

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Siska Dávid Bsc

Gazdaságinformatikus

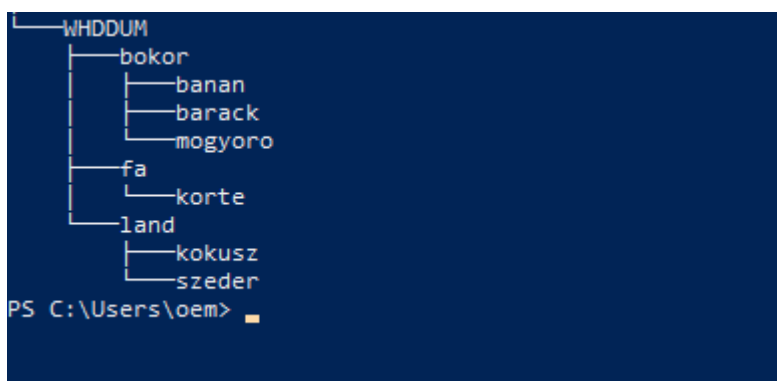
WHDDUM

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!

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



b) Készítsen másolatot:

- a neptunkod/ land/szeder katalógusról a neptunkod/fa katalógusba
- a neptunkod /bokor/banan katalógusról a neptunkod /fa katalógusba

```
PS C:\Users\oem> cp -r WHDDUM/land/szeder WHDDUM/fa
PS C:\Users\oem> cp -r WHDDUM/bokor/banan WHDDUM/fa
```

c) 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

```
PS C:\Users\oem> move WHDDUM/bokor/barack WHDDUM/fa
PS C:\Users\oem> move WHDDUM/land/kokusz WHDDUM/fa
```

d) Törölje a neptunkod/land katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:

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

```
PS C:\Users\oem\WHDDUM> cd..
PS C:\Users\oem> rm -r WHDDUM/land
PS C:\Users\oem> new-item WHDDUM/bokor/banan/leiras.txt

Directory: C:\Users\oem\WHDDUM\bokor\banan

Mode                LastWriteTime         Length Name
----                -
-a-----         2022. 02. 22.      21:11             0 leiras.txt
```

```
PS C:\Users\oem> mkdir WHDDUM/tree

Directory: C:\Users\oem\WHDDUM

Mode                LastWriteTime         Length Name
----                -
d-----          2022. 02. 22.   21:13         tree

PS C:\Users\oem> new-item WHDDUM/tree/felsorolas.txt

Directory: C:\Users\oem\WHDDUM\tree

Mode                LastWriteTime         Length Name
----                -
-a-----          2022. 02. 22.   21:13             0 felsorolas.txt
```

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

```
PS C:\Users\oem> set-content WHDDUM/bokor/banan/leiras.txt 'A barack egészséges
>> finom
>> gyümölcs'
PS C:\Users\oem> get-content WHDDUM/bokor/banan/leiras.txt
A barack egészséges
finom
gyümölcs
PS C:\Users\oem> set-content WHDDUM/tree/felsorolas.txt 'Milan
>> Mark
>> Kinga
>> David
>> Mate'
PS C:\Users\oem> get-content WHDDUM/tree/felsorolas.txt
Milan
Mark
Kinga
David
Mate
```

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

```
WHDDUM
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── tree
    └── felsorolas.txt
```

tree /f parancs segítségével lehetséges a feladat megvalósítása.

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

```
PS C:\Users\oem> cd WHDDUM
PS C:\Users\oem\WHDDUM> dir -s "?e*"

Directory: C:\Users\oem\WHDDUM\bokor\banan

Mode                LastWriteTime         Length Name
----                -
-a-----         2022. 02. 22.    21:39             37 leiras.txt

Directory: C:\Users\oem\WHDDUM\tree

Mode                LastWriteTime         Length Name
----                -
-a-----         2022. 02. 22.    21:41             29 felsorolas.txt

PS C:\Users\oem\WHDDUM>
```

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

```
PS C:\Users\oem\WHDDUM> icacls tree/felsorolas.txt
tree/felsorolas.txt NT AUTHORITY\SYSTEM:(I)(F)
                   BUILTIN\Rendszergazdák:(I)(F)
                   DESKTOP-EIIN6M9\oem:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\oem\WHDDUM>
```

