Mérési jegyzőkönyv

A Windows vizsgálata 3

A mérés helyszíne:	
A mérés időpontja:	
A mérést végezték:	
Ennek a fájlnak a neve:	
A mérésvezető neve:	

Tudnivalók:

- Csak a sárga színnel megjelölt részre írjon.
- A <<Képernyőkép>> helyőrzőt törölje ki, és a helyére illesszen be egy, a feladat megoldását igazoló képernyőképet.
- A nehezebb feladatokat *-gal jelöltük. Ezek többségének megoldása szükséges a megajánlott jegyhez.

Otthoni felkészülés a laborra:

1. Nézze át a feladatokat! Ha nem ért egy részt, olvasson utána!

   A laborok elején a feladatokkal kapcsolatos ellenőrző kérdéseket teszünk fel.
2. Ha még nem használt Windows 10-et, telepítse egy virtuális gépben, és próbálja ki!

   A Windows10 ingyenesen letölthető a http://msdnaa.bme.hu/ weboldalról.
3. Ha még nem oldotta meg a Windows Labor 1 és 2 méréseket, nézze át a feladatait!

   Ha nem ért valamit, járjon utána, mivel ez a labor épít az ott szerzett ismeretekre!
4. A laborfeladatok egy részét gyakorlásképpen otthon is megoldhatja!

   Ehhez az alábbi alkalmazások telepítésére van szükség:

   Sysnternals Suite és Total Commander

   Ha nem ismeri ezeket a programokat, gyakorolja a használatukat!

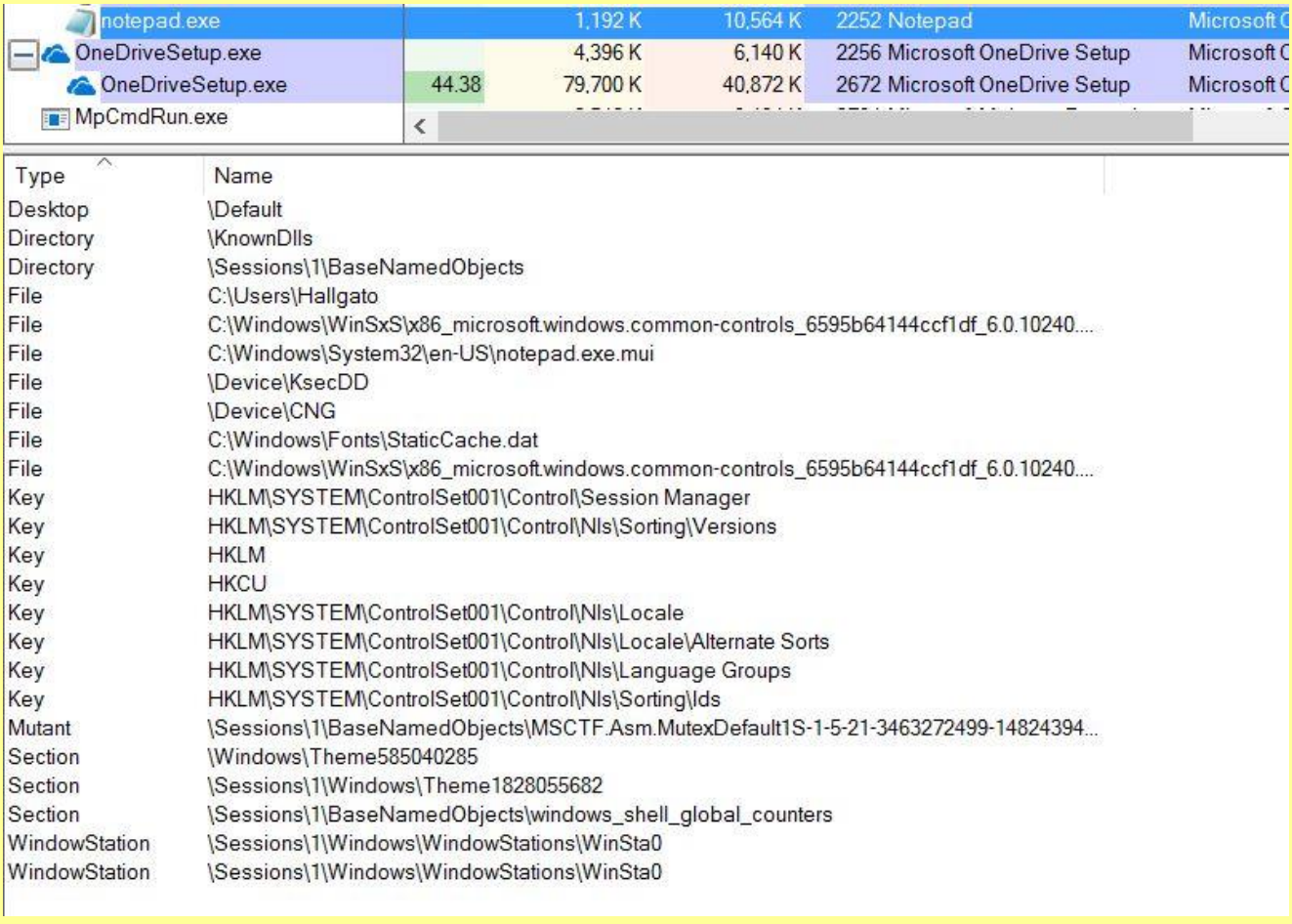
1. feladat: Leírók vizsgálata

Indítsuk el a Process Explorert!

