ADVANCED DIGITAL FORENSICS

PROCESS EXPLORER

By

DEWTON KIPROP

- Run Process Explorer
  Double-click on the procexp.exe file to launch Process Explorer. You may need to provide administrative privileges if prompted.
- Explore Process Information
  Once Process Explorer is running, you'll see a list of running processes on your system. Each process is represented by a row in the main window, displaying details such as process name, ID, CPU usage, memory usage, and more.
- View Process Properties
  To view detailed properties of a specific process, double-click on it or right-click and select "Properties".
  The process properties window provides in-depth information about the selected process, including its executable path, command-line arguments, loaded DLLs, and more.
- Search for Processes

Use the search functionality (Ctrl + F) to quickly find specific processes by name or other criteria.

- Terminate or Suspend Processes
  To terminate a process, select it and press the Delete key or right-click and choose "Kill Process". Be cautious when terminating processes, as terminating critical system processes can cause system instability.
- Filter Processes
  Process Explorer allows you to filter processes based on various criteria such as CPU usage, memory usage, process name, and more. Use the Filter menu to apply filters.
- Customize Columns
  You can customize the columns displayed in the main Process Explorer window to show additional information. Right-click on the column header and choose "Select Columns" to customize.
- Additional Features
  Explore other features of Process Explorer, such as system information, performance graphs, process tree view, and tooltips for more insights into system activity.
- Refer to Documentation
  If you encounter any issues or need assistance with specific features, refer to the Process Explorer documentation available on the Sysinternals website.
- Exit Process Explorer
  When you're done using Process Explorer, you can close the application by clicking on the "X" button in the top-right corner of the window or by selecting File > Exit.

