

Operációs rendszerek BSc

2. Gyak.

2022. 02. 16.

Készítette:

Palencsár Enikő Bsc

Mérnökinformatikus

YD11NL

Miskolc, 2022

1.Feladat

a) Hozza létre a következő mappa szerkezetet!

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>cd fa
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>md korte
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>cd ..
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>cd land
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\land>md szeder
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\land>md kokusz
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\land>cd..
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E92B
C:.
|-- bokor
|   |-- banan
|   |-- barack
|   |-- mogyoro
|-- fa
|   |-- korte
|-- land
|   |-- kokusz
|   |-- szeder
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>
```

b) Készítsen másolatot:

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

```

|-- kokusz
|-- szeder
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>cd .\land\szeder
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\land\szeder>write >tmp.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\land\szeder>cd..
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\land>cd..
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>xcopy .\land .\fa /T
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E92B
C:.
|-- bokor
|   |-- banan
|   |-- barack
|   |-- mogyoro
|-- fa
|   |-- banan
|   |-- korte
|   |-- szeder
|-- land
|   |-- kokusz
|   |-- szeder
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>del .\land\szeder/tmp.txt
Invalid switch - "land".
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>del .\land\szeder/tmp.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>del .\fa\szeder/tmp.txt
Could Not Find C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa\szeder/tmp.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>del .\bokor\banan/tmp.txt
```

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

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>move .\bokor\barack .\fa
1 dir(s) moved.
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>move .\land\kokusz .\fa
1 dir(s) moved.
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E92B
C:.
|-- bokor
|   |-- banan
|   |-- mogyoro
|-- fa
|   |-- banan
|   |-- barack
|   |-- kokusz
|   |-- korte
|   |-- szeder
|-- land
|   |-- szeder
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>
```

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

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

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>rmmdir /?
Removes (deletes) a directory.

RMDIR [/S] [/Q] [drive:]path
RD [/S] [/Q] [drive:]path

    /S      Removes all directories and files in the specified directory
            in addition to the directory itself. Used to remove a directory
            tree.

    /Q      Quiet mode, do not ask if ok to remove a directory tree with /S

C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>rmmdir /S land
land, Are you sure (Y/N)? Y

C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E928
C:.
├── bokor
│   ├── banan
│   └── mogyoro
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>
```

```
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>type leiras.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>cd ..
C:\Users\encip\OneDrive\Asztali gép\VD11NL>cd bokor\banan
C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor\banan>write >leiras.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor\banan>type leiras.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor\banan>cd ..
C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor>cd ..
C:\Users\encip\OneDrive\Asztali gép\VD11NL>del leiras.txt
Could Not Find C:\Users\encip\OneDrive\Asztali gép\VD11NL\leiras.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL>cd fa
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>del leiras.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>write >felsorolas.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>type felsorolas.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>dir
Volume in drive C is Windows-SSD
Volume Serial Number is F095-E928

Directory of C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa

2022. 02. 16. 09:00 <DIR>      .
2022. 02. 16. 09:00 <DIR>      ..
2022. 02. 16. 08:45 <DIR>      banan
2022. 02. 16. 08:24 <DIR>      barack
2022. 02. 16. 09:00           0 felsorolas.txt
2022. 02. 16. 08:25 <DIR>      kokusz
2022. 02. 16. 08:25 <DIR>      korte
2022. 02. 16. 08:44 <DIR>      szeder
                        1 File(s)      0 bytes
                        7 Dir(s)    106 206 851 072 bytes free
```

```
C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor>cd barack
A rendszer nem találja a megadott elérési utat.

C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor>cd banan
C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor\banan>dir
Volume in drive C is Windows-SSD
Volume Serial Number is F095-E928

Directory of C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor\banan

2022. 02. 16. 08:58 <DIR>      .
2022. 02. 16. 08:58 <DIR>      ..
2022. 02. 16. 08:58           0 leiras.txt
                        1 File(s)      0 bytes
                        2 Dir(s)    106 206 130 176 bytes free
```

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

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor\banan>echo A barack sarga szinu>leiras.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor\banan>echo A barack gyumolcs>>leiras.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor\banan>echo A barackot szeretik a gyerekek>>leiras.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor\banan>type leiras.txt
A barack sarga szinu
A barack gyumolcs
A barackot szeretik a gyerekek
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor\banan>
```

