\TEMP.IIT.000.001\Desktop\gyak\bokor>md barack
C:\Users\TEMP.IIT.000.001\Desktop\gyak\bokor>cd ..
C:\Users\TEMP.IIT.000.001\Desktop\gyak>cd fa
C:\Users\TEMP.IIT.000.001\Desktop\gyak\fa>md korte
C:\Users\TEMP.IIT.000.001\Desktop\gyak\fa>cd ..
C:\Users\TEMP.IIT.000.001\Desktop\gyak>cd land
C:\Users\TEMP.IIT.000.001\Desktop\gyak\land>md szeder
C:\Users\TEMP.IIT.000.001\Desktop\gyak\land>md kokusz
```

b.) Készítsen másolatot:

Az xcopy parancs segítségével átmásoltam minden mappát a megadott helyre

```
Command Prompt
Directory of C:\Users\TEMP.IIT.000.001\Desktop\gyak\land
2022. 02. 16. 12:31 <DIR>      .
2022. 02. 16. 12:31 <DIR>      ..
2022. 02. 16. 12:31 <DIR>      f5hv4g
2022. 02. 16. 12:30 <DIR>      kokusz
2022. 02. 16. 12:30 <DIR>      szeder
                0 File(s)        0 bytes
                5 Dir(s)  52 515 983 360 bytes free

C:\Users\TEMP.IIT.000.001\Desktop\gyak\land>cd ..
C:\Users\TEMP.IIT.000.001\Desktop\gyak>md f5hv4g
C:\Users\TEMP.IIT.000.001\Desktop\gyak>cd f5hv4g
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>xcopy
Invalid number of parameters
0 File(s) copied

C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>cd ..
C:\Users\TEMP.IIT.000.001\Desktop\gyak>xcopy /t "f5hv4g/land/szeder" "f5hv4g/fa"
C:\Users\TEMP.IIT.000.001\Desktop\gyak>xcopy /t /e "f5hv4g/land/szeder" "f5hv4g/fa"
C:\Users\TEMP.IIT.000.001\Desktop\gyak>xcopy /t "f5hv4g/land/szeder" "f5hv4g/fa"
C:\Users\TEMP.IIT.000.001\Desktop\gyak>xcopy /t "f5hv4g/bokor/banan" "f5hv4g/fa"
C:\Users\TEMP.IIT.000.001\Desktop\gyak>
```

c.)Végezze el a következő áthelyezéseket:

Egyszerűen egy move paranccsal a feladat leírása alapján áthelyeztem a mappákat

```
Command Prompt
C:\Users\TEMP.IIT.000.001\Desktop\gyak>move f5hv4g\bokor\barack f5hv4g\fa
1 dir(s) moved.

C:\Users\TEMP.IIT.000.001\Desktop\gyak>move f5hv4g\land\kokusz f5hv4g\fa
1 dir(s) moved.

C:\Users\TEMP.IIT.000.001\Desktop\gyak>
```

d.) Törölje a neptunkod/land katalógust és hozzon létre szöveges állományokat.

Az rmdir paranccsal sikeresen töröltem az adott katalógust a /s argumentummal ami lehetővé tette a nem üres mappák törlését is. A „type nul > allomany.txt” segítségével pedig egy üres szöveges állományt hoztam létre a megadott nevekkal.

```
Command Prompt
C:\Users\TEMP.IIT.000.001\Desktop\gyak>rmdir f5hv4g\land
Invalid switch - "land".

C:\Users\TEMP.IIT.000.001\Desktop\gyak>rmdir f5hv4g\land
The directory is not empty.

C:\Users\TEMP.IIT.000.001\Desktop\gyak>rmdir /s f5hv4g\land
f5hv4g\land, Are you sure (Y/N)? y

C:\Users\TEMP.IIT.000.001\Desktop\gyak>cd f5hv4g\bokor\banan
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\bokor\banan>type nul > leiras.txt
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\bokor\banan>cd ..
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\bokor>cd ..
C:\Users\TEMP.IIT.000.001\Desktop\gyak>cd fa
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>type nul > felsorolas.txt
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>
```

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

A copy con parancs segítségével megnyitottam az adott szöveges állományt és felsoroltam illetve írtam 3 sort a barackról majd a végén ctrl+c segítségével kiléptem a szerkesztésből.

```
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>copy con felsorolas.txt
kevin,vanda,máté,laci,matyi
Overwrite felsorolas.txt? (Yes/No/All): yes
kevin,vanda,máté,laci,matyi

1 file(s) copied.

C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>cd ..

C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>cd bokor/banan

C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\bokor\banan>copy con leiras.txt
finom a barack
Overwrite leiras.txt? (Yes/No/All): yes
fan terem a barack
szep a barack

1 file(s) copied.

