

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Nyíri Dániel Bprof

Üzemmérnök-Informatikus

AUGHMI

Miskolc, 2022

1. feladat

a) Hozza létre a következő mappa szerkezetet!

```
C:\Users\nyiri\AUGHMI>tree
Folder PATH listing for volume WIN10
Volume serial number is 0242-5905
C:.
|
+--- bokor
|   |
|   +--- banan
|   +--- barack
|   +--- mogyoro
|
+--- fa
|   |
|   +--- korte
|
+--- land
|   |
|   +--- kokusz
|   +--- szeder
```

C:\Users\nyiri\AUGHMI>

b) Készítsen másolatot:

Neptunkod/land/szeder katalógusról a *neptunkod/fa* katalógusba

```
Started : 2022. február 16., szerda 20:11:40
Source  : C:\Users\nyiri\AUGHMI\land\
Dest    : C:\Users\nyiri\AUGHMI\fa\

Files   : *.*

Exc Files : *

Options : *.* /S /E /DCOPY:DA /COPY:DAT /R:1000000 /W:30

-----

*EXTRA Dir      0      C:\Users\nyiri\AUGHMI\land\
New Dir        -1      C:\Users\nyiri\AUGHMI\fa\korte\
New Dir         0      C:\Users\nyiri\AUGHMI\land\kokusz\
New Dir         0      C:\Users\nyiri\AUGHMI\land\szeder\

-----

Total    Copied    Skipped    Mismatch    FAILED    Extras
 Dirs :      3         2         1         0         0         1
 Files :      0         0         0         0         0         0
 Bytes :      0         0         0         0         0         0
Times :  0:00:00  0:00:00                0:00:00  0:00:00
Ended : 2022. február 16., szerda 20:11:40

C:\Users\nyiri\AUGHMI>robocopy "C:\Users\nyiri\AUGHMI\land" "C:\Users\nyiri\AUGHMI\fa" /e /xf *
```

Neptunkod/bokor/banan katalógusról a *neptunkod/fa* katalógusba

```
Started : 2022. február 16., szerda 20:20:23
Source : C:\Users\nyiri\AUGHMI\bokor\
Dest : C:\Users\nyiri\AUGHMI\fa\

Files : *.*

Exc Files : *

Options : *.* /S /E /DCOPY:DA /COPY:DAT /R:1000000 /W:30

-----

          0      C:\Users\nyiri\AUGHMI\bokor\
*EXTRA Dir -1    C:\Users\nyiri\AUGHMI\fa\kokusz\
*EXTRA Dir -1    C:\Users\nyiri\AUGHMI\fa\korte\
*EXTRA Dir -1    C:\Users\nyiri\AUGHMI\fa\szeder\
New Dir    0      C:\Users\nyiri\AUGHMI\bokor\banan\
New Dir    0      C:\Users\nyiri\AUGHMI\bokor\barack\
New Dir    0      C:\Users\nyiri\AUGHMI\bokor\mogoró\

-----

      Total    Copied    Skipped    Mismatch    FAILED    Extras
Dirs :      4         3         1         0         0         3
Files :      0         0         0         0         0         0
Bytes :      0         0         0         0         0         0
Times :  0:00:00  0:00:00                0:00:00  0:00:00
Ended : 2022. február 16., szerda 20:20:23

C:\Users\nyiri\AUGHMI>robocopy "C:\Users\nyiri\AUGHMI\bokor" "C:\Users\nyiri\AUGHMI\fa" /e /xf *
```

c) Végezze el a következő áthelyezéseket:

Neptunkod/bokor/barack katalógust helyezze át a *Neptunkod/fa* katalógusba.

Neptunkod/land/kokusz katalógust helyezze át a *Neptunkod/fa* katalógusba.

```
C:\Users\nyiri>move C:\Users\nyiri\AUGHMI\bokor\barack C:\Users\nyiri\AUGHMI\fa
Overwrite C:\Users\nyiri\AUGHMI\fa\barack? (Yes/No/All): No
1 dir(s) moved.

C:\Users\nyiri>move C:\Users\nyiri\AUGHMI\land\kokusz C:\Users\nyiri\AUGHMI\fa
Overwrite C:\Users\nyiri\AUGHMI\fa\kokusz? (Yes/No/All): No
1 dir(s) moved.

C:\Users\nyiri>
```