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>echo Pazman Andras>felsorolas.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>echo Dobai Attila>>felsorolas.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>echo Gerocs Gergo>>felsorolas.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>echo Sikora David>>felsorolas.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>echo Nagy Bence>>felsorolas.txt
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>type felsorolas.txt
Pazman Andras
Dobai Attila
Gerocs Gergo
Sikora David
Nagy Bence
```

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

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>dir /S
Volume in drive C is Windows-SSD
Volume Serial Number is F095-E92B

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL

2022. 02. 16. 13:58 <DIR>      .
2022. 02. 16. 13:58 <DIR>      ..
2022. 02. 16. 13:56 <DIR>      bokor
2022. 02. 16. 14:02 <DIR>      fa
                0 File(s)          0 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor

2022. 02. 16. 13:56 <DIR>      .
2022. 02. 16. 13:56 <DIR>      ..
2022. 02. 16. 14:01 <DIR>      banan
2022. 02. 16. 13:22 <DIR>      mogyoro
                0 File(s)          0 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor\banan

2022. 02. 16. 14:01 <DIR>      .
2022. 02. 16. 14:01 <DIR>      ..
2022. 02. 16. 14:40          73 leiras.txt
                1 File(s)          73 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\bokor\mogyoro

2022. 02. 16. 13:22 <DIR>      .
2022. 02. 16. 13:22 <DIR>      ..
                0 File(s)          0 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa

2022. 02. 16. 14:02 <DIR>      .
2022. 02. 16. 14:02 <DIR>      ..
2022. 02. 16. 14:01 <DIR>      banan
2022. 02. 16. 13:42 <DIR>      barack
2022. 02. 16. 14:44          69 felsorolas.txt
2022. 02. 16. 13:25 <DIR>      kokusz
2022. 02. 16. 13:22 <DIR>      korte
2022. 02. 16. 13:46 <DIR>      szeder
```

```
2022. 02. 16. 14:01 <DIR>      .
2022. 02. 16. 14:01 <DIR>      ..
                0 File(s)          0 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa\barack

2022. 02. 16. 13:42 <DIR>      .
2022. 02. 16. 13:42 <DIR>      ..
                0 File(s)          0 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa\kokusz

2022. 02. 16. 13:25 <DIR>      .
2022. 02. 16. 13:25 <DIR>      ..
                0 File(s)          0 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa\korte

2022. 02. 16. 13:22 <DIR>      .
2022. 02. 16. 13:22 <DIR>      ..
                0 File(s)          0 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa\szeder

2022. 02. 16. 13:46 <DIR>      .
2022. 02. 16. 13:46 <DIR>      ..
                0 File(s)          0 bytes

Total Files Listed:
    2 File(s)          142 bytes
   29 Dir(s) 185 929 854 976 bytes free
C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL>
```

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

```

C:\Users\encip\OneDrive\Asztali gép\VD11NL>dir ?e* /s
Volume in drive C is Windows-SSD
Volume Serial Number is F095-E92B

Directory of C:\Users\encip\OneDrive\Asztali gép\VD11NL\bokor\banan

2022. 02. 16.  09:05                58 leiras.txt
                1 File(s)                58 bytes

Directory of C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa

2022. 02. 16.  09:12                70 felsorolas.txt
                1 File(s)                70 bytes

Total Files Listed:
                2 File(s)                128 bytes
                0 Dir(s)  106 209 079 296 bytes free

```

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

```

C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>icacls felsorolas.txt
felsorolas.txt NT AUTHORITY\SYSTEM:(I)(F)
                BUILTIN\Rendszergazdák:(I)(F)
                LAPTOP-4B3LNKVT\encip:(I)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>icacls felsorolas.txt /grant mindenki:(R)
processed file: felsorolas.txt
Successfully processed 1 files; Failed processing 0 files

C:\Users\encip\OneDrive\Asztali gép\Mappam\VD11NL\fa>icacls felsorolas.txt
felsorolas.txt Mindenki:(R)
                NT AUTHORITY\SYSTEM:(I)(F)
                BUILTIN\Rendszergazdák:(I)(F)
                LAPTOP-4B3LNKVT\encip:(I)(F)

Successfully processed 1 files; Failed processing 0 files

```

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

```

Total Files Listed:
                2 File(s)                142 bytes
                29 Dir(s)  105 930 055 600 bytes free

```

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

```

C:\Users\encip\OneDrive\Asztali gép\VD11NL>cd fa
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>type felsorolas.txt
Dobai Attila
Sikora David
Gerocs Gergo
Nagy Bence
Pazman Andras

C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>sort felsorolas.txt
Dobai Attila
Gerocs Gergo
Nagy Bence
Pazman Andras
Sikora David

```

```

C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>sort felsorolas.txt /OUTPUT felsorolas2.txt
C:\Users\encip\OneDrive\Asztali gép\VD11NL\fa>type felsorolas2.txt
Dobai Attila
Gerocs Gergo
Nagy Bence
Pazman Andras
Sikora David

```

2.Feladat

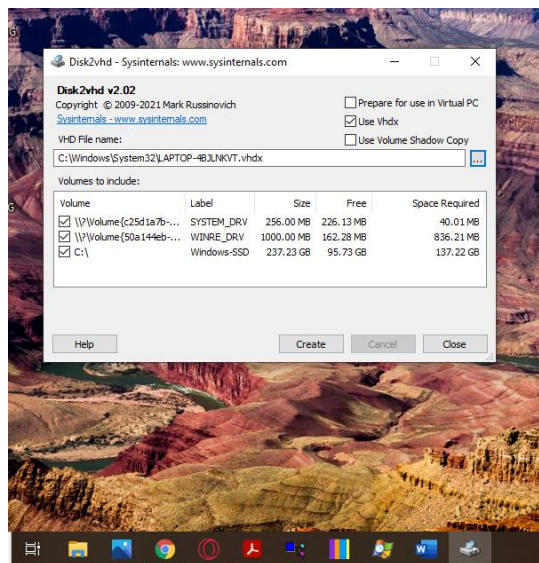
A felsorolt eszközök közül minden eszköz esetén töltsse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét - majd mentse el a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

a) File and Disk Utilities (Disk2vhd)

Szolgáltatások:

- virtuális másolat készítése fizikai lemezekről (virtuális géphez való használatra)
- egyszerű felület, 3 opcióval (Vhdx használata, felkészülés Virtuális PC-s használatra, árnyékmásolatok – azaz biztonsági mentések), valamint path választással

Eredmények: a képen látható, másolatot nem készítettem (nem is lett volna neki hely)



b) Networking Utilities (TCPView)

Szolgáltatások:

- megmutatja és részletezi a rendszer TCP és UDP végpontjait (IP címek)
- helyi és távoli címeket is mutat
- a TCP kapcsolatok állapotát jelzi (listen, established, wait)
- a hálózaton elküldött és fogadott csomagok, valamint bájtok számát tartja nyilván

Eredmények: (kép) Látható például, hogy a böngészésre használt chrome.exe folyamatosan kommunikál a szerverrel (30ezer feletti a küldött és a fogadott byte szám is), akárcsak a szövegszerkesztő winword.exe-je, de az Eset víruskereső is folyamatosan TCP kapcsolatban áll a távoli szerverrel.

TCPPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 6 UDP v4 6 UDP v6

Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	1060	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.13.10:59:24	RpcSs	
System	4	TCP	Listen	192.168.1.181	139	0.0.0.0	0	2022.02.16.14:30:04	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.16.14:29:58	System	
svchost.exe	4864	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.16.14:29:55	CDPSvc	
mDNSResponder.exe	4004	TCP	Listen	127.0.0.1	5354	0.0.0.0	0	2022.02.13.10:59:31	Bonjour Service	
lsass.exe	908	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.13.10:59:24	lsass.exe	
wininit.exe	712	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.13.10:59:24	wininit.exe	
svchost.exe	1808	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.13.10:59:25	EventLog	
svchost.exe	1560	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.13.10:59:25	Schedule	
spoolsv.exe	3816	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.13.10:59:30	Spooler	
services.exe	888	TCP	Listen	0.0.0.0	49676	0.0.0.0	0	2022.02.13.10:59:42	services.exe	
svchost.exe	4848	TCP	Established	192.168.1.181	56626	20.199.120.182	443	2022.02.16.14:30:06	WpnService	
svchost.exe	4848	TCP	Established	192.168.1.181	56629	20.199.120.182	443	2022.02.16.14:30:07	WpnService	
ekm.exe	2364	TCP	Established	192.168.1.181	56634	91.228.167.193	8883	2022.02.16.14:30:09	ekm	1
[Time Wait]		TCP	Time Wait	192.168.1.181	64053	52.109.88.180	443			
WINWORD.EXE	6720	TCP	Established	192.168.1.181	64061	20.189.173.6	443	2022.02.16.15:29:11	WINWORD.EXE	4
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2022.02.13.10:59:34	System	
svchost.exe	1060	TCPv6	Listen	::	135	::	0	2022.02.13.10:59:24	RpcSs	
System	4	TCPv6	Listen	::	445	::	0	2022.02.13.10:59:34	System	
lsass.exe	908	TCPv6	Listen	::	49664	::	0	2022.02.13.10:59:24	lsass.exe	
wininit.exe	712	TCPv6	Listen	::	49665	::	0	2022.02.13.10:59:24	wininit.exe	
svchost.exe	1808	TCPv6	Listen	::	49666	::	0	2022.02.13.10:59:25	EventLog	
svchost.exe	1560	TCPv6	Listen	::	49667	::	0	2022.02.13.10:59:25	Schedule	
spoolsv.exe	3816	TCPv6	Listen	::	49668	::	0	2022.02.13.10:59:30	Spooler	
jhi_service.exe	5572	TCPv6	Listen	:::1	49669	::	0	2022.02.13.10:59:34	jhi_service	
services.exe	888	TCPv6	Listen	::	49676	::	0	2022.02.13.10:59:42	services.exe	
chrome.exe	12504	TCPv6	Established	2001:4c4e2185:6900:d1c...	56996	2a00:1450:4025:401::bc	5228	2022.02.16.14:32:19	chrome.exe	
System	4	UDP		192.168.1.181	137	*		2022.02.16.14:30:04	System	
System	4	UDP		192.168.56.1	137	*		2022.02.16.14:29:58	System	
System	4	UDP		192.168.1.181	138	*		2022.02.16.14:30:04	System	
System	4	UDP		192.168.56.1	138	*		2022.02.16.14:29:58	System	

Endpoints: 73 Established: 5 Listening: 21 Time Wait: 1 Close Wait: Update: 2 sec States: (All)

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

Szolgáltatások – Process Monitor:

- valós időben mutatja a fájlrendszert és a processzeket, lehetővé teszi a szűrést is
- használhatjuk arra, hogy detektáljuk a sikertelen szerkesztését a Windows konfigurációs adatbázisának

Eredmények: Valóban valós időben fut és frissül a lista, a szűréseknek köszönhetően pedig rá lehet koncentrálni arra a területre, ahol problémát tapasztalunk. A program használható például arra, hogy kiderítsük, milyen függés mi tart nyitva egy fájlt, megakadályozva ezzel, hogy más programmal hozzáférhessünk annak tartalmához. Látható például, hogy amikor elmentem ezt a fájlt, a OneDrive.exe WriteFile műveletet végez.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 999 567, Le...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 999 683, Le...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 999 797, Le...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 999 915, Le...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 067, ...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 177, ...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 294, ...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 410, ...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 524, ...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 642, ...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 794, ...
17:57...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 000 904, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 021, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 137, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 251, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 369, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 521, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 631, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 748, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 864, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 001 978, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 002 096, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 002 248, ...
17:58...	OneDrive.exe	5824	WriteFile	C:\Users\lenovp\AppData\Local\Micros...	SUCCESS	Offset: 1 002 358, ...
17:58...	OneDrive.exe	5824	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
17:58...	OneDrive.exe	5824	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
17:58...	OneDrive.exe	5824	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWOW...
17:58...	OneDrive.exe	5824	RegCloseKey	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	
17:58...	OneDrive.exe	5824	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
17:58...	OneDrive.exe	5824	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
17:58...	OneDrive.exe	5824	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 20
17:58...	OneDrive.exe	5824	RegCloseKey	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	
17:58...	OneDrive.exe	5824	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
17:58...	OneDrive.exe	5824	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
17:58...	OneDrive.exe	5824	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 20
17:58...	OneDrive.exe	5824	RegCloseKey	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	

