

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 4, Task ID: 16

Task ID:	16
Risk Level:	3
Date Processed:	2016-03-29 03:27:45 (UTC)
Processing Time:	62.23 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\test12.jar.exe"
Sample ID:	4
Type:	basic
Owner:	admin
Label:	test12.jar
Date Added:	2016-03-29 03:27:44 (UTC)
File Type:	archive:jar:applet
File Size:	6213 bytes
MD5:	0fa3c06281d3b260bfccbb5a22dd74c5
SHA256:	1b7e0322a81be961ebce33aeb395124544cfb01a3ab54f23cf64400fb2b04c7
Description:	None

Pattern Matching Results

- 1 YARA score 1
- 2 ZIP archive format
- 3 Long sleep detected

Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable

Process/Thread Events

Creates process: C:\Program Files (x86)\Internet Explorer\iexplore.exe ["C:\Program Files (x86)\Internet Explorer\iexplore.exe" c:\windows\temp\test12.jar.html]
Creates process: C:\Program Files (x86)\Internet Explorer\iexplore.exe ["C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:2204 CREDAT:14337]
Creates process: C:\Program Files (x86)\Java\jre7\bin\jp2launcher.exe ["C:\Program Files (x86)\Java\jre7\bin\jp2launcher.exe" "C:\Program Files (x86)\Java\jre7" -D__jvm_launched=11365922646 -D__applet_launched=11365829866 -Xbootclasspath/a:C:\PROGRA~2\Java\jre7\lib\deploy.jar;C:\PROGRA~2\Java\jre7\lib\javaws.jar;C:\PROGRA~2\Java\jre7\lib\plugin.jar -Djava.class.path=C:\PROGRA~2\Java\jre7\classes -Dsun.awt.warmup=true --- -- sun.plugin2.main.client.PluginMain
write_pipe_name=jpi2_pid2300_pipe3,read_pipe_name=jpi2_pid2300_pipe2]
Creates process: C:\Program Files (x86)\Java\jre7\bin\java.exe ["C:\Program Files (x86)\Java\jre7\bin\java.exe" -D__jvm_launched=11365922646 -D__applet_launched=11365829866 "-Xbootclasspath/a:C:\PROGRA~2\Java\jre7\lib\deploy.jar;C:\PROGRA~2\Java\jre7\lib\javaws.jar;C:\PROGRA~2\Java\jre7\lib\plugin.jar" -Djava.class.path=C:\PROGRA~2\Java\jre7\classes" -Dsun.awt.warmup=true
sun.plugin2.main.client.PluginMain
write_pipe_name=jpi2_pid2300_pipe3,read_pipe_name=jpi2_pid2300_pipe2]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \Sessions\1\BaseNamedObjects\!MSFTHISTORY!
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!roaming!microsoft!windows!cookies!
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!history!history.ie5!
Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex: \Sessions\1\BaseNamedObjects\!BrowserEmulation!SharedMemory!Mutex
Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex: \Sessions\1\BaseNamedObjects\ConnHashTable<2204>_HashTable_Mutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates mutex: \Sessions\1\BaseNamedObjects\RSS Eventing Connection Database Mutex
0000089c
Creates mutex: \Sessions\1\BaseNamedObjects\Feed Eventing Shared Memory Mutex S-1-5-21-980053277-1733835069-2361817685-1001
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!feeds cache!
Creates mutex: \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex
Creates mutex: \Sessions\1\BaseNamedObjects\!SHMSFTHISTORY!
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!history!history.ie5!mshist012016032920160330!
Creates mutex: \Sessions\1\BaseNamedObjects\Feed Arbitration Shared Memory Mutex [User : S-1-5-21-980053277-1733835069-2361817685-1001]
Creates mutex: \Sessions\1\BaseNamedObjects\Feeds Store Mutex S-1-5-21-980053277-1733835069-2361817685-1001

Creates mutex: \Sessions\1\BaseNamedObjects__DDrawExclMode__
Creates mutex: \Sessions\1\BaseNamedObjects__DDrawCheckExclMode__
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (3F2112F3-
F55E-11E5-A3B1-080027B54693, 0)
Creates event: \BaseNamedObjects\SvcctlStartEvent_A3752DX
Creates event: \KernelObjects\MaximumCommitCondition
Creates event: \Sessions\1\BaseNamedObjects\0leDfRoot10149AB466B362D2
Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfcActivated.Default1
Creates event: \Sessions\1\BaseNamedObjects\0leDfRoot3215AE54820F0745
Creates event: \Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (3F2112F6-
F55E-11E5-A3B1-080027B54693, 0)
Creates event: \Sessions\1\BaseNamedObjects\RSS Eventing Event Event 0000089c
Creates event: \Sessions\1\BaseNamedObjects\IEFrame.EventCheckDefaultBrowser
Creates event: \Sessions\1\BaseNamedObjects\Feed Arbitration Lock Event [Process :
0x0000089c]
Creates event: \Sessions\1\BaseNamedObjects\Feed Arbitration Unlock Event [Process :
0x0000089c]
Creates event: \Sessions\1\BaseNamedObjects\0leDfRoot4FA2CD13BAC57191
Creates event: \Sessions\1\BaseNamedObjects\0leDfRoot6EA07F5C68573DFA
Creates event: \Sessions\1\BaseNamedObjects\0leDfRootB763631932A33D7A
Creates event: \Sessions\1\BaseNamedObjects\jpi2_pid2300_evt1
Creates event: \BaseNamedObjects\ConsoleEvent-0x00000000000009A4
Creates semaphore: \Sessions\1\BaseNamedObjects\IEFrame!GetAsyncKeyStateQuery!2204
Creates semaphore: \Sessions\1\BaseNamedObjects\IEFrame!GetAsyncKeyStateReply!2204

File System Events

Creates: C:\Users\Admin
Creates: C:\Users\Admin\AppData\Local
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates: C:\Users\Admin\AppData\Roaming
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates: C:\Users\Admin\Favorites
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacyIE
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Creates: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active\RecoveryStore.{3F2112F4-F55E-11E5-A3B1-080027B54693}.dat
Creates: C:\Users\Admin\AppData\Local\Temp\~DF4DF6756F691A8420.TMP
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
Creates: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active\{3F2112F5-F55E-11E5-A3B1-080027B54693}.dat
Creates: C:\Users\Admin\AppData\Local\Temp\~DF632967B28F9467CB.TMP
Creates: C:\Users\Admin\AppData\Local\Microsoft\Feeds
Creates: C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-
666AE6A92D3D}~WebSlices~
Creates: C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin
Creates: C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin\2300
Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016032920160330
Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016032920160330\index.dat
Creates: C:\Users\Admin\AppData\Local\Temp\~DFCCD0A6379E4D73A9.TMP
Creates: C:\Users\Admin\AppData\Local\Temp\~DFFE5A462C66AC3470.TMP
Creates: C:\Users\Admin\AppData\Local\Temp\~DFE5E3236B0CCE91A8A.TMP
Creates: C:\Users\Admin\AppData\Local\Temp\~DF7C53F95ED24A3051.TMP
Creates: C:\Users\Admin\AppData\Local\Temp\~DFB48F54514097C1F3.TMP
Creates: C:\Users\Admin\AppData\Local\Temp\~DFB834F245E303C31D.TMP
Creates: C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin\2460
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\0
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\1
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\2
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\3
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\4
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\5
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\6
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\7
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\8
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\9
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\10
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\11
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\12
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\13
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\14
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\15
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\16
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\17
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\18
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\19
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\20
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\21
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\22
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\23
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\24
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\25
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\26
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\27
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\28
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\29
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\30

Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\31
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\32
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\33
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\34
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\35
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\36
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\37
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\38
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\39
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\40
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\41
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\42
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\43
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\44
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\45
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\46
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\47
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\48
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\49
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\50
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\51
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\52
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\53
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\54
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\55
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\56
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\57
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\58
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\59
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\60
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\61
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\62
Creates: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\63
Opens: C:\Windows\Prefetch\IEXPLORE.EXE-4B6C9213.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Program Files (x86)\Internet Explorer\en-US\iexplore.exe.mui
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Program Files (x86)\Internet Explorer\IEFRAME.dll
Opens: C:\Windows\SysWOW64\ieframe.dll
Opens: C:\Program Files (x86)\Internet Explorer\OLEACC.dll
Opens: C:\Windows\SysWOW64\oleacc.dll
Opens: C:\Program Files (x86)\Internet Explorer\OLEACCRC.DLL
Opens: C:\Windows\SysWOW64\oleaccrc.dll
Opens: C:\Program Files (x86)\Internet Explorer\iexplore.exe.Local
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\wininet.dll
Opens: C:\Program Files (x86)\Internet Explorer\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\Desktop.ini
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\Desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
Opens: C:\Program Files (x86)\Internet Explorer\ntmarta.dll
Opens: C:\Windows\SysWOW64\ntmarta.dll
Opens: C:\Program Files (x86)\Internet Explorer\dnsapi.DLL
Opens: C:\Windows\SysWOW64\dnsapi.dll
Opens: C:\Program Files (x86)\Internet Explorer\iphlpapi.DLL
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens: C:\Program Files (x86)\Internet Explorer\WINNSI.DLL
Opens: C:\Windows\SysWOW64\winnsi.dll
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Program Files (x86)
Opens: C:\Program Files (x86)\Internet Explorer\sqmapi.dll

