

# Operációs rendszerek

## BSc 3.gyak.

2021. 02. 24.

**Készítette:**

Kacsir András Bsc

Programtervező

VSG9L4

**Miskolc, 2021**

**1. feladat** – Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.kiírása Megvalósítás

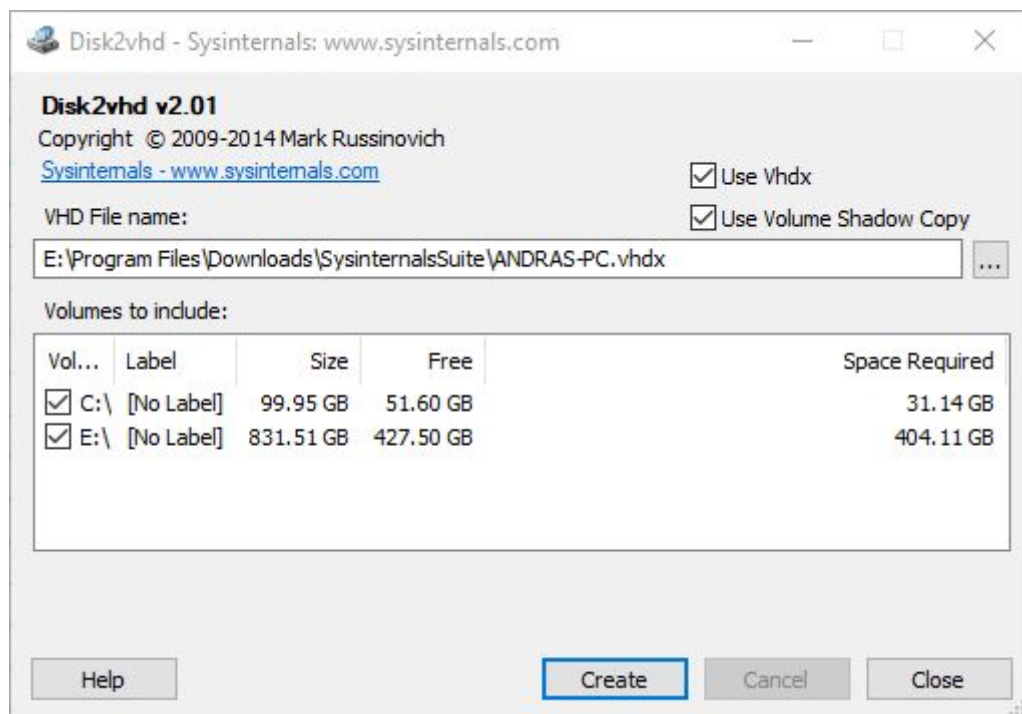
| SysinternalsSuite   |                  |                     |                       |          |  |
|---|------------------|---------------------|-----------------------|----------|--|
| Fájl Kezdőlap Megosztás Nézet   |                  |                     |                       |          |  |
| Ez a gép > Helyi lemez (E:) > Program Files > Downloads > SysinternalsSuite |                  |                     |                       |          |  |
|   | Név              | Módosítás dátuma    | Típus                 | Méret    |  |
| Gyors elérés  | accesschk        | 2020. 10. 15. 21:45 | Alkalmazás            | 1 347 KB |  |
| OneDrive  | accesschk64      | 2020. 10. 15. 21:45 | Alkalmazás            | 742 KB   |  |
| Ez a gép  | AccessEnum       | 2006. 11. 01. 23:06 | Alkalmazás            | 171 KB   |  |
| 3D objektumok   | AdExplorer       | 2020. 11. 04. 20:52 | Lefordított HTML-...  | 50 KB    |  |
| Asztal  | AdExplorer       | 2020. 11. 04. 20:52 | Alkalmazás            | 1 135 KB |  |
| Dokumentumok  | AdExplorer64     | 2020. 11. 04. 20:52 | Alkalmazás            | 603 KB   |  |
| Képek   | ADInsight        | 2020. 09. 14. 2:43  | Lefordított HTML-...  | 393 KB   |  |
| Letöltések  | ADInsight        | 2020. 09. 14. 2:36  | Alkalmazás            | 4 987 KB |  |
| Videók  | ADInsight64      | 2020. 09. 14. 2:33  | Alkalmazás            | 1 731 KB |  |
| Zene  | adrestore        | 2020. 11. 25. 9:59  | Alkalmazás            | 342 KB   |  |
| Helyi lemez (C:)  | adrestore64      | 2020. 11. 25. 9:59  | Alkalmazás            | 441 KB   |  |
| Helyi lemez (E:)  | Autologon        | 2020. 04. 06. 4:25  | Alkalmazás            | 334 KB   |  |
| Hálózati  | Autologon64      | 2020. 04. 06. 4:24  | Alkalmazás            | 431 KB   |  |
|   | autoruns         | 2020. 04. 06. 4:39  | Lefordított HTML-...  | 50 KB    |  |
|   | Autoruns         | 2020. 04. 06. 4:39  | Alkalmazás            | 738 KB   |  |
|   | Autoruns64.dll   | 2020. 04. 06. 4:35  | Alkalmazáskiterjes... | 735 KB   |  |
|   | Autoruns64       | 2020. 04. 06. 4:38  | Alkalmazás            | 850 KB   |  |
|   | Autoruns64a.dll  | 2020. 04. 06. 4:30  | Alkalmazáskiterjes... | 761 KB   |  |
|   | autorunsc        | 2020. 04. 06. 4:35  | Alkalmazás            | 659 KB   |  |
|   | autorunsc64      | 2020. 04. 06. 4:34  | Alkalmazás            | 753 KB   |  |
|   | Bginfo           | 2019. 09. 19. 22:17 | Alkalmazás            | 3 275 KB |  |
|   | Bginfo64         | 2019. 09. 19. 22:15 | Alkalmazás            | 4 494 KB |  |
|   | Cacheset         | 2006. 11. 01. 23:06 | Alkalmazás            | 151 KB   |  |
|   | Clockres         | 2020. 06. 22. 20:19 | Alkalmazás            | 331 KB   |  |
|   | Clockres64       | 2020. 06. 22. 20:17 | Alkalmazás            | 430 KB   |  |
|   | Contig           | 2016. 05. 27. 12:05 | Alkalmazás            | 248 KB   |  |
|   | Contig64         | 2016. 05. 27. 12:02 | Alkalmazás            | 263 KB   |  |
|   | Coreinfo         | 2020. 04. 27. 17:01 | Alkalmazás            | 967 KB   |  |
|   | Coreinfo64       | 2020. 04. 27. 16:58 | Alkalmazás            | 499 KB   |  |
|   | CPUSTRES         | 2019. 03. 25. 11:54 | Alkalmazás            | 2 131 KB |  |
|   | CPUSTRES64       | 2019. 03. 25. 11:53 | Alkalmazás            | 2 796 KB |  |
|   | ctrl2cap.amd.sys | 2006. 09. 28. 4:04  | Rendszerfájl          | 10 KB    |  |
|   | ctrl2cap         | 2006. 11. 01. 23:05 | Alkalmazás            | 147 KB   |  |
|   | ctrl2cap.nt4.sys | 1999. 11. 22. 3:20  | Rendszerfájl          | 3 KB     |  |