Showing 118 of 867 291 events (0.0%) Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
17:47...	Explorer.EXE	6308	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
17:47...	Explorer.EXE	6308	RegOpenKey	HKCU	SUCCESS	
17:47...	Explorer.EXE	6308	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
17:47...	Explorer.EXE	6308	RegOpenKey	HKCU\SOFTWARE\Microsoft\TabletT...	NAME NOT FOUND	Desired Access: Q...
17:47...	Explorer.EXE	6308	RegQueryKey	HKCU	SUCCESS	Query: Name, Len...
17:47...	Explorer.EXE	6308	RegQueryKey	HKCU	SUCCESS	Query: Name
17:47...	svchost.exe	2244	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppMod...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegOpenKey	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
17:47...	Explorer.EXE	6308	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
17:47...	svchost.exe	2244	RegOpenKey	HKCU\SOFTWARE\Microsoft\TabletT...	NAME NOT FOUND	Desired Access: Q...
17:47...	svchost.exe	2244	RegOpenKey	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 3 959 808, ...
17:47...	svchost.exe	2244	RegQueryKey	HKCU	SUCCESS	Query: Name, Len...
17:47...	svchost.exe	2244	RegQueryKey	HKCU	SUCCESS	Query: Name
17:47...	svchost.exe	2244	RegOpenKey	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
17:47...	svchost.exe	2244	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppMod...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
17:47...	svchost.exe	2244	RegOpenKey	HKCU	SUCCESS	
17:47...	svchost.exe	2244	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
17:47...	svchost.exe	2244	RegOpenKey	HKCU\SOFTWARE\Microsoft\TabletT...	NAME NOT FOUND	Desired Access: Q...
17:47...	svchost.exe	2244	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegQueryKey	HKCU	SUCCESS	Query: Name, Len...
17:47...	svchost.exe	2244	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
17:47...	svchost.exe	2244	RegQueryKey	HKCU	SUCCESS	Query: Name
17:47...	svchost.exe	2244	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...
17:47...	svchost.exe	2244	RegOpenKey	HKU\SOFTWARE\Microsoft\AppMod...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	Desired Access: R...
17:47...	svchost.exe	2244	RegQueryValue	HKU\DEFAULT\Control Panel\Desktop	NAME NOT FOUND	Length: 12
17:47...	svchost.exe	2244	RegCloseKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	
17:47...	svchost.exe	2244	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
17:47...	svchost.exe	2244	RegOpenKey	HKU\DEFAULT	SUCCESS	
17:47...	svchost.exe	2244	RegOpenKey	HKCU\SOFTWARE\Microsoft\TabletT...	NAME NOT FOUND	Desired Access: Q...
17:47...	svchost.exe	2244	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegQueryKey	HKCU	SUCCESS	Query: Name, Len...
17:47...	svchost.exe	2244	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
17:47...	svchost.exe	2244	RegOpenKey	HKCU	SUCCESS	Query: Name
17:47...	svchost.exe	2244	RegOpenKey	HKU\SOFTWARE\Microsoft\AppMod...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...
17:47...	svchost.exe	2244	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Desired Access: R...
17:47...	svchost.exe	2244	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...

Szolgáltatások – Process Explorer:

- információt ad a CPU használatról, a futó processzek számáról, a memóriahasználatról, a GPU és I/O használatról (a System Information ablakban grafikonok jeleníthetők meg)
- listázza az éppen aktív processzeket, azonosítóval, és a fenti információkkal együtt
- processzeket tudunk leállítani, felfüggeszteni, újraindítani

Eredmények: körülbelül 200 aktív processz, 60%-os processzorhasználat (kép). A Dependency Walker CPU használata olyan magas volt, hogy azonnal be is zártam, ne fusson a háttérben feleslegesen. Teszt: a Process Explorer felett a Wordbe írok, mire valóban megnő a CPU használata a winword.exének.

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-4BILNKVT\encip]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	188 K	14 452 K	48		
Registry		10 692 K	56 656 K	96		
System Idle Process	2.25	60 K	8 K	0		
System	10.71	200 K	24 K	4		
Interrupts	18.03	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 080 K	344 K	412		
Memory Compression	1.13	920 K	96 464 K	2732		
csrss.exe		2 124 K	2 616 K	564		
wininit.exe		1 620 K	2 808 K	712		
services.exe	1.13	6 756 K	7 008 K	888		
svchost.exe	< 0.01	17 412 K	26 180 K	352	Windows-szolgáltatások gaz...	Microsoft Corporation
dlh.exe		3 496 K	2 772 K	6928		
WmiPrivSE.exe	3.38	15 168 K	18 768 K	6744		
Eap3Host.exe		2 200 K	9 304 K	8324		
StartMenuExperience...		30 324 K	19 292 K	11984		
RuntimeBroker.exe		5 800 K	7 536 K	6284	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	143 412 K	31 484 K	11176	Search application	Microsoft Corporation
RuntimeBroker.exe		14 972 K	12 796 K	10056	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	30 952 K	1 908 K	9638		Microsoft Corporation
SettingSyncHost.exe	0.56	3 980 K	3 276 K	9760	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		4 320 K	10 812 K	14224	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 952 K	6 500 K	1408	Runtime Broker	Microsoft Corporation
unsecapp.exe		1 372 K	1 168 K	2444	Sink to receive asynchronou...	Microsoft Corporation
Cortana.exe		28 608 K	10 504 K	2164	Cortana	Microsoft Corporation
RuntimeBroker.exe		3 660 K	2 088 K	10748	Runtime Broker	Microsoft Corporation
Win32Bridge.Serv...		8 896 K	712 K	8936	Cortana System Service	Microsoft Corporation
SystemSettings.exe	Susp...	24 492 K	2 056 K	9604	Gepláz	Microsoft Corporation
ApplicationFrameHost...		11 468 K	9 268 K	8352	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		1 992 K	4 216 K	4736	User OOBEBroker	Microsoft Corporation
Video.UI.exe	Susp...	18 364 K	1 792 K	9612		
TextInputHost.exe		13 036 K	13 908 K	2900		Microsoft Corporation
ShellExperienceHost...		14 052 K	7 084 K	4472	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2 732 K	17 072 K	10844	Runtime Broker	Microsoft Corporation
dlh.exe		3 540 K	5 884 K	14128	COM Surrogate	Microsoft Corporation
smartscreen.exe		9 644 K	27 428 K	4976	Windows Defender SmartScr...	Microsoft Corporation
WmiPrivSE.exe		2 548 K	9 748 K	8848		
WUDFHost.exe		6 488 K	9 024 K	988		
svchost.exe	< 0.01	13 936 K	14 832 K	1060	Windows-szolgáltatások gaz...	Microsoft Corporation

