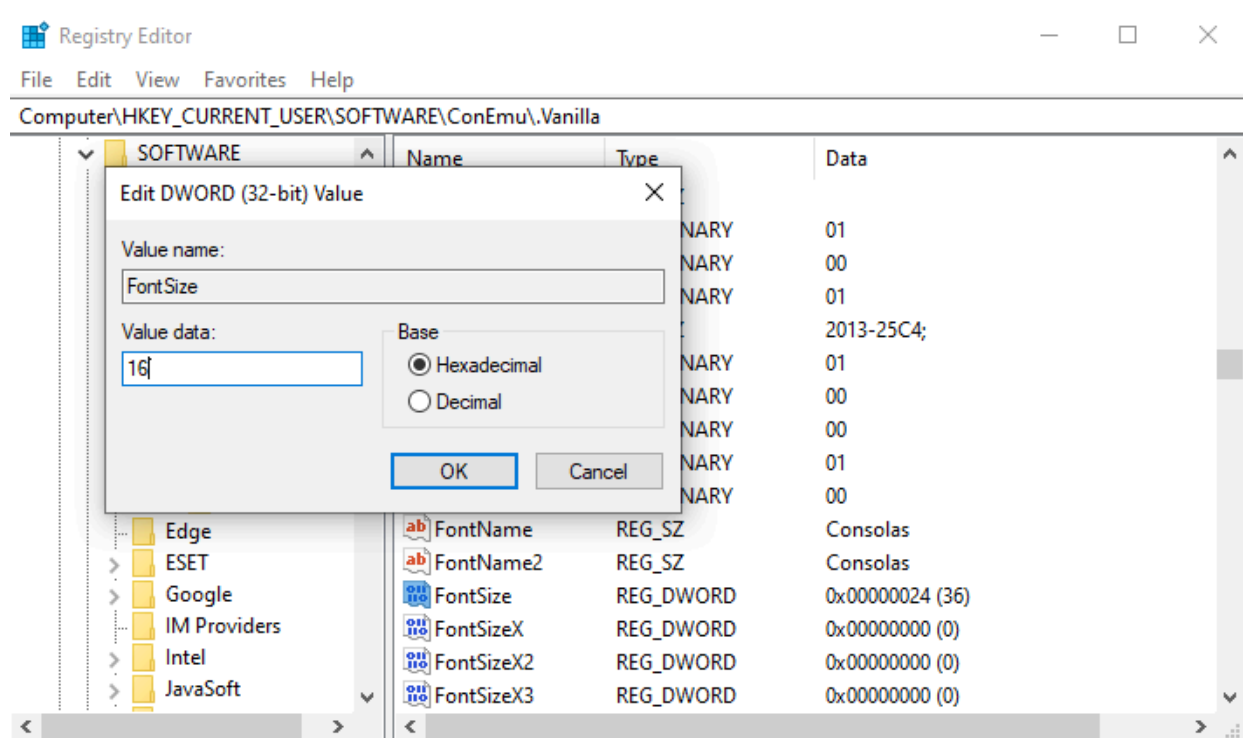
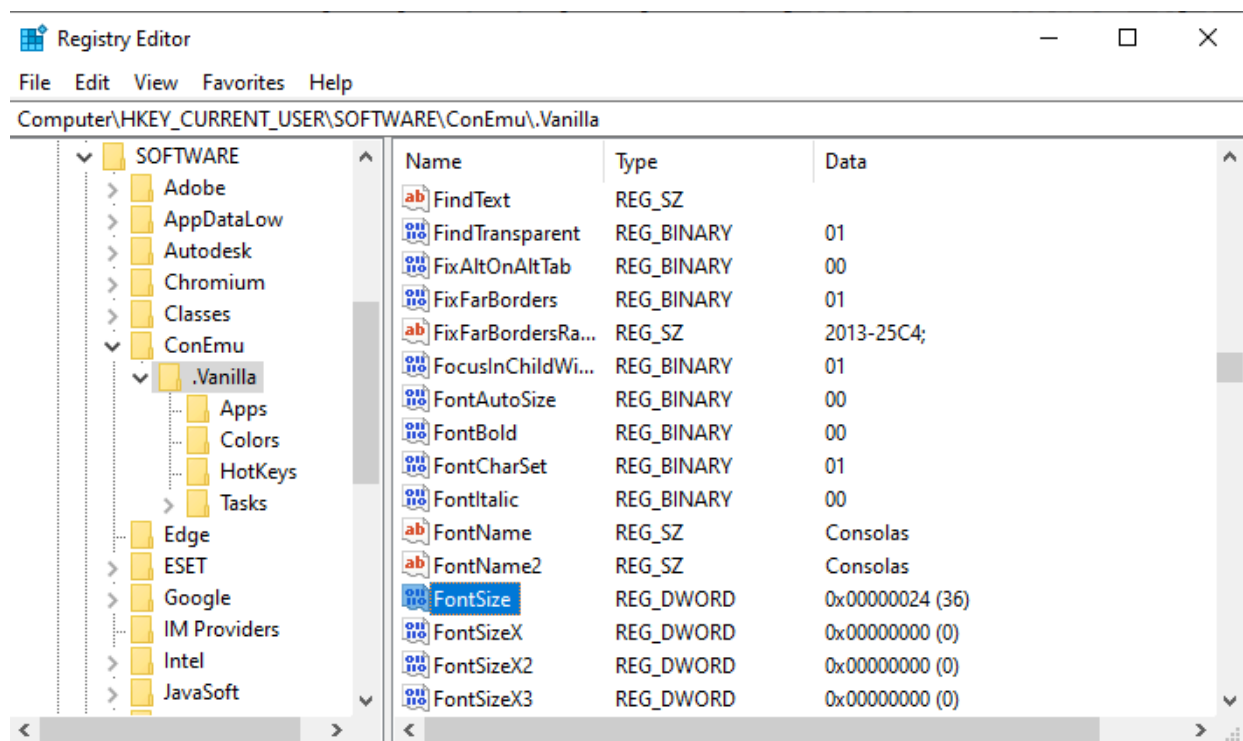
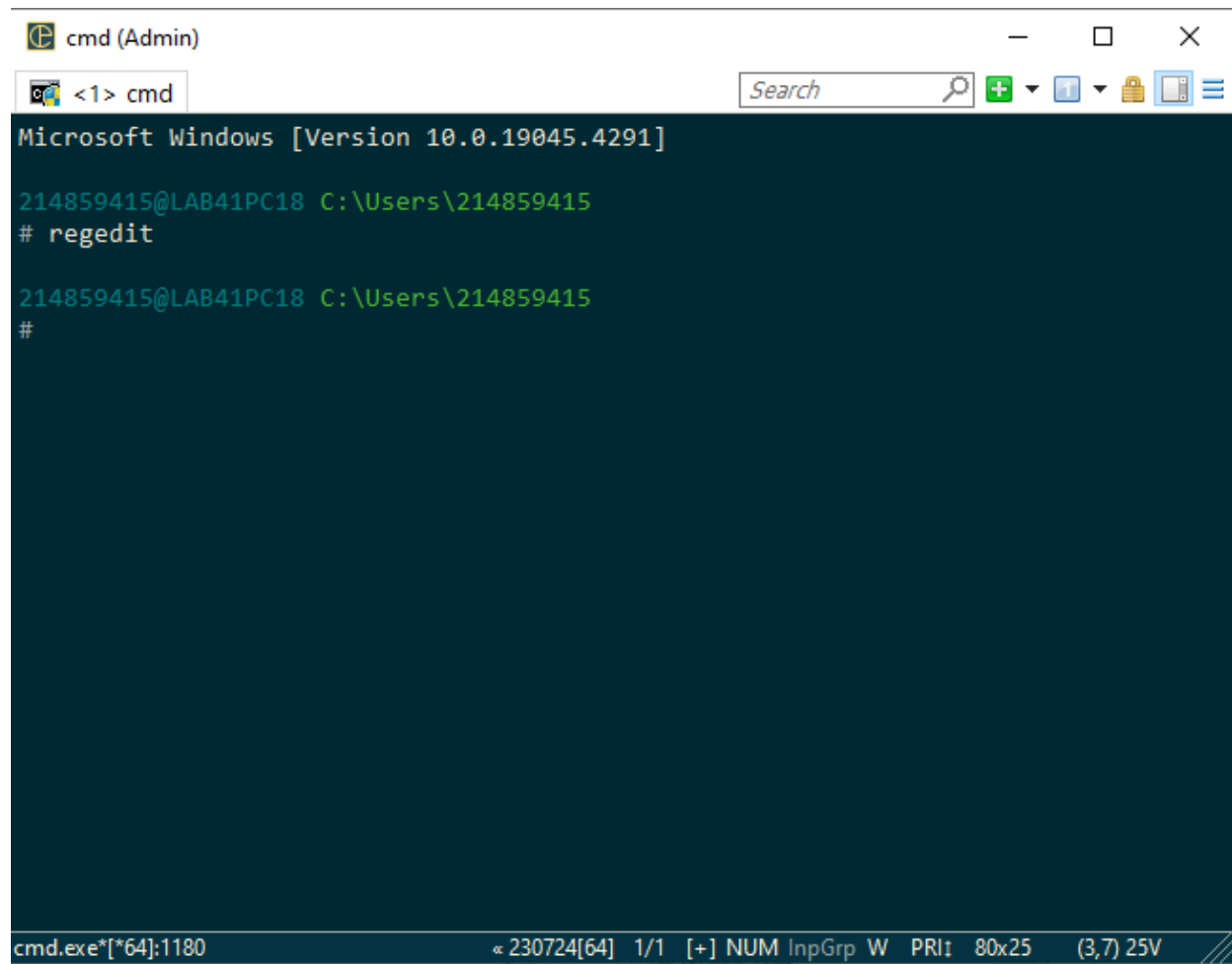