Opens: C:\Program Files (x86)\Internet Explorer\RpcRtRemote.dll
Opens: C:\Windows\SysWOW64\RpcRtRemote.dll
Opens: C:\Program Files (x86)\Internet Explorer\dwmmapi.dll
Opens: C:\Windows\SysWOW64\dwmmapi.dll
Opens: C:\Users\Admin\Desktop
Opens: C:\Program Files (x86)\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
Opens: C:\Program Files (x86)\Common Files
Opens: C:\Program Files (x86)\Common Files\Adobe
Opens: C:\Program Files (x86)\Common Files\Adobe\Acrobat
Opens: C:\Program Files (x86)\Java\jre7\bin\jp2ssv.dll
Opens: C:\Program Files (x86)\Java
Opens: C:\Program Files (x86)\Java\jre7
Opens: C:\Program Files (x86)\Java\jre7\bin
Opens: C:\Users\Admin\Favorites
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Local\Microsoft
Opens: C:\Users\Admin\AppData
Opens: C:\Users
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Roaming\Microsoft
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low
Opens: C:\Users\Admin\AppData\Local\Temp\Low
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Program Files (x86)\Internet Explorer\RASAPI32.dll
Opens: C:\Windows\SysWOW64\rasapi32.dll
Opens: C:\Program Files (x86)\Internet Explorer\rasman.dll
Opens: C:\Windows\SysWOW64\rasman.dll
Opens: C:\Program Files (x86)\Internet Explorer\rtutils.dll
Opens: C:\Windows\SysWOW64\rtutils.dll
Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\
Opens: C:\Windows\SysWOW64\ras
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
Opens: C:\Program Files (x86)\Internet Explorer\sensapi.dll
Opens: C:\Windows\SysWOW64\SensApi.dll
Opens: C:\Windows\SysWOW64\nlaapi.dll
Opens: C:\Program Files (x86)\Internet Explorer\rasadhlp.dll
Opens: C:\Windows\SysWOW64\rasadhlp.dll
Opens: C:\Windows\SysWOW64\en-US\ieframe.dll.mui
Opens: C:\Program Files (x86)\Internet Explorer\IEUI.dll
Opens: C:\Windows\SysWOW64\ieui.dll
Opens: C:\Program Files (x86)\Internet Explorer\MSIMG32.dll
Opens: C:\Windows\SysWOW64\msimg32.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active
Opens: C:\Program Files (x86)\Internet Explorer\CRYPTSP.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\Program Files (x86)\Internet Explorer\ieproxy.dll
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens: C:\
Opens: C:\Windows\Temp
Opens: C:\Windows\SysWOW64\url.dll
Opens: C:\Program Files (x86)\Internet Explorer\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\Windows\SysWOW64\en-US\urlmon.dll.mui
Opens: C:\Users\Admin\Favorites\Links
Opens: C:\Windows\SysWOW64\xmlite.dll
Opens: C:\Windows\SysWOW64\propsys.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000001.db
Opens: C:\Users\desktop.ini
Opens: C:\Users\Admin\Favorites\desktop.ini
Opens: C:\Users\Admin\Desktop\desktop.ini
Opens: C:\Windows\SysWOW64\ExplorerFrame.dll
Opens: C:\Windows\SysWOW64\duser.dll
Opens: C:\Windows\SysWOW64\dui70.dll
Opens: C:\Users\Admin\Favorites\Links\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\frameiconcache.dat
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Program Files (x86)\Internet Explorer\iexplore.exe
Opens: C:\Program Files (x86)\Internet Explorer\en\iexplore.exe.mui
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Program Files (x86)\Internet Explorer\msfeeds.dll
Opens: C:\Windows\SysWOW64\msfeeds.dll

Opens: C:\Program Files (x86)\Internet Explorer\IEShims.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}\WebSlices~
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~
Opens: C:\Users\Admin\Favorites\Links\Suggested Sites.url
Opens: C:\Program Files (x86)\Internet Explorer\MLANG.dll
Opens: C:\Windows\SysWOW64\mlang.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\VB8EH8F1\favicon[1].ico
Opens: C:\Users\Admin\Favorites\Links\Web Slice Gallery.url
Opens: C:\Program Files (x86)\Internet Explorer\url.dll
Opens: C:\url.dll
Opens: C:\Program Files (x86)\Internet Explorer\apphelp.dll
Opens: C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
Opens: C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
Opens: C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcpr80.dll
Opens: C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\msvcr100.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\java.exe
Opens: C:\Program Files (x86)\Java\jre7\bin\client\jvm.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\server\jvm.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\index.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\desktop.ini
Opens: C:\Program Files (x86)\Internet Explorer\SXS.DLL
Opens: C:\Windows\SysWOW64\sxs.dll
Opens: C:\Windows\Temp\test12.jar.html
Opens: C:\Windows\Temp\test12.jar.html:Zone.Identifier
Opens: C:\Windows\SysWOW64\mshtml.dll
Opens: C:\Windows\SysWOW64\msls31.dll
Opens: C:\Windows\SysWOW64\stdole2.tlb
Opens: C:\Windows\SysWOW64\msimtf.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\jp2iexp.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\client
Opens: C:\Windows\SysWOW64\tzres.dll
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens: C:\Program Files (x86)\Internet Explorer\WSOCK32.dll
Opens: C:\Windows\SysWOW64\wsck32.dll
Opens: C:\Program Files (x86)\Internet Explorer\WINMM.dll
Opens: C:\Windows\SysWOW64\winmm.dll
Opens: C:\Windows\System32\propsys.dll
Opens: C:\Windows\SysWOW64\en-US\propsys.dll.mui
Opens: C:\Program Files (x86)\Java\jre7\bin\verify.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\java.dll
Opens: C:\hotspotrc
Opens: C:\PROGRA-2\Java\jre7\lib\endorsed
Opens: C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin
Opens: C:\Windows\Fonts\times.ttf
Opens: C:\Program Files (x86)\Java\jre7\bin\zip.dll
Opens: C:\Program Files (x86)\Java\jre7\lib
Opens: C:\Program Files (x86)\Java\jre7\lib\meta-index
Opens: C:\Windows\SysWOW64\en-US\mshtml.dll.mui
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016032920160330\
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016032920160330
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016032920160330\index.dat
Opens: C:\Program Files (x86)\Java\jre7\bin\client\classes.jsa
Opens: C:\Windows\SysWOW64\en-US\shell32.dll.mui
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico
Opens: C:\Program Files (x86)\Java\jre7\lib\rt.jar
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}\WebSlices~\Suggested Sites~.feed-ms
Opens: C:\Windows\SysWOW64\msxml3.dll
Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens: C:\Windows\SysWOW64\msxml3r.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds\FeedsStore.feed-sdb-ms
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}\WebSlices~\Web Slice Gallery~.feed-ms
Opens: C:\Program Files (x86)\Java\jre7\lib\deploy.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\javaws.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\plugin.jar
Opens: C:\hotspot_compiler
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\meta-index
Opens: C:\Program Files (x86)\Java\jre7\lib\ext
Opens: C:\Windows\Sun\Java\lib\ext\meta-index
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\dnsns.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\localedata.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunec.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunjs_provider.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunmscapi.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunpkcs11.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\zipfs.jar
Opens: C:\Windows\Sun\Java\lib\ext