CPU Usage: 96.93% Commit Charge: 60.73% Processes: 217 Physical Usage: 91.53%

Szolgáltatások – Autoruns:

- azt lehet megnézni, mely programok indulnak el automatikusan a Windows-zal, bejelentkezéskor
- kategóriákra bontva is megtekinthetjük
- információkat kapunk a programok kibocsátójáról, az elérési útvonalukról
- különböző színek jelzik például, ha az Autoruns nem találja meg a program kibocsátóját, vagy az nem ellenőrzött gyártó
- segítségével kiszűrhetjük a vírusokat, melyek futása automatikusan, a Windows-zal együtt indul, ezeket le is tudjuk törölni a listáról, ezáltal megelőzhetjük, hogy a legközelebbi indításkor futni kezdjenek
- lehetővé teszi azt is, hogy ha egy listát elmentünk, egy későbbi időpontban megnézhetjük (compare), melyek az újonnan megjelent programok a listában

A futtatás eredménye: (kép) A listában szerepel a OneDrive, a Teams és a Discord, az Eset víruskereső parancssori interfésze, vagy a Java frissítés ütemezője. A listában szerepelnek driverek (pl: Bluetooth driver) és ütemezett feladatok is (pl: Microsoft Office updaterek, melyek lehetővé teszik az Installernek, hogy frissítéseket keressen).

Auturuns Entry	Description	Publisher	Image Path	Timestamp
Logon				
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Tue Dec 28 10:58:25
<input checked="" type="checkbox"/> com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Appl...	C:\Users\encip\AppData\Local\Microsoft\Teams\Update.exe	Tue Dec 21 20:08:54
<input checked="" type="checkbox"/> Discord	Update	(Verified) Discord Inc.	C:\Users\encip\AppData\Local\Discord\Update.exe	Thu Dec 3 22:43:28
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\encip\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Tue Feb 8 23:04:00
<input checked="" type="checkbox"/> Opera GX Browser Assistant	Opera GX Browser Assistant	(Verified) Opera Software AS	C:\Users\encip\AppData\Local\Programs\Opera GX\assistant\browser...	Mon Feb 1 17:18:2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Sat Mar 13 21:48:06
<input checked="" type="checkbox"/> egui	ESET command line interface	(Verified) ESET, spol. s r.o.	C:\Program Files\ESET\ESET Security\ecmds.exe	Tue Jan 18 20:27:35
<input checked="" type="checkbox"/> RtkAudUService	Realtek HD Audio Universal Service	(Verified) Realtek Semiconductor ...	C:\WINDOWS\System32\RtkAudUService64.exe	Tue Mar 24 05:59:31
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Sat Dec 7 10:15:08
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sat Mar 13 20:29:42
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Tue Mar 16 20:59:18
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files (x86)\Google\Chrome\Application\98.0.4758.102\Insta...	Tue Feb 15 16:54:56
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.50\Install...	Sat Feb 12 10:26:35
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Dec 7 10:10:05
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Sat Dec 25 12:22:06
<input checked="" type="checkbox"/> CancelAutoPlay_df		(Verified) ZTE CORPORATION	C:\Program Files (x86)\4G Hostless Modem\4G Hostless Modem\Cance...	Tue May 21 11:08:4
<input checked="" type="checkbox"/> CheckGDISPort57ac06		(Verified) ZTE CORPORATION	C:\Program Files (x86)\4G Hostless Modem\4G Hostless Modem\Check...	Tue May 21 11:08:4
<input checked="" type="checkbox"/> SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Mon Sep 27 07:32:3
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Tue Mar 16 20:59:18
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Dec 7 10:10:05
C:\Users\encip\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				

d) Security Utilities (LogonSession)

Szolgáltatások – Autoruns:

- kilistázza az aktív belépéseket, a létesített üléseket, azok azonosítóit, a belépő nevét és a belépés típusát, továbbá a belépés pontos idejét
- információt ad a DNS domainről és a belépéshez használt szerverről is

