

Operációs rendszerek BSc

2. Gyak.

2022. 02. 20.

Készítette:

Szabó Larion Bsc

BGI

NWS74Y

Miskolc, 2022

1. feladat

a, mkdir parancsal létrehoztam a mappákat

```
C:\>cd C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>$ mkdir bokor
'$' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>mkdir bokor
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>mkdir fa
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>mkdir land
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>cd bokor
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor>mkdir banan
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor>mkdir mogyoro
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor>mkdir barack
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor>cd -
The system cannot find the path specified.
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor>cd.
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor>cd..
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>cd fa
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>mkdir korte
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>cd..
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>cd land
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\land>mkdir szeder
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\land>mkdir kokusz
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\land>cd..
```

b, Átmásoltam a két mappát az xcopy /t parancssal

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>xcopy /t C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\land\
szeder C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>xcopy /t C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\
```

c, a move parancssal áthelyeztem a következő mappákat

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>move C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\bar
ack C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa
1 dir(s) moved.
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>move C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\land\koku
sz C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa
1 dir(s) moved.
```

D, Az rmdir parancsar töröltem a land mappát az alábbi módon és létrehoztam az alábbi fájlokat a type nul > paranccsal a következő .txt állományokat

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>rmdir C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\land\sze
der
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>rmdir C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\land
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>type nul C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor
\banan\Leiras.txt
The system cannot find the file specified.
Error occurred while processing: C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan\Leiras.txt.
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>type nul > C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bok
or\banan\Leiras.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>type nul > C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\
Felsorolas.txt
```

E, Az átirányítás operátor > és az echo segítségével írtam a txt fileokba a szövegeket

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan>cd C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216
\bokor\banan
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan>echo "Eheto" > Leiras.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan>echo "Ledus" >> Leiras.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan>echo "Finom" >> Leiras.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan>cd C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216
\fa
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>echo "Dávid, Péter, Tamás, Szilvi, Anna" > Leiras.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>echo "Dávid, Péter, Tamás, Szilvi, Anna" > Felsorolas.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>echo "David, Peter, Tamas, Szilvi, Anna" > Felsorolas.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>
```

F, TREE paranccsal kilistáztam a mappa tartalmát

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>tree C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216
Folder PATH listing
Volume serial number is 00000064 CECF:546E
C:\USERS\LARION\DOCUMENTS\REPO\NWS74Y0SGYAK\NWS74Y_0216
├── bokor
│   ├── banan
│   └── mogyoro
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>
```

G, Az e-vel kezdődő karakterek listázása.

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa>cd..
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>dir /s "?e*"
Volume in drive C has no label.
Volume Serial Number is CECF-546E

Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan

02/23/2022  10:45 AM                30 Leiras.txt
               1 File(s)                30 bytes

Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa

02/23/2022  10:47 AM                38 Felsorolas.txt
               1 File(s)                38 bytes

Total Files Listed:
               2 File(s)                68 bytes
               0 Dir(s)  9,196,531,712 bytes free

C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>
```

H, Az icacls parancsal jogosultságot adtam a file olvasására

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>icacls C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\Felsorolas.txt
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\Felsorolas.txt NT AUTHORITY\SYSTEM:(I)(F)
                                          BUILTIN\Rendszergazdak:(I)(F)
                                          Larion-PC\Larion:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

I, A dir paranccsal kiíratam a mappa méretét

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>dir /s C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216
Volume in drive C has no label.
Volume Serial Number is CECF-546E
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216
```

```
02/23/2022  10:16 AM    <DIR>        .
02/23/2022  10:16 AM    <DIR>        ..
02/23/2022  10:12 AM    <DIR>        bokor
02/23/2022  10:46 AM    <DIR>        fa
               0 File(s)                0 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor
```

```
02/23/2022  10:12 AM    <DIR>        .
02/23/2022  10:12 AM    <DIR>        ..
02/23/2022  10:19 AM    <DIR>        banan
02/23/2022  09:20 AM    <DIR>        mogyoro
               0 File(s)                0 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\banan
```

```
02/23/2022  10:19 AM    <DIR>        .
02/23/2022  10:19 AM    <DIR>        ..
02/23/2022  10:45 AM             30 Leiras.txt
               1 File(s)                30 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\bokor\mogyoro
```

```
02/23/2022  09:20 AM    <DIR>        .
02/23/2022  09:20 AM    <DIR>        ..
               0 File(s)                0 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa
```