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

Neptunkod/bokor/banan/leiras.txt

Neptunkod/tree/felsorolas.txt

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

```
C:\Users\nyiri>rmdir C:\Users\nyiri\AUGHMI\land /S
C:\Users\nyiri\AUGHMI\land, Are you sure (Y/N)? Y

C:\Users\nyiri>
```

```
C:\Users\nyiri\AUGHMI\bokor\banan>copy con leiras.txt
Az őszibarack nyár közepén érik
85-90%-a víz
Legközelebbi rokona a mandula^Z
      1 file(s) copied.

C:\Users\nyiri\AUGHMI\bokor\banan>
```

```
C:\Users\nyiri\AUGHMI\fa>copy con felsorolas.txt
Bence Sarosi
Gergely Nemesi^Z
      1 file(s) copied.

C:\Users\nyiri\AUGHMI\fa>
```

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

```
C:\Users\nyiri\AUGHMI>dir /A /B /S /O:N
C:\Users\nyiri\AUGHMI\bokor
C:\Users\nyiri\AUGHMI\fa
C:\Users\nyiri\AUGHMI\bokor\banan
C:\Users\nyiri\AUGHMI\bokor\barack
C:\Users\nyiri\AUGHMI\bokor\mogoro
C:\Users\nyiri\AUGHMI\bokor\banan\leiras.txt
C:\Users\nyiri\AUGHMI\fa\banan
C:\Users\nyiri\AUGHMI\fa\barack
C:\Users\nyiri\AUGHMI\fa\felsorolas.txt
C:\Users\nyiri\AUGHMI\fa\kokusz
C:\Users\nyiri\AUGHMI\fa\korte
C:\Users\nyiri\AUGHMI\fa\mogoro
C:\Users\nyiri\AUGHMI\fa\szeder

C:\Users\nyiri\AUGHMI>
```

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

```
C:\Users\nyiri\AUGHMI>dir ?e* /B /S
C:\Users\nyiri\AUGHMI\bokor\banan\leiras.txt
C:\Users\nyiri\AUGHMI\fa\felsorolas.txt

C:\Users\nyiri\AUGHMI>
```

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

```
C:\Users\nyiri\AUGHMI\fa>cacls felsorolas.txt /e /p Mindenki:R
processed file: C:\Users\nyiri\AUGHMI\fa\felsorolas.txt

C:\Users\nyiri\AUGHMI\fa>
```

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

```
      Total Files Listed:
           2 File(s)          104 bytes
        35 Dir(s)  18 345 361 408 bytes free

C:\Users\nyiri>dir /s AUGHMI
```

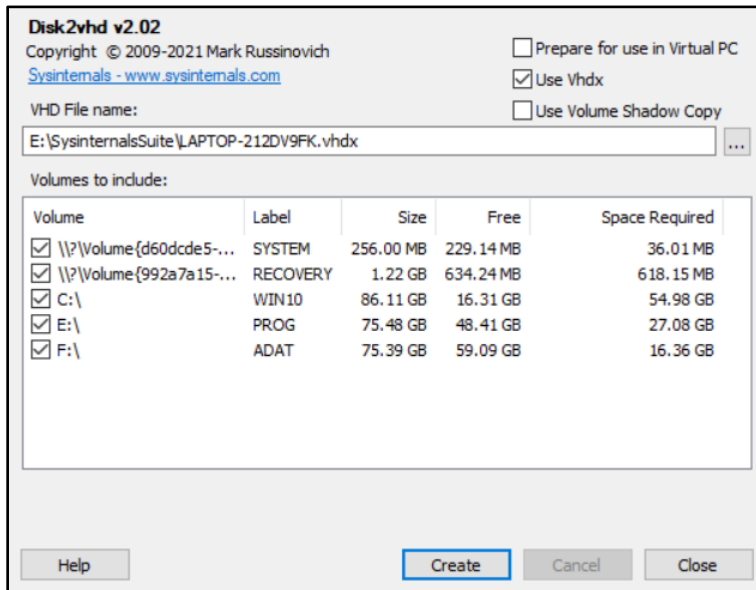
j) Rendezze ABC-szerint a *felsorolas.txt* file tartalmát.

```
C:\Users\nyiri\AUGHMI\fa>sort /r felsorolas.txt
Gergely Nemesi
Bence Sarosi

C:\Users\nyiri\AUGHMI\fa>
```

2. feladat

a) File and Disk Utilities (*Disk2vhd*)



A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-változatait (Virtual Hard Disk – Microsoft Virtual Machine lemezformátuma) Microsoft Virtual PC-ben vagy Microsoft Hyper-V virtuális gépekben (VM-ekben) való használatra.