1.1 Leírók megnézése

Indítsunk egy Jegyzettömböt!

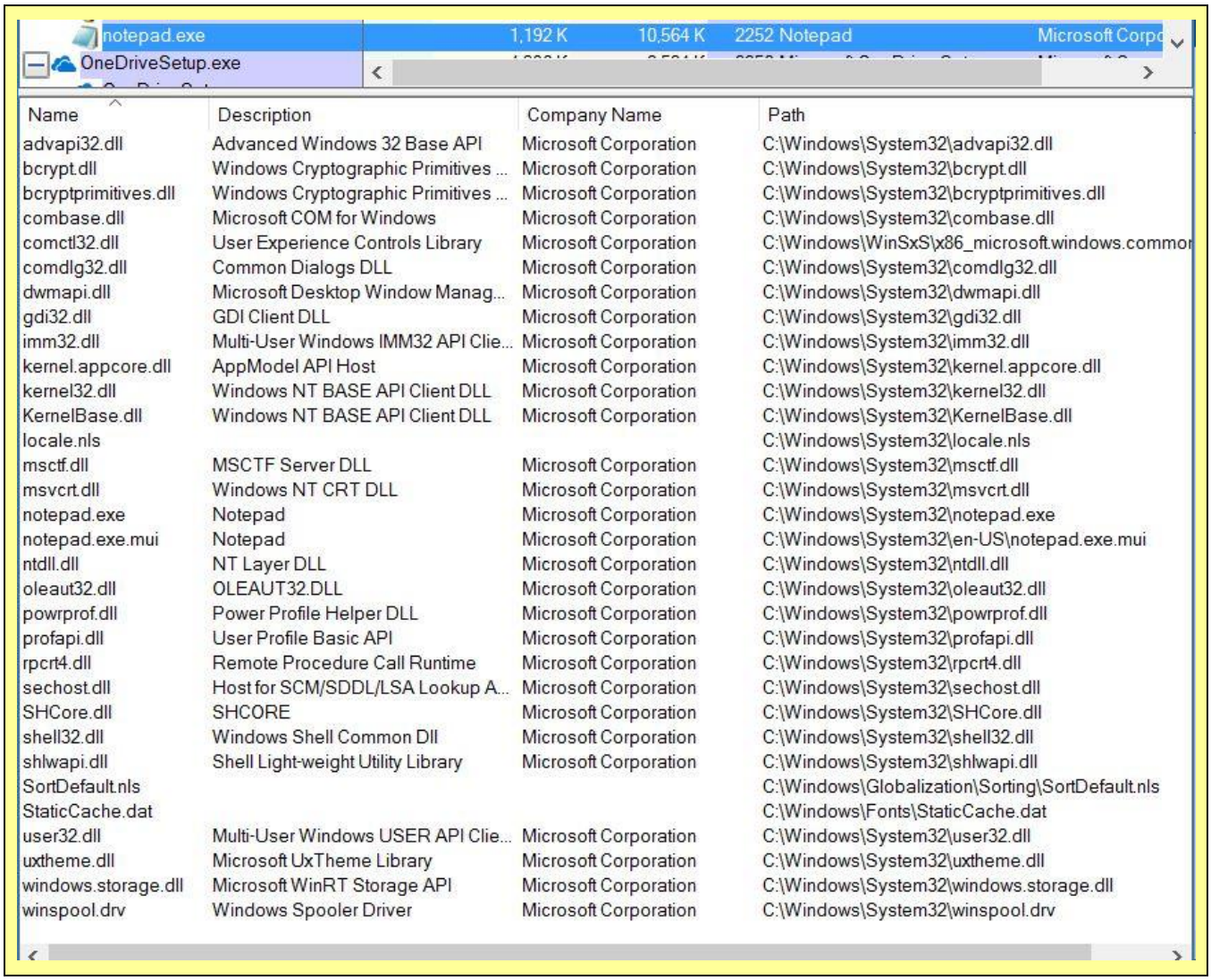
Nézzük meg, hogy milyen registry kulcsokat ér el (`Ctrl + H`)!



notepad.exe		1,192 K	10,564 K	2252 Notepad	Microsoft C
OneDriveSetup.exe		4,396 K	6,140 K	2256 Microsoft OneDrive Setup	Microsoft C
OneDriveSetup.exe	44.38	79,700 K	40,872 K	2672 Microsoft OneDrive Setup	Microsoft C
MpCmdRun.exe					

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
File	C:\Users\Hallgato
File	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.10240....
File	C:\Windows\System32\en-US\notepad.exe.mui
File	\Device\KsecDD
File	\Device\CNG
File	C:\Windows\Fonts\StaticCache.dat
File	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.10240....
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKCU
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\Alternate Sorts
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Language Groups
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Mutant	\Sessions\1\BaseNamedObjects\MSCTF.Asm.MutexDefault1S-1-5-21-3463272499-14824394...
Section	\Windows\Theme585040285
Section	\Sessions\1\Windows\Theme1828055682
Section	\Sessions\1\BaseNamedObjects\windows_shell_global_counters
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0

Nézzük meg a Jegyzettömb által megnyitott DLL-ek listáját (`Ctrl + D`)!



Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\WinSxS\x86_microsoft.windows.commor
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	C:\Windows\System32\comdlg32.dll
dwmapi.dll	Microsoft Desktop Window Manag...	Microsoft Corporation	C:\Windows\System32\dwmapi.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
imm32.dll	Multi-User Windows IMM32 API Clie...	Microsoft Corporation	C:\Windows\System32\imm32.dll
kernel.appcore.dll	AppModel API Host	Microsoft Corporation	C:\Windows\System32\kernel.appcore.dll
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
locale.nls			C:\Windows\System32\locale.nls
msctf.dll	MSCTF Server DLL	Microsoft Corporation	C:\Windows\System32\msctf.dll
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcrt.dll
notepad.exe	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe
notepad.exe.mui	Notepad	Microsoft Corporation	C:\Windows\System32\en-US\notepad.exe.mui
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
oleaut32.dll	OLEAUT32.DLL	Microsoft Corporation	C:\Windows\System32\oleaut32.dll
powrprof.dll	Power Profile Helper DLL	Microsoft Corporation	C:\Windows\System32\powrprof.dll
profapi.dll	User Profile Basic API	Microsoft Corporation	C:\Windows\System32\profapi.dll
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll
sechost.dll	Host for SCM/SDDL/LSA Lookup A...	Microsoft Corporation	C:\Windows\System32\sechost.dll
SHCore.dll	SHCORE	Microsoft Corporation	C:\Windows\System32\SHCore.dll
shell32.dll	Windows Shell Common Dll	Microsoft Corporation	C:\Windows\System32\shell32.dll
shlwapi.dll	Shell Light-weight Utility Library	Microsoft Corporation	C:\Windows\System32\shlwapi.dll
SortDefault.nls			C:\Windows\Globalization\Sorting\SortDefault.nls
StaticCache.dat			C:\Windows\Fonts\StaticCache.dat
user32.dll	Multi-User Windows USER API Clie...	Microsoft Corporation	C:\Windows\System32\user32.dll
uxtheme.dll	Microsoft UxTheme Library	Microsoft Corporation	C:\Windows\System32\uxtheme.dll
windows.storage.dll	Microsoft WinRT Storage API	Microsoft Corporation	C:\Windows\System32\windows.storage.dll
winspool.drv	Windows Spooler Driver	Microsoft Corporation	C:\Windows\System32\winspool.drv

1.2 Nyitott leírók keresése

Windows esetén nem mindig lehet lecserélni vagy törölni egy fájlt, ha arra éppen nyitva tart valaki egy leírót. Annak kiderítésében, hogy ki tart nyitva egy adott fájlt, segít a Process Explorer Find / Find Handle or DLL… parancsa.

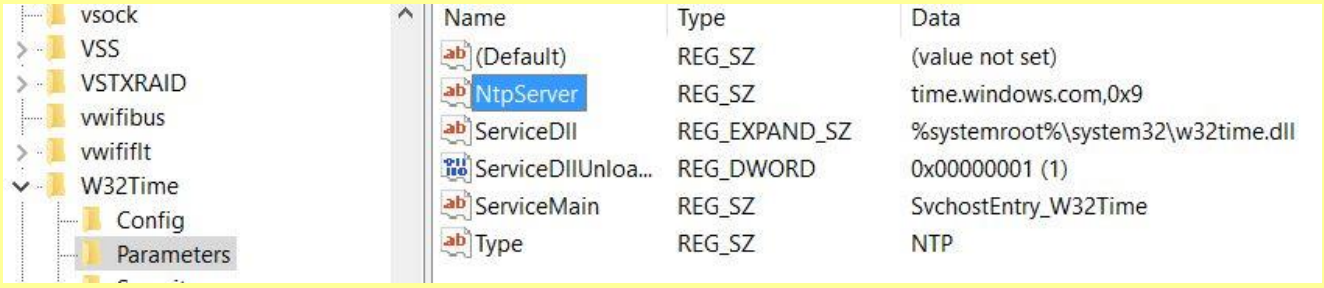
Keressük ki, hogy használja-e most valamelyik folyamat a OneDrive-hoz kapcsolódó update (log) fájlt!

Válasz: Igen, használja.

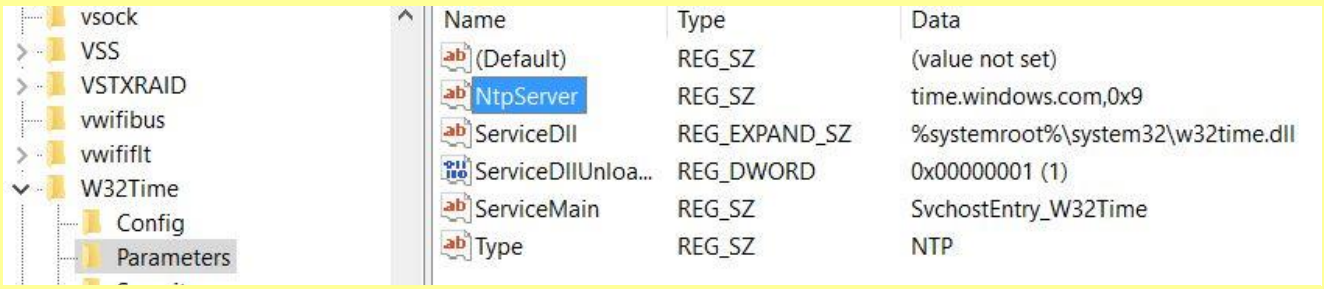
1.3 Szolgáltatások beállításainak tárolása

Nézzük meg, hogy a *Windows Time* szolgáltatáshoz milyen beállítások tartoznak a rendszerleíró adatbázisban (*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* résznél)!