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

```
PS C:\Users\oem\WHDDUM> dir -s

Directory: C:\Users\oem\WHDDUM

Mode                LastWriteTime         Length Name
----                -
d-----         2022. 02. 22.    20:59      bokor
d-----         2022. 02. 22.    20:59      fa
d-----         2022. 02. 22.    21:13      tree

Directory: C:\Users\oem\WHDDUM\bokor

Mode                LastWriteTime         Length Name
----                -
d-----         2022. 02. 22.    21:11      banan
d-----         2022. 02. 22.    20:08      mogyoro

Directory: C:\Users\oem\WHDDUM\bokor\banan

Mode                LastWriteTime         Length Name
----                -
-a-----         2022. 02. 22.    21:39             37 leiras.txt

Directory: C:\Users\oem\WHDDUM\fa

Mode                LastWriteTime         Length Name
----                -
d-----         2022. 02. 22.    20:48      banan
d-----         2022. 02. 22.    20:08      barack
d-----         2022. 02. 22.    20:09      kokusz
d-----         2022. 02. 22.    20:09      korte
d-----         2022. 02. 22.    20:48      szeder

Directory: C:\Users\oem\WHDDUM\tree

Mode                LastWriteTime         Length Name
----                -
-a-----         2022. 02. 22.    21:41             29 felsorolas.txt
```

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

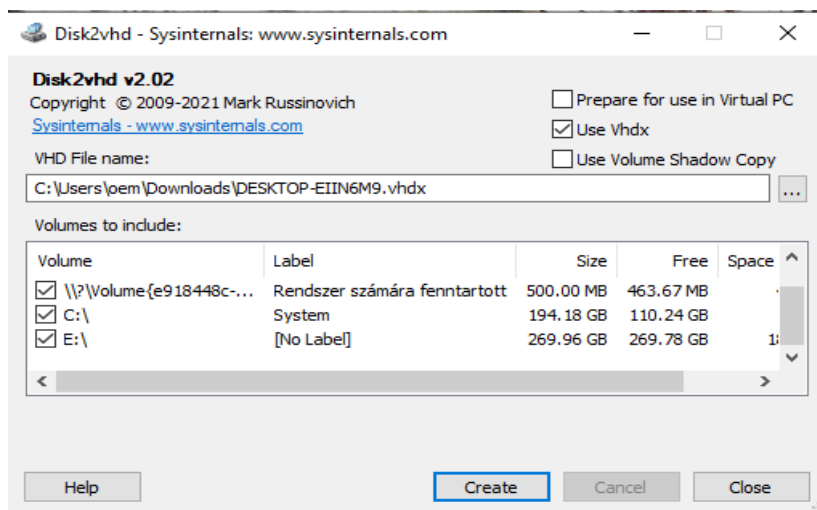
```
PS C:\Users\oem> get-content WHDDUM/tree/felsorolas.txt | Sort-Object
David
Kinga
Mark
Mate
Milan
```

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>

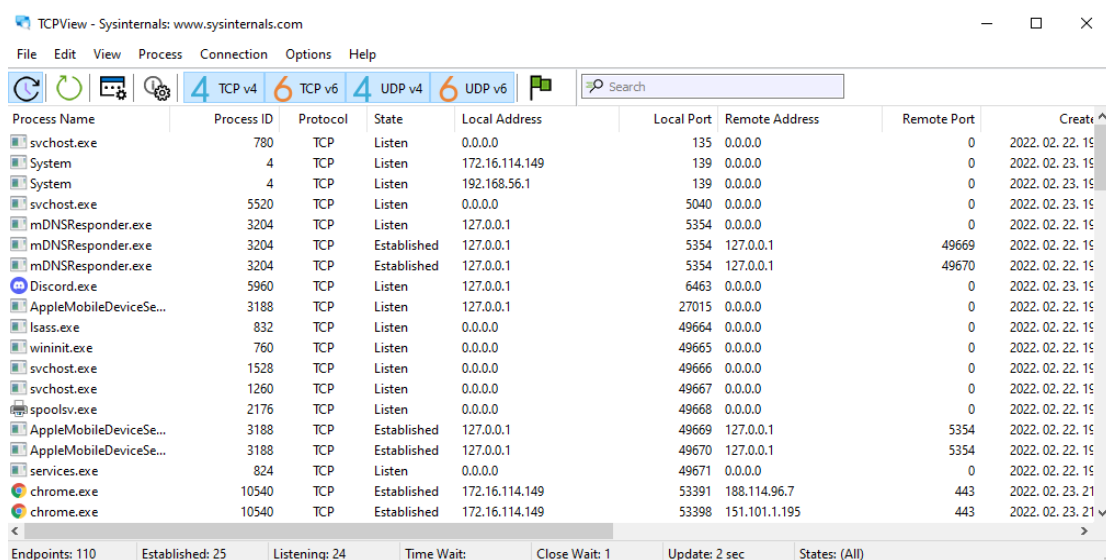
A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

a) File and Disk Utilities (Disk2vhd)



A Disk2vhd felhasználói felület felsorolja rendszerben jelenlévő köteteket. .vhd fájlokat készíti a lemezekről, amelyen a kiválasztott kötetek tartózkodnak. Ez megőrzi a partíciókat, csak átmásolja az adatokat.