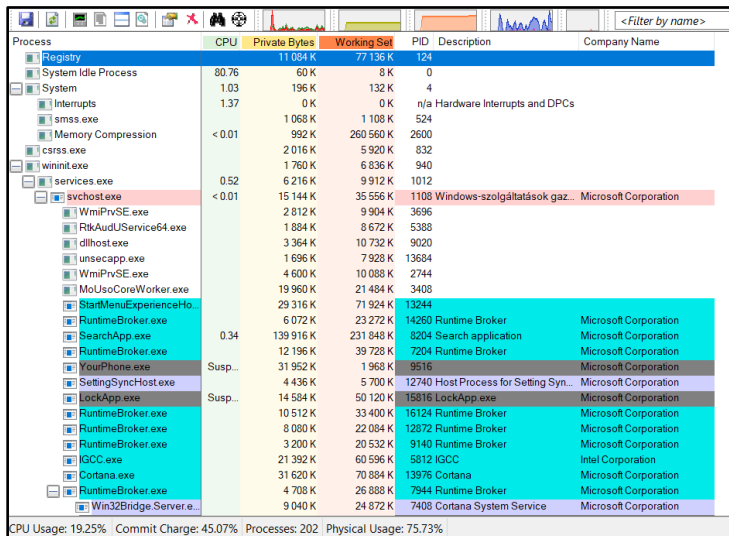
b) Networking Utilities (*TCPView*)

| Process Name | Process ID | Protocol | State | Local Address | Local Port | Remote Address | Remote Port | Create Time | Module Name |
|------------------------|------------|----------|-------------|---------------|------------|----------------|-------------|---------------------|------------------|
| svchost.exe | 1280 | TCP | Listen | 0.0.0.0 | 135 | 0.0.0.0 | 0 | 2022.02.15.16:58:35 | RpcSs |
| System | 4 | TCP | Listen | 192.168.1.114 | 139 | 0.0.0.0 | 0 | 2022.02.17.19:08:50 | System |
| System | 4 | TCP | Listen | 192.168.56.1 | 139 | 0.0.0.0 | 0 | 2022.02.17.19:08:49 | System |
| svchost.exe | 9612 | TCP | Listen | 0.0.0.0 | 5040 | 0.0.0.0 | 0 | 2022.02.17.19:08:46 | CDPSvc |
| FontReaderConnected... | 14204 | TCP | Established | 127.0.0.1 | 44430 | 127.0.0.1 | 59107 | 2022.02.17.19:46:26 | FontReaderCon... |
| FontReaderConnected... | 14204 | TCP | Listen | 127.0.0.1 | 44430 | 0.0.0.0 | 0 | 2022.02.17.19:46:26 | FontReaderCon... |
| lsass.exe | 84 | TCP | Listen | 0.0.0.0 | 49664 | 0.0.0.0 | 0 | 2022.02.15.16:58:35 | lsass.exe |
| wininit.exe | 940 | TCP | Listen | 0.0.0.0 | 49665 | 0.0.0.0 | 0 | 2022.02.15.16:58:35 | wininit.exe |
| svchost.exe | 1796 | TCP | Listen | 0.0.0.0 | 49666 | 0.0.0.0 | 0 | 2022.02.15.16:58:35 | Eventlog |
| svchost.exe | 2336 | TCP | Listen | 0.0.0.0 | 49667 | 0.0.0.0 | 0 | 2022.02.15.16:58:35 | Schedule |
| spoolsv.exe | 3780 | TCP | Listen | 0.0.0.0 | 49668 | 0.0.0.0 | 0 | 2022.02.15.16:58:36 | Spooler |
| services.exe | 1012 | TCP | Listen | 0.0.0.0 | 49670 | 0.0.0.0 | 0 | 2022.02.15.16:58:40 | services.exe |
| ASUSLinkNear.exe | 4052 | TCP | Listen | 0.0.0.0 | 49671 | 0.0.0.0 | 0 | 2022.02.15.16:58:40 | ASUSLinkNear... |
| ASUSLinkNear.exe | 4052 | TCP | Listen | 0.0.0.0 | 49672 | 0.0.0.0 | 0 | 2022.02.15.16:58:41 | ASUSLinkNear... |
| avp.exe | 4184 | TCP | Established | 127.0.0.1 | 49673 | 127.0.0.1 | 49674 | 2022.02.15.16:58:41 | AWP21.3 |
| avp.exe | 4184 | TCP | Established | 127.0.0.1 | 49674 | 127.0.0.1 | 49673 | 2022.02.15.16:58:41 | AWP21.3 |
| avp.exe | 4184 | TCP | Established | 127.0.0.1 | 49683 | 127.0.0.1 | 49684 | 2022.02.15.16:58:46 | AWP21.3 |
| avp.exe | 4184 | TCP | Established | 127.0.0.1 | 49684 | 127.0.0.1 | 49683 | 2022.02.15.16:58:46 | AWP21.3 |
| avp.exe | 4184 | TCP | Listen | 127.0.0.1 | 49688 | 0.0.0.0 | 0 | 2022.02.15.16:58:46 | AWP21.3 |
| avp.exe | 4184 | TCP | Established | 127.0.0.1 | 49688 | 127.0.0.1 | 58744 | 2022.02.17.19:09:32 | AWP21.3 |
| avp.exe | 4184 | TCP | Established | 127.0.0.1 | 49688 | 127.0.0.1 | 58775 | 2022.02.17.19:09:57 | AWP21.3 |
| avp.exe | 4184 | TCP | Established | 127.0.0.1 | 49688 | 127.0.0.1 | 58725 | 2022.02.17.19:09:28 | AWP21.3 |