Opens: C:\PROGRA~2\Java\jre7\lib\management\usagetracker.properties
 Opens: C:\Program Files (x86)\Java\jre7\bin\deploy.dll
 Opens: C:\PROGRA~2\Java\jre7\lib\bin\jp2native.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\jp2native.dll
 Opens: C:\PROGRA~2\Java\jre7\lib\bin\deploy.dll
 Opens: C:\Users\Admin\AppData\LocalLow
 Opens: C:\Windows\Sun\Java\Deployment\deployment.config
 Opens: C:\Program Files (x86)\Java\jre7\lib\deployment.config
 Opens: C:\PROGRA~2\Java\jre7\lib\deployment.config
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\deployment.properties
 Opens: C:\Program Files (x86)\Java\jre7\bin\net.dll
 Opens: C:\Windows\SysWOW64\mswsock.dll
 Opens: C:\Windows\SysWOW64\wsip6.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\nio.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\javaw.exe
 Opens: C:\Program Files (x86)\Java\jre7\lib\security\java.security
 Opens: C:\Windows\Sun\Java\Deployment\lib\trusted
 Opens: C:\Program Files (x86)\Java\jre7\bin\jp2launcher.exe
 Opens: C:\Windows\AppPatch\sysmain.sdb
 Opens: C:\Windows\Prefetch\JP2LAUNCHER.EXE-6240744E.pf
 Opens: C:\Windows\AppPatch\AcLayers.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\USERENV.dll
 Opens: C:\Windows\SysWOW64\userenv.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\profapi.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\WINSPOOL.DRV
 Opens: C:\Windows\SysWOW64\winspool.drv
 Opens: C:\Program Files (x86)\Java\jre7\bin\MPR.dll
 Opens: C:\Windows\SysWOW64\mpr.dll
 Opens: C:\Program
 Opens: C:\Program.exe
 Opens: C:\Program Files
 Opens: C:\Program Files (x86)\Java\jre7\bin\ui\SwDRM.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\jpishare.dll
 Opens: C:\bin\launch.exe
 Opens: C:\Windows\Prefetch\JAVA.EXE-07FE5A9A.pf
 Opens: C:\Program Files (x86)\Java\jre7\bin\java.exe.Local\
 Opens: C:\Program Files (x86)\Java\jre7\lib\i386\jvm.cfg
 Opens: C:\Program Files (x86)\Java\jre7\bin\WSOCK32.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\WINMM.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\awt.dll
 Opens: C:\Program Files (x86)\Java\jre7\lib\endorsed
 Opens: C:\Windows\SysWOW64\d3d9.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\VERSION.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\d3d8thk.dll
 Opens: C:\Windows\SysWOW64\d3d8thk.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\dwmapi.dll
 Opens: C:\Program Files (x86)\Java\jre7\classes
 Opens: C:\Program Files (x86)\Java\jre7\lib\management\usagetracker.properties
 Opens: C:\Windows\System32\vga.dll
 Opens: C:\Windows\System32\vga256.dll
 Opens: C:\Windows\System32\vga64k.dll
 Opens: C:\Program Files (x86)\Java\jre7\bin\vga.dll
 Opens: C:\Program Files (x86)\Java\jre7\lib\resources.jar
 Opens: C:\Program Files (x86)\Java\jre7\lib\sunrsasn.jar
 Opens: C:\Program Files (x86)\Java\jre7\lib\jsse.jar
 Opens: C:\Program Files (x86)\Java\jre7\lib\jce.jar
 Opens: C:\Program Files (x86)\Java\jre7\lib\charsets.jar
 Opens: C:\Program Files (x86)\Java\jre7\meta-index
 Opens: C:\Program Files (x86)\Java\jre7\lib\net.properties
 Opens: C:\Users\Admin\accessibility.properties
 Opens: C:\Program Files (x86)\Java\jre7\lib\accessibility.properties
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment
 Opens: C:\Windows\Sun\Java\Deployment
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\log
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\security
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\ext
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\host
 Opens: C:\Program Files (x86)\Java\jre7\lib\security\java.policy
 Opens: C:\Program Files (x86)\Java\jre7\lib\ext*
 Opens: C:\Windows\Sun
 Opens: C:\Windows\Sun\Java
 Opens: C:\Windows\Sun\Java\lib\ext*
 Opens: C:\-
 Opens: C:\Users\Admin\java.policy
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\security\java.policy
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\muffin
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\tmp
 Opens: C:\Users\Admin\AppData\LocalLow\Sun
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java
 Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache
 Opens: C:\Program Files (x86)\Java\jre7\bin\dnsapi.DLL
 Opens: C:\Program Files (x86)\Java\jre7\bin\iphlpapi.DLL
 Opens: C:\Program Files (x86)\Java\jre7\bin\WINNSI.DLL
 Opens: C:\Program Files (x86)\Java\jre7\lib\management
 Opens: C:\Windows\SysWOW64\user32.dll
 Opens: C:\etc\release
 Opens: C:\Windows\Fonts\courer.fon
 Opens: C:\Windows\Fonts\sserife.fon
 Opens: C:\Windows\Fonts\vgafix.fon
 Opens: C:\Program Files (x86)\Java\jre7\lib\swing.properties

Opens: C:\Program Files (x86)\Java\jre7\lib\fonts
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\LucidaSansRegular.ttf
Opens: C:\Program Files (x86)\Java\jre7\bin\fontmanager.dll
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\badfonts.txt
Opens: C:\Program Files (x86)\Java\jre7\lib\fontconfig.7.properties
Opens: C:\Program Files (x86)\Java\jre7\lib\fontconfig.7.bfc
Opens: C:\Program Files (x86)\Java\jre7\lib\fontconfig.properties
Opens: C:\Program Files (x86)\Java\jre7\lib\fontconfig.bfc
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\fallback
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\COURBI.TTF
Opens: C:\Windows\Fonts
Opens: C:\Windows\Fonts\courbi.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\WINGDING.TTF
Opens: C:\Windows\Fonts\wingding.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\SYMBOL.TTF
Opens: C:\Windows\Fonts\symbol.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\TIMES.TTF
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\TIMESBD.TTF
Opens: C:\Windows\Fonts\timesbd.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\TIMESBI.TTF
Opens: C:\Windows\Fonts\timesbi.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\TIMESI.TTF
Opens: C:\Windows\Fonts\timesi.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\ARIAL.TTF
Opens: C:\Windows\Fonts\arial.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\ARIALBD.TTF
Opens: C:\Windows\Fonts\arialbd.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\ARIALBI.TTF
Opens: C:\Windows\Fonts\arialbi.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\ARIALI.TTF
Opens: C:\Windows\Fonts\ariali.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\COUR.TTF
Opens: C:\Windows\Fonts\cour.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\COURI.TTF
Opens: C:\Windows\Fonts\couri.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\COURBD.TTF
Opens: C:\Windows\Fonts\courbd.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\SIMSUN.TTC
Opens: C:\Windows\Fonts\simsun.ttc
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\SIMSUNB.TTF
Opens: C:\Windows\Fonts\simsunb.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\SIMSUN18030.TTC
Opens: C:\Windows\Fonts\SIMSUN18030.TTC
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\hkscsm3u.ttf
Opens: C:\Windows\Fonts\hkscsm3u.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\MINGLIUB.TTC
Opens: C:\Windows\Fonts\mingliub.ttc
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\sylfaen.ttf
Opens: C:\Windows\Fonts\sylfaen.ttf
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\MINGLIU.TTC
Opens: C:\Windows\Fonts\mingliu.ttc
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\MSMINCHO.TTC
Opens: C:\Windows\Fonts\msmincho.ttc
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\batang.TTC
Opens: C:\Windows\Fonts\batang.ttc
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\MSGOTHIC.TTC
Opens: C:\Windows\Fonts\msgothic.ttc
Opens: C:\Program Files (x86)\Java\jre7\lib\fonts\gulim.TTC
Opens: C:\Windows\Fonts\gulim.ttc
Opens: C:\Program Files (x86)\Java\jre7\lib\applet
Opens: C:\Windows\Sun\Java\Deployment\Lib\Untrusted
Opens: C:\Program Files (x86)\Java\jre7\lib\currency.data
Opens: C:\Program Files (x86)\Java\jre7\lib\currency.properties
Opens: C:\Windows\Temp\test12.jar.exe
Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\security\blacklist
Opens: C:\Program Files (x86)\Java\jre7\lib\security
Opens: C:\Program Files (x86)\Java\jre7\lib\security\blacklist
Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\security\trusted.libraries
Opens: C:\Program Files (x86)\Java\jre7\lib\security\trusted.libraries
Opens: C:\Program Files (x86)\Java\jre7\axbridge\lib
Opens: C:\Program Files (x86)\Java\jre7\bin\vt2k.dll
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active\RecoveryStore.{3F2112F4-F55E-11E5-A3B1-080027B54693}.dat
Writes to: C:\Users\Admin\AppData\Local\Temp\~DF4DF6756F691A8420.TMP
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active\{3F2112F5-F55E-11E5-A3B1-080027B54693}.dat
Writes to: C:\Users\Admin\AppData\Local\Temp\~DF632967B28F9467CB.TMP
Writes to:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016032920160330\index.dat
Reads from: C:\Users\Admin\AppData\Local\Temp\~DF4DF6756F691A8420.TMP
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active\RecoveryStore.{3F2112F4-F55E-11E5-A3B1-080027B54693}.dat
Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Users\desktop.ini
Reads from: C:\Users\Admin\Favorites\desktop.ini
Reads from: C:\Users\Admin\Desktop\desktop.ini
Reads from: C:\Users\Admin\Favorites\Links\desktop.ini
Reads from: C:\Users\Admin\AppData\Local\Temp\~DF632967B28F9467CB.TMP
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active\{3F2112F5-F55E-11E5-A3B1-080027B54693}.dat
Reads from: C:\Program Files (x86)\Internet Explorer\iexplore.exe

```

Reads from:          C:\Users\Admin\Favorites\Links\Suggested Sites.url
Reads from:          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\favicon[1].ico
Reads from:          C:\Users\Admin\Favorites\Links\Web Slice Gallery.url
Reads from:          C:\Program Files (x86)\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
Reads from:          C:\Windows\Temp\test12.jar.html
Reads from:          C:\Windows\SysWOW64\ieframe.dll
Reads from:          C:\Windows\SysWOW64\stdole2.tlb
Reads from:          C:\Program Files (x86)\Java\jre7\lib\meta-index
Reads from:          C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
Reads from:          C:\Program Files (x86)\Java\jre7\bin\client\classes.jsa
Reads from:          C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico
Reads from:          C:\Program Files (x86)\Java\jre7\lib\rt.jar
Reads from:          C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-
666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms
Reads from:          C:\Users\Admin\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms
Reads from:          C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-
666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-ms
Reads from:          C:\Program Files (x86)\Java\jre7\lib\deploy.jar
Reads from:          C:\Program Files (x86)\Java\jre7\lib\javaws.jar
Reads from:          C:\Program Files (x86)\Java\jre7\lib\plugin.jar
Reads from:          C:\Program Files (x86)\Java\jre7\lib\ext\meta-index
Reads from:
C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\deployment.properties
Reads from:          C:\Program Files (x86)\Java\jre7\lib\security\java.security
Reads from:          C:\Program Files (x86)\Java\jre7\bin\java.exe
Reads from:          C:\Program Files (x86)\Java\jre7\lib\jvm.cfg
Reads from:          C:\Program Files (x86)\Java\jre7\lib\net.properties
Reads from:          C:\Program Files (x86)\Java\jre7\lib\security\java.policy
Reads from:          C:\Program Files (x86)\Java\jre7\lib\fontconfig.bfc
Reads from:          C:\Program Files (x86)\Java\jre7\lib\currency.data
Reads from:          C:\Windows\Temp\test12.jar.exe
Reads from:          C:\Program Files (x86)\Java\jre7\lib\security\blacklist
Reads from:          C:\Program Files (x86)\Java\jre7\lib\security\trusted.libraries
Reads from:          C:\Program Files (x86)\Java\jre7\lib\jsse.jar
Reads from:          C:\Windows\Fonts\arial.ttf
Reads from:          C:\Windows\Fonts\wingding.ttf
Reads from:          C:\Windows\Fonts\symbol.ttf