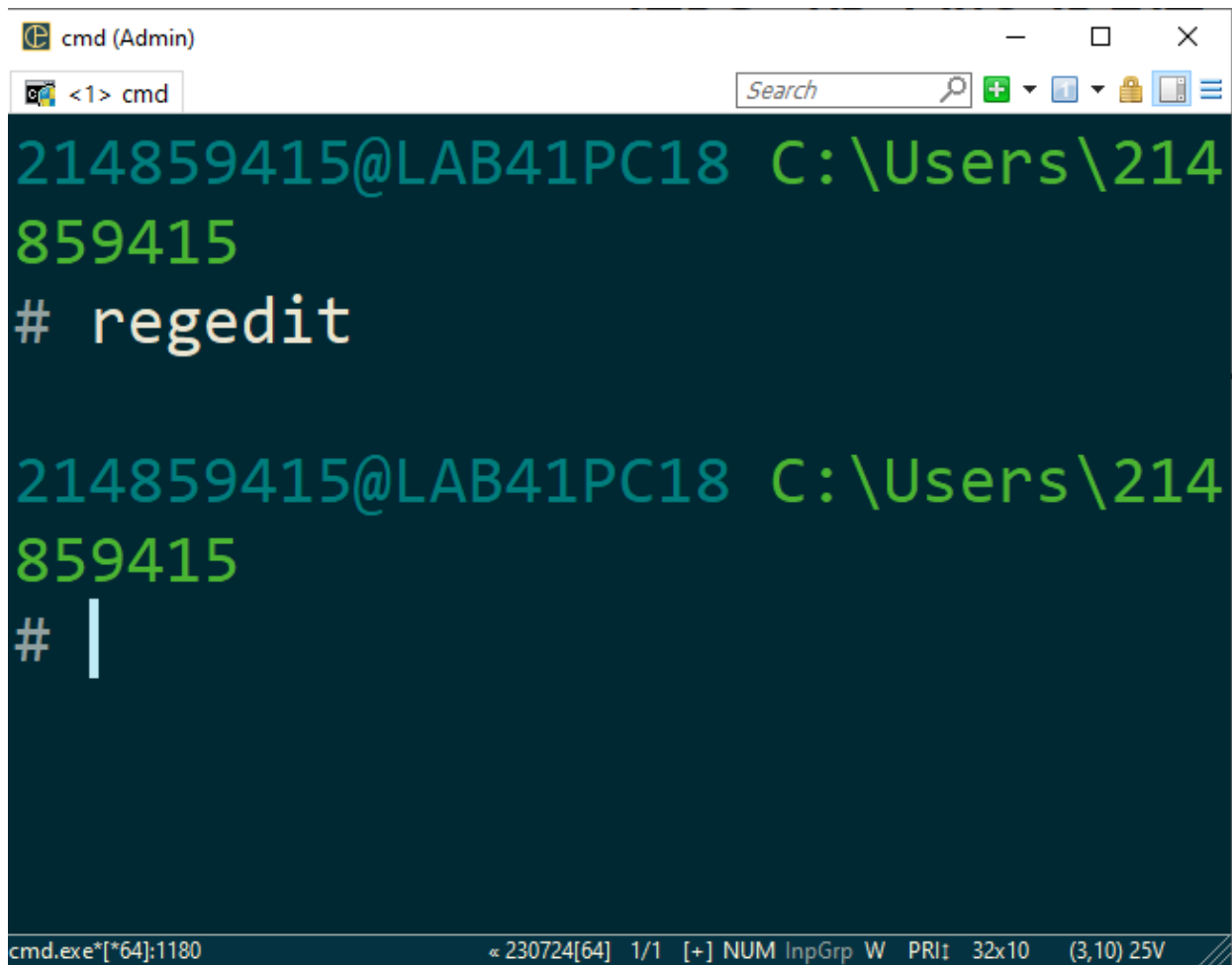
1.





```
cmd (Admin)
Search
214859415@LAB41PC18 C:\Users\214859415
# regedit
214859415@LAB41PC18 C:\Users\214859415
#
```