A TCPView egy Windows-program, amely megmutatja a rendszer összes TCP- és UDP-végpontjának részletes listáját, beleértve a helyi és távoli címeket és a TCP-kapcsolatok állapotát.

c) Process Utilities

(Process Explorer)

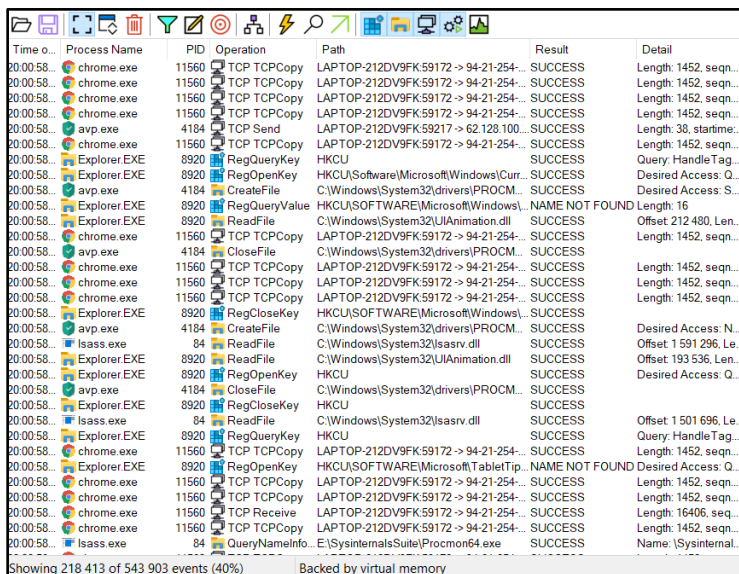


| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|--------------------------|---------|---------------|-------------|-------|---------------------------------|-----------------------|
| Registry | | 11 084 K | 77 136 K | 124 | | |
| System Idle Process | 80.76 | 60 K | 8 K | 0 | | |
| System | 1.03 | 196 K | 132 K | 4 | | |
| Interrupts | 1.37 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| smss.exe | | 1 068 K | 1 108 K | 524 | | |
| Memory Compression | < 0.01 | 992 K | 260 560 K | 2600 | | |
| csrss.exe | | 2 016 K | 5 920 K | 832 | | |
| wininit.exe | | 1 760 K | 6 836 K | 940 | | |
| services.exe | 0.52 | 6 216 K | 9 912 K | 1012 | | |
| svchost.exe | < 0.01 | 15 144 K | 35 556 K | 1108 | Windows-szolgáltatások gaz... | Microsoft Corporation |
| WmiPrvSE.exe | | 2 812 K | 9 904 K | 3696 | | |
| RtkAudUService64.exe | | 1 884 K | 8 672 K | 5388 | | |
| dllhost.exe | | 3 364 K | 10 732 K | 9020 | | |
| unsecapp.exe | | 1 696 K | 7 928 K | 13684 | | |
| WmiPrvSE.exe | | 4 600 K | 10 088 K | 2744 | | |
| MoUsocoreWorker.exe | | 19 960 K | 21 484 K | 3408 | | |
| StartMenuExperienceHo... | | 29 316 K | 71 924 K | 13244 | | |
| RuntimeBroker.exe | | 6 072 K | 23 272 K | 14260 | Runtime Broker | Microsoft Corporation |
| SearchApp.exe | 0.34 | 139 916 K | 231 848 K | 8204 | Search application | Microsoft Corporation |
| RuntimeBroker.exe | | 12 196 K | 39 728 K | 7204 | Runtime Broker | Microsoft Corporation |
| Phone.exe | Susp... | 31 952 K | 1 968 K | 9516 | | Microsoft Corporation |
| SettingSyncHost.exe | | 4 436 K | 5 700 K | 12740 | Host Process for Setting Syn... | Microsoft Corporation |
| LockApp.exe | Susp... | 14 584 K | 50 120 K | 15816 | LockApp.exe | Microsoft Corporation |
| RuntimeBroker.exe | | 10 512 K | 33 400 K | 16124 | Runtime Broker | Microsoft Corporation |
| RuntimeBroker.exe | | 8 080 K | 22 084 K | 12872 | Runtime Broker | Microsoft Corporation |
| RuntimeBroker.exe | | 3 200 K | 20 532 K | 9140 | Runtime Broker | Microsoft Corporation |
| IGCC.exe | | 21 392 K | 60 596 K | 5812 | IGCC | Intel Corporation |
| Cortana.exe | | 31 620 K | 70 884 K | 13976 | Cortana | Microsoft Corporation |
| RuntimeBroker.exe | | 4 708 K | 26 888 K | 7944 | Runtime Broker | Microsoft Corporation |
| Win32Bridge.Server.e... | | 9 040 K | 24 872 K | 7408 | Cortana System Service | Microsoft Corporation |