C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\bokor\banan>_
```

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

A tree paranccsal kilistáztam mindent.

```
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>tree
Folder PATH listing for volume Windows 10
Volume serial number is D4A7-7617
C:.
├── bokor
│   ├── banan
│   └── mogyoro
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>
```

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

A dir ?e* /B /S paranccsal oldottam meg amibe egy regurális kifejezést írtam.

```
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>dir ?e* /B /S
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\bokor\banan\leiras.txt
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa\felsorolas.txt

C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>
```

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

icaccls parancs segítségével a /GRANT argumentummal mindenkinek olvashatóvá tettem.

```
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>cd fa
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>Icacls felsorolas.txt /GRANT *S-1-1-0:(d,w,dac)
processed file: felsorolas.txt
Successfully processed 1 files; Failed processing 0 files
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>_
```

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

A dir /a /s paranccsal valósítottam meg így kiírva minden mappa és almappának a méretét a képen látva összegezve

```
2022. 02. 16. 12:30 <DIR> .
2022. 02. 16. 12:30 <DIR> ..
0 File(s) 0 bytes

Total Files Listed:
2 File(s) 82 bytes
29 Dir(s) 48 554 487 808 bytes free
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g>dir /a/s_
```

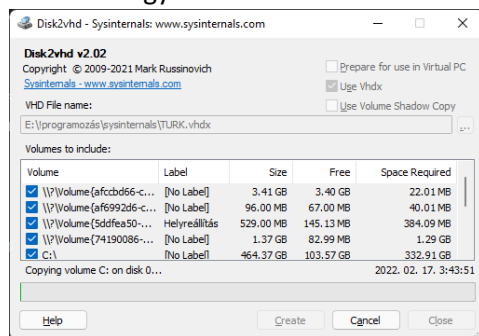
j.) Rendezze ABC-szerint a felsorolas.txt file tartalmát.

A sort parancs egyszerűen ABC sorrendbe rendezte a szöveges állományt.