```

Windows Registry Events

```

Creates key:          HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:          HKCU\software\microsoft\windows\currentversion\internet
settings\connections
Creates key:          HKCU\software\microsoft\internet explorer\main
Creates key:          HKCU\software\appdata\low
Creates key:          HKCU\software\microsoft\internet explorer\internetregistry
Creates key:          HKCU\software\microsoft\internet explorer\lowregistry
Creates key:          HKCU\software\microsoft\internet
explorer\lowregistry\dontshowmethisdialagain
Creates key:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
Creates key:          HKCU\software\microsoft\internet explorer\intelliforms
Creates key:          HKCU\software\microsoft\internet explorer\toolbar
Creates key:          HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
Creates key:          HKCU\software\microsoft\internet explorer\pagesetup
Creates key:          HKCU\software\microsoft\windows\currentversion\internet
settings\passport\lowdamap
Creates key:          HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Creates key:          HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
Creates key:          HKCU\software\microsoft\internet explorer\zoom
Creates key:          HKCU\software\microsoft\internet explorer\browseremulation\lowmic
Creates key:          HKCU\software\microsoft\internet explorer\ietyl\lowmic
Creates key:          HKLM\software\wow6432node\microsoft\tracing
Creates key:          HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
Creates key:          HKCU\software\microsoft\internet explorer\recovery\admininactive
Creates key:          HKCU\software\microsoft\internet explorer\main\windowssearch
Creates key:          HKCU\software\microsoft\windows\currentversion\internet settings\zones
Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites\links
Creates key:          HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore
Creates key:          HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}\iexplore
Creates key:          HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
11cf-aaa5-00401c608501}\iexplore
Creates key:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330
Creates key:          HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
Creates key:          HKCU\software\microsoft\internet explorer\linksbar\itemcache\1
Creates key:          HKLM\software\wow6432node\registeredapplications
Creates key:          HKLM\software\registeredapplications
Creates key:          HKCU\software\microsoft\direct3d\mostrecentapplication
Creates key:          HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000
Deletes value:         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]

```


Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
Deletes value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[expiration]
Deletes value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[expiration]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\main\featurecontrol
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enablesafesearchpath_kb963027
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enablesafesearchpath_kb963027
Opens key: HKLM\software\wow6432node\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software\wow6432node
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer\low rights
Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\low rights
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\low rights
Opens key: HKCU\software\policies\microsoft\internet explorer\main
Opens key: HKCU\software\microsoft\internet explorer\main

Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\system
Opens key: HKLM\software\microsoft\windows\currentversion\policies\system
Opens key: HKCU\software\microsoft\internet explorer\setup
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\internet explorer
Opens key: HKLM\software\wow6432node\microsoft\internet explorer
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqlclient\windows
Opens key: HKLM\software\microsoft\sqlclient\windows
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfolderssettings
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore

Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1a677c0f-15708810
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1a677c0f
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKU\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solids_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solids_in_userinfo_kb932562
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\safety\privacie
Opens key: HKLM\software\policies\microsoft\internet explorer\safety\privacie
Opens key: HKCU\software\microsoft\internet explorer\safety\privacie
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\safety\privacie
Opens key: HKCU\software\microsoft\internet explorer\new windows
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\new windows
Opens key: HKCU\software\microsoft\internet explorer\sqm
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\sqm
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
Opens key: HKCU\software\microsoft\internet
explorer\browseremulation\clearablelistdata
Opens key: HKCU\software\microsoft\internet explorer\browseremulation
Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}\propertybag
Opens key: HKLM\software\policies\microsoft\internet explorer\toolbars\restrictions
Opens key: HKCU\software\microsoft\internet explorer\toolbars\restrictions
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\toolbars\restrictions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\extension
compatibility\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\classes\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\treatas
Opens key: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\extension
compatibility\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\treatas
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\toolbar
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\tracing\iexplore_rasapi32
Opens key: HKLM\software\wow6432node\microsoft\tracing\iexplore_rasmancs
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledsessions\
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\wow6432node\microsoft\directui
Opens key: HKCU\software\classes\appid\iexplore.exe
Opens key: HKCR\appid\iexplore.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\software\wow6432node\microsoft\com3
Opens key: HKLM\software\microsoft\com3
Opens key: HKCU\software\classes\wow6432node\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}
Opens key: HKCR\wow6432node\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}
Opens key: HKCU\software\classes\wow6432node\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\treatas
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\progid
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\progid
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{7673b35e-907a-449d-a49f-
e5ce47f0b0b2}
Opens key: HKCR\wow6432node\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}
Opens key: HKCU\software\classes\wow6432node\interface\{7673b35e-907a-449d-a49f-
e5ce47f0b0b2}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{7673b35e-907a-449d-a49f-
e5ce47f0b0b2}\proxystubclsid32
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\tabbedbrowsing
Opens key: HKLM\software\policies\microsoft\internet explorer\tabbedbrowsing
Opens key: HKCU\software\microsoft\internet explorer\tabbedbrowsing
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\tabbedbrowsing
Opens key: HKCU\software\microsoft\internet explorer\main\windowssearch
Opens key: HKLM\software\policies\microsoft\internet explorer\feeds
Opens key: HKCU\software\microsoft\internet explorer\feeds
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\feeds
Opens key: HKLM\software\wow6432node\microsoft\windows search
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0