cmd.exe[\*64]:1180      α 230724[64] 1/1 [+] NUM InpGrp W PRI: 80x25 (3,7) 25V

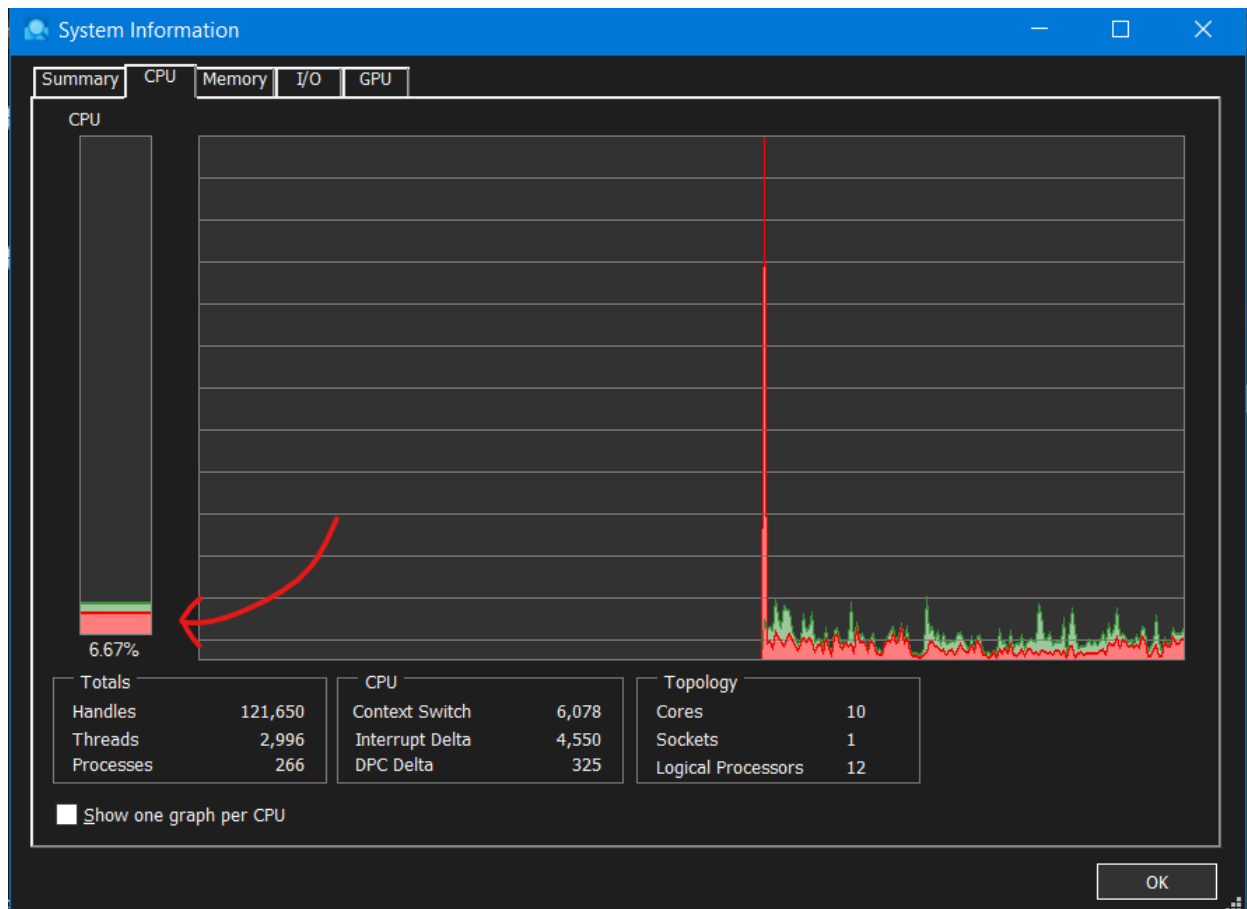


```
cmd (Admin)
<1> cmd
214859415@LAB41PC18 C:\Users\214859415
# regedit
214859415@LAB41PC18 C:\Users\214859415
# |
cmd.exe[*64]:1180 « 230724[64] 1/1 [+] NUM InpGrp W PRI: 32x10 (3,10) 25V
```