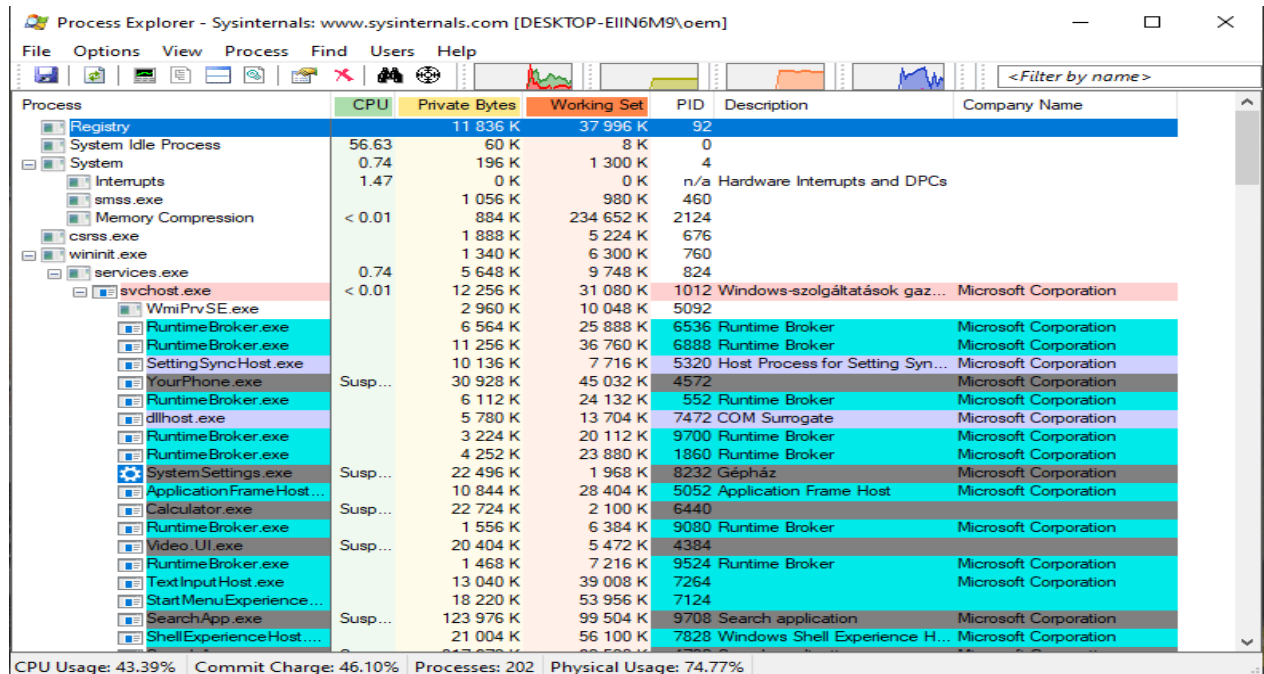
b) Networking Utilities (TCPView)



A TCPView egy Windows program, amely részletes listában mutatja be a rendszer összes TCP- és UDP-végpontját, beleértve a helyi és távoli címeket, valamint a TCP-kapcsolatok állapotát. A Windows Server 2008, Vista és XP rendszeren a TCPView a végpont tulajdonában található folyamat nevét is jelenti.