[illegible]

Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
08002b30309d}\shellfolder
Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}\
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key: HKCU\software\classes\drive\shellex\folderextensions
Opens key: HKCR\drive\shellex\folderextensions
Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\wow6432node\microsoft\windows\shell\registeredapplications\urlassociations\directory\openwithprogids
Opens key: HKCU\software\microsoft\windows\shell\associations\urlassociations\directory
Opens key: HKCU\software\classes\directory
Opens key: HKCR\directory
Opens key: HKCU\software\classes\directory\curver
Opens key: HKCR\directory\curver
Opens key: HKCR\directory\
Opens key: HKCU\software\classes\directory\shellex\iconhandler
Opens key: HKCR\directory\shellex\iconhandler
Opens key: HKCU\software\classes\folder
Opens key: HKCR\folder
Opens key: HKCU\software\classes\folder\shellex\iconhandler
Opens key: HKCR\folder\shellex\iconhandler
Opens key: HKCU\software\classes\allfilesystemobjects
Opens key: HKCR\allfilesystemobjects
Opens key: HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
Opens key: HKCR\allfilesystemobjects\shellex\iconhandler
Opens key: HKCU\software\classes\directory\docobject
Opens key: HKCR\directory\docobject
Opens key: HKCU\software\classes\folder\docobject
Opens key: HKCR\folder\docobject
Opens key: HKCU\software\classes\allfilesystemobjects\docobject
Opens key: HKCR\allfilesystemobjects\docobject
Opens key: HKCU\software\classes\directory\browseinplace
Opens key: HKCR\directory\browseinplace
Opens key: HKCU\software\classes\folder\browseinplace
Opens key: HKCR\folder\browseinplace
Opens key: HKCU\software\classes\allfilesystemobjects\browseinplace
Opens key: HKCR\allfilesystemobjects\browseinplace
Opens key: HKCU\software\classes\directory\clsid
Opens key: HKCR\directory\clsid
Opens key: HKCU\software\classes\folder\clsid
Opens key: HKCR\folder\clsid
Opens key: HKCU\software\classes\allfilesystemobjects\clsid
Opens key: HKCR\allfilesystemobjects\clsid
Opens key: HKCU\software\classes\.html
Opens key: HKCR\.html
Opens key: HKCU\software\classes\.html\openwithprogids
Opens key: HKCR\.html\openwithprogids
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html\openwithprogids
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html\userchoice
Opens key: HKCU\software\classes\htmlfile
Opens key: HKCR\htmlfile
Opens key: HKCU\software\classes\htmlfile\curver
Opens key: HKCR\htmlfile\curver
Opens key: HKCR\htmlfile\
Opens key: HKCU\software\classes\htmlfile\shellex\iconhandler
Opens key: HKCR\htmlfile\shellex\iconhandler
Opens key: HKCU\software\classes\htmlfile\docobject
Opens key: HKCR\htmlfile\docobject
Opens key: HKCU\software\classes\systemfileassociations\.html
Opens key: HKCR\systemfileassociations\.html
Opens key: HKCU\software\classes\systemfileassociations\.html\docobject
Opens key: HKCR\systemfileassociations\.html\docobject
Opens key: HKCU\software\classes\systemfileassociations\document

Opens key: HKCR\systemfileassociations\document
 Opens key: HKCU\software\classes\htmlfile\browseinplace
 Opens key: HKCR\htmlfile\browseinplace
 Opens key: HKCU\software\classes\systemfileassociations\.html\browseinplace
 Opens key: HKCR\systemfileassociations\.html\browseinplace
 Opens key: HKCU\software\classes\htmlfile\clsid
 Opens key: HKCR\htmlfile\clsid
 Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}
 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\toolbar\webbrowser
 Opens key: HKLM\software\policies\microsoft\internet explorer\toolbar\webbrowser
 Opens key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\toolbar\webbrowser
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\ieak
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ieak
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\ieak
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\commandbar
 Opens key: HKLM\software\policies\microsoft\internet explorer\commandbar
 Opens key: HKCU\software\microsoft\internet explorer\commandbar
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\commandbar
 Opens key: HKCU\software\classes\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
 Opens key: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
 Opens key: HKCU\software\classes\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\treatas
 Opens key: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\treatas
 Opens key: HKCU\software\classes\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\progid
 Opens key: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\progid
 Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
 Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
 Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\progid
 Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\progid
 Opens key: HKCU\software\classes\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32
 Opens key: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32
 Opens key: HKCU\software\classes\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler32
 Opens key: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler32
 Opens key: HKCU\software\classes\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler
 Opens key: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler
 Opens key: HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
 Opens key: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\protocoldefaults\
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap\domains\
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\fontsubstitutes
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\infodelivery\restrictions
 Opens key: HKLM\software\policies\microsoft\internet explorer\infodelivery\restrictions
 Opens key: HKCU\software\policies\microsoft\internet explorer\infodelivery\restrictions
 Opens key: HKCU\software\microsoft\internet explorer\searchurl
 Opens key: HKCU\software\microsoft\internet explorer\searchscopes
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\searchscopes
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
 Opens key: HKLM\software\policies\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
 Opens key: HKCU\software\policies\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
 Opens key: HKCU\software\policies\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\searchscopes

Opens key: HKLM\software\policies\microsoft\internet explorer\searchscopes

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination

Opens key: HKCU\software\microsoft\internet explorer\ietld

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\toolbar

Opens key: HKLM\software\policies\microsoft\internet explorer\toolbar

Opens key: HKCU\software\microsoft\internet explorer\toolbar

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\toolbars\restrictions

Opens key: HKCU\software\policies\microsoft\internet explorer\toolbars\restrictions

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\linksbar

Opens key: HKLM\software\policies\microsoft\internet explorer\linksbar

Opens key: HKCU\software\microsoft\internet explorer\linksbar

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\linksbar

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\migration

Opens key: HKCU\software\microsoft\internet explorer\linksbar\itemcache

Opens key: HKCU\software\microsoft\internet explorer\linksbar\itemcache\0

Opens key: HKCU\software\microsoft\internet explorer\linksbar\itemcache\1

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\advanced

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid

Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid

Opens key: HKCU\software\microsoft\internet explorer\extensions

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\extensions

Opens key: HKLM\software\wow6432node\microsoft\windows\tablet pc\

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\restrictions

Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions

Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\iedevtools

Opens key: HKLM\software\policies\microsoft\internet explorer\iedevtools

Opens key: HKCU\software\microsoft\internet explorer\iedevtools

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\iedevtools

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler

Opens key: HKCU\software\microsoft\internet explorer\lowregistry\commandbar

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}

Opens key: HKCU\software\microsoft\internet explorer\linksexplorer

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\linksexplorer

Opens key: HKCU\software\classes\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}

Opens key: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}

Opens key: HKCU\software\classes\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\treatas

Opens key: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\progid

Opens key: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\progid

Opens key: HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}

Opens key: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}

Opens key: HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\progid

Opens key: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}\propertybag

Opens key: HKCU\software\classes\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}

006097c9a090}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprochandler
Opens key: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprochandler
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-
4901-4acc-8648-d5d44b04ef8f}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-
4901-4acc-8648-d5d44b04ef8f}\propertybag
Opens key: HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
Opens key: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}\shellfolder
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-
89c5-5595fe6b30ee}\shellfolder
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-
ab48-4ec1-ba1f-a1ef4146fc19}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-
ab48-4ec1-ba1f-a1ef4146fc19}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-
d62e-491d-aa7c-e74b8be3b067}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-
d62e-491d-aa7c-e74b8be3b067}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\user
shell folders
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-
ebd2-438a-8655-8a092e34987a}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-
ebd2-438a-8655-8a092e34987a}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-
ae11-4ae3-864c-16f3910ab8fe}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-
ae11-4ae3-864c-16f3910ab8fe}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\ctf\compatibility\iexplore.exe
Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\wow6432node\microsoft\ctf\
Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}
Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\treatas
Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\progid
Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler

Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\inprochandler

Opens key: HKCU\software\classes\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}

Opens key: HKCR\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}

Opens key: HKCU\software\classes\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\treatas