```
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>sort felsorolas.txt
kevin
laci
mate
matyi
vanda
C:\Users\TEMP.IIT.000.001\Desktop\gyak\f5hv4g\fa>
```

2.feladat Sysinternals Suite csomag „elemzése”

a.)A disk2vhd egy virtuális lemezt csinál a választott már létező fizikai lemez(ek)ből



b.)A tcpview minden processnek írja azt az ip címet,portot és egyéb adatokat ahova csatlakozik

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit View, Protocols, Connections, Options, and Help. Below the menu is a toolbar with various icons for file operations, packet selection, and analysis. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List: Shows a list of captured packets. Packet 443 is selected, which is a NetBIOS session setup request from 192.168.1.10 to 192.168.1.1.

Packet Details: Displays the hierarchical structure of the selected packet. The top-level protocol is NetBIOS. The details pane shows the following fields:

- NetBIOS:**
 - Session Setup Request:**
 - Name:** 192.168.1.10
 - Length:** 10
 - Session ID:** 1

Packet Bytes: Shows the raw data of the selected packet in hexadecimal and ASCII format.

c.) Process utilities

process explorer: minden processnek a cpu és ram fogyasztását mutatja meg

Process Explorer - Sysinternals: www.sysinternals.com [TURKIROB]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8 752 K	76 416 K	176		
System Idle Process	77.08	60 K	8 K	0		
System	2.27	80 K	10 852 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 092 K	1 732 K	556		
Memory Compression	< 0.01	2 068 K	634 300 K	2508		
csrss.exe	< 0.01	2 156 K	12 980 K	836		
wininit.exe		1 372 K	15 900 K	924		
services.exe	< 0.01	6 152 K	33 476 K	996		
svchost.exe		12 316 K	58 492 K	1088	Host Process for Windows S...	Microsoft Corporation
WmiPrivSE.exe		3 904 K	11 296 K	4756		
WmiPrivSE.exe		15 000 K	21 120 K	5684		
YourPhone.exe	Susp...	54 000 K	177 960 K	8312		Microsoft Corporation
Shell Experience Host...	Susp...	36 104 K	150 316 K	11132	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2 916 K	35 772 K	10368	Runtime Broker	Microsoft Corporation
dihost.exe		3 204 K	11 064 K	12180		
unscapp.exe		2 940 K	19 736 K	14220	Sink to receive asynchronou...	Microsoft Corporation
RuntimeBroker.exe		2 840 K	18 936 K	16412	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...	< 0.01	71 184 K	42 464 K	13752	Application Frame Host	Microsoft Corporation
Video.UI.exe	Susp...	40 680 K	2 896 K	18476		
RuntimeBroker.exe		1 436 K	6 876 K	5724	Runtime Broker	Microsoft Corporation
Microsoft.Photos.exe	Susp...	78 544 K	3 608 K	10968		
RuntimeBroker.exe		16 864 K	34 324 K	10376	Runtime Broker	Microsoft Corporation
DataExchangeHost.exe		53 312 K	30 608 K	11492	Data Exchange Host	Microsoft Corporation
dihost.exe		48 660 K	8 916 K	4328	COM Surrogate	Microsoft Corporation
XboxPcApp.exe	< 0.01	261 744 K	283 472 K	19984		
RuntimeBroker.exe		4 556 K	28 280 K	2844	Runtime Broker	Microsoft Corporation
XboxAppServices.exe		55 904 K	37 480 K	5376		
smartscreen.exe		56 308 K	27 704 K	5864	Windows Defender SmartScr...	Microsoft Corporation

CPU Usage: 22.92% Commit Charge: 52.67% Processes: 250 Physical Usage: 51.17%

process monitor: A folyamatok tevékenységeit mutatja meg

Time	Process Name	PID	Operation	Path	Result	Detail
120.5	MalwareEng.exe	3836	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3174 400...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 1105 820...
120.5	svchost.exe	2916	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 704 512 Le...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15 587 568...
120.5	svchost.exe	3092	UDP Receive	tuk.53348 -> hosted by 3d.net 50006	SUCCESS	Length: 43, sequ...
120.5	MalwareEng.exe	3836	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 999 424 Le...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2149 824...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 610 432...
120.5	svchost.exe	2916	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 839 680 Le...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 692 224 Le...
120.5	svchost.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3153 920...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1495 040...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 741 504...
120.5	svchost.exe	1016	Thread Create		SUCCESS	Thread ID: 9704
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 831 488 Le...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 2 961 408...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1478 656...
120.5	svchost.exe	2916	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 647 168 Le...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 765 952 Le...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 1 036 288...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 392 640...
120.5	svchost.exe	2916	ReadFile	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Exclusive: Failu...
120.5	svchost.exe	2916	UnlockFileSingle	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Offset: 124 Length...
120.5	svchost.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 2 933 184...
120.5	svchost.exe	1016	QueryNameInfo	E:\Programozas\sysinterna\Procom6...	SUCCESS	Name: \Programoz...
120.5	svchost.exe	1016	QueryNameInfo	E:\Programozas\sysinterna\Procom6...	SUCCESS	Name: \Programoz...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 589 856...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 753 664 Le...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15 794 176...