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

Process Explorer

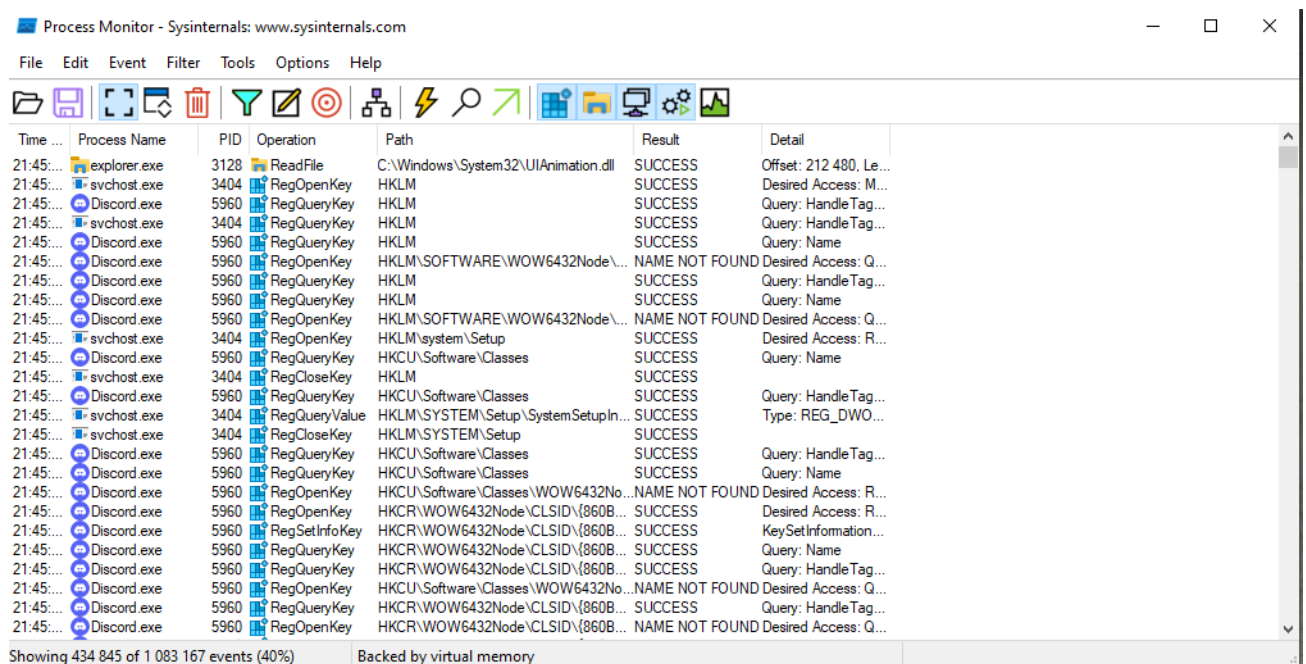


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		11 836 K	37 996 K	92		
System Idle Process	56.63	60 K	8 K	0		
System	0.74	196 K	1 300 K	4		
Interrupts	1.47	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 056 K	980 K	460		
Memory Compression	< 0.01	884 K	234 652 K	2124		
csrss.exe		1 888 K	5 224 K	676		
wininit.exe		1 340 K	6 300 K	760		
services.exe	0.74	5 648 K	9 748 K	824		
svchost.exe	< 0.01	12 256 K	31 080 K	1012	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrivSE.exe		2 960 K	10 048 K	5092		
RuntimeBroker.exe		6 564 K	25 888 K	6536	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		11 256 K	36 760 K	6888	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		10 136 K	7 716 K	5320	Host Process for Setting Syn...	Microsoft Corporation
YourPhone.exe	Susp...	30 928 K	45 032 K	4572		Microsoft Corporation
RuntimeBroker.exe		6 112 K	24 132 K	552	Runtime Broker	Microsoft Corporation
dllhost.exe		5 780 K	13 704 K	7472	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		3 224 K	20 112 K	9700	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4 252 K	23 880 K	1860	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	22 496 K	1 968 K	8232	Gépház	Microsoft Corporation
ApplicationFrameHost...		10 844 K	28 404 K	5052	Application Frame Host	Microsoft Corporation
Calculator.exe	Susp...	22 724 K	2 100 K	6440		
RuntimeBroker.exe		1 556 K	6 384 K	9080	Runtime Broker	Microsoft Corporation
Video.UI.exe	Susp...	20 404 K	5 472 K	4384		
RuntimeBroker.exe		1 468 K	7 216 K	9524	Runtime Broker	Microsoft Corporation
TextInputHost.exe		13 040 K	39 008 K	7264		Microsoft Corporation
StartMenuExperience...		18 220 K	53 956 K	7124		
SearchApp.exe	Susp...	123 976 K	99 504 K	9708	Search application	Microsoft Corporation
ShellExperienceHost....		21 004 K	56 100 K	7828	Windows Shell Experience H...	Microsoft Corporation

CPU Usage: 43.39% Commit Charge: 46.10% Processes: 202 Physical Usage: 74.77%

A Process Explorer segítségével részletesen nyomon követhetjük, lebonthatjuk a futó processzeket, a DLL eljárásokat vagy éppen a szolgáltatásokat. Ezeket leállíthatjuk, módosíthatjuk a prioritásukat, jellemzőit, vagy vizuálisan láthatjuk gépünk működését a monitor ablak segítségével.