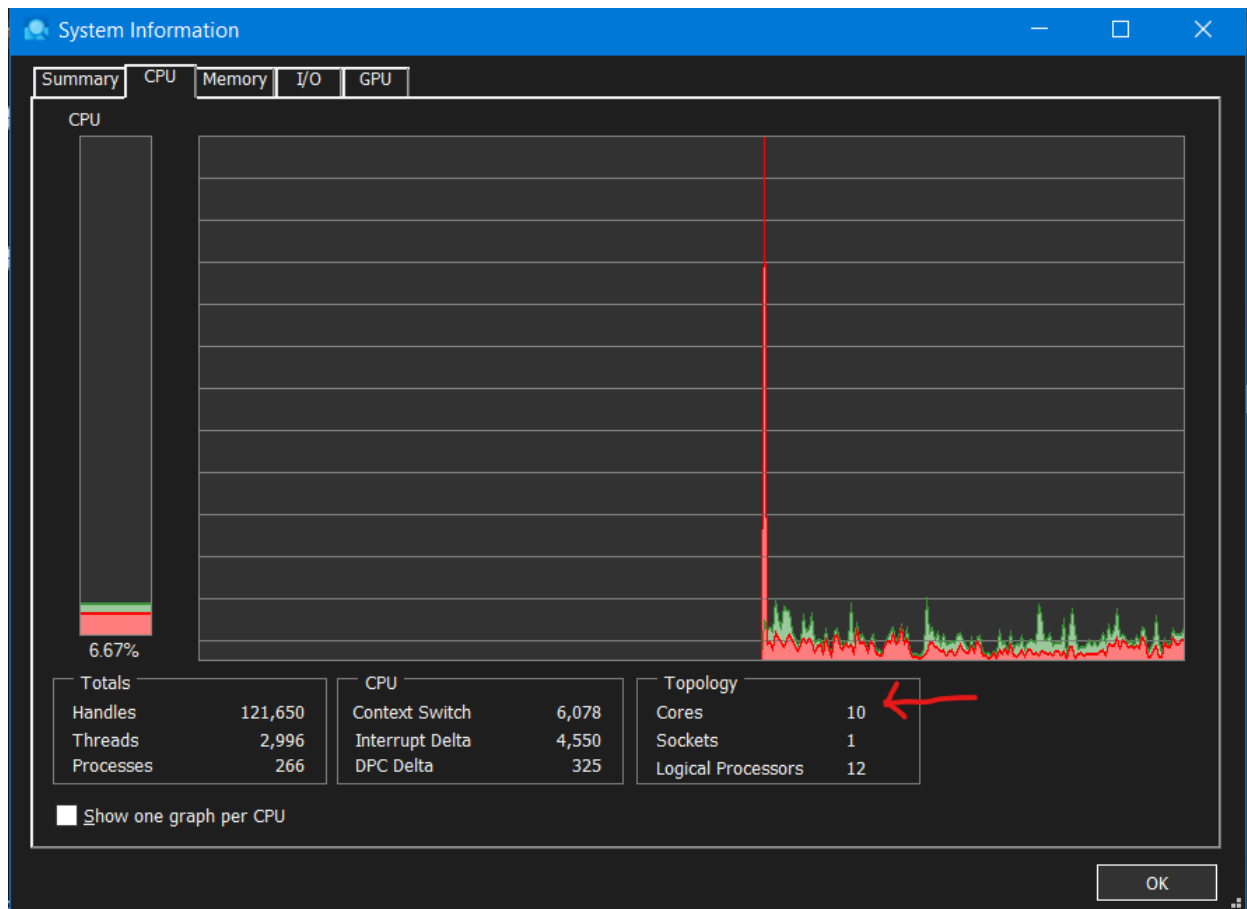
החסרונות בשמירה ב registry:  
בגלל שב registry שומרים נתונים והגדרות של מערכת ההפעלה, שימוש לא נכון יכול לגרום נזק למערכת ההפעלה ולמחשב. בנוסף, שינויים שנשמרו ב registry לא מתעדכנים אוטומטית- נדרש לסגור את התוכנית ולהריץ אותה שוב.