A futtatás eredménye: (kép) A program csak Powershellben, adminisztrátorként megnyitva futott. Kilistázta az aktív belépéseimet, az üléseket megszámozva, így képet kaptam arról, pontosan mikor használtam a számítógépet. Láthattam például azt is, hogy 13-án a Font Driver Host általi belépés történt a Windowsra, ami azóta is aktív. A -p kapcsolóval a belépéskor futó programokat is kilistáztam.

```
PS C:\Users\encip\Downloads\SysinternalsSuite> C:\Users\encip\Downloads\
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\LAPTOP-4BJLNKVT$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2022. 02. 13. 10:59:23
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:000134f2:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2022. 02. 13. 10:59:23
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:00013b59:
User name: Font Driver Host\UMFD-0
Auth package: Negotiate
Logon type: Interactive
Session: 0
Sid: S-1-5-96-0-0
Logon time: 2022. 02. 13. 10:59:23
Logon server:
DNS Domain:
UPN:

[3] Logon session 00000000:000003e5:
User name: NT AUTHORITY\HELVI SZOLGALTATAS
Auth package: Negotiate
Logon type: Service

2098: conhost.exe
13152: logonsessions.exe

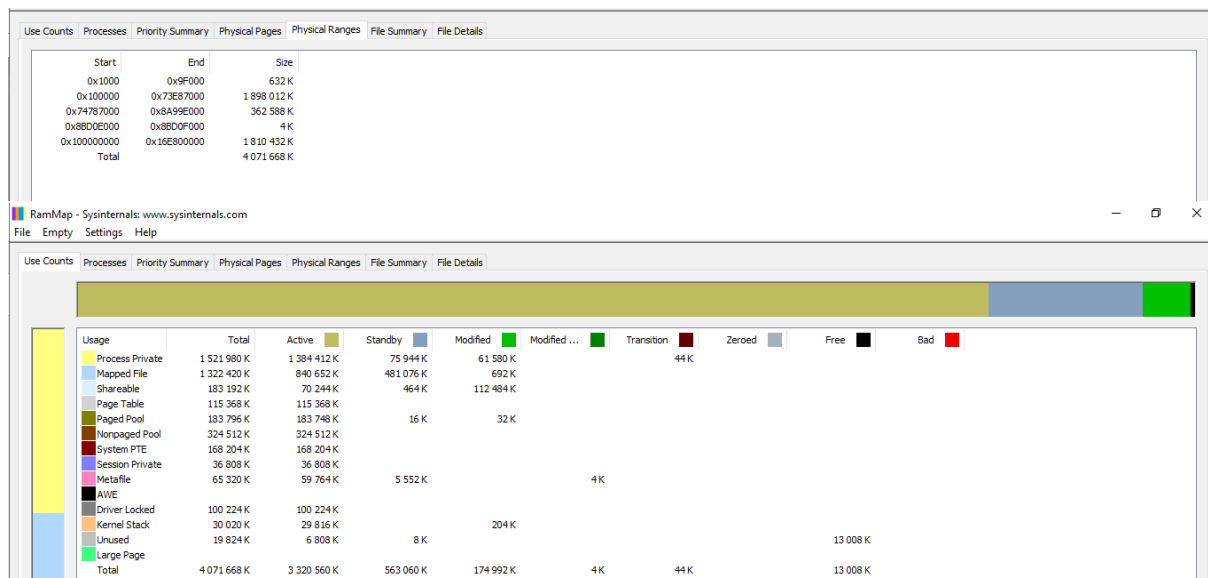
[21] Logon session 00000000:08d87450:
User name: LAPTOP-4BJLNKVT\encip
Auth package: CloudAP
Logon type: Interactive
Session: 7
Sid: S-1-5-21-3878768777-2480252345-888559105-1002
Logon time: 2022. 02. 16. 14:29:56
Logon server:
DNS Domain:
UPN:
3056: uihost.exe
10932: SymTPEnh.exe
2728: sihost.exe
12096: svchost.exe
13964: svchost.exe
6460: igfxEM.exe
11928: taskhostw.exe
13212: WacomTabletUser.exe
6308: explorer.exe
9668: ctfmon.exe
3752: svchost.exe
11984: StartMenuExperienceHost.exe
6284: RuntimeBroker.exe
11176: SearchApp.exe
10056: RuntimeBroker.exe
9760: SettingsSyncHost.exe
14224: RuntimeBroker.exe
11196: SecurityHealthSystray.exe
5228: RtkAudioService64.exe
6356: eguiProxy.exe
5824: OneDrive.exe
9224: browser_assistant.exe
348: browser_assistant.exe
2444: unsecapp.exe
12700: utility.exe
7576: ONENOTEM.EXE
2164: Cortana.exe
1492: CheckDISPort_df.exe
10748: RuntimeBroker.exe
2092: CancelAutoPlay_df.exe
13188: jusched.exe
5224: svchost.exe
```

e) Information Utilities (RAMMap)

Szolgáltatások:

- megmutatja, hogyan menedzseli a Windows a memóriát az eszközön
- láthatjuk a processzek memóriahasználatát, a fizikai címekhez társított virtuális címeket
- megmutatja a fájlok méretét, pontos helyét az eszközön

A futtatás eredménye: (képek) Megtekinthetők például a VirtualBox, az Eset, a CodeBlocks és számos dll fájl prioritási szintje, fizikai címei, az általuk foglalt memória mérete, a fizikai címtartományok és a memórialapok, valamint egy összesítés az aktív és a standby RAMról.