CPU Usage: 19.25% Commit Charge: 45.07% Processes: 202 Physical Usage: 75.73%

A Process Explorer képernyő két ablakból áll. A felső ablakban mindig megjelenik az aktuálisan aktív folyamatok listája, beleértve a tulajdonos fiókjai neve is, míg az alsó ablakban megjelenő információ attól függ, hogy a Process Explorer milyen módban van: *kezelő mód* vagy *Process DDL mód*.

(Process Monitor)

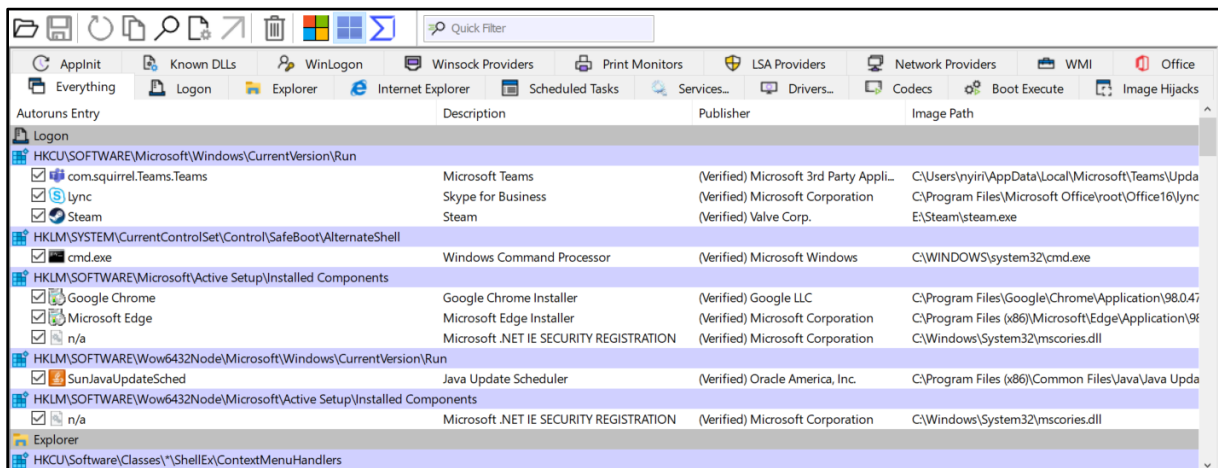


| Time | Process Name | PID | Operation | Path | Result | Detail |
|-------------|--------------|-------|---------------|---|----------------|-------------------------|
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | avp.exe | 4184 | TCP Send | LAPTOP-212DV9FK59217 -> 62-128-100-... | SUCCESS | Length: 38, startime... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | Explorer EXE | 8920 | RegQueryValue | HKCU | SUCCESS | Query: HandleTag... |
| 20:00:58... | Explorer EXE | 8920 | RegOpenKey | HKCU\Software\Microsoft\Windows\Curr... | SUCCESS | Desired Access: Q... |
| 20:00:58... | avp.exe | 4184 | CreateFile | C:\Windows\System32\drivers\PROCM... | SUCCESS | Desired Access: S... |
| 20:00:58... | Explorer EXE | 8920 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Windows\... | NAME NOT FOUND | Length: 16 |
| 20:00:58... | Explorer EXE | 8920 | ReadFile | C:\Windows\System32\UIAnimation.dll | SUCCESS | Offset 212 480, Len... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | avp.exe | 4184 | CloseFile | C:\Windows\System32\drivers\PROCM... | SUCCESS | |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | Explorer EXE | 8920 | RegCloseKey | HKCU\SOFTWARE\Microsoft\Windows\... | SUCCESS | |
| 20:00:58... | avp.exe | 4184 | CreateFile | C:\Windows\System32\drivers\PROCM... | SUCCESS | Desired Access: N... |
| 20:00:58... | Isass.exe | 84 | ReadFile | C:\Windows\System32\Isasrv.dll | SUCCESS | Offset 1 591 296, L... |
| 20:00:58... | Explorer EXE | 8920 | ReadFile | C:\Windows\System32\UIAnimation.dll | SUCCESS | Offset 193 536, Len... |
| 20:00:58... | Explorer EXE | 8920 | RegOpenKey | HKCU | SUCCESS | Desired Access: Q... |
| 20:00:58... | avp.exe | 4184 | CloseFile | C:\Windows\System32\drivers\PROCM... | SUCCESS | |
| 20:00:58... | Explorer EXE | 8920 | RegCloseKey | HKCU | SUCCESS | |
| 20:00:58... | Isass.exe | 84 | ReadFile | C:\Windows\System32\Isasrv.dll | SUCCESS | Offset 1 501 696, L... |