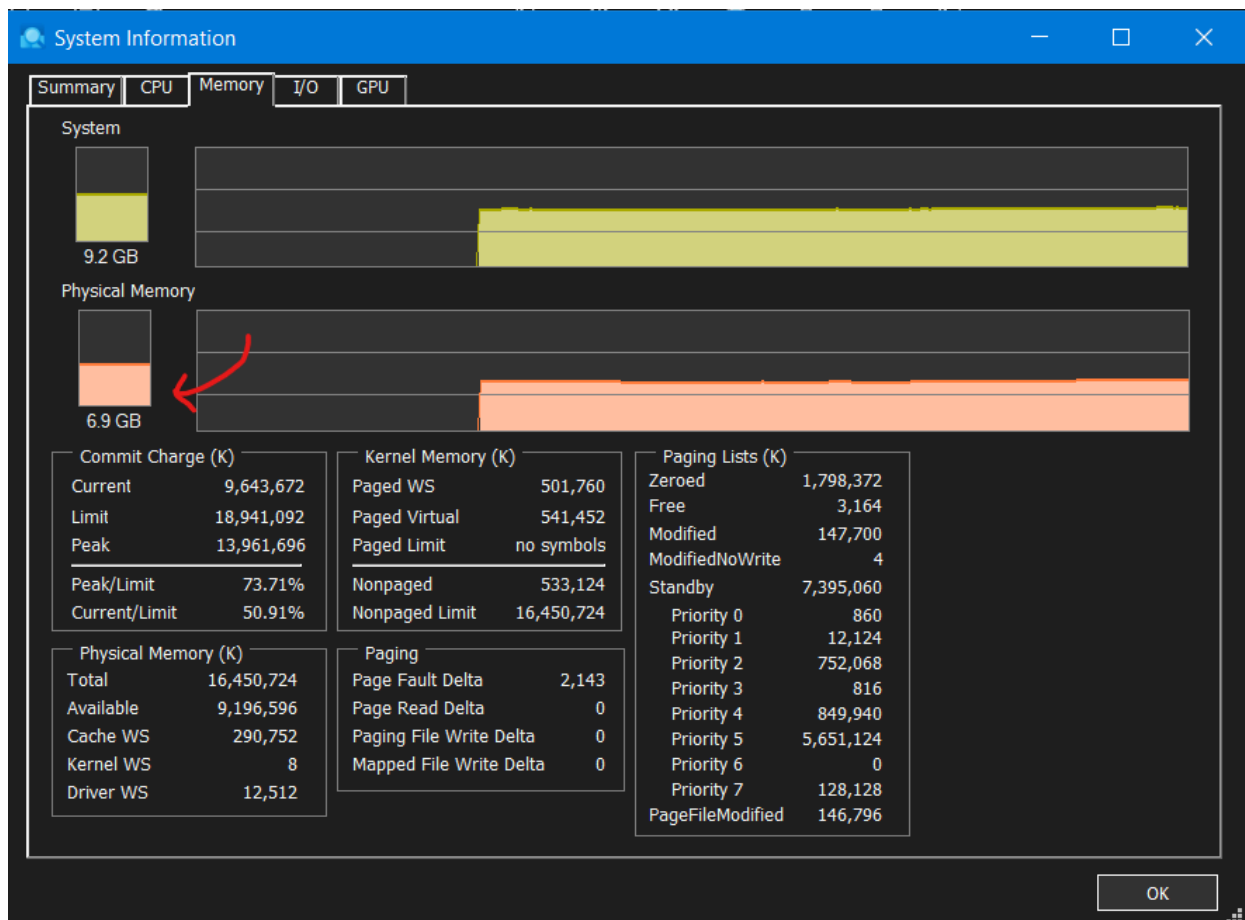


.7 .x

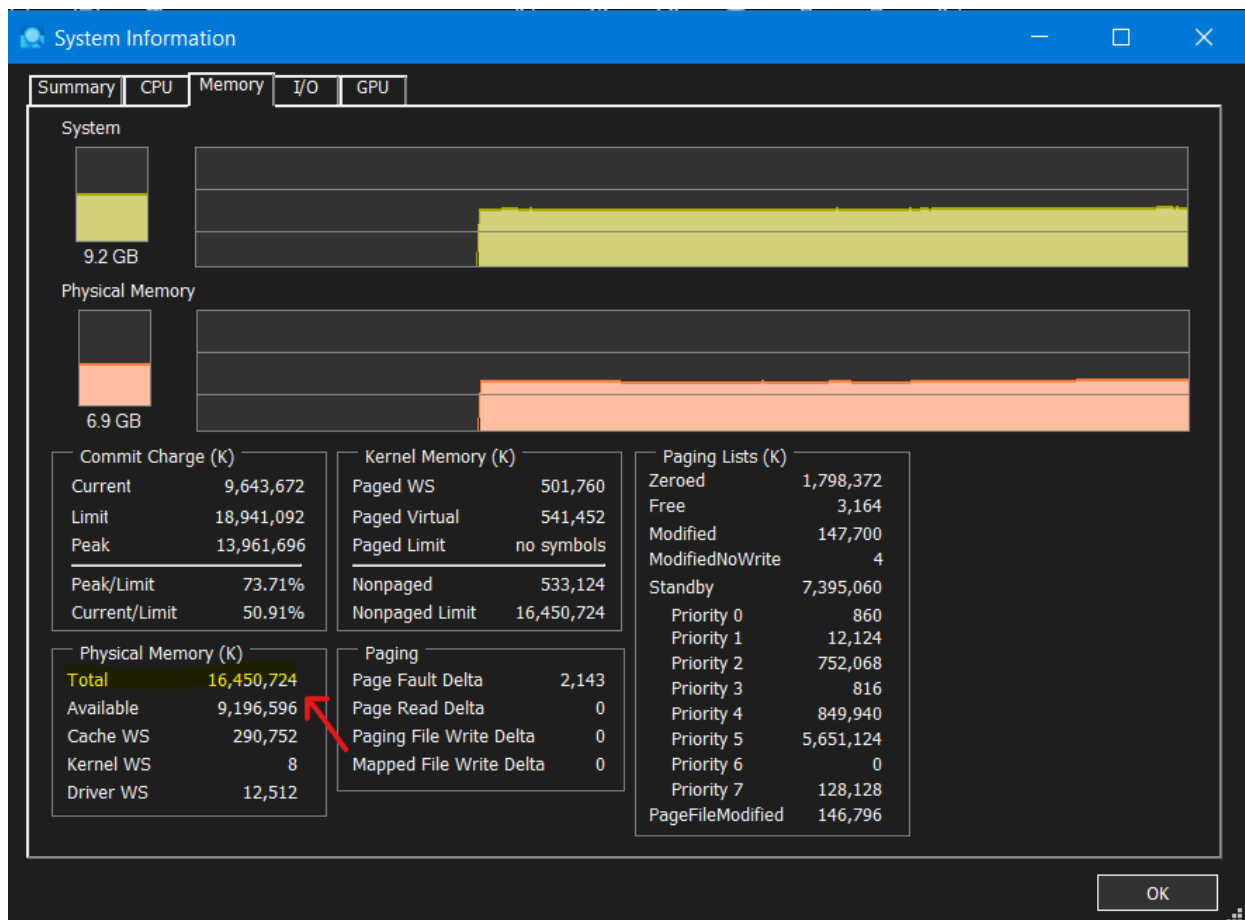