```
02/23/2022  10:46 AM    <DIR>        .
02/23/2022  10:46 AM    <DIR>        ..
02/23/2022  10:01 AM    <DIR>        banan
02/23/2022  09:20 AM    <DIR>        barack
02/23/2022  10:47 AM             38 Felsorolas.txt
02/23/2022  09:22 AM    <DIR>        kokusz
02/23/2022  09:21 AM    <DIR>        korte
02/23/2022  09:56 AM    <DIR>        szeder
               1 File(s)                38 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\banan
```

```
02/23/2022  10:01 AM    <DIR>        .
02/23/2022  10:01 AM    <DIR>        ..
               0 File(s)                0 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\barack
```

```
02/23/2022  09:20 AM    <DIR>        .
02/23/2022  09:20 AM    <DIR>        ..
               0 File(s)                0 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\kokusz
```

```
02/23/2022  09:22 AM    <DIR>        .
02/23/2022  09:22 AM    <DIR>        ..
               0 File(s)                0 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\korte
```

```
02/23/2022  09:21 AM    <DIR>        .
02/23/2022  09:21 AM    <DIR>        ..
               0 File(s)                0 bytes
```

```
Directory of C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\szeder
```

```
02/23/2022  09:56 AM    <DIR>        .
02/23/2022  09:56 AM    <DIR>        ..
               0 File(s)                0 bytes
```

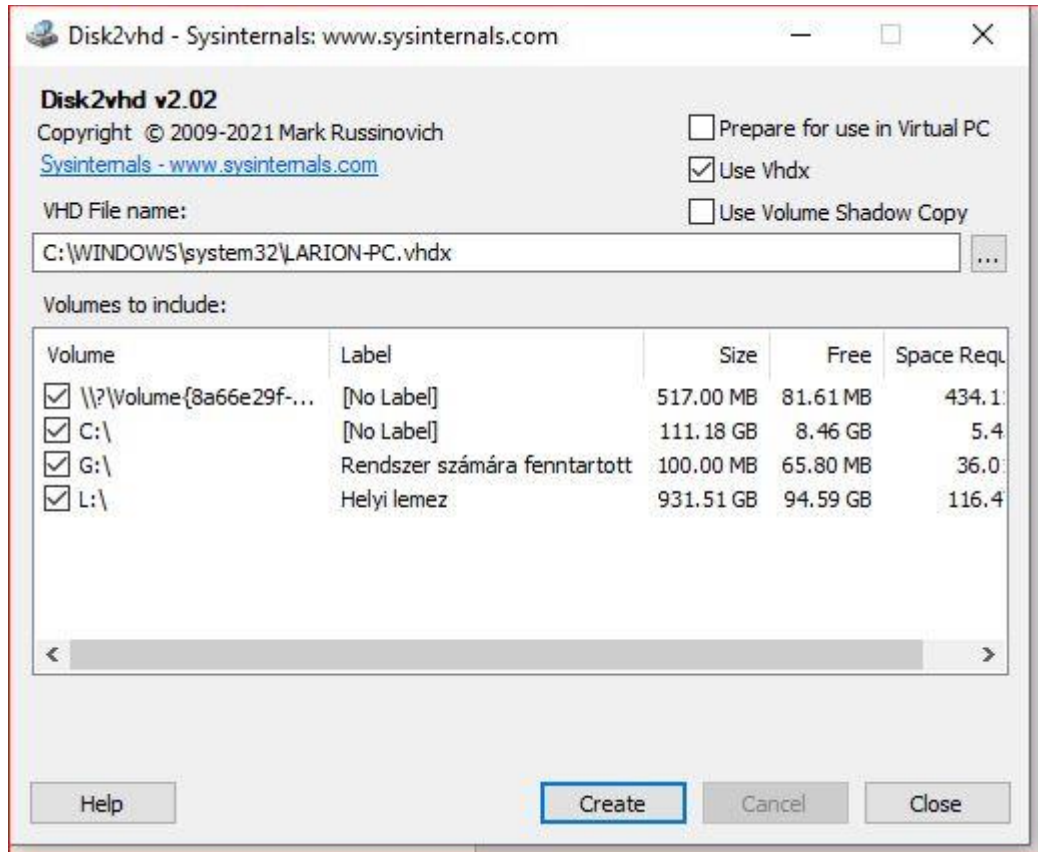
```
Total Files Listed:
          2 File(s)                68 bytes
        29 Dir(s)    9,197,420,544 bytes free
```


J, A sort paranccsal rendeztem a file tartalmát