Opens key: HKCR\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\progid

Opens key: HKCR\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\progid

Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}

Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}

Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\progid

Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler

Opens key: HKCR\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler

Opens key: HKCU\software\classes\htmlfile\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCR\htmlfile\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCU\software\classes\.html\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCR\.html\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCU\software\classes\systemfileassociations\.html\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCR\systemfileassociations\.html\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\shellfolder

Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\shellfolder

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\shellfolder

Opens key: HKCU\software\classes*

Opens key: HKCR*

Opens key: HKCU\software\classes*\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCR*\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCU\software\classes\allfilesystemobjects\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKCR\allfilesystemobjects\shellex\{000214f9-0000-0000-c000-000000000046}

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\url history

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\url history

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\url history

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\url history

Opens key: HKCU\software\classes\wow6432node\interface\{9ec704ba-e1d4-45c5-9b59-bfae07d9f04e}

Opens key: HKCR\wow6432node\interface\{9ec704ba-e1d4-45c5-9b59-bfae07d9f04e}

Opens key: HKCU\software\classes\wow6432node\interface\{9ec704ba-e1d4-45c5-9b59-bfae07d9f04e}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{9ec704ba-e1d4-45c5-9b59-bfae07d9f04e}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}

Opens key: HKCR\wow6432node\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}

Opens key: HKCU\software\classes\wow6432node\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}

Opens key: HKCR\wow6432node\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}

Opens key: HKCU\software\classes\wow6432node\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{f704b7e0-4760-46ff-bbdb-7439e0a2a814}

Opens key: HKCR\wow6432node\interface\{f704b7e0-4760-46ff-bbdb-7439e0a2a814}

Opens key: HKCU\software\classes\wow6432node\interface\{f704b7e0-4760-46ff-bbdb-7439e0a2a814}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{f704b7e0-4760-46ff-bbdb-7439e0a2a814}\proxystubclsid32

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iexplore.exe

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\iexplore.exe
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites\links\
Opens key: HKCU\control panel\international\calendars\twodigityearmax
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\hardware
profiles\current\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-
1e1a187c13e9}\0000
Opens key: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000
Opens key: HKCU\software\microsoft\windows\currentversion\app_paths\iexplore.exe
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\iexplore.exe
Opens key: HKLM\software\microsoft\windows\currentversion\app_paths\iexplore.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\marlett
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\treatas
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\progid
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\progid
Opens key: HKCU\software\classes\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}
Opens key: HKCU\software\classes\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\progid
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\inprochandler
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance
Opens key: HKCU\software\classes\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}
Opens key: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-d3202aaa02da}
Opens key: HKCU\software\classes\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\treatas
Opens key: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\progid
Opens key: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\progid
Opens key: HKCU\software\classes\clsid\{942bc614-676c-464e-b384-d3202aaa02da}
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}
Opens key: HKCU\software\classes\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\progid
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\inprochandler
Opens key: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-
d3202aaa02da}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\initpropertybag
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\initpropertybag
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_urlfile_cache\flush_kb936881

Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_urlfile_cache\flush_kb936881
Opens key: HKCU\software\classes\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}
Opens key: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}
Opens key: HKCU\software\classes\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\treatas
Opens key: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\progid
Opens key: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\progid
Opens key: HKCU\software\classes\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}
Opens key: HKCU\software\classes\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\progid
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprochandler
Opens key: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}
Opens key: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}
Opens key: HKCU\software\classes\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\treatas
Opens key: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\progid
Opens key: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\progid
Opens key: HKCU\software\classes\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}
Opens key: HKCU\software\classes\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\progid
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\inprochandler
Opens key: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}\2
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}\2
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\8
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\8
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\9
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\9
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\3
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\3
Opens key: HKCU\software\classes\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2
Opens key: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1a677c0f-1bdb9cfc
Opens key: HKLM\software\wow6432node\microsoft\rpc\securityservice
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ext\clsid

Opens key: HKLM\software\microsoft\windows\currentversion\policies\ext\clsid
Opens key: HKCU\software\microsoft\windows\currentversion\policies\ext\clsid
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ext
Opens key: HKLM\software\microsoft\windows\currentversion\policies\ext
Opens key: HKCU\software\microsoft\windows\currentversion\policies\ext
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\acroiehlpshim.dll
Opens key: HKCU\software\classes\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\progid
Opens key: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandler
Opens key: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\treatas
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\progid
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\jp2ssv.dll
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\progid
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\progid
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\jp2ssv.dll
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\progid
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler
Opens key: HKLM\software\wow6432node\javasoft
Opens key: HKLM\software\wow6432node\javasoft\java plug-in
Opens key: HKLM\software\wow6432node\javasoft\java plug-in\10.2.0
Opens key: HKLM\software\wow6432node\javasoft\java plug-in\1.7.0_02
Opens key: HKLM\software\wow6432node\javasoft\java runtime environment
Opens key: HKLM\software\wow6432node\javasoft\java runtime environment\1.7.0_02
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
Opens key: HKLM\software\wow6432node\microsoft\feeds
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\suggested sites
Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\classes\typelib
Opens key: HKCR\typelib
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}
Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0
Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0

Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32
Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprocserver32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shell
extensions\blocked
Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\shellfolder
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\treatas
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\progid
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\progid
Opens key: HKCU\software\classes\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}
Opens key: HKCR\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}
Opens key: HKCU\software\classes\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\progid
Opens key: HKCR\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprochandler
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\browseremulation
Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\progid
Opens key: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\progid
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\progid
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
Opens key: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\mediatypeclass
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\accepted documents
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ratings
Opens key: HKLM\software\microsoft\windows\currentversion\policies\ratings
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler\about\
Opens key: HKCR\protocols\name-space handler\about
Opens key: HKCU\software\classes\protocols\name-space handler*\
Opens key: HKCR\protocols\name-space handler*
Opens key: HKCU\software\classes\protocols\handler\about
Opens key: HKCR\protocols\handler\about
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr

Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_object_caching
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_object_caching
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
 Opens key: HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_cleanup_at_fl
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_cleanup_at_fl
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
 paths\outlook.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\application
 compatibility
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet
 explorer\domstorage
 Opens key: HKLM\software\policies\microsoft\internet explorer\domstorage
 Opens key: HKCU\software\microsoft\internet explorer\domstorage
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\domstorage
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_mime_handling
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_mime_handling
 Opens key: HKCU\software\classes\protocols\name-space handler\file
 Opens key: HKCR\protocols\name-space handler\file
 Opens key: HKCU\software\classes\protocols\filter\text/html
 Opens key: HKCR\protocols\filter\text/html
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_mime_sniffing
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_mime_sniffing
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
 Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
 Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
 Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
 Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler
 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_manage_script_circular_refs
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_manage_script_circular_refs
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_restrict_filedownload
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_restrict_filedownload
 Opens key: HKCU\software\classes\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}
 Opens key: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}
 Opens key: HKCU\software\classes\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\treatas
 Opens key: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\treatas
 Opens key: HKCU\software\classes\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\progid

Opens key: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\progid
 Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}
 Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}
 Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\progid
 Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\progid
 Opens key: HKCU\software\classes\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32
 Opens key: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32
 Opens key: HKCU\software\classes\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandler32
 Opens key: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandler32
 Opens key: HKCU\software\classes\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandler
 Opens key: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandler
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\security\floppy access
 Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof detection
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\security\adv addrbar spoof detection
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\zoom
 Opens key: HKLM\software\policies\microsoft\internet explorer\zoom
 Opens key: HKCU\software\microsoft\internet explorer\zoom
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\zoom
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\phishingfilter
 Opens key: HKLM\software\policies\microsoft\internet explorer\phishingfilter
 Opens key: HKCU\software\microsoft\internet explorer\phishingfilter
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
 Opens key: HKCU\software\microsoft\internet explorer\international
 Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts
 Opens key: HKCU\software\microsoft\internet explorer\international\scripts
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\international\scripts
 Opens key: HKLM\software\policies\microsoft\internet explorer\settings
 Opens key: HKCU\software\microsoft\internet explorer\settings
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\settings
 Opens key: HKCU\software\microsoft\internet explorer\styles
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\activedesktop
 Opens key: HKCU\software\microsoft\windows\currentversion\policies
 Opens key: HKCU\software\microsoft\internet explorer\pagesetup
 Opens key: HKCU\software\microsoft\internet explorer\menuext
 Opens key: HKCU\software\microsoft\internet explorer\menuext\%s
 Opens key: HKLM\system\currentcontrolset\control\nls\codepage
 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\travellog
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\travellog
 Opens key: HKCU\software\classes\wow6432node\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}
 Opens key: HKCR\wow6432node\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}
 Opens key: HKCU\software\classes\wow6432node\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}\proxystubclsid32
 Opens key: HKCR\wow6432node\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}\proxystubclsid32
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\version vector
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_sslux
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_sslux
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\browseremulation
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user agent
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\user agent
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\user agent
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\user agent