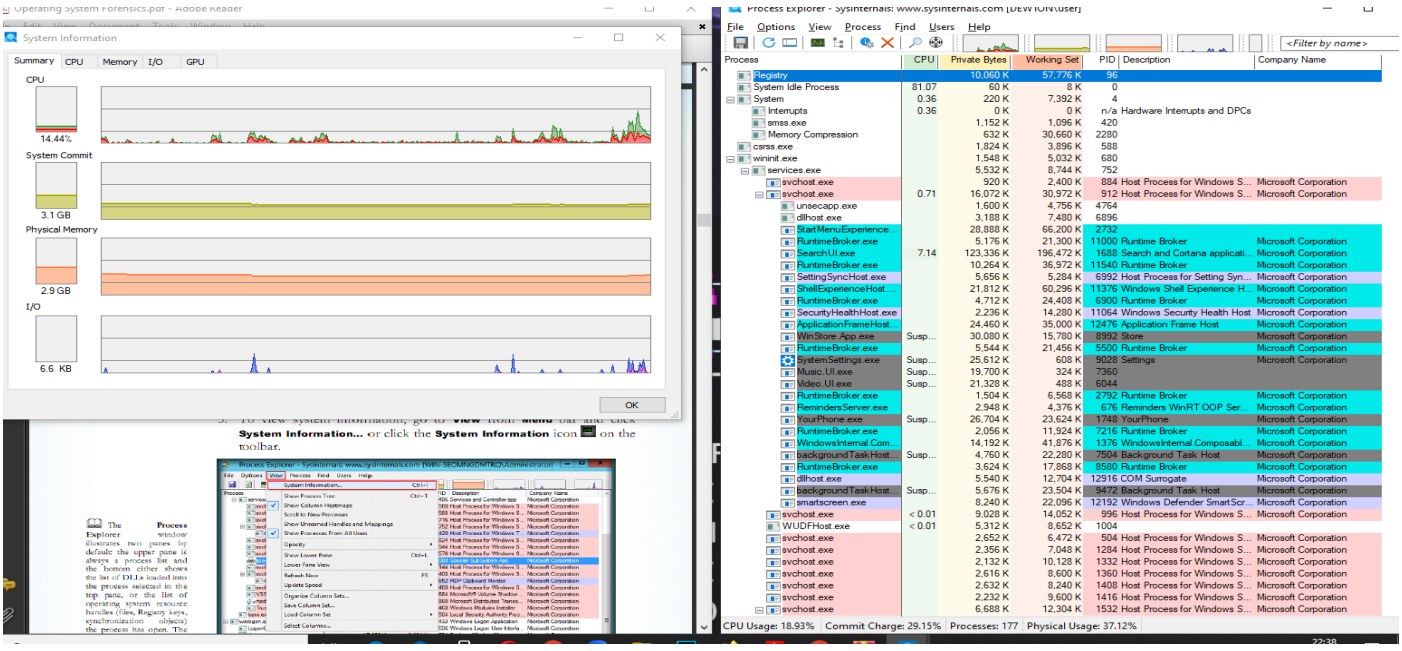

Fig 1 : system information

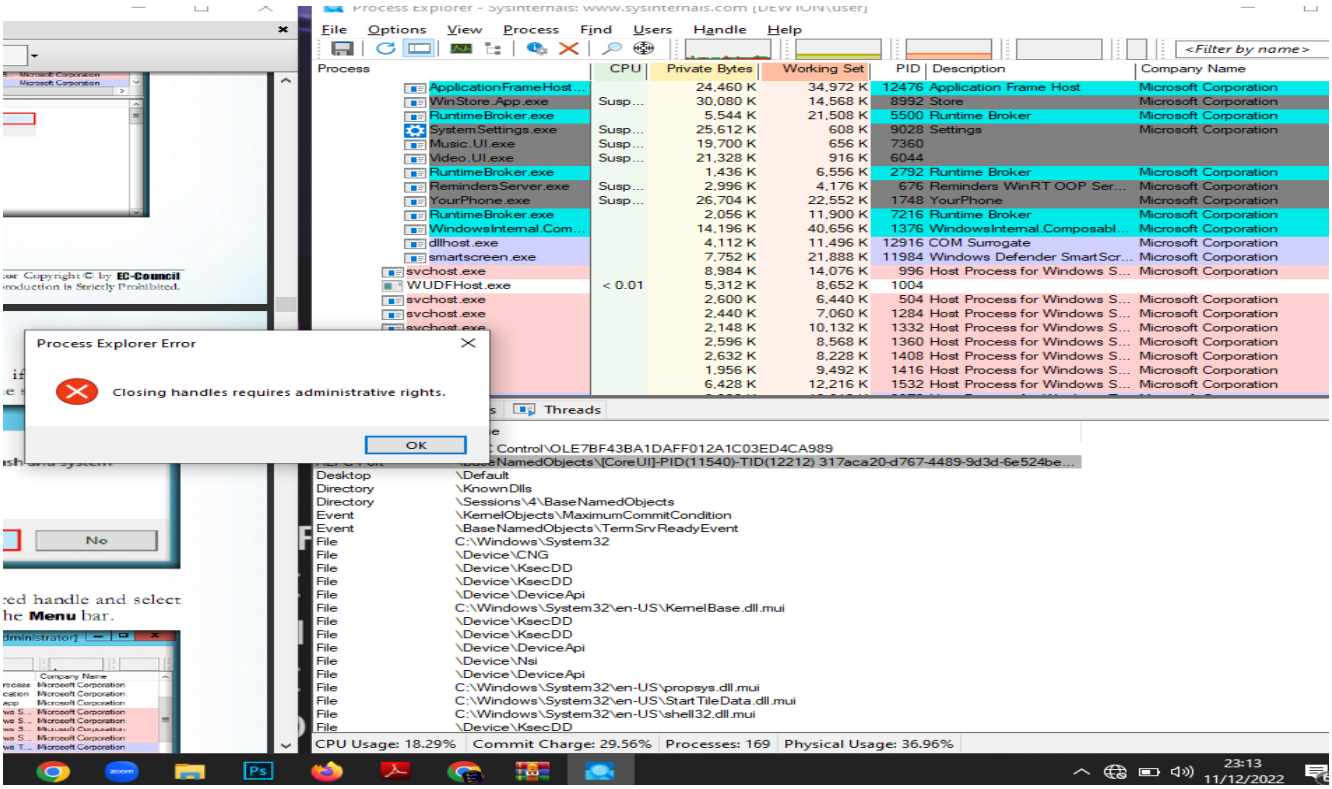

Fig 2: closing handle

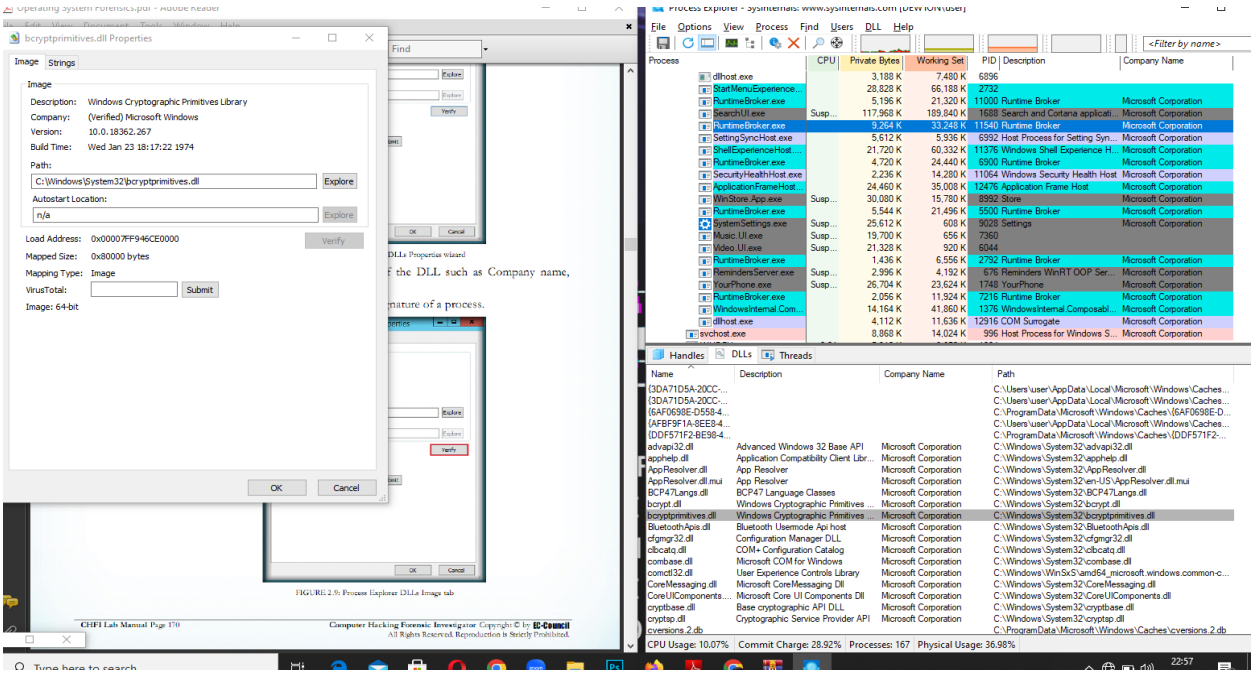

Fig 3: DLL properties verification

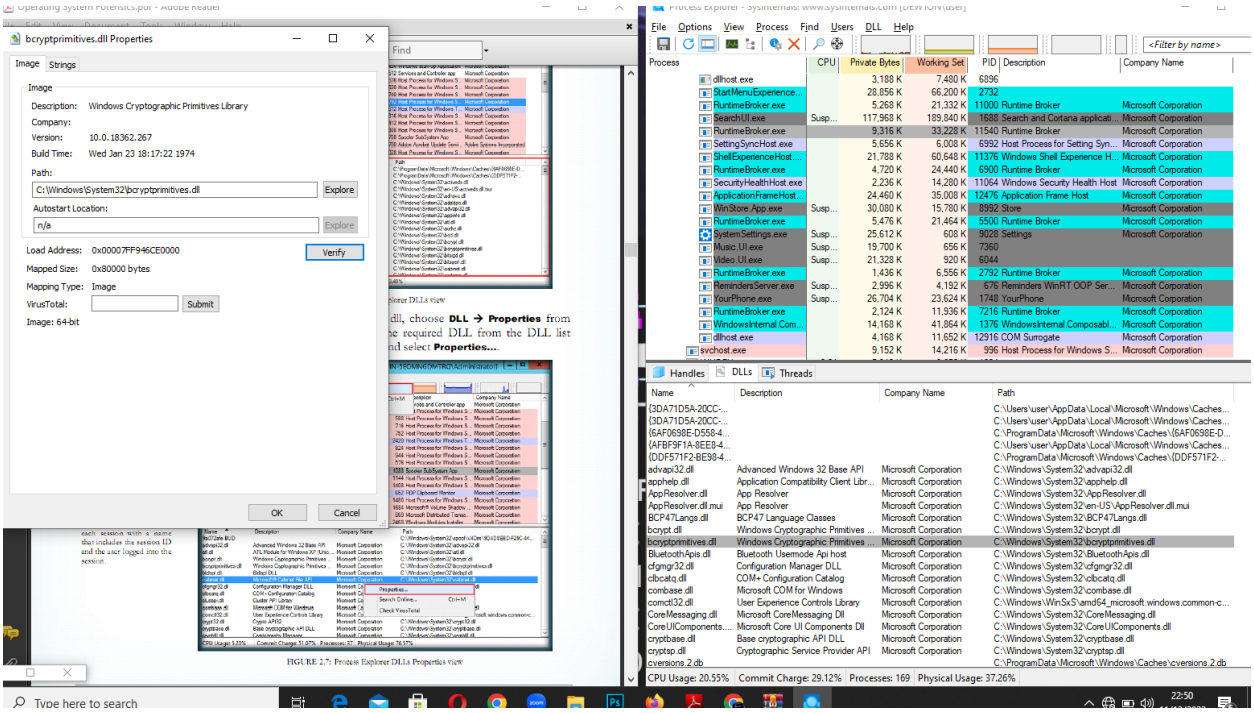

Fig 4: image DLL viewing

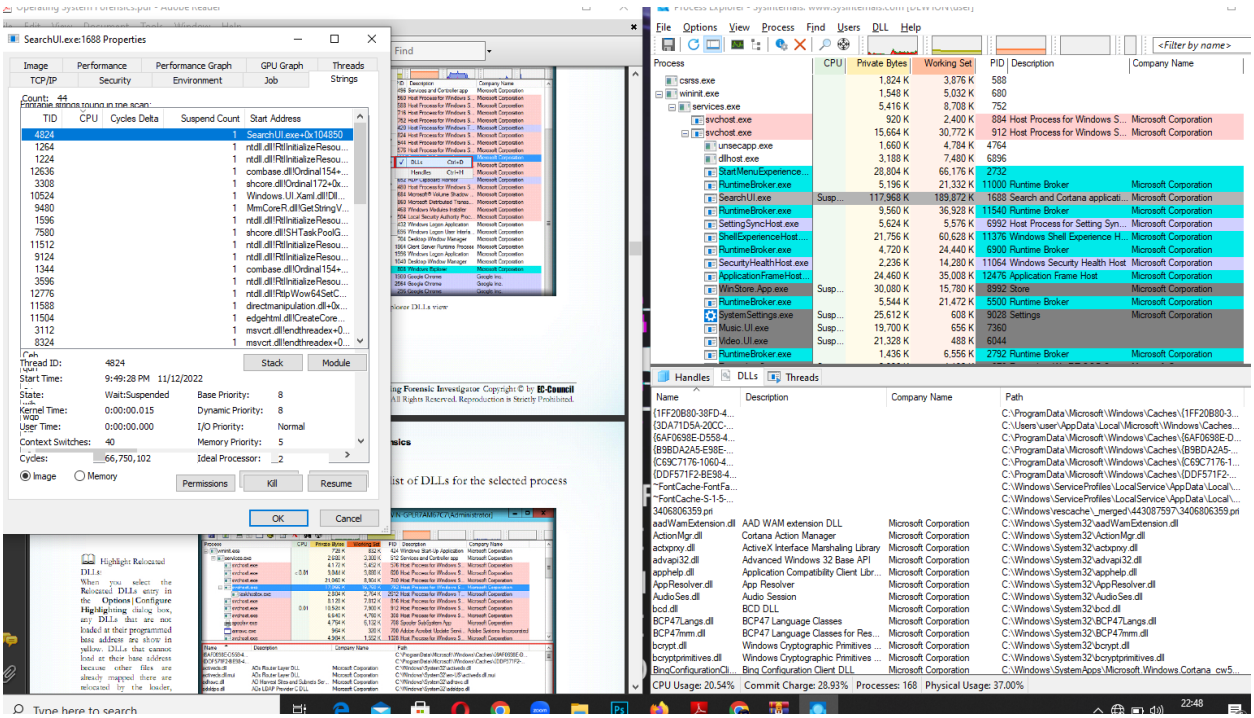

Fig 5 : view DLL

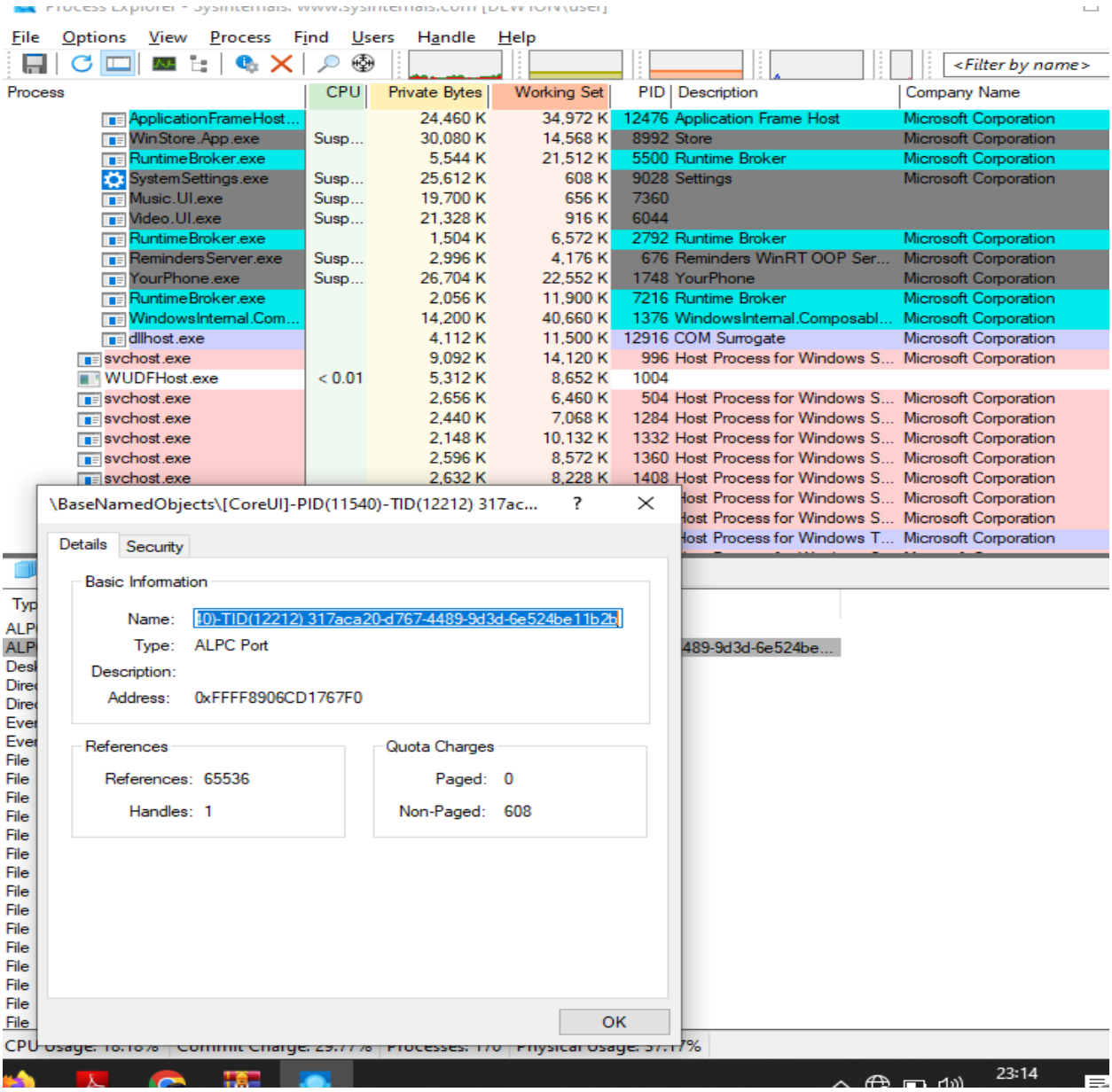

Fig 6: handle properties view

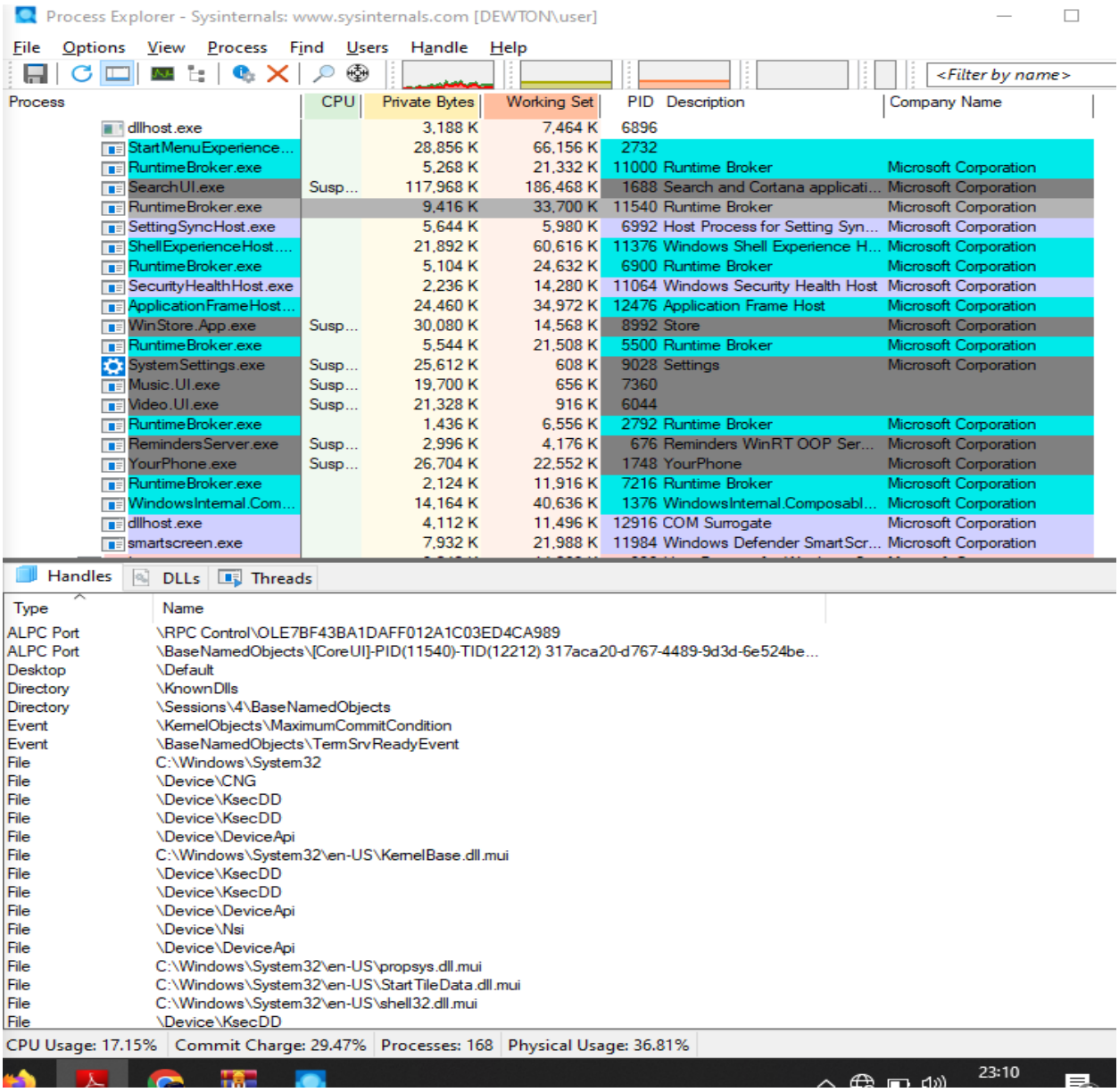

Fig 7: handles

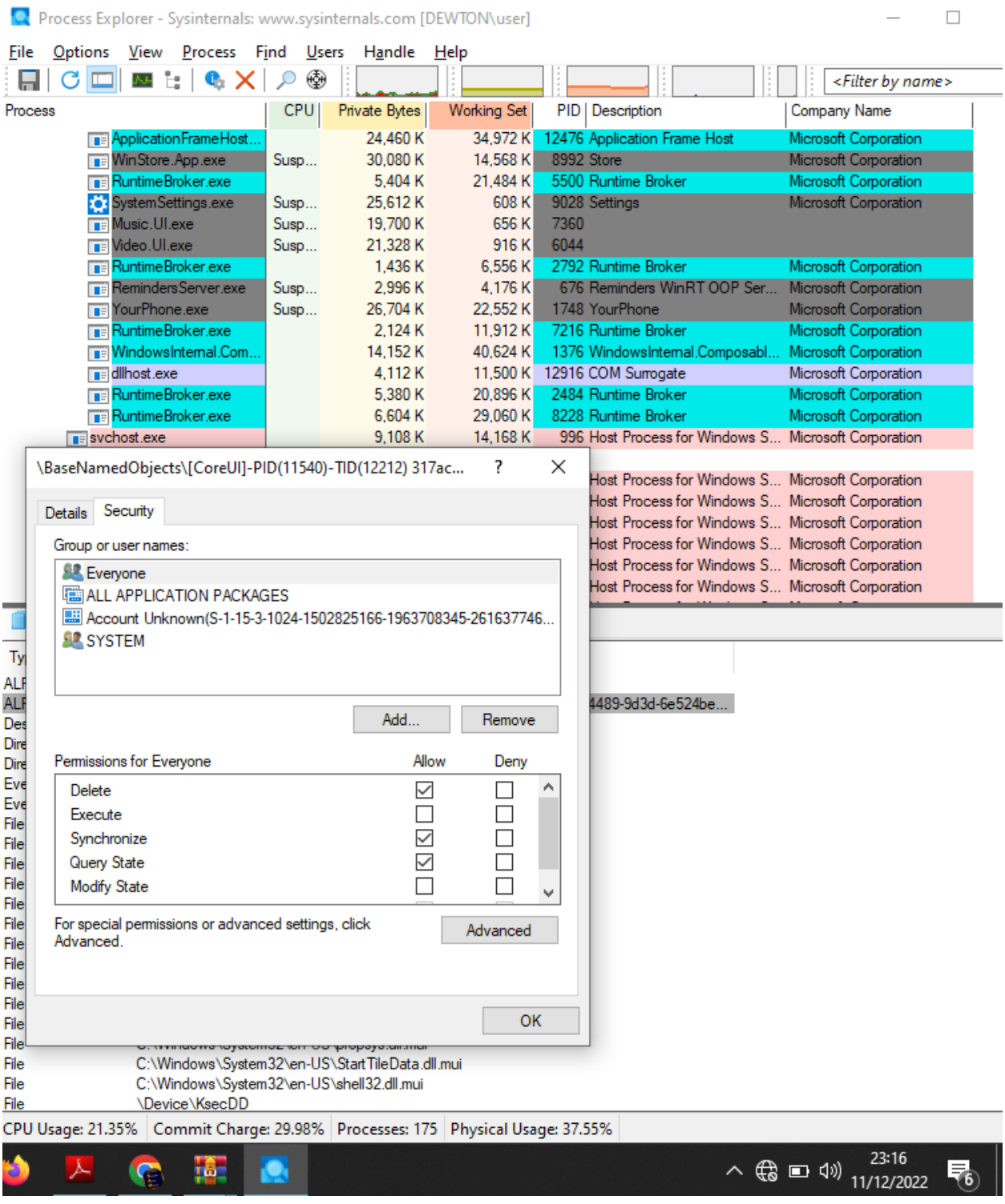

Fig 8 : handle security properties.

Notepad work saved

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		7,184 K	55,396 K	96		

System Idle Process		84.83	60 K	8 K	0			
System	< 0.01	220 K	7,432 K	4				
Interrupts		1.49	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe			1,152 K	1,096 K	420			