| 20:00:58... | Explorer EXE | 8920 | RegQueryValue | HKCU | SUCCESS | Query: HandleTag... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | Explorer EXE | 8920 | RegOpenKey | HKCU\SOFTWARE\Microsoft\TabletTip... | NAME NOT FOUND | Desired Access: Q... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | chrome.exe | 11560 | TCP Receive | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 16406, seq... |
| 20:00:58... | chrome.exe | 11560 | TCP TCPCopy | LAPTOP-212DV9FK59172 -> 94-21-254-... | SUCCESS | Length: 1452, seqn... |
| 20:00:58... | Isass.exe | 84 | QueryNameInfo | E:\SysinternalsSuite\Procmon64.exe | SUCCESS | Name: (Sysinternal... |

Showing 218 413 of 543 903 events (40%) Backed by virtual memory

A Process Monitor egy fejlett megfigyelő eszköz a Windows számára, amely valós idejű fájlrendszert, rendszerleíró adatbázist és folyamat/szál tevékenységet mutat.

(AutoRuns)



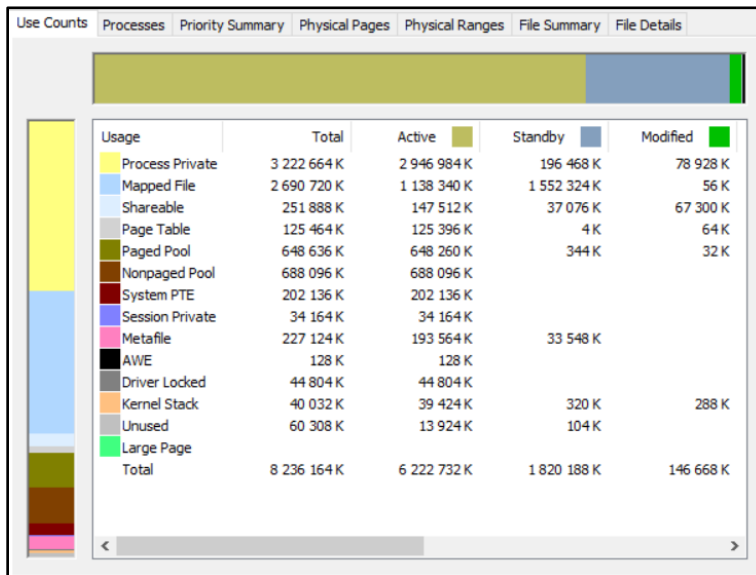
| Autoruns Entry | Description | Publisher | Image Path |
|---|---|---|--|
| Logon | | | |
| HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | | | |
| com.squirrel.Teams.Teams | Microsoft Teams | (Verified) Microsoft 3rd Party Appli... | C:\Users\jnyin\AppData\Local\Microsoft\Teams\Upda |
| lync | Skype for Business | (Verified) Microsoft Corporation | C:\Program Files\Microsoft Office\root\Office16\lync |
| Steam | Steam | (Verified) Valve Corp. | E:\Steam\steam.exe |
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell | | | |
| cmd.exe | Windows Command Processor | (Verified) Microsoft Windows | C:\WINDOWS\system32\cmd.exe |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components | | | |
| Google Chrome | Google Chrome Installer | (Verified) Google LLC | C:\Program Files\Google\Chrome\Application\98.0.47 |
| Microsoft Edge | Microsoft Edge Installer | (Verified) Microsoft Corporation | C:\Program Files (x86)\Microsoft\Edge\Application\98 |
| n/a | Microsoft .NET IE SECURITY REGISTRATION | (Verified) Microsoft Corporation | C:\Windows\System32\mscories.dll |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run | | | |
| SunJavaUpdateSched | Java Update Scheduler | (Verified) Oracle America, Inc. | C:\Program Files (x86)\Common Files\Java\Java Upda |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components | | | |
| n/a | Microsoft .NET IE SECURITY REGISTRATION | (Verified) Microsoft Corporation | C:\Windows\System32\mscories.dll |
| Explorer | | | |
| HKCU\Software\Classes*\ShellEx\ContextMenuHandlers | | | |