Use Counts							
Processes							
Priority Summary							
Physical Pages							
Physical Ranges							
File Summary							
File Details							
Process	Session	PID	Private	Standby	Modified	Page Table	Total
System	-1	4	0 K	0 K	0 K	56 K	56 K
Registry	-1	96	9 316 K	0 K	16 K	356 K	9 688 K
Secure System	-1	48	0 K	0 K	0 K	52 K	52 K
svchost.exe	0	12232	340 K	0 K	0 K	308 K	648 K
svchost.exe	0	2772	448 K	0 K	0 K	268 K	716 K
MemCompres...	-1	2732	57 688 K	72 516 K	18 516 K	828 K	149 548 K
svchost.exe	0	2672	312 K	0 K	0 K	248 K	560 K
svchost.exe	0	2664	1 596 K	0 K	0 K	316 K	1 912 K
svchost.exe	0	6724	820 K	0 K	0 K	380 K	1 200 K
Lenovo.Mod...	0	4264	10 648 K	12 K	12 K	716 K	11 388 K
svchost.exe	0	4300	648 K	0 K	0 K	352 K	1 000 K
svchost.exe	0	4184	340 K	0 K	0 K	268 K	608 K
LMS.exe	0	4380	0 K	0 K	0 K	232 K	232 K
smss.exe	-1	412	80 K	0 K	0 K	148 K	228 K
Lenovo.Mod...	7	13100	4 748 K	0 K	0 K	552 K	5 300 K
Lsaliso.exe	0	900	0 K	652 K	0 K	164 K	816 K
css.exe	0	564	720 K	0 K	0 K	236 K	956 K
amsvc.exe	0	4012	0 K	0 K	0 K	204 K	204 K
svchost.exe	0	3736	460 K	0 K	0 K	316 K	776 K
wininit.exe	0	712	0 K	0 K	8 K	252 K	260 K
svchost.exe	0	3728	260 K	0 K	0 K	272 K	532 K
services.exe	0	888	3 036 K	0 K	0 K	332 K	3 368 K
lsass.exe	0	908	4 864 K	4 K	0 K	440 K	5 308 K
mDNSRespon...	0	4004	224 K	0 K	0 K	224 K	448 K
svchost.exe	0	3928	712 K	0 K	0 K	300 K	1 012 K
fontdrvhost.exe	0	68	64 K	0 K	0 K	180 K	244 K
WacomHost...	6	6324	0 K	0 K	0 K	28 K	28 K
svchost.exe	0	352	11 804 K	0 K	0 K	584 K	12 388 K
WUDFHost.exe	0	988	832 K	0 K	0 K	328 K	1 160 K
svchost.exe	0	1180	964 K	0 K	0 K	292 K	1 256 K
WUDFHost.exe	0	1128	0 K	0 K	0 K	236 K	236 K
svchost.exe	0	4080	592 K	0 K	0 K	244 K	836 K
svchost.exe	0	1060	9 460 K	0 K	4 K	392 K	9 856 K
svchost.exe	0	1352	216 K	0 K	0 K	216 K	432 K

3.Feladat

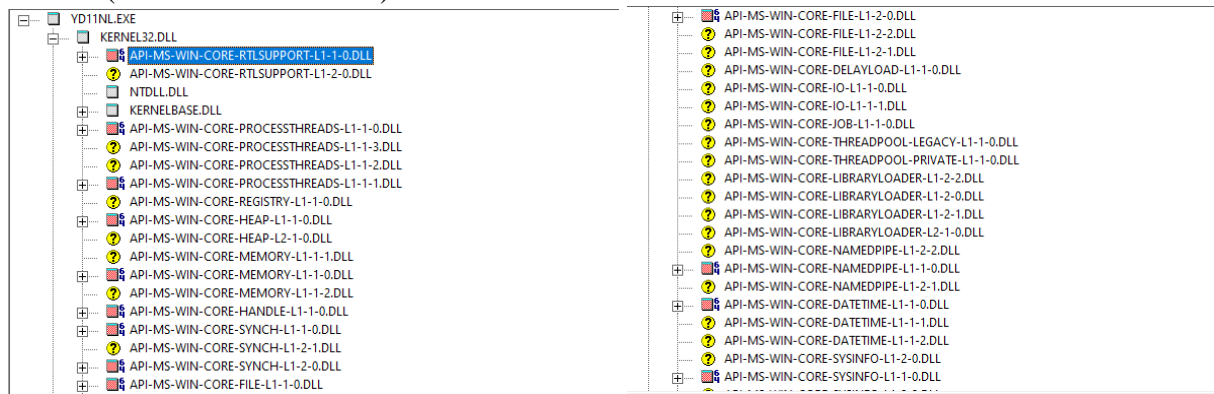
Töltse le a következő programot: Dependency Walker Készítsen egy *neptunkod.c* nevű forráskódot, amely egy *vezeteknev.txt* fájl létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc.

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

```
C:\Users\encip\OneDrive\Asztali gép\Mappam>gcc YD11NL.c -o YD11NL
C:\Users\encip\OneDrive\Asztali gép\Mappam>YD11NL.exe
C:\Users\encip\OneDrive\Asztali gép\Mappam>type palencsar.txt
Nev: Palencsar Eniko
Neptun: YD11NL
Szak: Mernokinformatikus
Kepzes: nappali
Szint: Bsc
C:\Users\encip\OneDrive\Asztali gép\Mappam>
```

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)!