Memory Compression			632 K	30,652 K	2280			
csrss.exe			1,824 K	3,888 K	588			
wininit.exe			1,548 K	5,032 K	680			
services.exe			5,520 K	8,744 K	752			
svchost.exe			920 K	2,400 K	884	Host Process for Windows Services	Microsoft Corporation	
svchost.exe			15,772 K	30,856 K	912	Host Process for Windows Services	Microsoft Corporation	
unsecapp.exe			1,632 K	4,772 K	4764			
dllhost.exe			3,188 K	7,460 K	6896			
StartMenuExperienceHost.exe				28,856 K	66,156 K	2732		
RuntimeBroker.exe			5,196 K	21,320 K	11000	Runtime Broker	Microsoft Corporation	
SearchUI.exe	Suspended		117,968 K	186,468 K	1688	Search and Cortana application	Microsoft Corporation	
RuntimeBroker.exe			9,496 K	33,756 K	11540	Runtime Broker	Microsoft Corporation	
SettingSyncHost.exe			5,612 K	5,392 K	6992	Host Process for Setting Synchronization	Microsoft Corporation	
ShellExperienceHost.exe				21,740 K	60,260 K	11376	Windows Shell Experience Host	Microsoft Corporation
RuntimeBroker.exe			4,740 K	24,476 K	6900	Runtime Broker	Microsoft Corporation	
SecurityHealthHost.exe				2,236 K	14,280 K	11064	Windows Security Health Host	Microsoft Corporation
ApplicationFrameHost.exe				24,460 K	34,972 K	12476	Application Frame Host	Microsoft Corporation
WinStore.App.exe	Suspended			30,080 K	14,568 K	8992	Store	Microsoft Corporation
RuntimeBroker.exe			5,544 K	21,512 K	5500	Runtime Broker	Microsoft Corporation	
SystemSettings.exe	Suspended			25,612 K	608 K	9028	Settings	Microsoft Corporation

Music.UI.exe Suspended 19,700 K 656 K 7360

Video.UI.exe Suspended 21,328 K 916 K 6044

RuntimeBroker.exe 1,504 K 6,568 K 2792 Runtime Broker Microsoft Corporation

RemindersServer.exe Suspended 2,996 K 4,176 K 676 Reminders WinRT OOP Server Microsoft Corporation

YourPhone.exe Suspended 26,704 K 22,552 K 1748 YourPhone Microsoft Corporation

RuntimeBroker.exe 2,056 K 11,900 K 7216 Runtime Broker Microsoft Corporation

WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.exe 14,180 K 40,640 K 1376 WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.exe Microsoft Corporation

dllhost.exe 4,112 K 11,500 K 12916 COM Surrogate Microsoft Corporation

dllhost.exe 1,644 K 6,832 K 11208 COM Surrogate Microsoft Corporation

svchost.exe < 0.01 8,996 K 14,088 K 996 Host Process for Windows Services Microsoft Corporation