```
C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216>sort C:\Users\Larion\Documents\repo\NWS74Y0sGyak\NWS74Y_0216\fa\Felso  
olas.txt  
Anna  
David  
Peter  
Szilvi  
Tamas
```

2. feladat

a, Ez másolja a meghajtómat egy fájlba



B, A hálózat forgalmamat figyeli

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	940	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2/23/2022 8:00:22 AM	RpcSs	
System	4	TCP	Listen	192.168.1.68	139	0.0.0.0	0	2/23/2022 8:00:27 AM	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2/23/2022 8:00:18 AM	System	
svchost.exe	4008	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2/23/2022 8:00:30 AM	CDPSvc	
TeamViewer_Service.exe	5480	TCP	Listen	127.0.0.1	5939	0.0.0.0	0	2/23/2022 8:00:30 AM	TeamViewer	
RemoteServerWin.exe	10404	TCP	Listen	0.0.0.0	9510	0.0.0.0	0	2/23/2022 8:01:04 AM	RemoteServerWin.exe	
RemoteServerWin.exe	10404	TCP	Listen	0.0.0.0	9512	0.0.0.0	0	2/23/2022 8:01:04 AM	RemoteServerWin.exe	
lsass.exe	772	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2/23/2022 8:00:22 AM	lsass.exe	
wininit.exe	672	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2/23/2022 8:00:22 AM	wininit.exe	
svchost.exe	1556	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2/23/2022 8:00:22 AM	EventLog	
svchost.exe	1380	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2/23/2022 8:00:22 AM	Schedule	
spoolsv.exe	4072	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	2/23/2022 8:00:27 AM	Spooler	
services.exe	748	TCP	Listen	0.0.0.0	49674	0.0.0.0	0	2/23/2022 8:00:28 AM	services.exe	
svchost.exe	4840	TCP	Listen	0.0.0.0	49676	0.0.0.0	0	2/23/2022 8:00:28 AM	PolicyAgent	
svchost.exe	5432	TCP	Established	192.168.1.68	49694	20.199.120.182	443	2/23/2022 8:00:34 AM	WpnService	
[Time Wait]		TCP	Time Wait	192.168.1.68	50337	80.99.194.96	39475			
[Time Wait]		TCP	Time Wait	192.168.1.68	50574	5.39.217.125	2710			
[Time Wait]		TCP	Time Wait	192.168.1.68	50602	217.197.185.119	61404			
[Time Wait]		TCP	Time Wait	192.168.1.68	50610	77.221.50.129	55282			
[Time Wait]		TCP	Time Wait	192.168.1.68	50630	89.134.100.232	16881			
[Time Wait]		TCP	Time Wait	192.168.1.68	50640	80.99.81.203	8999			
[Time Wait]		TCP	Time Wait	192.168.1.68	50641	188.36.219.192	46696			
helper.exe	11096	TCP	Established	192.168.1.68	50646	54.205.140.90	443	2/23/2022 11:22:08 AM	helper.exe	
[Time Wait]		TCP	Time Wait	192.168.1.68	50647	188.6.119.174	56623			
[Time Wait]		TCP	Time Wait	192.168.1.68	50680	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50681	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50686	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50687	52.182.143.208	443			
[Time Wait]		TCP	Time Wait	192.168.1.68	50688	52.182.143.208	443			
msedge.exe	2920	TCP	Established	192.168.1.68	50706	204.79.197.219	443	2/23/2022 11:22:16 AM	msedge.exe	
msedge.exe	2920	TCP	Established	192.168.1.68	50707	13.107.6.158	443	2/23/2022 11:22:16 AM	msedge.exe	

Endpoints: 290 Established: 53 Listening: 32 Time Wait: 43 Close Wait: 7 Update: 2 sec States: (All)