Használjuk ehhez a *regedit.exe* alkalmazást!



Melyik kulcsban tárolja, hogy milyen NTP (Network Time Protocol) kiszolgálóhoz csatlakozik?



Válasz: REG_SZ

Összefoglalás

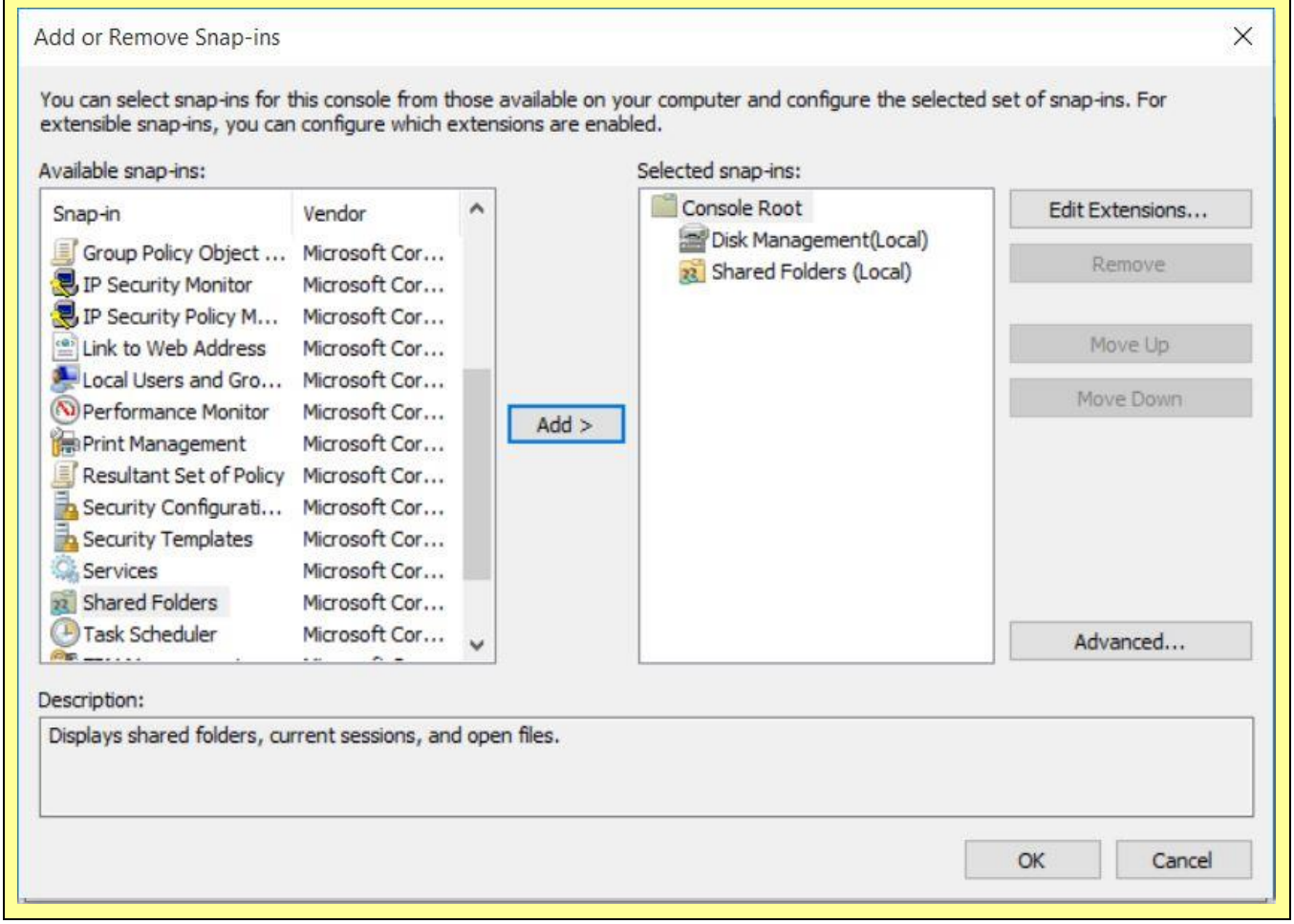
A feladat végére tudni és érteni kell, hogy hogyan egy folyamathoz tartozó leírókat (fájlokat, DLL-ek) megnézni, és hogyan lehet a nyitott leírókra keresni.

2. feladat: Rendszereszközök használata

2.1 MMC modulok

Indítsunk el egy konzolt (`mmc.exe`)!