WUDFHost.exe < 0.01 5,312 K 8,652 K 1004

svchost.exe 2,656 K 6,472 K 504 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,440 K 7,064 K 1284 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,148 K 10,132 K 1332 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,596 K 8,564 K 1360 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,632 K 8,228 K 1408 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,956 K 9,492 K 1416 Host Process for Windows Services Microsoft Corporation

svchost.exe < 0.01 6,532 K 12,252 K 1532 Host Process for Windows Services Microsoft Corporation

taskhostw.exe 8,392 K 18,620 K 8372 Host Process for Windows Tasks Microsoft Corporation

svchost.exe 14,944 K 14,372 K 1644 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,180 K 6,360 K 1668 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,708 K 3,744 K 1692 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,280 K 6,564 K 1708 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,840 K 9,108 K 1756 Host Process for Windows Services Microsoft Corporation

svchost.exe 4,352 K 6,156 K 1824 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,660 K 5,508 K 1968 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,492 K 4,748 K 2008 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,676 K 7,832 K 568 Host Process for Windows Services Microsoft Corporation

sihost.exe 6,268 K 24,656 K 7576 Shell Infrastructure Host Microsoft Corporation

svchost.exe 1,960 K 5,356 K 2132 Host Process for Windows Services Microsoft Corporation

svchost.exe < 0.01 84,752 K 86,792 K 2176 Host Process for Windows Services Microsoft Corporation

svchost.exe 9,428 K 16,156 K 2184 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,332 K 3,468 K 2236 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,980 K 6,380 K 2376 Host Process for Windows Services Microsoft Corporation

svchost.exe 3,380 K 6,128 K 2388 Host Process for Windows Services Microsoft Corporation

svchost.exe < 0.01 5,360 K 10,644 K 2416 Host Process for Windows Services Microsoft Corporation

igfxCUIService.exe 2,208 K 6,272 K 2464 igfxCUIService Module Intel Corporation

svchost.exe 4,092 K 8,224 K 2520 Host Process for Windows Services Microsoft Corporation

dasHost.exe		3,532 K	9,932 K	5088	
svchost.exe		2,200 K	6,216 K	2556	Host Process for Windows Services Microsoft Corporation
svchost.exe		1,836 K	5,460 K	2568	Host Process for Windows Services Microsoft Corporation
svchost.exe		3,188 K	6,964 K	2644	Host Process for Windows Services Microsoft Corporation
svchost.exe		3,484 K	12,136 K	2684	Host Process for Windows Services Microsoft Corporation
svchost.exe	< 0.01	12,132 K	16,708 K	2796	Host Process for Windows Services Microsoft Corporation
svchost.exe		2,376 K	7,612 K	2888	Host Process for Windows Services Microsoft Corporation
svchost.exe		1,852 K	5,140 K	2972	Host Process for Windows Services Microsoft Corporation
svchost.exe		4,472 K	11,940 K	2704	Host Process for Windows Services Microsoft Corporation
svchost.exe		1,680 K	4,144 K	3076	Host Process for Windows Services Microsoft Corporation
svchost.exe		2,820 K	7,184 K	3096	Host Process for Windows Services Microsoft Corporation
svchost.exe		7,420 K	16,616 K	3236	Host Process for Windows Services Microsoft Corporation
svchost.exe		3,096 K	11,616 K	3328	Host Process for Windows Services Microsoft Corporation
spoolsv.exe		5,580 K	9,572 K	3492	Spooler SubSystem App Microsoft Corporation
svchost.exe		3,624 K	11,364 K	3528	Host Process for Windows Services Microsoft Corporation
svchost.exe		12,316 K	17,848 K	3560	Host Process for Windows Services Microsoft Corporation
svchost.exe		2,024 K	4,940 K	3604	Host Process for Windows Services Microsoft Corporation
AdobeUpdateService.exe	< 0.01	1,488 K	5,848 K	3808	Adobe Update Service Adobe Inc.

svchost.exe 5,772 K 14,640 K 3820 Host Process for Windows Services Microsoft Corporation

svchost.exe 19,584 K 34,508 K 3828 Host Process for Windows Services Microsoft Corporation

fpCSEvtSvc.exe 6,392 K 5,180 K 3836

svchost.exe 28,860 K 37,732 K 3852 Host Process for Windows Services Microsoft Corporation

svchost.exe 3,680 K 10,124 K 3880 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,580 K 3,432 K 3948 Host Process for Windows Services Microsoft Corporation

SebWindowsServiceWCF.exe 15,880 K 22,652 K 3956 SEB Windows Service with WCF ETH Zurich

svchost.exe 2,012 K 5,572 K 3988 Host Process for Windows Services Microsoft Corporation

SynTPEnhService.exe 1,184 K 3,520 K 3996 64-bit Synaptics Pointing Enhance Service Synaptics Incorporated

SynTPEnh.exe 1.79 7,228 K 22,832 K 12792 Synaptics TouchPad 64-bit Enhancements Synaptics Incorporated

svchost.exe 2,288 K 6,084 K 4008 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,324 K 3,436 K 4056 Host Process for Windows Services Microsoft Corporation

vmware-authd.exe 3,696 K 8,420 K 4064 VMware Authorization Service VMware, Inc.

vmnetdhcp.exe < 0.01 7,752 K 4,080 K 4072 VMware VMnet DHCP service VMware, Inc.

valWBFPolicyService.exe 1,340 K 2,304 K 4088 SynapticsWBF Policy Service (COGENT) Synaptics Incorporated

vmware-usbarbitrator64.exe < 0.01 3,504 K 7,564 K 3164 VMware USB Arbitration Service VMware, Inc.

vmnat.exe < 0.01 2,480 K 6,332 K 4104 VMware NAT Service VMware, Inc.