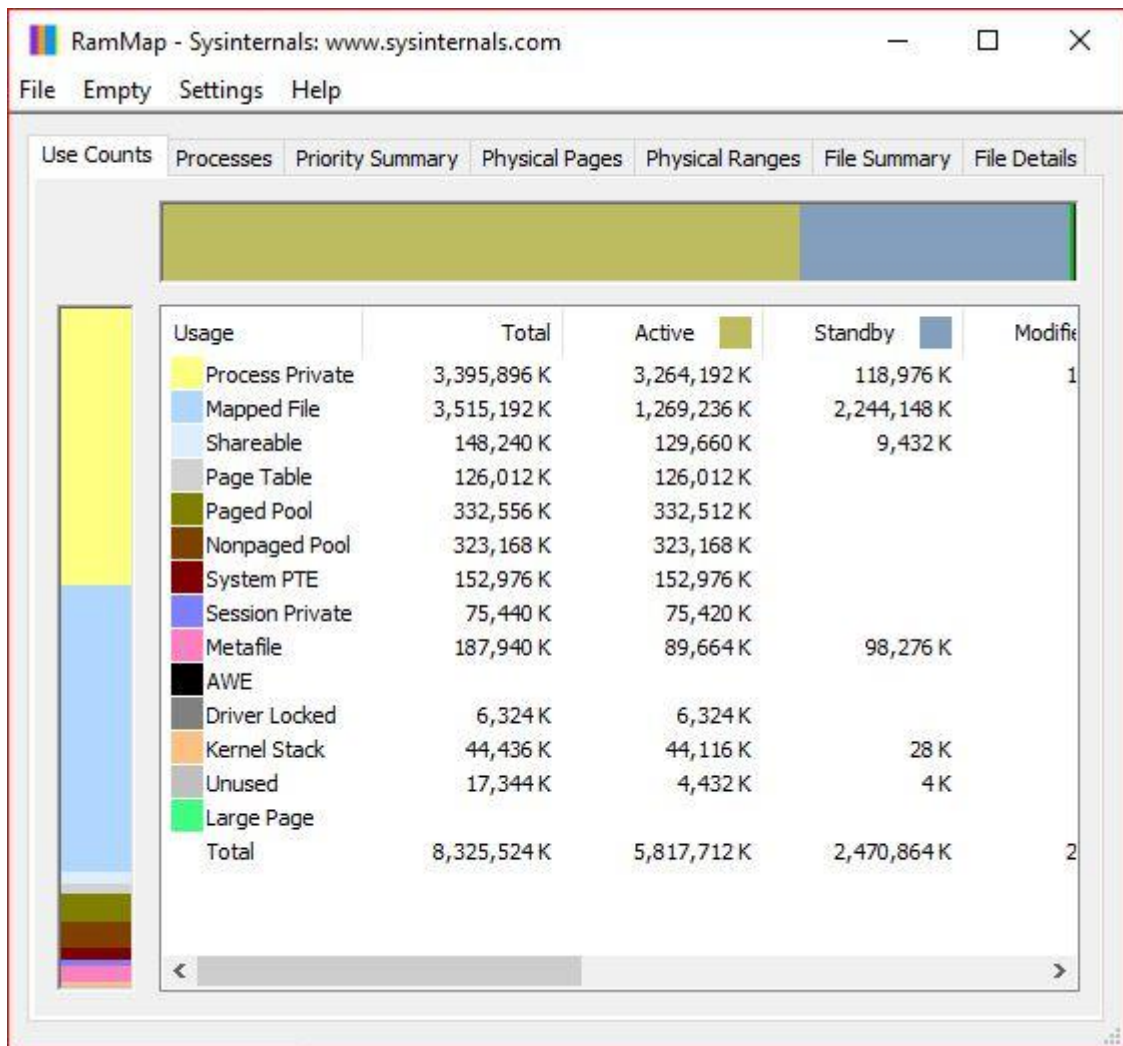
C, processzor kihasználtságot ill a processzek erőforrás igényét méri

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		12,064 K	94,360 K	108		
System Idle Process	76.29	60 K	8 K	0		
System	0.38	192 K	140 K	4		
Interrupts	0.76	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,068 K	1,048 K	384		
Memory Compression	< 0.01	1,416 K	333,192 K	2544		
csrss.exe		1,836 K	5,192 K	540		
wininit.exe		1,364 K	6,332 K	672		
services.exe		6,444 K	9,940 K	748		
svchost.exe		11,644 K	28,696 K	984	Host Process for Windows S...	Microsoft Corporation
SettingSyncHost.exe		2,612 K	6,136 K	2248	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperience...		48,384 K	96,876 K	4900		
RuntimeBroker.exe		7,276 K	27,968 K	7248	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	323,128 K	113,276 K	7488	Search application	Microsoft Corporation
RuntimeBroker.exe		16,444 K	50,508 K	7796	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	32,896 K	2,084 K	9044		Microsoft Corporation
RuntimeBroker.exe		8,596 K	28,336 K	8228	Runtime Broker	Microsoft Corporation
dllhost.exe		9,968 K	18,460 K	5060	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		3,120 K	19,176 K	9548	Runtime Broker	Microsoft Corporation
Cortana.exe	Susp...	32,428 K	59,900 K	10352	Cortana	Microsoft Corporation
RuntimeBroker.exe		4,024 K	22,100 K	11280	Runtime Broker	Microsoft Corporation
ShellExperienceHost...	Susp...	13,988 K	41,948 K	12220	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2,772 K	16,272 K	11152	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		12,724 K	34,120 K	5652	Application Frame Host	Microsoft Corporation
Calculator.exe	Susp...	23,604 K	1,684 K	14132		
RuntimeBroker.exe		1,580 K	6,264 K	14168	Runtime Broker	Microsoft Corporation
UserOOBEBroker.exe		2,000 K	9,172 K	13452	User OOBEBroker	Microsoft Corporation
TextInputHost.exe		16,344 K	40,848 K	8756		Microsoft Corporation
SearchApp.exe	Susp...	339,500 K	86,404 K	13012	Search application	Microsoft Corporation

CPU Usage: 22.89% Commit Charge: 70.10% Processes: 208

D, Ezt nem tudtam megcsinálni, nem tudtam feltelepíteni a szükséges programot a win 10-re.

E, Ram kihasználtságot figyeli



3. Feladat

A,

The screenshot shows the Dependency Walker window for the executable 'neptunkod.exe'. The left pane displays a tree of loaded modules, including 'MSCOREE.DLL', 'API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL', 'NTDLL.DLL', 'KERNELBASE.DLL', and several 'API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL' and 'EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL' modules. The right pane shows the 'Function' list for the selected module, listing various Windows API functions like 'AcquireSRWLockExclusive', 'CloseHandle', 'CreateEventW', 'CreateFileMappingW', 'CreateFileW', 'CreateMutexW', 'CreateSemaphoreW', and 'CreateToolhelp32Snapshot'. The bottom pane shows the 'Module' list, which includes 'API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL' and 'API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL'. The status bar at the bottom indicates 'Error: At least one required implicit or forwarded dependency was not found.' and 'Warning: At least one delay-load dependency module was not found.'