Nézzük át, hogy milyen beépülő modulokat lehetne hozzáadni. Készítsünk egy olyan konzolt, amin a lemezekkel és megosztásokkal kapcsolatos eszközöket gyűjtjük össze!

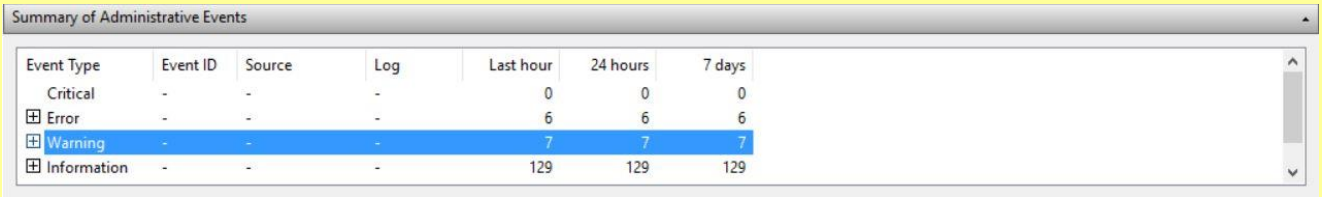


2.2 Eseménynapló felülete

Indítsuk el az Event viewer programot! Volt-e hiba vagy figyelmeztetés típusú bejegyzés az elmúlt hét napban (bármelyik naplóban)? Ha igen, milyen forrás naplózta? Használjuk az Eseménynapló kezdőképernyőjén megjelenő összesítést!

Források:

- Apps
- NDIS

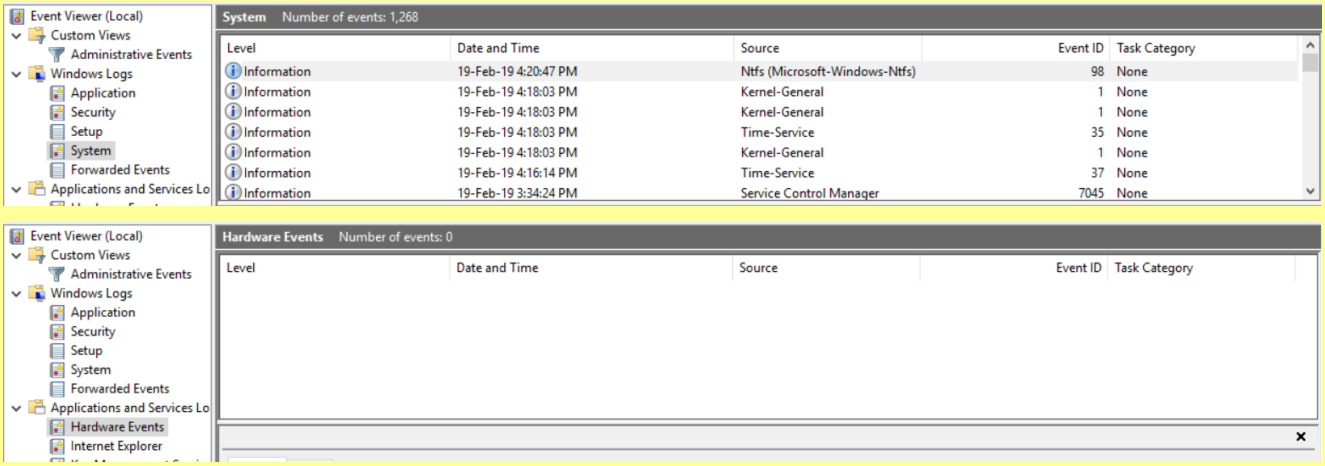


2.3 Keresés az Eseménynaplóban

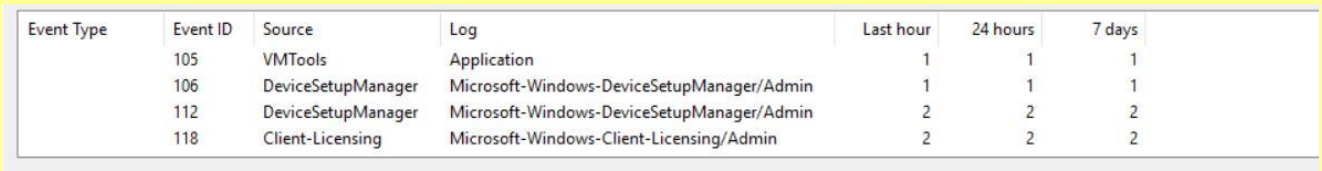
Tegyük fel, hogy egy új USB kulcsot szeretne csatlakoztatni a számítógépéhez, azonban az illesztőprogram (driver) installálása nem sikerül. Hogyan tudna a fellépett hiba részleteinek utána nézni az eseménynaplóban? Milyen hibaforrást keresne?