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\ua tokens
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\pre platform
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\post platform
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
Opens key: HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}
Opens key: HKCR\wow6432node\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\treatas
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\progid
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\progid
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\progid
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\treatas
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\progid
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\progid
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
Opens key: HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-

000000000046}\progid
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\progid
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\progid
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key: HKCU\software\classes\wow6432node\interface\{9d973e3b-f610-4f03-83d3-
aed90c3237ac}
Opens key: HKCR\wow6432node\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac}
Opens key: HKCU\software\classes\wow6432node\interface\{9d973e3b-f610-4f03-83d3-
aed90c3237ac}\synchronousinterface
Opens key: HKCR\wow6432node\interface\{9d973e3b-f610-4f03-83d3-
aed90c3237ac}\synchronousinterface
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_status_bar_throttling
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_status_bar_throttling
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceAAF59cfc}
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceAAF59cfc}\treatas
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceAAF59cfc}\progid
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\progid
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceAAF59cfc}\progid
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceAAF59cfc}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\inprochandler

Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceAAF59cfc}\inprochandler

Opens key: HKCU\software\policies\microsoft\internet explorer\control panel

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\

Opens key: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex compatibility

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\ext\settings\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_alloveddomainlist

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_alloveddomainlist

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\extension compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall

Opens key: HKCU\software\classes\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}

Opens key: HKCR\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}

Opens key: HKCU\software\microsoft\code store database\distribution units

Opens key: HKLM\software\wow6432node\microsoft\code store database\distribution units

Opens key: HKLM\software\wow6432node\microsoft\code store database\distribution units\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\availableversion

Opens key: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\availableversion

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\installedversion

Opens key: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\installedversion

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\appid

Opens key: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\appid

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\localserver32

Opens key: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\localserver32

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915

Opens key: HKCU\software\classes\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas

Opens key: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}

Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\treatas

Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\progid

Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\progid

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}

abcdeffedcbb}\progid
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\progid
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprochandler
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprochandler
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\kindmap
Opens key: HKCU\software\classes\htmlfile\shell
Opens key: HKCR\htmlfile\shell
Opens key: HKCU\software\classes\htmlfile\shell\opennew
Opens key: HKCR\htmlfile\shell\opennew
Opens key: HKCU\software\classes\htmlfile\shell\edit
Opens key: HKCR\htmlfile\shell\edit
Opens key: HKCU\software\classes\htmlfile\shell\edit\command
Opens key: HKCR\htmlfile\shell\edit\command
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default html
editor
Opens key: HKCU\software\classes\.html\openwithlist
Opens key: HKCR\.html\openwithlist
Opens key: HKCU\software\microsoft\internet explorer\default html editor
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default html
editor\
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default html
editor\shell\edit
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default html
editor\shell\edit\command
Opens key: HKCU\software\microsoft\internet explorer\default mhtml editor
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default mhtml
editor
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default mhtml
editor\shell\edit\command
Opens key: HKCU\software\classes\.htm
Opens key: HKCR\.htm
Opens key: HKCU\software\classes\.htm\openwithprogid
Opens key: HKCR\.htm\openwithprogid
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm\openwithprogid
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm\
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm\userchoice
Opens key: HKCU\software\classes\.htm\openwithlist
Opens key: HKCR\.htm\openwithlist
Opens key: HKCU\software\classes\applications\notepad.exe
Opens key: HKCR\applications\notepad.exe
Opens key: HKCR\applications\notepad.exe\
Opens key: HKCU\software\classes\applications\notepad.exe\shell\edit
Opens key: HKCR\applications\notepad.exe\shell\edit
Opens key: HKCU\software\classes\applications\notepad.exe\shell\edit\command
Opens key: HKCR\applications\notepad.exe\shell\edit\command
Opens key: HKLM\software\policies\microsoft\internet explorer\feed discovery
Opens key: HKCU\software\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\feed discovery\
Opens key: HKCU\software\microsoft\internet explorer\feed discovery\
Opens key: HKCU\software\microsoft\ftp
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\services
Opens key: HKLM\software\policies\microsoft\internet explorer\services
Opens key: HKCU\software\microsoft\internet explorer\services
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\activities
Opens key: HKLM\software\policies\microsoft\internet explorer\activities
Opens key: HKCU\software\microsoft\internet explorer\activities
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activities
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\shellfolder
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\treatas
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\progid
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\progid
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-
c2a7-11cf-bff4-444553540000}
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace\namecustomizations
Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}
Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}
Opens key: HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}
Opens key: HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\forward
Opens key: HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\forward
Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\forward
Opens key: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\forward
Opens key: HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\typelib
Opens key: HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\typelib
Opens key: HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-
00aa006009fa}
Opens key: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
Opens key: HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-
00aa006009fa}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-
00aa006009fa}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{b722bccb-4e68-101b-a2bc-
00aa00404770}
Opens key: HKCR\wow6432node\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
Opens key: HKCU\software\classes\wow6432node\interface\{b722bccb-4e68-101b-a2bc-
00aa00404770}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{b722bccb-4e68-101b-a2bc-
00aa00404770}\proxystubclsid32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-
5ca8-4905-ae3b-bf251ea09b53}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-
5ca8-4905-ae3b-bf251ea09b53}\propertybag
Opens key: HKCU\software\classes\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}
Opens key: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{f02c1a0d-
be21-4350-88b0-7367fc96ef3c}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-
bbf8-452a-850d-79d08e667ca7}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-
bbf8-452a-850d-79d08e667ca7}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
11cf-aaa5-00401c608501}\iexplore
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\caretbrowsing
Opens key: HKLM\software\policies\microsoft\internet explorer\caretbrowsing
Opens key: HKCU\software\microsoft\internet explorer\caretbrowsing
Opens key: HKLM\software\wow6432node\clients\startmenuinternet\iexplore.exe\installinfo
Opens key: HKLM\software\clients\startmenuinternet\iexplore.exe\installinfo
Opens key: HKCU\software\classes\wow6432node\clsid\{591209c7-767b-42b2-9fba-
44ee4615f2c7}
Opens key: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}
Opens key: HKCU\software\classes\wow6432node\clsid\{591209c7-767b-42b2-9fba-
44ee4615f2c7}\treatas
Opens key: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\progid

Opens key: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\progid

Opens key: HKCU\software\classes\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}

Opens key: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}

Opens key: HKCU\software\classes\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\progid

Opens key: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler

Opens key: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler

Opens key: HKCU\software\classes\url

Opens key: HKCR\url

Opens key: HKCU\software\classes\url\openwithprogid

Opens key: HKCR\url\openwithprogid

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\url\openwithprogid

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\url

Opens key: HKCU\software\classes\internetshortcut

Opens key: HKCR\internetshortcut

Opens key: HKCU\software\classes\internetshortcut\curver

Opens key: HKCR\internetshortcut\curver

Opens key: HKCR\internetshortcut\

Opens key: HKCU\software\classes\internetshortcut\shellex\iconhandler

Opens key: HKCR\internetshortcut\shellex\iconhandler

Opens key: HKCU\software\classes\internetshortcut\docobject

Opens key: HKCR\internetshortcut\docobject

Opens key: HKCU\software\classes\systemfileassociations\url

Opens key: HKCR\systemfileassociations\url

Opens key: HKCU\software\classes\internetshortcut\browseinplace

Opens key: HKCR\internetshortcut\browseinplace

Opens key: HKCU\software\classes\internetshortcut\clsid

Opens key: HKCR\internetshortcut\clsid

Opens key: HKCU\software\classes\wow6432node\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\implemented categories\{00021490-0000-0000-c000-000000000046}

Opens key: HKCR\wow6432node\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\implemented categories\{00021490-0000-0000-c000-000000000046}

Opens key: HKCU\software\microsoft\internet explorer\linksbar\itemcache\2

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\fileassociations

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\capabilities

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\mht

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\mht\

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\mht\userchoice

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\mhtml

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\mhtml\

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\mhtml\userchoice

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\urlassociations

Opens key: HKCU\software\microsoft\windows\shell\associations\urlassociations\https

Opens key: HKCU\software\microsoft\windows\shell\associations\urlassociations\ftp

Opens key: HKCU\software\microsoft\windows\shell\associations\urlassociations\http