B,

The screenshot shows the Dependency Walker window for the executable 'neptunkod.exe'. The left pane displays a tree of loaded modules, including 'MSCOREE.DLL', 'API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL', 'NTDLL.DLL', 'KERNELBASE.DLL', and several 'API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL' and 'EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL' modules. The right pane shows the 'Function' list for the selected module, listing various Windows API functions like 'N/A', 'CsrAllocateCaptureBuffer', 'CsrAllocateMessagePointer', 'CsrCaptureMessageBuffer', 'CsrCaptureMessageMultiUnicodeStringsInPlace', 'CsrClientCallServer', 'CsrClientConnectToServer', 'CsrFreeCaptureBuffer', and 'CsrGetProcessId'. The bottom pane shows the 'Module' list, which includes 'API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL' and 'API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL'. The status bar at the bottom indicates 'Error: At least one required implicit or forwarded dependency was not found.' and 'Warning: At least one delay-load dependency module was not found.'

NTDLL.DLL (itt kezdődnek a user módú komponensek) Az NTDLL.DLL egy speciális, dinamikusan kapcsolódó (kölsön)könyvtár (Dynamically Linked Library / Dinamikusan kapcsolódó [kölsön]könyvtár. A kölcsönkönyvtár fogalmi magyarázata egy korábbi fejezetben már szerepelt.) A Windows NT alapú operációs rendszerekben az NTDLL.DLL használata megkerülhetetlen a user mód és a kernel mód közötti kommunikáció lebonyolításához. Az executive rétegben már tárgyalt objektumok közötti kapcsolattartás, az LPC (Local Procedure Call / Lokális eljárás hívás) az, amely a megfelelő függvényhívások segítségével teszi lehetővé ezt a kommunikációt is. A

felhasználói objektumok csak az NTDLL.DLL igénybe vételével érhetik el az operációs rendszer kernel módban működő részét, illetve a hardvert.

Magát a kommunikációt az NTDLL.DLL néhány egyszerű lépésben hajtja végre.

1. lépés Az NTDLL.DLL-hez függvényhívás érkezik valamelyik felsőbb rétegből.
2. lépés Az NTDLL.DLL ellenőrzi a függvényhívás hívás paramétereit. (Normál esetben nincs szükség hibakezelésre.)
3. lépés Végre kell hajtani egy user mód – kernel mód váltást.
4. lépés Az NTDLL.DLL átadja a rendszerhívást a system service dispatcher-nek.
5. lépés Az operációs rendszer így már képes meghívni a kért funkciót realizáló kernel módú függvényét.

NTDLL.DLL tartalmilag az executive által kiajánlott függvényeknek megfelelő függvény csonkokból áll, melyek ugyanolyan a paraméterezésűek, mint az executive-ban lévő párjuk. Ezen kívül tartalmaz számos további függvény az alrendszerek támogatására.

Ezek közül a két legfontosabb:

- dinamikus memória kezelés (Heap)
- Image Loader