Források:

- System
- Hardware Events



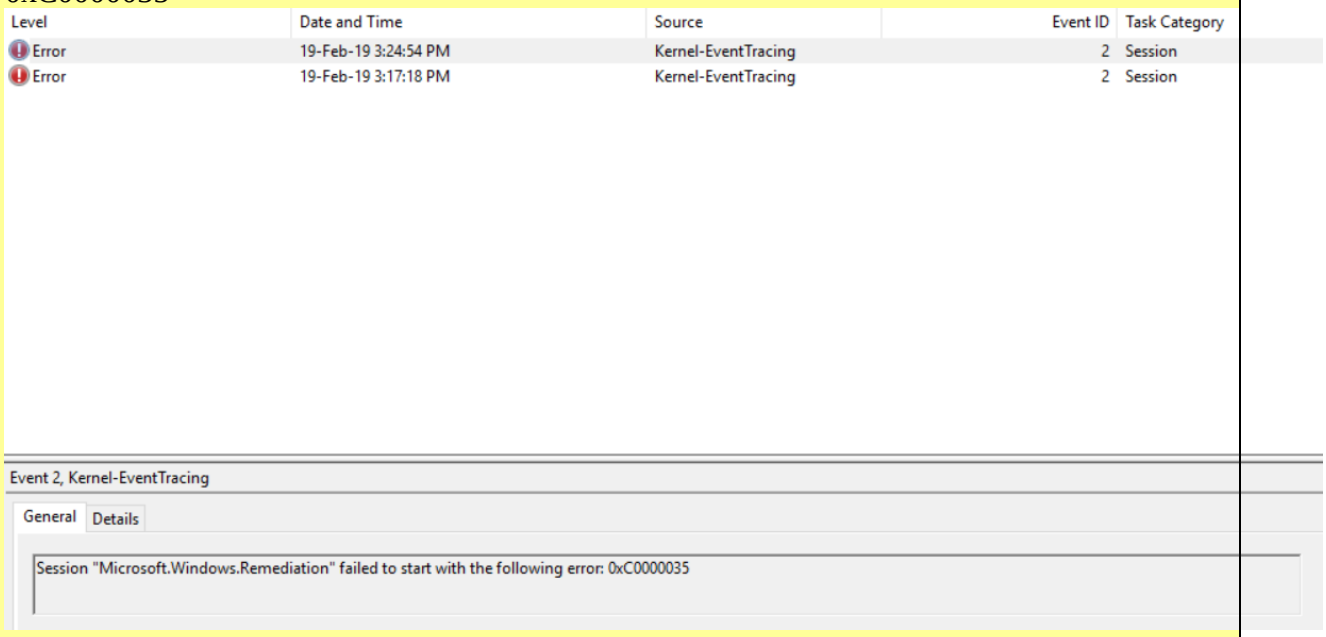
Vizsgáljuk meg milyen eseményazonosítókat naplózott a Device Setup Manager a szűrés és csoportosítás funkciók segítségével!



Soroljuk fel az eseményazonosító – esemény részletes szövege párok közül legalább hármat!

Eseményazonosító – hozzátartozó részletes szöveg:

- 2 - Session "Microsoft.Windows.Remediation" failed to start with the following error: 0xC0000035



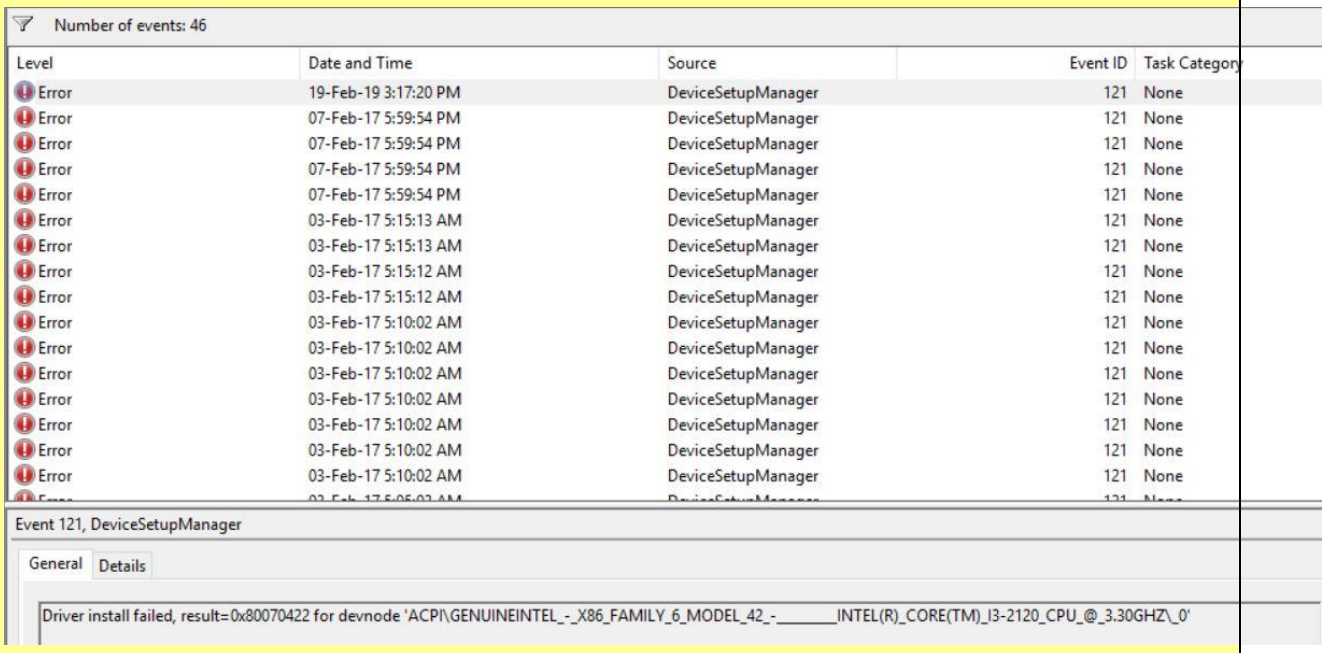
Level	Date and Time	Source	Event ID	Task Category
Error	19-Feb-19 3:24:54 PM	Kernel-EventTracing	2	Session
Error	19-Feb-19 3:17:18 PM	Kernel-EventTracing	2	Session