Process Monitor

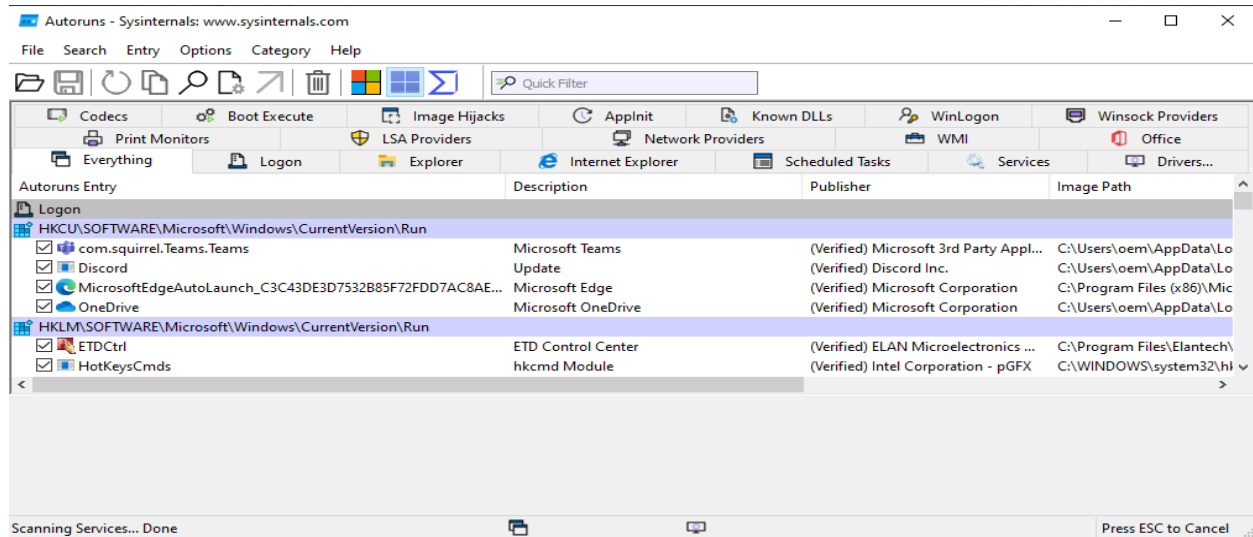


Time	Process Name	PID	Operation	Path	Result	Detail
21:45:...	explorer.exe	3128	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 212 480, Le...
21:45:...	svchost.exe	3404	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
21:45:...	Discord.exe	5960	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
21:45:...	svchost.exe	3404	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
21:45:...	Discord.exe	5960	RegQueryKey	HKLM	SUCCESS	Query: Name
21:45:...	Discord.exe	5960	RegOpenKey	HKLM\SOFTWARE\WOW6432Node\...	NAME NOT FOUND	Desired Access: Q...
21:45:...	Discord.exe	5960	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
21:45:...	Discord.exe	5960	RegQueryKey	HKLM	SUCCESS	Query: Name
21:45:...	Discord.exe	5960	RegOpenKey	HKLM\SOFTWARE\WOW6432Node\...	NAME NOT FOUND	Desired Access: Q...
21:45:...	svchost.exe	3404	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...
21:45:...	Discord.exe	5960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
21:45:...	svchost.exe	3404	RegCloseKey	HKLM	SUCCESS	
21:45:...	Discord.exe	5960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
21:45:...	svchost.exe	3404	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...
21:45:...	svchost.exe	3404	RegOpenKey	HKLM\SYSTEM\Setup	SUCCESS	
21:45:...	Discord.exe	5960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
21:45:...	Discord.exe	5960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
21:45:...	Discord.exe	5960	RegOpenKey	HKCU\Software\Classes\WOW6432No...	NAME NOT FOUND	Desired Access: R...
21:45:...	Discord.exe	5960	RegOpenKey	HKCR\WOW6432Node\CLSID\{860B...	SUCCESS	Desired Access: R...
21:45:...	Discord.exe	5960	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{860B...	SUCCESS	KeySetInformation...
21:45:...	Discord.exe	5960	RegQueryKey	HKCR\WOW6432Node\CLSID\{860B...	SUCCESS	Query: Name
21:45:...	Discord.exe	5960	RegQueryKey	HKCR\WOW6432Node\CLSID\{860B...	SUCCESS	Query: HandleTag...
21:45:...	Discord.exe	5960	RegOpenKey	HKCU\Software\Classes\WOW6432No...	NAME NOT FOUND	Desired Access: Q...
21:45:...	Discord.exe	5960	RegQueryKey	HKCR\WOW6432Node\CLSID\{860B...	SUCCESS	Query: HandleTag...
21:45:...	Discord.exe	5960	RegOpenKey	HKCR\WOW6432Node\CLSID\{860B...	NAME NOT FOUND	Desired Access: Q...