162 elem

letöltve

**2. feladat** - A Sysinternals weboldalon kategóriákba sorolva hasznos programok érhetők el:

a) File and Disk Utilities (Disk2vhd)



feladata hogy megnézzé milyen meghatjóim vannak (C,E) és mennyi hely van rajta

b) Networking Utilities (TCPView)

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

| Process /       | PID | Protocol | Local Address | Local Port | Remote Address       | Remote Port | State     | Sent Packets | Sent Bytes | Rcvd Packets |
|-----------------|-----|----------|---------------|------------|----------------------|-------------|-----------|--------------|------------|--------------|
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64561       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64591       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64594       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64570       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64592       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64534       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64572       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64573       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64574       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64576       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64578       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64580       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64581       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64582       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64583       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64584       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64586       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64587       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64588       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64589       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64590       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64591       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64627       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64593       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64694       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64596       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64599       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64600       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64602       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64603       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64604       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64605       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64608       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64609       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64610       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64614       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64615       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64617       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64619       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64620       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64623       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64624       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64701       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64630       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64637       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 1120       | localhost            | 64622       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | andras-pc     | 29626      | 94.21.174-40.pool... | 64597       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | andras-pc     | 64448      | muc03s07-in-f118...  | https       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | andras-pc     | 64571      | muc03s07-in-f106...  | https       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | Andras-pc     | 64630      | localhost            | 1120        | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | andras-pc     | 64521      | bus02s22-in-10.1...  | https       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | andras-pc     | 64673      | 13.107.6.198         | https       | TIME_WAIT |              |            |              |
| [System Proc... | 0   | TCP      | andras-pc     | 64674      | 13.107.6.198         | https       | TIME_WAIT |              |            |              |