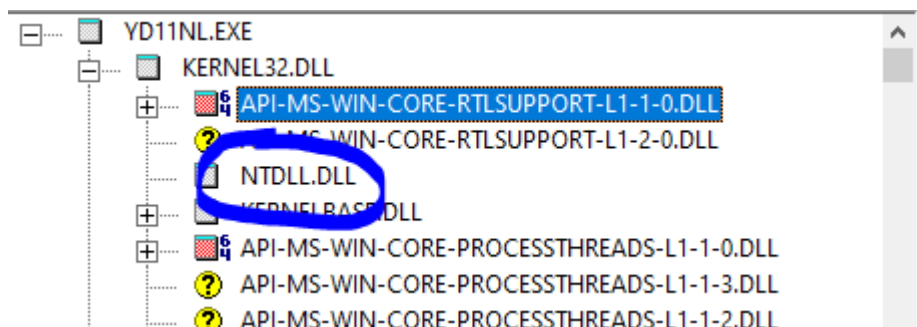


...

Ebben a viszonylag kicsi programban is rengeteg API hívás történik, melyek a teljesség igénye nélkül kapcsolatosak: processz szálakkal, a kupac kezelésével, a memóriával, a szinkronizációval, a fájlkezeléssel, az inputtal/outputtal, a konzollal, a debuggolással és a hibajelzéssel. Van köztük rendszerinformációkkal és könyvtárbetöltéssel kapcsolatos API is.

- 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 fájl kernel függvényeket tartalmaz, a Windows Native API-t exportálja, mely az OS user-módbeli komponensei (melyeknek a Win32 és egyéb API alrendszerek nélkül kell futniuk) által használt interfész. Éppen ezért nagyon fontos rendszerfájl, a user mód és a kernel mód határán.



Az exportált függvények között szerepel például az RtlCreateHeap, ami kupac memóriaterületet hoz létre, vannak továbbá virtuális memória allokáló, hozzáférést ellenőrző függvények is.

E	Ordinal ^	Hint	Function	Entry Point
	852 (0x0354)	838 (0x0346)	RtlCreateActivationContext	0x000632E0
	853 (0x0355)	839 (0x0347)	RtlCreateAndSetSD	0x000B5D90
	854 (0x0356)	840 (0x0348)	RtlCreateAtomTable	0x00060050
	855 (0x0357)	841 (0x0349)	RtlCreateBootStatusDataFile	0x000D0B10
	856 (0x0358)	842 (0x034A)	RtlCreateBoundaryDescriptor	0x0002A210
	857 (0x0359)	843 (0x034B)	RtlCreateEnvironment	0x0005AD10
	858 (0x035A)	844 (0x034C)	RtlCreateEnvironmentEx	0x0005AD40
	859 (0x035B)	845 (0x034D)	RtlCreateHashTable	0x000DAFB0
	860 (0x035C)	846 (0x034E)	RtlCreateHashTableEx	0x000DAFE0
	861 (0x035D)	847 (0x034F)	RtlCreateHeap	0x00040FA0
	862 (0x035E)	848 (0x0350)	RtlCreateMemoryBlockLookaside	0x0002A990
	863 (0x035F)	849 (0x0351)	RtlCreateMemoryZone	0x0002AAF0
	864 (0x0360)	850 (0x0352)	RtlCreateProcessParameters	0x000B5A90
	865 (0x0361)	851 (0x0353)	RtlCreateProcessParametersEx	0x000B5AD0
	866 (0x0362)	852 (0x0354)	RtlCreateProcessParametersWithTemplate	0x000282C0

E	Ordinal ^	Hint	Function	Entry Point
	205 (0x00CD)	190 (0x00BE)	NlsMbCodePageTag	0x00126930
	206 (0x00CE)	191 (0x00BF)	NlsMbOemCodePageTag	0x00126918
	207 (0x00CF)	192 (0x00C0)	NtAcceptConnectPort	0x000729D0
	208 (0x00D0)	193 (0x00C1)	NtAccessCheck	0x000729B0
	209 (0x00D1)	194 (0x00C2)	NtAccessCheckAndAuditAlarm	0x00072C60
	210 (0x00D2)	195 (0x00C3)	NtAccessCheckByType	0x00073000
	211 (0x00D3)	196 (0x00C4)	NtAccessCheckByTypeAndAuditAlarm	0x00072F60
	212 (0x00D4)	197 (0x00C5)	NtAccessCheckByTypeResultList	0x00073010
	213 (0x00D5)	198 (0x00C6)	NtAccessCheckByTypeResultListAndAuditAlarm	0x00073020
	214 (0x00D6)	199 (0x00C7)	NtAccessCheckByTypeResultListAndAuditAlarmByHandle	0x00073030
	215 (0x00D7)	200 (0x00C8)	NtAcquireCrossVmMutant	0x00073040
	216 (0x00D8)	201 (0x00C9)	NtAcquireProcessActivityReference	0x00073050
	217 (0x00D9)	202 (0x00CA)	NtAddAtom	0x00072E40
	218 (0x00DA)	203 (0x00CB)	NtAddAtomEx	0x00073060
	219 (0x00DB)	204 (0x00CC)	NtAddBootEntry	0x00073070

Mentés: Írja le a program szolgáltatásait és a futtatás eredményét a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

Szolgáltatások:

- egy alkalmazás függőségeinek vizsgálata, az általa használt API-k megismerése
- importált és exportált függvények listázása
- mindazon elemek faszervezetbe rendezése, melyek egy adott program futásához szükségesek, ez könnyebbé teszi a problémák forrásának megtalálását
- általános rendszerinformációk lekérdezése

The screenshot shows the Dependency Walker interface for the file WD11N1L.exe. The left pane displays a tree view of dependencies, including various Windows system DLLs. The right pane shows a list of functions and their entry points. The bottom pane shows a list of modules and their properties, including File Time Stamp, Link Time Stamp, File Size, Attr., Link Checksum, Real Checksum, CPU, Subsystem, Symbols, and Preferred Base.