.1



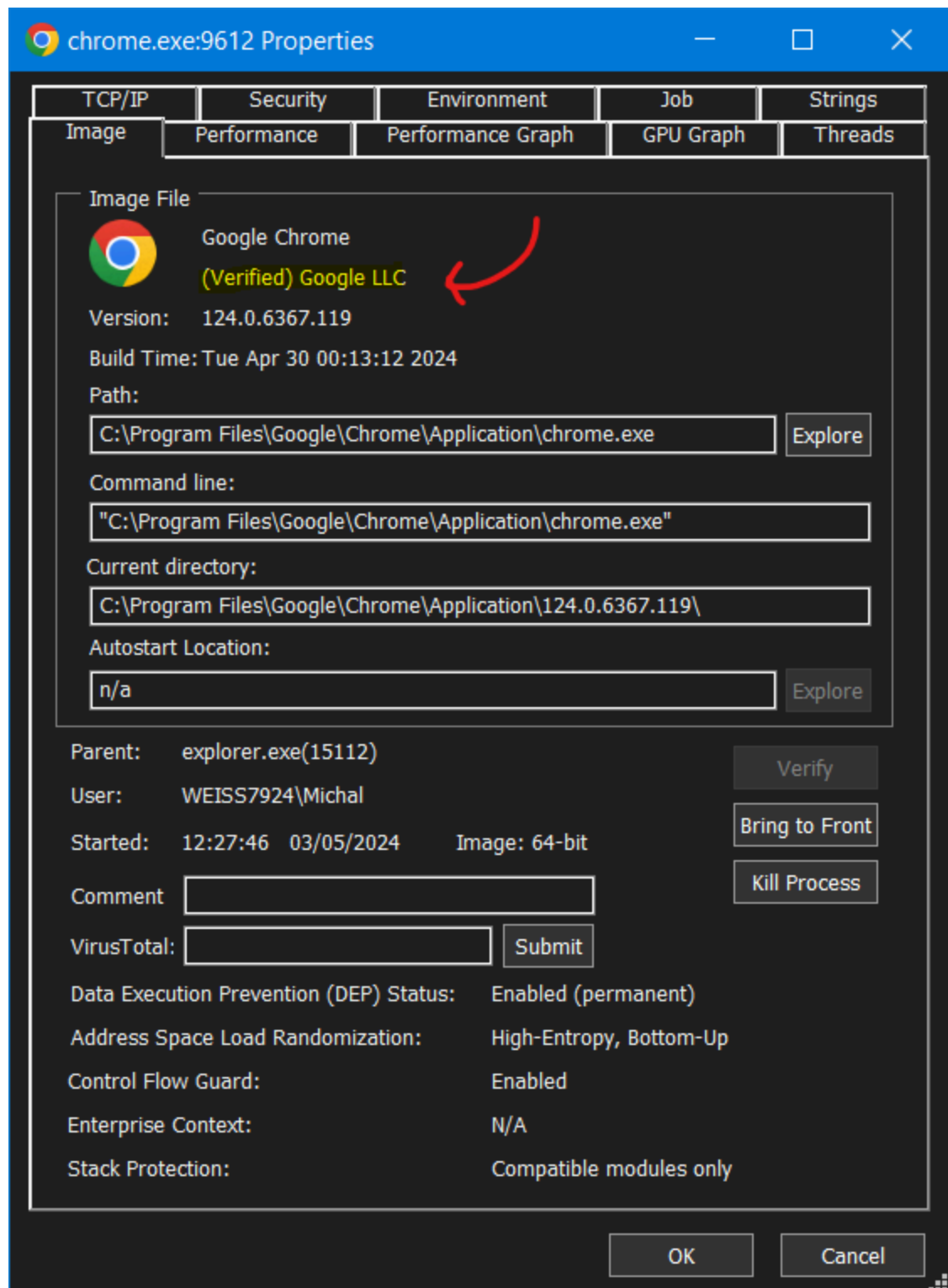


.T



.X .8





0/76 ב.  
again א.