MsMpEng.exe 0.60 257,816 K 194,444 K 4200 Antimalware Service Executable Microsoft Corporation

MpCopyAccelerator.exe 2,204 K 3,652 K 10064

svchost.exe 4,904 K 19,708 K 4212 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,600 K 3,496 K 4332 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,792 K 5,424 K 4620 Host Process for Windows Services Microsoft Corporation

AGMService.exe 3,948 K 10,444 K 4648 Adobe Genuine Software Service Adobe Systems, Incorporated

AGSService.exe 5,572 K 14,528 K 4656 Adobe Genuine Software Integrity Service Adobe Systems, Incorporated

OfficeClickToRun.exe < 0.01 41,228 K 36,448 K 4740 Microsoft Office Click-to-Run (SxS) Microsoft Corporation

httpd.exe 10,292 K 12,232 K 5020 Apache HTTP Server Apache Software Foundation

httpd.exe < 0.01 17,564 K 12,724 K 8132

svchost.exe 2,460 K 5,324 K 3984 Host Process for Windows Services Microsoft Corporation

svchost.exe < 0.01 3,376 K 9,132 K 5368 Host Process for Windows Services Microsoft Corporation

mysqld.exe < 0.01 211,000 K 19,900 K 5612

svchost.exe 4,456 K 14,968 K 3412 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,784 K 5,244 K 1916 Host Process for Windows Services Microsoft Corporation

ctfmon.exe 7,648 K 18,604 K 11832

svchost.exe 5,992 K 19,080 K 6344 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,808 K 6,644 K 5832 Host Process for Windows Services Microsoft Corporation

SearchIndexer.exe 43,376 K 55,192 K 7368 Microsoft Windows Search Indexer Microsoft Corporation

SearchProtocolHost.exe 2,404 K 7,996 K 7808

SearchFilterHost.exe 1,724 K 6,592 K 12184

svchost.exe 2,136 K 7,836 K 2604 Host Process for Windows Services Microsoft Corporation

SecurityHealthService.exe 5,112 K 14,724 K 5640 Windows Security Health Service Microsoft Corporation

NisSrv.exe 6,220 K 8,500 K 5532 Microsoft Network Realtime Inspection Service Microsoft Corporation

svchost.exe 5,004 K 8,448 K 6168 Host Process for Windows Services Microsoft Corporation

SgrmBroker.exe 3,640 K 5,364 K 3500 System Guard Runtime Monitor Broker Service Microsoft Corporation

svchost.exe 1,164 K 3,288 K 7820 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,312 K 7,448 K 2396 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,700 K 8,172 K 4276 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,588 K 6,660 K 6816 Host Process for Windows Services Microsoft Corporation

svchost.exe 6,424 K 21,960 K 6020 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,392 K 6,024 K 8480 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,568 K 4,020 K 6464 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,836 K 6,988 K 8816 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,428 K 8,888 K 8784 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,320 K 7,216 K 9552 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,352 K 5,540 K 9056 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,356 K 5,416 K 11864 Host Process for Windows Services Microsoft Corporation

svchost.exe < 0.01 9,300 K 32,632 K 11508 Host Process for Windows Services Microsoft Corporation

svchost.exe < 0.01 8,408 K 33,748 K 7760 Host Process for Windows Services Microsoft Corporation

svchost.exe 3,656 K 21,892 K 11032 Host Process for Windows Services Microsoft Corporation

svchost.exe 5,256 K 22,000 K 4360 Host Process for Windows Services Microsoft Corporation

svchost.exe < 0.01 2,880 K 11,376 K 8892 Host Process for Windows Services Microsoft Corporation

svchost.exe 2,524 K 7,288 K 5540 Host Process for Windows Services Microsoft Corporation

svchost.exe 3,716 K 11,356 K 10496 Host Process for Windows Services Microsoft Corporation

svchost.exe 1,368 K 5,660 K 9388 Host Process for Windows Services Microsoft Corporation

lsass.exe < 0.01 7,592 K 16,408 K 760 Local Security Authority Process Microsoft Corporation

fontdrvhost.exe 1,572 K 1,212 K 904

GoogleCrashHandler.exe 1,832 K 140 K 7328

GoogleCrashHandler64.exe 1,884 K 124 K 8000

csrss.exe 0.60 2,268 K 5,688 K 7784

winlogon.exe 2,500 K 9,588 K 2272

fontdrvhost.exe 4,012 K 8,164 K 1616

dwm.exe 0.60 56,452 K 85,240 K 6584

explorer.exe 0.60 75,504 K 150,880 K 1400 Windows Explorer Microsoft Corporation

SecurityHealthSystray.exe 1,708 K 8,492 K 2172 Windows Security notification icon Microsoft Corporation

softinfo.exe < 0.01 6,620 K 20,636 K 11564 Software Informer Informer Technologies, Inc.

AcroRd32.exe < 0.01 78,136 K 96,004 K 11988 Adobe Reader 9.0 Adobe Systems Incorporated

chrome.exe	< 0.01	111,812 K	194,192 K	7264	Google Chrome	Google LLC
chrome.exe		2,144 K	6,872 K	9644	Google Chrome	Google LLC
chrome.exe		56,292 K	73,272 K	12404	Google Chrome	Google LLC
chrome.exe		22,876 K	45,884 K	11764	Google Chrome	Google LLC
chrome.exe		8,044 K	18,332 K	8476	Google Chrome	Google LLC
chrome.exe	< 0.01	51,328 K	97,336 K	11468	Google Chrome	Google LLC
chrome.exe	< 0.01	25,048 K	55,636 K	9708	Google Chrome	Google LLC
chrome.exe		13,860 K	27,164 K	11120	Google Chrome	Google LLC
WinRAR.exe	< 0.01	18,808 K	57,140 K	8996	WinRAR archiver	Alexander Roshal
procexp64.exe	9.52	77,176 K	103,108 K	10540	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com
SnippingTool.exe		17,952 K	54,580 K	2540	Snipping Tool	Microsoft Corporation
SynTPHelper.exe		1,060 K	4,584 K	13168		
igfxHK.exe		2,368 K	9,032 K	3224	igfxHK Module	Intel Corporation
igfxTray.exe		3,024 K	11,276 K	6808		
CCXProcess.exe		580 K	2,212 K	9812	CCXProcess	Adobe Systems Incorporated
node.exe		49,200 K	74,212 K	6200	Node.js: Server-side JavaScript	Node.js
conhost.exe		6,516 K	10,884 K	2156	Console Window Host	Microsoft Corporation
AdobeIPCBroker.exe		2,880 K	10,828 K	9136	Adobe IPC Broker	Adobe Inc

Process: RuntimeBroker.exe Pid: 11540

Type	Name
ALPC Port	\RPC Control\OLE7BF43BA1DAFF012A1C03ED4CA989
ALPC Port	\BaseNamedObjects\[CoreUI]-PID(11540)-TID(12212) 317aca20-d767-4489-9d3d-6e524be11b2b
Desktop	\Default
Directory	\KnownDlls