Event 2, Kernel-EventTracing

General Details

Session "Microsoft.Windows.Remediation" failed to start with the following error: 0xC0000035

- 121 - Driver install failed, result=0x80070422 for devnode 'ACPI\GENUINEINTEL_-_X86_FAMILY_6_MODEL_42_-_____INTEL(R)_CORE(TM)_I3-2120_CPU_@_3.30GHZ_0'



Number of events: 46

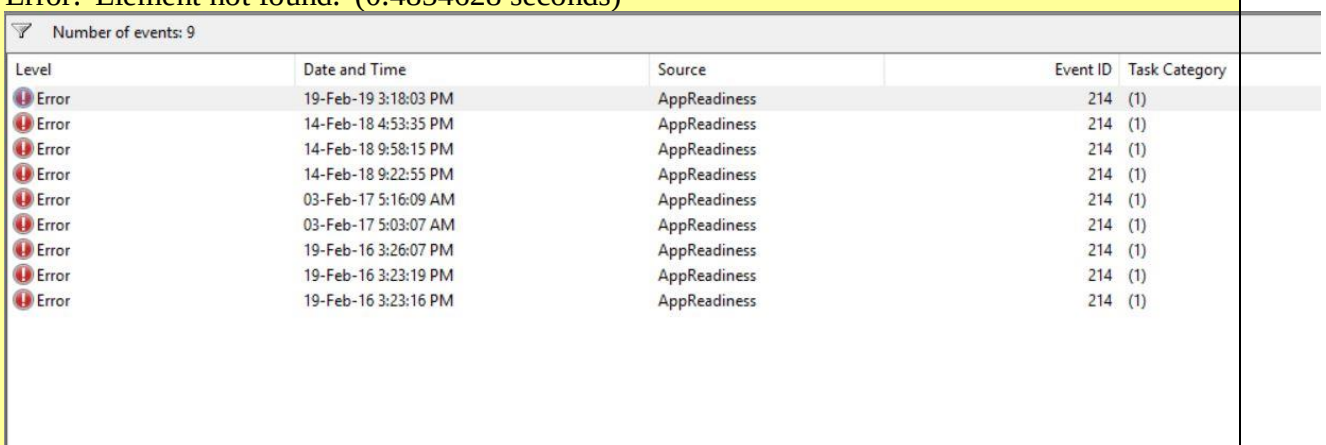
Level	Date and Time	Source	Event ID	Task Category
Error	19-Feb-19 3:17:20 PM	DeviceSetupManager	121	None
Error	07-Feb-17 5:59:54 PM	DeviceSetupManager	121	None
Error	07-Feb-17 5:59:54 PM	DeviceSetupManager	121	None
Error	07-Feb-17 5:59:54 PM	DeviceSetupManager	121	None
Error	07-Feb-17 5:59:54 PM	DeviceSetupManager	121	None
Error	03-Feb-17 5:15:13 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:15:13 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:15:12 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:15:12 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:10:02 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:10:02 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:10:02 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:10:02 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:10:02 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:10:02 AM	DeviceSetupManager	121	None
Error	03-Feb-17 5:10:02 AM	DeviceSetupManager	121	None

Event 121, DeviceSetupManager

General Details

Driver install failed, result=0x80070422 for devnode 'ACPI\GENUINEINTEL_-_X86_FAMILY_6_MODEL_42_-_____INTEL(R)_CORE(TM)_I3-2120_CPU_@_3.30GHZ_0'

- 214 - 'microsoft.windowscommunicationsapps_8wekyb3d8bbwe' install failed for Hallgato. Error: 'Element not found.' (0.4854628 seconds)



Number of events: 9

Level	Date and Time	Source	Event ID	Task Category
Error	19-Feb-19 3:18:03 PM	AppReadiness	214	(1)
Error	14-Feb-18 4:53:35 PM	AppReadiness	214	(1)
Error	14-Feb-18 9:58:15 PM	AppReadiness	214	(1)
Error	14-Feb-18 9:22:55 PM	AppReadiness	214	(1)
Error	03-Feb-17 5:16:09 AM	AppReadiness	214	(1)
Error	03-Feb-17 5:03:07 AM	AppReadiness	214	(1)
Error	19-Feb-16 3:26:07 PM	AppReadiness	214	(1)
Error	19-Feb-16 3:23:19 PM	AppReadiness	214	(1)
Error	19-Feb-16 3:23:16 PM	AppReadiness	214	(1)

Összefoglalás

A feladat végére tudni és érteni kell, hogy hogyan MMC modulokat összeválogatni, hogy lehet az eseménynaplóból hibákat megnézni, hogyan lehet az eseményekre szűrni és keresni.