Ez a segédprogram, amely a legátfogóbb ismeretekkel rendelkezik az indítási monitorok automatikus indítási helyeiről, megmutatja, milyen programok vannak beállítva a rendszerindítás vagy bejelentkezés során, valamint a különféle beépített Windows-alkalmazások indításakor.

d) Security Utilities (*LogonSession*)

Nem nyílt meg a program!

e) Information Utilities (*RAMMap*)



| Usage | Total | Active | Standby | Modified |
|-----------------|--------------------|--------------------|--------------------|------------------|
| Process Private | 3 222 664 K | 2 946 984 K | 196 468 K | 78 928 K |
| Mapped File | 2 690 720 K | 1 138 340 K | 1 552 324 K | 56 K |
| Shareable | 251 888 K | 147 512 K | 37 076 K | 67 300 K |
| Page Table | 125 464 K | 125 396 K | 4 K | 64 K |
| Paged Pool | 648 636 K | 648 260 K | 344 K | 32 K |
| Nonpaged Pool | 688 096 K | 688 096 K | | |
| System PTE | 202 136 K | 202 136 K | | |
| Session Private | 34 164 K | 34 164 K | | |
| Metafile | 227 124 K | 193 564 K | 33 548 K | |
| AWE | 128 K | 128 K | | |
| Driver Locked | 44 804 K | 44 804 K | | |
| Kernel Stack | 40 032 K | 39 424 K | 320 K | 288 K |
| Unused | 60 308 K | 13 924 K | 104 K | |
| Large Page | | | | |
| Total | 8 236 164 K | 6 222 732 K | 1 820 188 K | 146 668 K |

A RAMMap segítségével megértheti, hogyan kezeli a Windows memóriát, hogyan elemzi az alkalmazások memóriahasználatát, vagy válaszoljon a RAM lefoglalásával kapcsolatos konkrét kérdésekre.

a) Vizsgálja meg, hogy a *neptunkod.exe* milyen API hívásokat használ a kernel32.dll-ből

Dependency Walker - [AUGMHM32.DLL]

File Edit View Options Profile Window Help

Module
 AUGMHM32.DLL
 API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
 NTDLL.DLL
 KERNELBASE.DLL
 NTDLL.DLL
 API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
 API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
 API-MS-WIN-CORE-APIQUERY-L1-1-1.D
 EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
 EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
 API-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
 EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
 API-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
 EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL

| PI | Ordinal | Hint | Function | Entry Point |
|-----|--------------|------|-----------------------|-------------|
| N/A | 269 (0x010D) | | DeleteCriticalSection | Not Bound |
| N/A | 305 (0x0131) | | EnterCriticalSection | Not Bound |
| N/A | 536 (0x0218) | | GetCurrentProcess | Not Bound |
| N/A | 537 (0x0219) | | GetCurrentProcessId | Not Bound |
| N/A | 541 (0x021D) | | GetCurrentThreadid | Not Bound |
| N/A | 612 (0x0262) | | GetLastError | Not Bound |
| N/A | 722 (0x02D2) | | GetStartupInfoA | Not Bound |