Endpoints: 252   Established: 90   Listening: 31   Time Wait: 55   Close Wait: 3

Megmutatja az összes TCP and UDP végpontjait

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

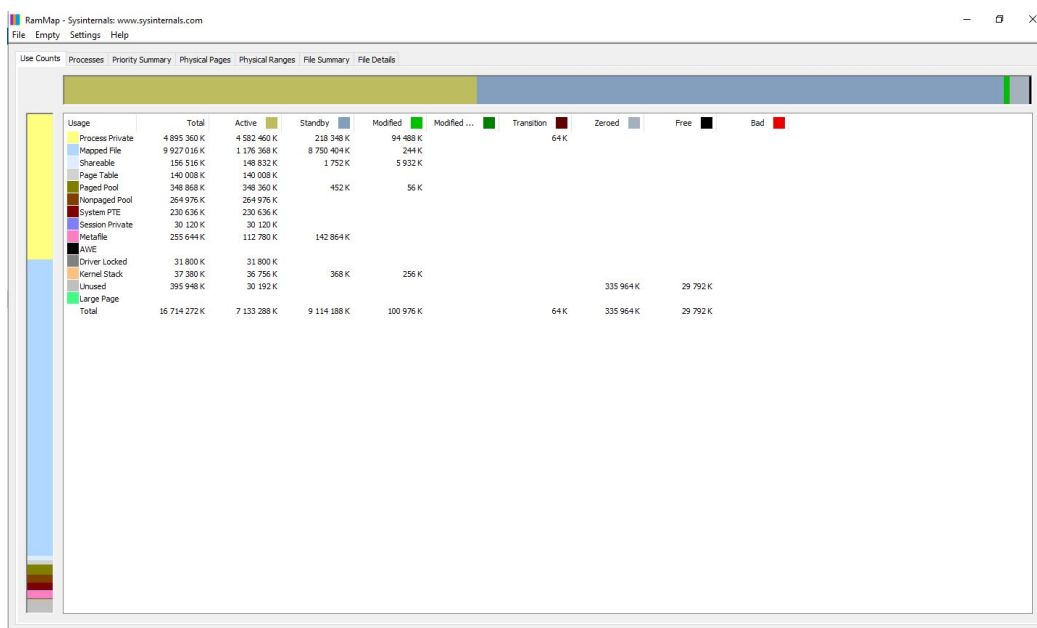
[illegible]

Megmutatja a registryket és a processzeket valós időben

d)Security Utilities (LogonSession)

elindult az exe majd rögtön bezárult így nem tudtam elindítani

## e) Information Utilities (RAMMap)



Megmutatja hogy mennyi memóriát használnak az adott programok

**3. feladat** - Töltse le és végezzen vizsgálatot az AIDA64\_Engineer\_v5.98.4800\_Portable, CPU-Z, GPU-Z programokkal.

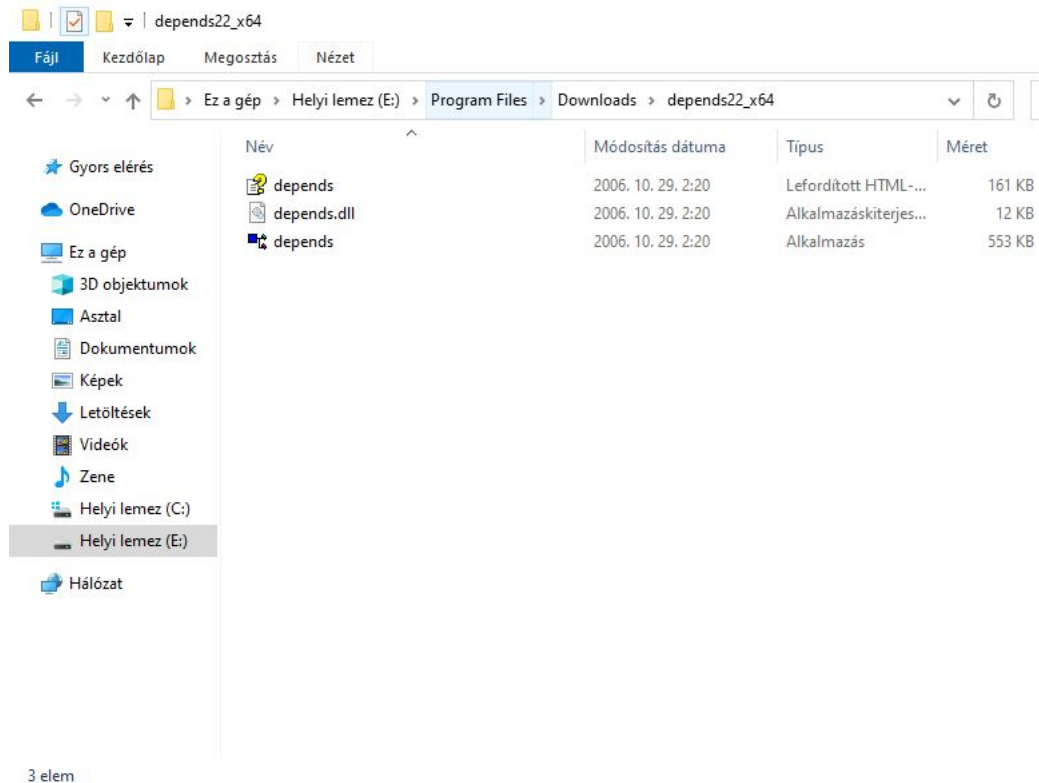
Nekem már lent volt és el is használtam a 30 napon trialomat