Showing 434 845 of 1 083 167 events (40%) Backed by virtual memory

Valós idejű fájlrendszer-, beállításjegyzék- és folyamat-/száltevékenységet mutat be. Számos fejlesztést tartalmaz, többek között gazdag és nem kipusztító szűrést, átfogó eseménytulajdonságokat, például munkamenet-azonosítókat és felhasználóneveket, megbízható folyamatinformációkat, teljes szálkészleteket az egyes műveletek integrált szimbólumtámogatásával, a fájlba történő egyidejű naplózást.

AutoRuns



A program futtatásakor átfogó listát ad az összes programról, amely a Windows indításakor futtatásra van beállítva.

d) Security Utilities (LogonSession)

```
Administrator: Command Prompt
UPN:

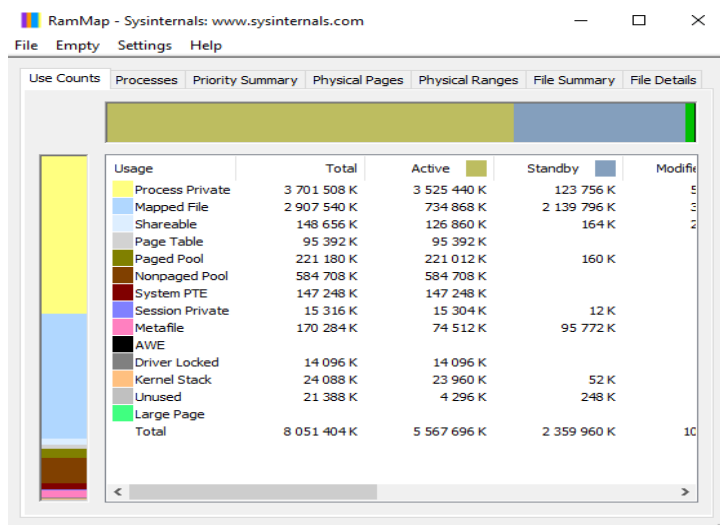
C:\>logonsessions -p

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\DESKTOP-MO4J1HK$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 5/14/2021 1:28:56 PM
Logon server:
DNS Domain:
UPN:
616: lsass.exe
768: svchost.exe
888: winlogon.exe
1056: svchost.exe
1268: svchost.exe
1276: svchost.exe
1308: svchost.exe
1416: svchost.exe
1440: svchost.exe
1980: svchost.exe
1988: svchost.exe
```

Felsorolja az aktuálisan aktív bejelentkezési munkameneteket, és ha megadja a -p kapcsolót, az egyes munkamenetekben futó folyamatokat.

e) Information Utilities (RAMMap)



A RAMMap használatával megértheti, hogyan kezeli Windows a memóriahasználatot, elemezheti az alkalmazás memóriahasználatát, vagy választ ad a RAM kiosztásával kapcsolatos konkrét kérdésekre.

3.feladat - 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 vezeteknev.txt fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc.

```
using System;
using System.IO;

namespace WHDOUM
{
    class Program
    {
        static void Main(string[] args)
        {
            StreamWriter sw = new StreamWriter("vezeteknev.txt");

            sw.WriteLine("Siska Dávid");
            sw.WriteLine("Gazdaságinformatikus");
            sw.WriteLine("WHDOUM");

            sw.Close();

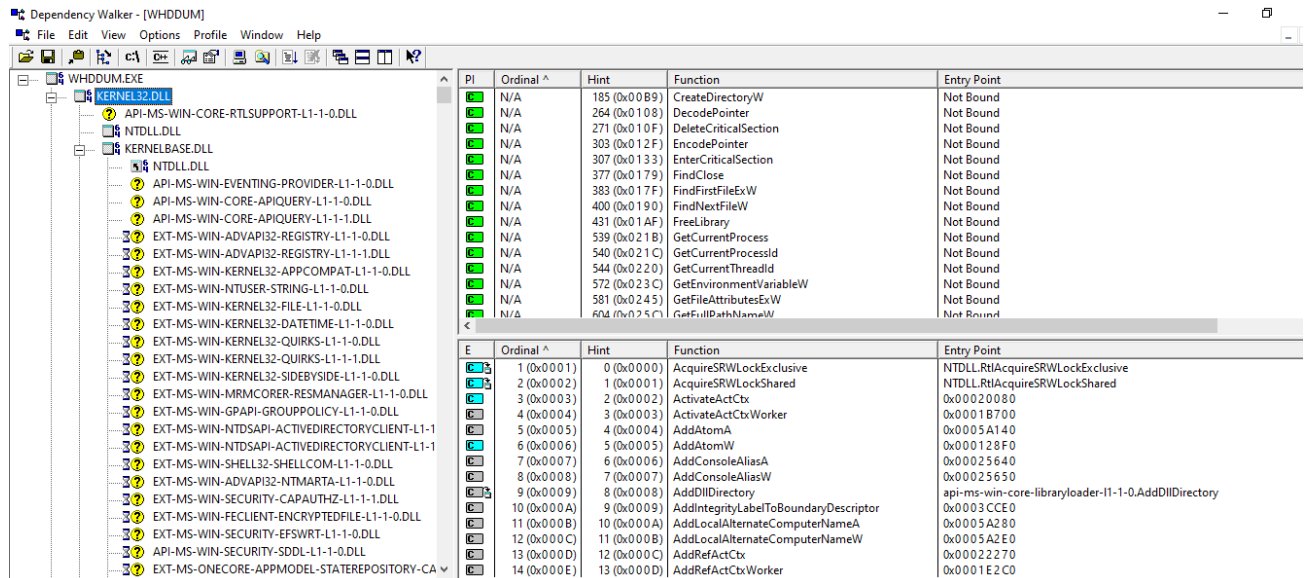
            StreamReader sr = new StreamReader("vezeteknev.txt");

            string text = sr.ReadLine();
            while (text != null)
            {
                Console.WriteLine(text);
                text = sr.ReadLine();
            }
            sr.Close();
        }
    }
}
```