| E | Ordinal | Hint | Function | Entry Point |
|---|------------|------------|-------------------------|----------------------------------|
| 0 | 0 (0x0001) | 0 (0x0001) | AcquireSRWLockExclusive | NTDLL.RtlAcquireSRWLockExclusive |
| 1 | 2 (0x0002) | 1 (0x0001) | AcquireSRWLockShared | NTDLL.RtlAcquireSRWLockShared |
| 2 | 3 (0x0003) | 2 (0x0002) | ActivateActCt | 0x00020080 |
| 3 | 4 (0x0004) | 3 (0x0003) | ActivateActCtWorker | 0x0001B700 |
| 4 | 5 (0x0005) | 4 (0x0004) | AddAtomA | 0x0005A140 |
| 5 | 6 (0x0006) | 5 (0x0005) | AddAtomW | 0x000128F0 |

| Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum | CPU | Subsystem |
|--------------------------------------|--|-----------------|-----------|-------|---------------|---------------|-----|-----------|
| API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL | Error opening file. A rendizser nem találta a megadott fajt (2). | | | | | | | |
| API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL | Error opening file. A rendizser nem találta a megadott fajt (2). | | | | | | | |
| API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL | Error opening file. A rendizser nem találta a megadott fajt (2). | | | | | | | |
| API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL | Error opening file. A rendizser nem találta a megadott fajt (2). | | | | | | | |
| API-MS-WIN-CORE-COMM-L1-1-0.DLL | Error opening file. A rendizser nem találta a megadott fajt (2). | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL | Error opening file. A rendizser nem találta a megadott fajt (2). | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL | Error opening file. A rendizser nem találta a megadott fajt (2). | | | | | | | |

Error: At least one required implicit or forwarded dependency was not found.
 Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
 Error: A circular dependency was detected.
 Warning: At least one delay-load dependency module was not found.
 Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1.

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

Dynamic Link Library fájlok, mint ntdll.dll, alapvetően "útmutató könyvek", amelyek információkat és útmutatásokat tartalmaznak a végrehajtható (EXE) fájlokhoz. Ezeket a fájlokat úgy hozták létre, hogy több program megoszthat azonos ntdll.dll fájlt, ezáltal értékes memória-allokációt takarít meg, így a számítógép hatékonyabban működik.

Dependency Walker - [AUGMH.EXE]

File Edit View Options Profile Window Help

Module List:

- AUGMH.EXE
- KERNEL32.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- NTDDI.DLL
- KERNELBASE.DLL
- API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
- API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
- API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
- EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
- EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
- EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL

| Module | Ordinal | Hint | Function | Entry Point |
|---------------------------------------|---------|--------------|---|-------------|
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 20 (0x00141) | CsrAllocateCaptureBuffer | Not Bound |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 21 (0x00151) | CsrAllocateMessagePointer | Not Bound |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 23 (0x00171) | CsrCaptureMessageMultiUnicodeStringsInPlace | Not Bound |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 24 (0x00181) | CsrCaptureMessageString | Not Bound |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 26 (0x001A1) | CsrClientCallServer | Not Bound |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 28 (0x001C1) | CsrFreeCaptureBuffer | Not Bound |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 32 (0x00201) | CsrVerifyRegion | Not Bound |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | N/A | 34 (0x00221) | DbgPrint | Not Bound |

| Module | Ordinal | Hint | Function | Entry Point |
|---------------------------------------|--------------|-------------|---|-------------|
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | 8 (0x00081) | N/A | N/A | 0x0007F110 |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | 9 (0x00091) | 0 (0x00001) | A_SHAFinal | 0x00040230 |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | 10 (0x000A1) | 1 (0x00011) | A_SHAInit | 0x00041060 |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | 11 (0x000B1) | 2 (0x00021) | A_SHAUpdate | 0x000410A0 |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | 12 (0x000C1) | 3 (0x00031) | AlpcAdjustCompletionListConcurrencyCount | 0x000E0740 |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | 13 (0x000D1) | 4 (0x00041) | AlpcFreeCompletionListMessage | 0x00070620 |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | 14 (0x000E1) | 5 (0x00051) | AlpcGetCompletionListLastMessageInformation | 0x000E0770 |

| Module | File Time Stamp | Link Time Stamp | File Size | Attr | Link Checksum | Real Checksum | CPU | Subsystem |
|---------------------------------------|-----------------|-----------------|-----------|------|---------------|---------------|-----|-----------|
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | | | | | | | | |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-1.DLL | | | | | | | | |
| API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL | | | | | | | | |
| API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL | | | | | | | | |
| API-MS-WIN-CORE-COMM-L1-1-0.DLL | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L1-1-1.DLL | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL | | | | | | | | |

Error: At least one required implicit or forwarded dependency was not found.
 Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
 Error: A circular dependency was detected.
 Warning: At least one delay-load dependency module was not found.
 Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1