**4. feladat** - Töltse le a következő programot: Dependency Walker



URL: <http://www.dependencywalker.com/>

Feladata: a segédprogram megvizsgálja milyen könyvtárakra, és azon belül milyen függvényekre hivatkozik egy elindított program.



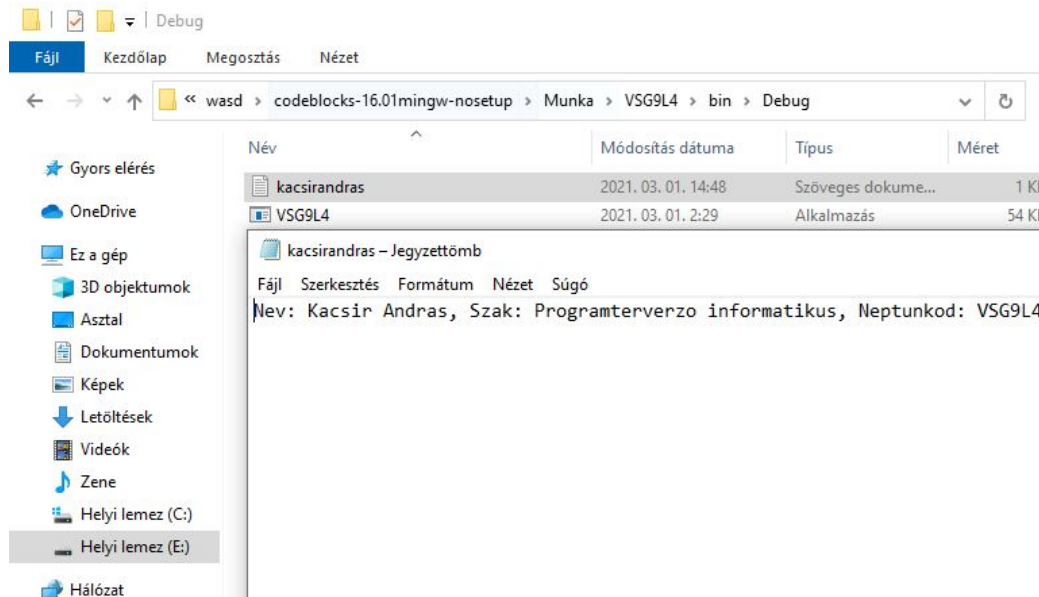
Készítsen egy neptunkod.c nevű forráskódot, amely egy vezeteknev.txt fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc.

```
main.c X
1  #include <stdio.h>
2  #define FILE_NAME "kacsirandras.txt"
3
4
5  int main()
6  {
7      FILE* file_ptr = fopen(FILE_NAME, "w+");
8      fprintf(file_ptr, "Nev: Kacsir Andras, Szak: Programtervező informatikus, Neptunkod: VSG9L4");
9      fclose(file_ptr);
10     return 0;
11 }
12
```