Fordítsa le kódot a C fordító, majd tegye futtathatóvá az állományt: neptunkod.exe

A Dependency Walker segítségével végezze el a következő feladatokat.
Nyissa meg a neptunkod.exe fájlt!

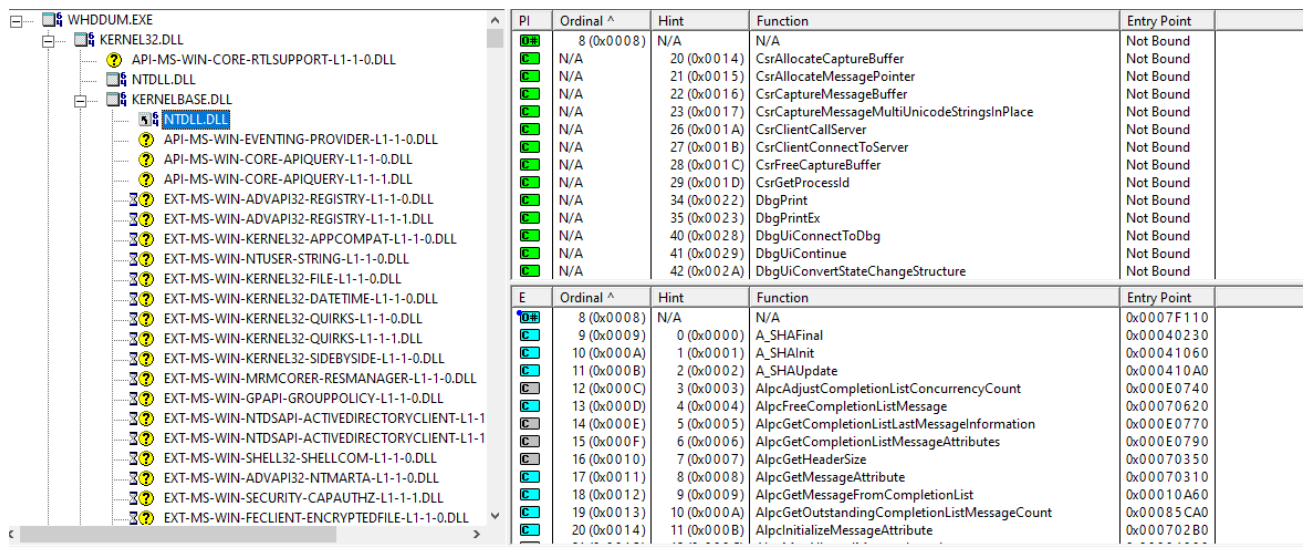
a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!