120.5	svchost.exe	7520	ReadFile	C:\Windows\System32\SHCore.dll	SUCCESS	Offset: 802 816 Le...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1470 464...
120.5	svchost.exe	2916	ReadFile	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Exclusive: Failu...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 159 744 Le...
120.5	MalwareEng.exe	3836	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15 556 586...
120.5	svchost.exe	2916	UnlockFileSingle	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Offset: 124 Length...
120.5	Explorer.exe	7520	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
120.5	Explorer.exe	7520	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: HandleTag
120.5	Explorer.exe	7520	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: HandleTag
120.5	Explorer.exe	7520	RegOpenKey	HKEY\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: R...
120.5	svchost.exe	7520	RegOpenKey	HKEY\Applications\Procom64.exe	NAME NOT FOUND	Desired Access: R...
120.5	svchost.exe	1016	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 376 256...

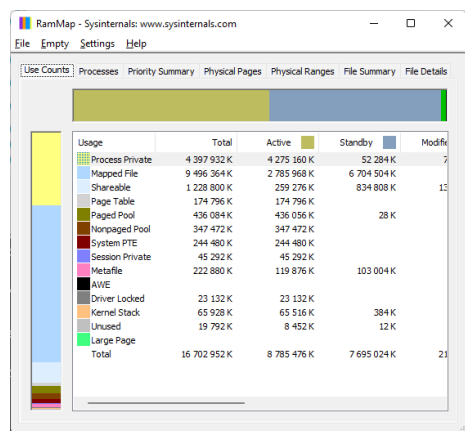
autoruns: Azt mutatja meg, hogy a programok mikor nyílnak meg

Name	Description	Publisher	Image Path	Timestamp
HKLM\Software\Classes\Protocols\Filter				Wed Feb 2 14:15:57 2022
test.xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VF\ProgramFilesCommonX64...	Wed Feb 2 14:15:17 2022
HKLM\Software\Classes\Protocols\Handler				Wed Feb 2 14:15:57 2022
mso-minib-roaming-16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL	Wed Feb 2 14:14:40 2022
mso-minib-16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL	Wed Feb 2 14:14:40 2022
oef-roaming-16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL	Wed Feb 2 14:14:40 2022
oef-16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL	Wed Feb 2 14:14:40 2022
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				Tue Feb 15 16:32:33 2022
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\22.012.0117.0003\FileSyncShell64...	Tue Feb 15 16:32:28 2022
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll	Thu Feb 21 17:00:00 2019
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers				Wed Feb 16 16:06:00 2022
MBAMSHExt	Malwarebytes	(Verified) Malwarebytes Corporati...	C:\Program Files\Malwarebytes\Anti-Malware\mbshlex.dll	Sat Oct 9 13:09:26 2021
StartAllBack Menu Pin	StartAllBack main library	(Verified) Stanislav Zinukhov	C:\Program Files\StartAllBack\StartAllBackX64.dll	Fri Dec 3 06:45:22 2021
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				Tue Feb 15 16:32:33 2022
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\22.012.0117.0003\FileSyncShell64...	Tue Feb 15 16:32:28 2022
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll	Thu Feb 21 17:00:00 2019
HKLM\Software\Classes\Directory\ShellEx\DropDropHandlers				Wed Oct 13 15:37:22 2021
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll	Thu Feb 21 17:00:00 2019
HKLM\Software\Classes\Directory\ShellEx\CoppyHookHandlers				Sun Oct 17 03:36:38 2021
WinSCP CopyHook	Drag&Drop shell extension for WinSCP (...)	(Verified) Martin Prikyl	C:\Program Files (x86)\WinSCP\DragExt64.dll	Wed Jul 21 13:16:48 2021
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers				Tue Feb 15 16:32:33 2022
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\22.012.0117.0003\FileSyncShell64...	Tue Feb 15 16:32:28 2022

d) Security Utilities(logon session)

Nem nyílik meg de gondolom a belépéseket figyeli

e) **Information Utilities(RAMMap)**A ramról mutat meg többféle információt például,hogy melyik címek vannak lefoglalva és mi foglalja őket



3. feladat – Az írt C program elemzése

a.)API hívások kernel32.dll-ből

Memóracímeket hasonlít össze stb.

The screenshot shows the Dependency Walker application. The 'kernel32.dll' is selected in the left pane. The right pane displays a list of API calls with their ordinal numbers, hints, functions, and entry points.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	0 (0x0000)	RtlAddFunctionTable	Not Bound
	N/A	2 (0x0002)	RtlCaptureContext	Not Bound
	N/A	5 (0x0005)	RtlCompareMemory	Not Bound
	N/A	6 (0x0006)	RtlDeleteFunctionTable	Not Bound
	N/A	9 (0x0009)	RtlInstallFunctionTableCallback	Not Bound
	N/A	11 (0x000B)	RtlLookupFunctionEntry	Not Bound
	N/A	12 (0x000C)	RtlPcToFileHeader	Not Bound
	N/A	13 (0x000D)	RtlRaiseException	Not Bound
	N/A	14 (0x000E)	RtlRestoreContext	Not Bound
	N/A	15 (0x000F)	RtlUnwind	Not Bound
	N/A	16 (0x0010)	RtlUnwindEx	Not Bound
	N/A	17 (0x0011)	RtlVirtualUnwind	Not Bound

b.) NTDLL.DLL szerepe

Mindenféle windows kernel funkciókat tartalmaz
Memóriát kezel,az adatok olvassa be stb.

The screenshot shows the Dependency Walker application. The 'ntdll.dll' is selected in the left pane. The right pane displays a list of API calls with their ordinal numbers, hints, functions, and entry points.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	20 (0x0014)	CoAllocCaptureBuffer	Not Bound
	N/A	21 (0x0015)	CoAllocMessagePointer	Not Bound
	N/A	23 (0x0017)	CoCaptureMessageAutoReleaseObjectInPlace	Not Bound
	N/A	24 (0x0018)	CoCaptureMessageString	Not Bound
	N/A	26 (0x001A)	CoClientCallName	Not Bound
	N/A	28 (0x001C)	CoFreeCaptureBuffer	Not Bound
	N/A	32 (0x0020)	CoVerifyRegion	Not Bound
	N/A	34 (0x0022)	DbgPrint	Not Bound
	N/A	35 (0x0023)	DbgPrintEx	Not Bound
	N/A	45 (0x002D)	DbgUiThreadDebugObject	Not Bound
	N/A	46 (0x002E)	DbgUiUserInterface	Not Bound
	N/A	57 (0x0039)	EventEnabled	Not Bound
	N/A	59 (0x003B)	EventRegister	Not Bound
	N/A	61 (0x003D)	EventUnregister	Not Bound