Fordítsa le kódot a C fordító, amely létrehoz egy objektum kódot,

ezután egy linker

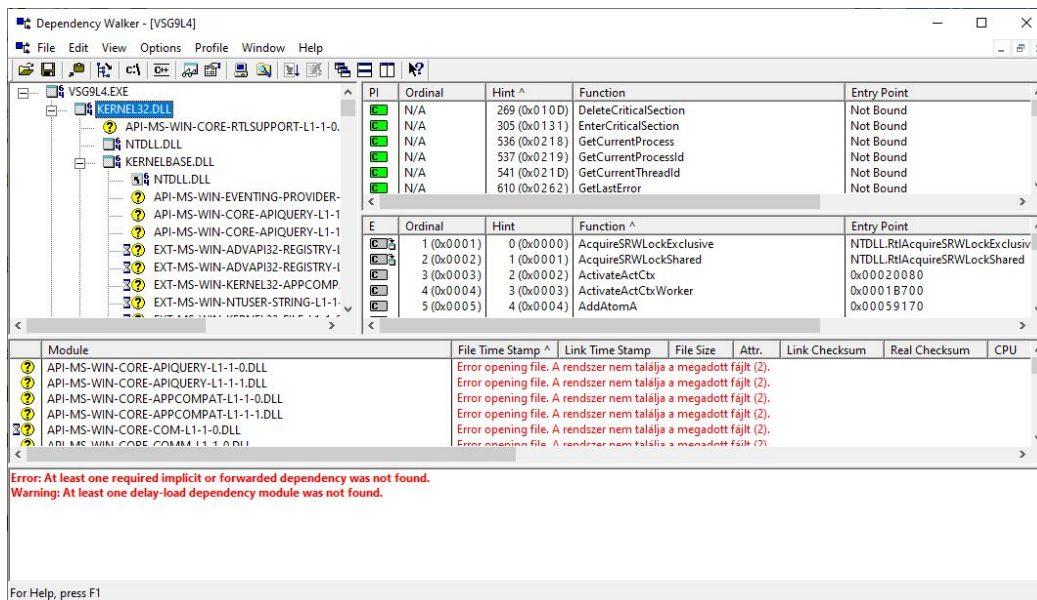
segítségével készítsen egy végrehajtó állományt: neptunkod.exe



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)!



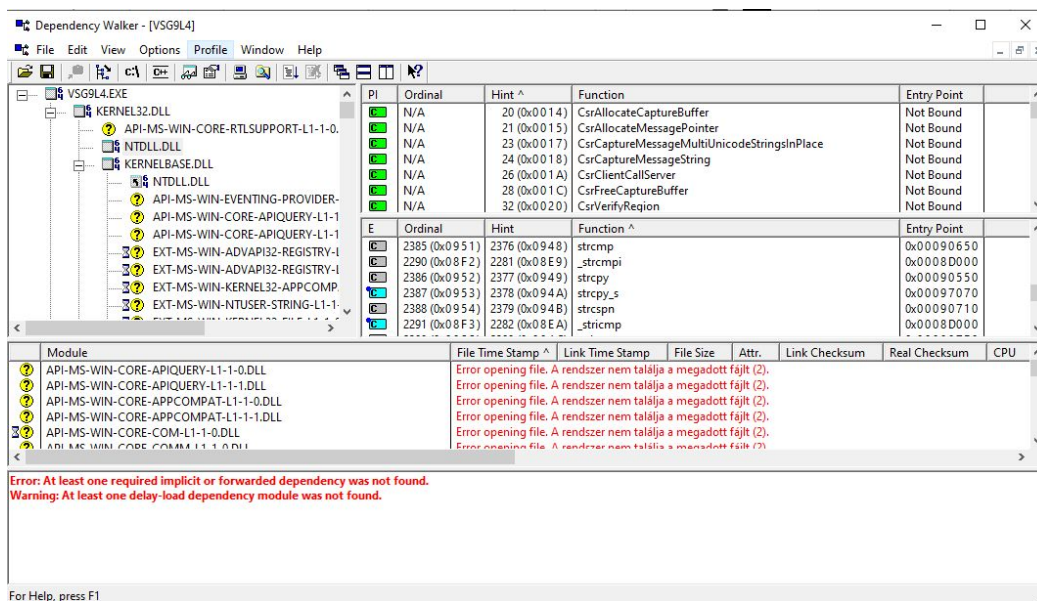
Api hívás például API-MS-WIN-CORE....

b.) Milyen függőségei vannak a kernel32.dll-nek!

felül az import és alul az export függvények

c.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált

függvényeket, milyen információkat kap az NT API-ról!



Felhasználta a program az strcpy parancsot ami c nyelvben megtalálható parancs