PI	Ordinal ^	Hint	Function	Entry Point
N/A		185 (0x0089)	CreateDirectoryW	Not Bound
N/A		264 (0x0108)	DecodePointer	Not Bound
N/A		271 (0x010F)	DeleteCriticalSection	Not Bound
N/A		303 (0x012F)	EncodePointer	Not Bound
N/A		307 (0x0133)	EnterCriticalSection	Not Bound
N/A		377 (0x0179)	FindClose	Not Bound
N/A		383 (0x017F)	FindFirstFileExW	Not Bound
N/A		400 (0x0190)	FindNextFileW	Not Bound
N/A		431 (0x01AF)	FreeLibrary	Not Bound
N/A		539 (0x0218)	GetCurrentProcess	Not Bound
N/A		540 (0x021C)	GetCurrentProcessId	Not Bound
N/A		544 (0x0220)	GetCurrentThreadId	Not Bound
N/A		572 (0x023C)	GetEnvironmentVariableW	Not Bound
N/A		581 (0x0245)	GetFileAttributesExW	Not Bound
N/A		604 (0x025C)	GetFullPathNameW	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
1 (0x0001)	0 (0x0000)		AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
2 (0x0002)	1 (0x0001)		AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
3 (0x0003)	2 (0x0002)		ActivateActCtx	0x00020080
4 (0x0004)	3 (0x0003)		ActivateActCtxWorker	0x0001B700
5 (0x0005)	4 (0x0004)		AddAtomA	0x0005A140
6 (0x0006)	5 (0x0005)		AddAtomW	0x000128F0
7 (0x0007)	6 (0x0006)		AddConsoleAliasA	0x00025640
8 (0x0008)	7 (0x0007)		AddConsoleAliasW	0x00025650
9 (0x0009)	8 (0x0008)		AddDllDirectory	api-ms-win-core-libraryloader-l1-1-0.AddDllDirectory
10 (0x000A)	9 (0x0009)		AddIntegrityLabelToBoundaryDescriptor	0x0003CCE0
11 (0x000B)	10 (0x000A)		AddLocalAlternateComputerNameA	0x0005A280
12 (0x000C)	11 (0x000B)		AddLocalAlternateComputerNameW	0x0005A2E0
13 (0x000D)	12 (0x000C)		AddRefActCtx	0x00022270
14 (0x000E)	13 (0x000D)		AddRefActCtxWorker	0x0001E2C0

b.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról! ,



PI	Ordinal ^	Hint	Function	Entry Point
N/A	8 (0x0008)	N/A	N/A	Not Bound
N/A		20 (0x0014)	CsrAllocateCaptureBuffer	Not Bound
N/A		21 (0x0015)	CsrAllocateMessagePointer	Not Bound
N/A		22 (0x0016)	CsrCaptureMessageBuffer	Not Bound
N/A		23 (0x0017)	CsrCaptureMessageMultiUnicodeStringsInPlace	Not Bound
N/A		26 (0x001A)	CsrClientCallServer	Not Bound
N/A		27 (0x001B)	CsrClientConnectToServer	Not Bound
N/A		28 (0x001C)	CsrFreeCaptureBuffer	Not Bound
N/A		29 (0x001D)	CsrGetProcessId	Not Bound
N/A		34 (0x0022)	DbgPrint	Not Bound
N/A		35 (0x0023)	DbgPrintEx	Not Bound
N/A		40 (0x0028)	DbgUiConnectToDbg	Not Bound
N/A		41 (0x0029)	DbgUiContinue	Not Bound
N/A		42 (0x002A)	DbgUiConvertStateChangeStructure	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
8 (0x0008)	N/A		N/A	0x0007F110
9 (0x0009)	0 (0x0000)		A_SHAFinal	0x00040230
10 (0x000A)	1 (0x0001)		A_SHAInit	0x00041060
11 (0x000B)	2 (0x0002)		A_SHAUpdate	0x000410A0
12 (0x000C)	3 (0x0003)		AlpcAdjustCompletionListConcurrencyCount	0x000E0740
13 (0x000D)	4 (0x0004)		AlpcFreeCompletionListMessage	0x00070620
14 (0x000E)	5 (0x0005)		AlpcGetCompletionListLastMessageInformation	0x000E0770
15 (0x000F)	6 (0x0006)		AlpcGetCompletionListMessageAttributes	0x000E0790
16 (0x0010)	7 (0x0007)		AlpcGetHeaderSize	0x00070350
17 (0x0011)	8 (0x0008)		AlpcGetMessageAttribute	0x00070310
18 (0x0012)	9 (0x0009)		AlpcGetMessageFromCompletionList	0x00010A60
19 (0x0013)	10 (0x000A)		AlpcGetOutstandingCompletionListMessageCount	0x00085CA0
20 (0x0014)	11 (0x000B)		AlpcInitializeMessageAttribute	0x00070280

Az ntdll.dll egy olyan modul, amely NT rendszerfunkciókat tartalmaz. Az ntdll.dll fájl a Microsoft által létrehozott fájl, amely az „NT Layer DLL” leírását tartalmazza, és amely az NT kernel funkcióit tartalmazza. Ez a fájl a c:\windows\system32 vagy c:\winnt\system32 könyvtárban található, és a c:\i386 könyvtárban is megtalálható.