Emelt szintű feladatok

* E.1 Leírók vizsgálata

[*] Mi történik akkor, ha megnyitunk a jegyzettömbben egy szövegfájlt?

Újabb szálak jelennek meg a Process Explorerben

[*] Mi lehet ezek funkciója? Válasszon ki egyet és vizsgálja meg!

Azért nyílik meg ez a szál, hogy legyen egy elkülönített erőforrás, ha elvégezzük a feladatot a szál felszabadul.

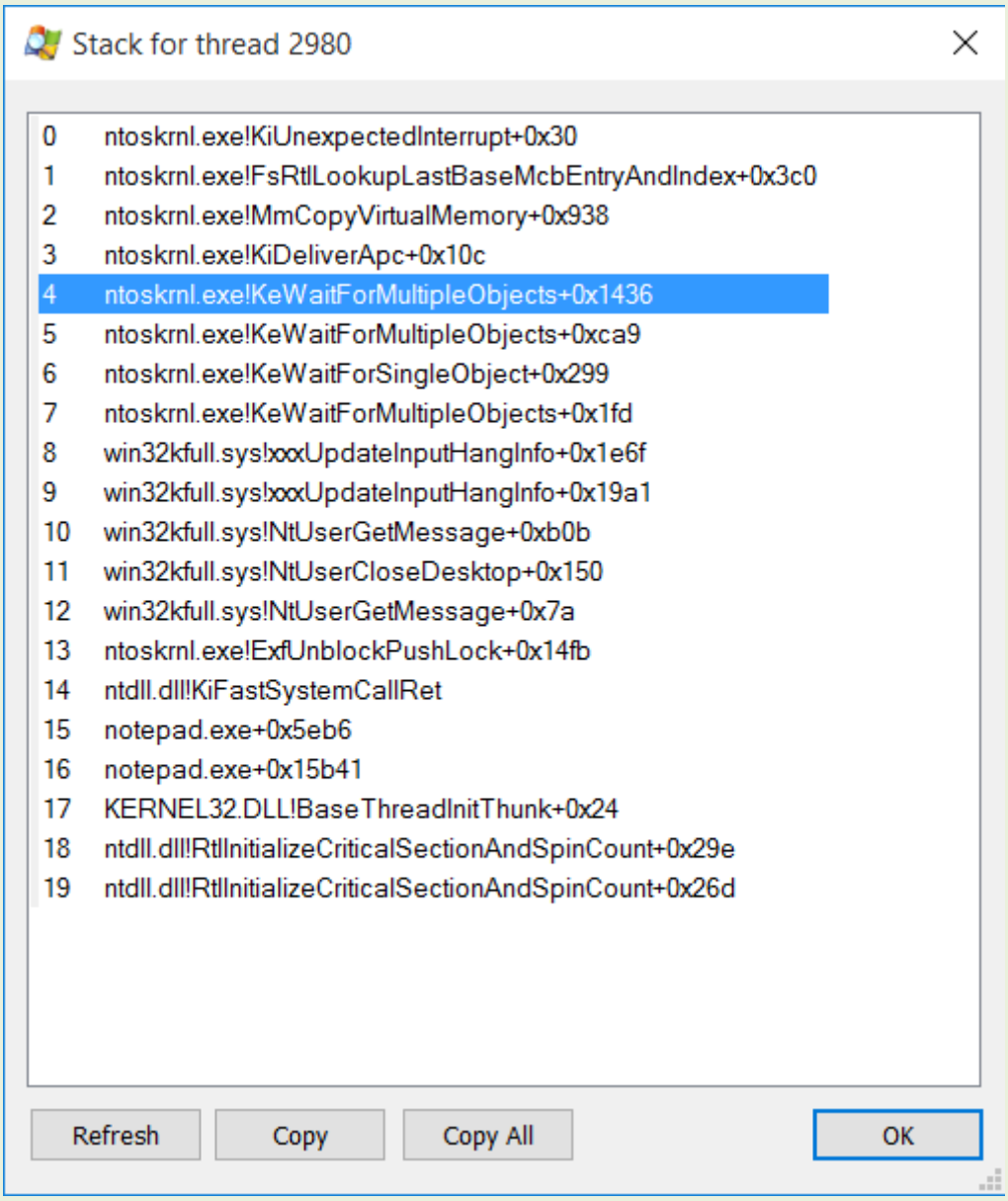
* E.2 Szálak és vermek

Indítsa el a Process Explorert!

Egy folyamat egy adott szálát megvizsgálva a Stack (verem) gomb segítségével tudjuk megnézni, hogy az adott szál milyen függvényhívásokon keresztül jutott el az aktuális állapotba. Próbáljunk értelmezni egy ilyen veremtartalmat!

A szál addig él, amíg a stackben lévő legutolsó feladat el nem végződik, mindaddig a szál fenntartja az erőforrást.

Honnan látszik, hogy melyik hívásokat hajtotta végre kernel és melyiket felhasználói módban?



Miket futtathat a System folyamat a hozzá tartozó szálak alapján (legalább 3 feladat vagy eszközmeghajtó felsorolása)?

- HTTP.sys
- ntskrnl.exe
- Ndu.sys