Directory \Sessions\4\BaseNamedObjects

Event \KernelObjects\MaximumCommitCondition

Event \BaseNamedObjects\TermSrvReadyEvent

File C:\Windows\System32

File \Device\CNG

File \Device\KsecDD

File \Device\KsecDD

File \Device\DeviceApi

File C:\Windows\System32\en-US\KernelBase.dll.mui

File \Device\KsecDD

File \Device\KsecDD

File \Device\DeviceApi

File \Device\Nsi

File \Device\DeviceApi

File C:\Windows\System32\en-US\propsys.dll.mui

File C:\Windows\System32\en-US\StartTileData.dll.mui

File C:\Windows\System32\en-US\shell32.dll.mui

File \Device\KsecDD

File C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.267_none_e6c5adbd130e444d

File C:\Windows\SystemResources\imageres.dll.mun

File C:\Windows\System32\en-US\AppResolver.dll.mui

Key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Key HKLM\SYSTEM\ControlSet001\Control\Session Manager

Key HKCR

Key HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions

Key HKLM

Key HKLM\SOFTWARE\Microsoft\Ole

Key HKCU\Software\Classes\Local Settings

Key HKCR

Key HKLM\SOFTWARE\Microsoft\WindowsRuntime

Key HKLM\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId

Key HKLM\SOFTWARE\Microsoft\WindowsRuntime\Server

Key HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters

Key HKCU\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager

Key HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

Key HKU

Key HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids

Key HKCU

Key HKCU\Software\Microsoft\Windows\CurrentVersion\Mobility

Key HKLM\SYSTEM\ControlSet001\Control\Terminal Server

Key HKCU\Software\Microsoft\Windows\CurrentVersion\Holographic

Key HKCU\Software\Microsoft\Input\EC

Key HKCU\Software\Microsoft\Windows\CurrentVersion\CDP

Key HKLM

Key HKCU\Software\Microsoft\Windows\CurrentVersion\Lock Screen

Key HKLM\SYSTEM\ControlSet001\Control\NetworkUxManager

Key HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9

Key HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5

Key HKCU\Software\Classes\Local Settings\Software\Microsoft

Key HKCU\Software\Classes

Key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\PropertyBag

Key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PropertyBag

Key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\PropertyBag

Key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\PropertyBag

Key HKCR\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance

Key HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer

Key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager

Key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\PropertyBag

Key HKCR\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance

Key HKCR\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance

Key HKCR\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\Open

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\OpenFileLocation

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\OpenFileLocation

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\Open

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\Open

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\OpenNewWindow

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\OpenFileLocation

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\OpenNewWindow

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\OpenNewWindow

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\RunAs

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\RunAs

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\RunAs

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\RunAsUser

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\RunAsUser

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\RunAsUser

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\Uninstall

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\Uninstall

Key HKCR\Launcher.AllAppsDesktopApplication

Key HKCR\Launcher.AllAppsDesktopApplication\Shell\Uninstall

Mutant \Sessions\4\BaseNamedObjects\SM0:11540:304:WilStaging_02

Mutant \Sessions\4\BaseNamedObjects\SM0:11540:120:WilError_02

Section \Sessions\4\BaseNamedObjects\windows_shell_global_counters

Section \BaseNamedObjects__ComCatalogCache__

Section \BaseNamedObjects__ComCatalogCache__

Section \Windows\Theme3098080658

Section \Sessions\4\Windows\Theme4146189822

Section \BaseNamedObjects\windows_shell_global_counters

Section \Sessions\4\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x000000000000009d.db

Section \Sessions\4\BaseNamedObjects\C:*Users*user*AppData*Local*Microsoft*Windows*Caches*cversions.3.ro

Section \Sessions\4\BaseNamedObjects\C:*Users*user*AppData*Local*Microsoft*Windows*Caches*{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000350.db

Section \Sessions\4\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro

Section \Sessions\4\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro

Section \Sessions\4\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000001.db

Section \Sessions\4\BaseNamedObjects\C:*Users*user*AppData*Local*Microsoft*Windows*Caches*cversions.3.ro

Section \Sessions\4\BaseNamedObjects\C:*Users*user*AppData*Local*Microsoft*Windows*Caches*cversions.3.ro

Section \Sessions\4\BaseNamedObjects\C:*Users*user*AppData*Local*Microsoft*Windows*Caches*cversions.3.ro

Section \Sessions\4\BaseNamedObjects\C:*Users*user*AppData*Local*Microsoft*Windows*Caches*{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000350.db

Semaphore \Sessions\4\BaseNamedObjects\SM0:11540:304:WilStaging_02_p0

Semaphore \Sessions\4\BaseNamedObjects\SM0:11540:304:WilStaging_02_p0h

Semaphore \Sessions\4\BaseNamedObjects\SM0:11540:120:WilError_02_p0

Semaphore \Sessions\4\BaseNamedObjects\SM0:11540:120:WilError_02_p0h

Thread RuntimeBroker.exe(11540): 8280

Thread RuntimeBroker.exe(11540): 9576

Thread RuntimeBroker.exe(11540): 9576

Thread RuntimeBroker.exe(11540): 12212

Thread RuntimeBroker.exe(11540): 13160

Thread RuntimeBroker.exe(11540): 10788

Thread RuntimeBroker.exe(11540): 12212

Thread RuntimeBroker.exe(11540): 10788

Thread RuntimeBroker.exe(11540): 10728

Thread RuntimeBroker.exe(11540): 10728

Thread RuntimeBroker.exe(11540): 9576

Thread RuntimeBroker.exe(11540): 12212

Thread RuntimeBroker.exe(11540): 7364

Thread RuntimeBroker.exe(11540): 1100

Thread RuntimeBroker.exe(11540): 12564

Thread RuntimeBroker.exe(11540): 2900

Thread RuntimeBroker.exe(11540): 7364

Thread RuntimeBroker.exe(11540): 12932

Thread RuntimeBroker.exe(11540): 12564

Thread RuntimeBroker.exe(11540): 2208

Thread RuntimeBroker.exe(11540): 12932

Thread RuntimeBroker.exe(11540): 6352

Thread RuntimeBroker.exe(11540): 12656

Thread RuntimeBroker.exe(11540): 13160

Thread RuntimeBroker.exe(11540): 11816

WindowStation \Sessions\4\Windows\WindowStations\WinSta0

WindowStation \Sessions\4\Windows\WindowStations\WinSta0