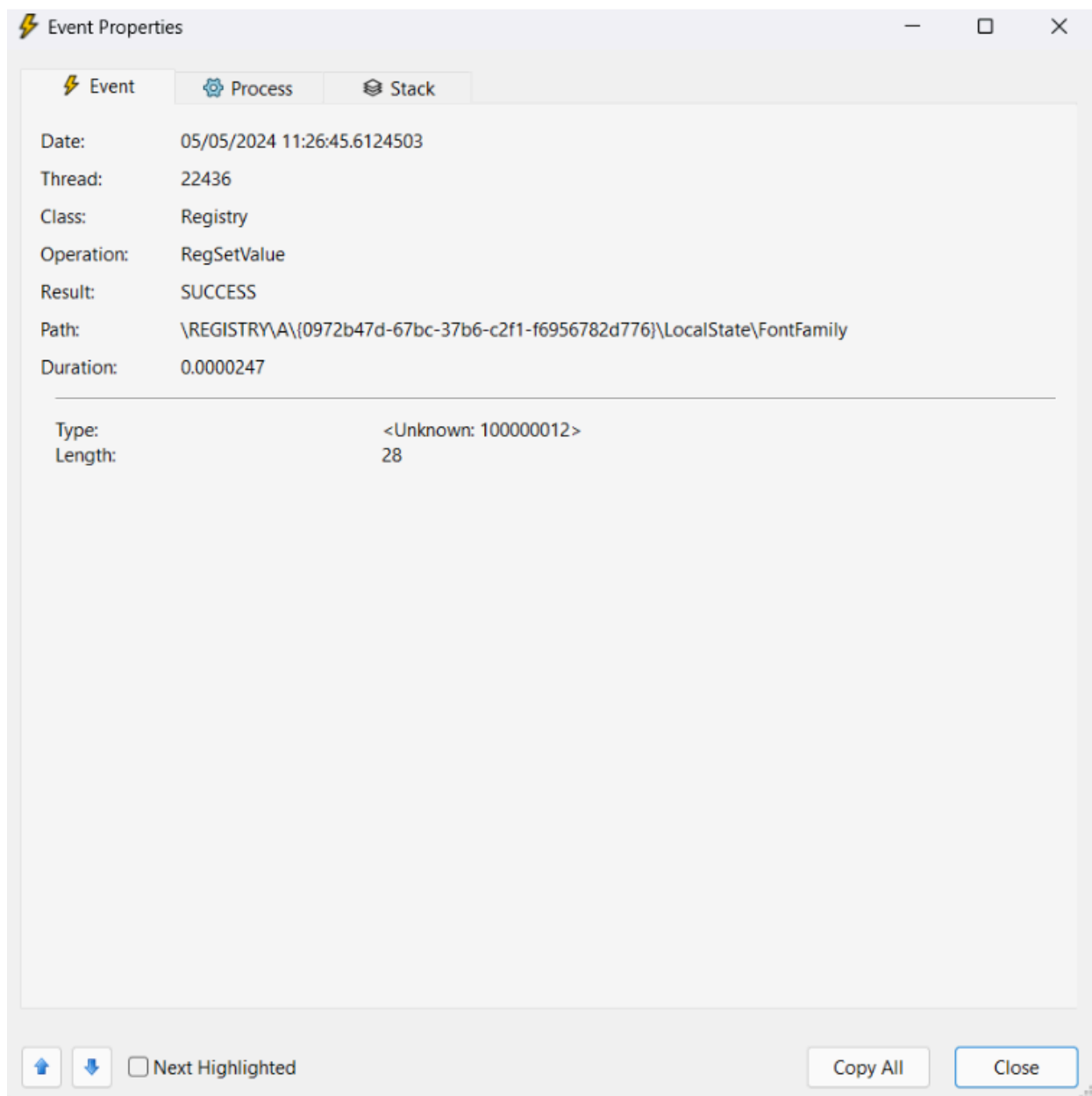
98.6 .T

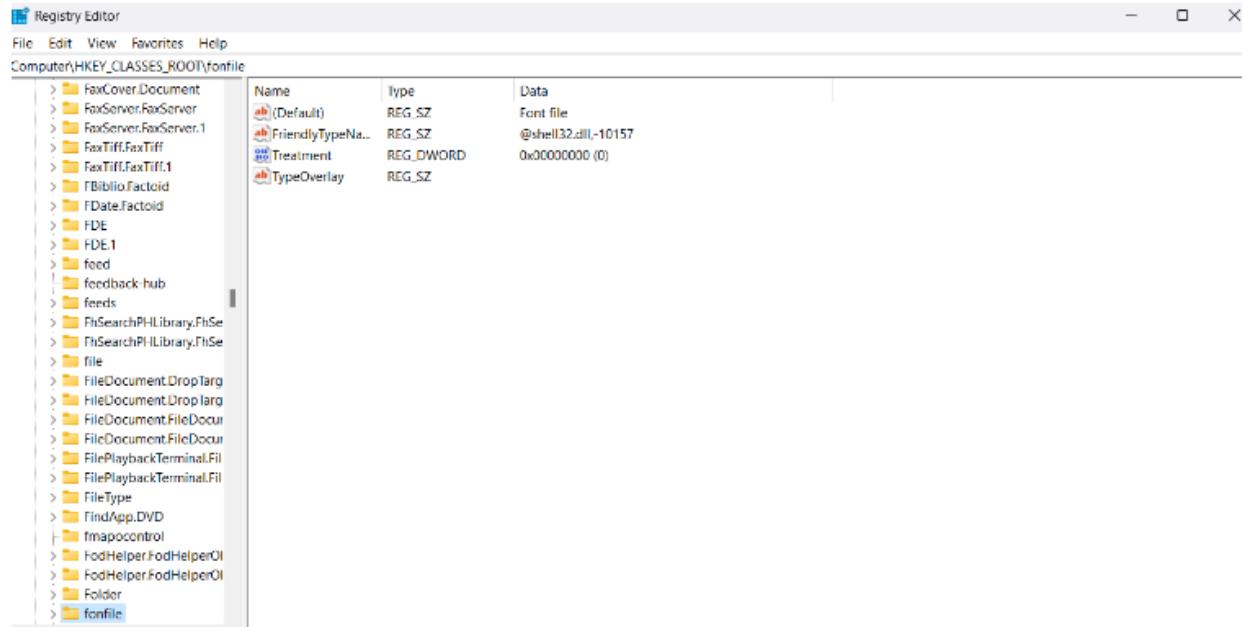
283 .ה

א7 .I

WINWORD.EXE .9

Procmon





Time el...	Process Name	PID	Operation	Path	Result	Detail
1:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,009, Len...
1:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,021, Len...
1:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,028, Len...
1:27:00	chrome.exe	13845	ReadFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 35,192, Leng...
1:27:00	chrome.exe	13845	ReadFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 35,228, Leng...
1:27:00	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 35,192, Leng...
1:27:00	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 35,228, Leng...
1:27:00	chrome.exe	13845	ReadFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,476, Leng...
1:27:00	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,512, Leng...
1:27:00	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,512, Leng...
1:27:00	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,476, Leng...
1:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,040, Len...
1:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,058, Len...
1:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,066, Len...
1:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,078, Len...
1:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,086, Len...
1:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,097, Len...
1:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,104, Len...
1:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,116, Len...
1:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,123, Len...
1:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,136, Len...
1:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efadn...	SUCCESS	Offset 717,142, Len...
1:27:02	chrome.exe	13845	ReadFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 57,908, Leng...
1:27:02	chrome.exe	13845	ReadFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 105,284, Len...
1:27:02	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 57,908, Leng...
1:27:02	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 105,284, Len...
1:27:02	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,548, Leng...
1:27:02	chrome.exe	13845	ReadFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,476, Leng...
1:27:02	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,476, Leng...
1:27:02	chrome.exe	13845	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,548, Leng...

Time	Process Name	PID	Operation	Path	Result	Detail
11:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 716,990 Len...
11:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,002 Len...
11:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,009 Len...
11:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,021 Len...
11:26:59	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,028 Len...
11:27:00	svchost.exe	3004	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Licensing-Platform%4Admin.evtx	SUCCESS	Offset 593,920 Len...
11:27:00	svchost.exe	3004	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx	SUCCESS	Offset 331,776 Len...
11:27:00	svchost.exe	3004	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Store%4Operational.evtx	SUCCESS	Offset 18,147,392 L...
11:27:00	svchost.exe	3004	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx	SUCCESS	Offset 383,640 Len...
11:27:00	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 35,192 Len...
11:27:00	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 35,228 Len...
11:27:00	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,476 Len...
11:27:00	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,512 Len...
11:27:00	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,476 Len...
11:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,040 Len...
11:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,047 Len...
11:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,059 Len...
11:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,066 Len...
11:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,070 Len...
11:27:00	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,085 Len...
11:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,091 Len...
11:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,104 Len...
11:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,116 Len...
11:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,123 Len...
11:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,135 Len...
11:27:01	chrome.exe	18968	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\efaidn...	SUCCESS	Offset 717,142 Len...
11:27:02	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 57,908 Len...
11:27:02	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 105,204 Len...
11:27:02	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,548 Len...
11:27:02	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,476 Len...
11:27:02	chrome.exe	13848	WriteFile	C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\data_0	SUCCESS	Offset 93,548 Len...

Showing 21,568 of 851,698 events (2.5%)      Backed by virtual memory

Time	Process Name	PID	Operation	Path	Result	Detail
11:26:28	SearchHost.exe	10388	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx\PackageRepositoryRoot	BUFFER OVERFL...	Length 12
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Metada...	SUCCESS	Type: REG_DW...
11:26:28	SearchHost.exe	10388	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx\PackageRepositoryRoot	SUCCESS	Type: REG_SZ Le...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	BUFFER OVERFL...	Length 12
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	SearchHost.exe	10388	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx\PackageRepositoryRoot	SUCCESS	Type: REG_SZ Le...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Metada...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	BUFFER OVERFL...	Length 144
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_SZ Le...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\NT\CurrentVersion\OEMDeviceForm	NAME NOT FOUND	Length 20
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_DW...
11:26:28	SearchHost.exe	10388	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\NT\CurrentVersion\LocalState\DefaultSettingsVersion	SUCCESS	Type: <Unknown: 1...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Package\Datatbl\MutableLink	TYPE: REG_NONE...	Type: REG_NONE...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Metada...	SUCCESS	Type: REG_DW...
11:26:28	SearchHost.exe	10388	RegQueryValue	REGISTRY\A(ae655bcb-f7b3-0d0f-20f-3329acdd13d3)\LocalState\AppIndexer\CurrentScaleFactor	BUFFER OVERFL...	Length 12
11:26:28	SearchHost.exe	10388	RegQueryValue	REGISTRY\A(ae655bcb-f7b3-0d0f-20f-3329acdd13d3)\LocalState\AppIndexer\CurrentScaleFactor	SUCCESS	Type: <Unknown: 1...
11:26:28	SearchHost.exe	10388	RegQueryValue	REGISTRY\A(ae655bcb-f7b3-0d0f-20f-3329acdd13d3)\LocalState\AppIndexer\CurrentScaleFactor	SUCCESS	Type: <Unknown: 1...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Metada...	SUCCESS	Type: REG_DW...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	BUFFER OVERFL...	Length 144
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_SZ Le...
11:26:28	RuntimeBroker...	10904	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Packa...	SUCCESS	Type: REG_NONE...

Showing 48,875 of 851,698 events (5.7%)      Backed by virtual memory

NtQueryValueKey

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time o...	Process Name	PID	Operation	Path	Result	Detail
1:25:23	Conhost.exe	10300	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:23	Conhost.exe	3620	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:28	Conhost.exe	15200	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:28	Conhost.exe	10104	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:33	Conhost.exe	16028	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:33	Conhost.exe	13292	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:38	Conhost.exe	12132	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:38	Conhost.exe	15528	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:44	Conhost.exe	4312	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:44	Conhost.exe	22400	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:49	Conhost.exe	14960	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:49	Conhost.exe	15416	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:54	Conhost.exe	20020	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:54	Conhost.exe	6052	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:59	Conhost.exe	5240	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...
1:25:59	Conhost.exe	15984	RegQueryValue	HKCU\Console/FontSize	SUCCESS	Type: REG_DWO...

ConHost.exe

תרגיל סיכום