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\mimeassociations

Opens key: HKCU\software\microsoft\windows\shell\associations\mimeassociations\message/rfc822\userchoice

Opens key: HKCU\software\microsoft\windows\shell\associations\mimeassociations\text/html\userchoice

Opens key: HKCU\software\classes\http

Opens key: HKCR\http

Opens key: HKCU\software\classes\http\shell\open\ddeexec\ifexec

Opens key: HKCR\http\shell\open\ddeexec\ifexec

Opens key: HKCU\software\classes\https

Opens key: HKCR\https

Opens key: HKCU\software\classes\https\shell\open\ddeexec\ifexec

Opens key: HKCR\https\shell\open\ddeexec\ifexec

Opens key: HKCU\software\classes\ftp

Opens key: HKCR\ftp

Opens key: HKCU\software\classes\internetshortcut\defaulticon

Opens key: HKCR\internetshortcut\defaulticon

Opens key: HKCU\software\classes\http\shell\open\command

Opens key: HKCR\http\shell\open\command

Opens key: HKCU\software\classes\http\shell\open\ddeexec

Opens key: HKCR\http\shell\open\ddeexec

Opens key: HKCU\software\classes\http\shell\open\ddeexec\application

Opens key: HKCR\http\shell\open\ddeexec\application

Opens key: HKCU\software\classes\http\shell\open\ddeexec\topic

Opens key: HKCR\http\shell\open\ddeexec\topic

Opens key: HKCU\software\classes\https\shell\open\command

Opens key: HKCR\https\shell\open\command

Opens key: HKCU\software\classes\https\shell\open\ddeexec

Opens key: HKCR\https\shell\open\ddeexec
Opens key: HKCU\software\classes\https\shell\open\ddeexec\application
Opens key: HKCR\https\shell\open\ddeexec\application
Opens key: HKCU\software\classes\https\shell\open\ddeexec\topic
Opens key: HKCR\https\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\ftp\shell\open\command
Opens key: HKCR\ftp\shell\open\command
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec
Opens key: HKCR\ftp\shell\open\ddeexec
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\ifexec
Opens key: HKCR\ftp\shell\open\ddeexec\ifexec
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\application
Opens key: HKCR\ftp\shell\open\ddeexec\application
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\topic
Opens key: HKCR\ftp\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\htmlfile\shell\open
Opens key: HKCR\htmlfile\shell\open
Opens key: HKCU\software\classes\htmlfile\shell\open\command
Opens key: HKCR\htmlfile\shell\open\command
Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec
Opens key: HKCR\htmlfile\shell\open\ddeexec
Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec\application
Opens key: HKCR\htmlfile\shell\open\ddeexec\application
Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec\topic
Opens key: HKCR\htmlfile\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\mhtmlfile\shell
Opens key: HKCR\mhtmlfile\shell
Opens key: HKCU\software\classes\htmlfile\shell\opennew\command
Opens key: HKCR\htmlfile\shell\opennew\command
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec
Opens key: HKCR\htmlfile\shell\opennew\ddeexec
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCR\htmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\application
Opens key: HKCR\htmlfile\shell\opennew\ddeexec\application
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\topic
Opens key: HKCR\htmlfile\shell\opennew\ddeexec\topic
Opens key: HKCU\software\classes\.mht
Opens key: HKCR\.mht
Opens key: HKCU\software\classes\.mhtml
Opens key: HKCR\.mhtml
Opens key: HKCU\software\classes\mhtmlfile\shell\open
Opens key: HKCR\mhtmlfile\shell\open
Opens key: HKCU\software\classes\mhtmlfile\shell\open\command
Opens key: HKCR\mhtmlfile\shell\open\command
Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec
Opens key: HKCR\mhtmlfile\shell\open\ddeexec
Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec\application
Opens key: HKCR\mhtmlfile\shell\open\ddeexec\application
Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec\topic
Opens key: HKCR\mhtmlfile\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew
Opens key: HKCR\mhtmlfile\shell\opennew
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\command
Opens key: HKCR\mhtmlfile\shell\opennew\command
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\application
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\application
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\topic
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\topic
Opens key: HKCU\software\classes\internetshortcut\shell\open
Opens key: HKCR\internetshortcut\shell\open
Opens key: HKCU\software\classes\internetshortcut\shell\open\command
Opens key: HKCR\internetshortcut\shell\open\command
Opens key: HKCU\software\classes\wow6432node\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}
Opens key: HKCR\wow6432node\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}
Opens key: HKCU\software\classes\applications\iexplore.exe\shell\open\command
Opens key: HKCR\applications\iexplore.exe\shell\open\command
Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32
Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
Opens key: HKCU\software\microsoft\internet explorer\user preferences
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\treatas
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\progid
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\msxml30
Opens key: HKCU\software\policies\microsoft\internet explorer\feeds
Opens key: HKCU\software\microsoft\feeds
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}\propertybag
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6
Opens key: HKLM\software\wow6432node\oracle\javafx
Opens key: HKLM\software\wow6432node\javasoft\java runtime environment\1.7
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\jp2launcher.exe
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags\custom\jp2launcher.exe
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\java.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\java.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000
Opens key: HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
Opens key: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000
Opens key: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\0000
Opens key: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000
Opens key: HKLM\software\wow6432node\microsoft\direct3d
Opens key: HKLM\software\wow6432node\microsoft\direct3d\drivers
Opens key: HKCU\software\microsoft\direct3d
Opens key: HKLM\system\currentcontrolset\control\graphicsdrivers\scheduler
Opens key: HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist
Opens key: HKCU\software\microsoft\direct3d\drivers
Opens key: HKLM\software\wow6432node\microsoft\direct3d\drivers\direct3d_hal
Opens key: HKLM\software\wow6432node\microsoft\direct3d\drivers\ramp emulation
Opens key: HKLM\software\wow6432node\microsoft\direct3d\drivers\rgb emulation
Opens key: HKCU\system\currentcontrolset\control\graphicsdrivers\scheduler
Opens key: HKLM\system\currentcontrolset\control\watchdog\display
Opens key: HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480
Opens key: HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02\device parameters
Opens key: HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1a3e7dae-2a650609
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1a3e7dae
Opens key: HKLM\software\wow6432node\javasoft\java update\policy
Opens key: HKCU\control panel\desktop>windowmetrics
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32\placesbar
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKCU\euodc\1252
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\locale\customlocale[empty]
Queries value: HKLM\system\currentcontrolset\control\locale\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatetocodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[iexplore]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[depoﬀ]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\low
rights[protectedmodeoﬀforallzones]
Queries value: HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[tabprocgrowth]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\low
rights[luaoﬀlorieon]
Queries value: HKCU\software\microsoft\internet
explorer\setup[havecreatedquicklaunchitems]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup\systemsetupinprogress]
Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-

33be-4251-ba85-6007caedcf9d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cache limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruser item]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruser item]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parent folder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource type]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parent folder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-

65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cache-limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cache-repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cache-path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cache-prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cache-limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cache-options]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cache-repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cache-path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cache-prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cache-limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cache-options]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache-repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache-path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache-prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache-limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache-options]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache-repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache-path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache-prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache-limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache-options]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache-repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache-path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache-prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache-limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache-options]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mcbsservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcscapiforcrack]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernames]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[receptivetimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receptivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablenlmpreauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrevcing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:

[illegible]

```
settings[disablebranchcache]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet explorer\main[start page]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[iexplore.exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
  Queries value: HKCU\software\microsoft\internet explorer\main[secondary start pages]
  Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[secondary
start pages]
  Queries value: HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[frametabwindow]
  Queries value: HKCU\software\microsoft\internet explorer\main[framemerging]
  Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]
  Queries value: HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[sessionmerging]
  Queries value: HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[admintabprocs]
  Queries value: HKCU\software\microsoft\internet explorer\main[hangresistance]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[hangresistance]
  Queries value: HKCU\software\microsoft\internet explorer\main[compatibilityflags]
  Queries value: HKCU\software\microsoft\internet explorer\new windows[detourdialogs]
  Queries value: HKCU\software\microsoft\internet explorer\sqm[serverfreezeonupload]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parsiname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
```

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[unattendloaded]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[tldupdates]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-

db2c-424c-b029-7fe99a87c641}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[flags]
Queries value: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[vercache]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore[loadtime]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}[flags]
Queries value: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}[vercache]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore[loadtime]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[relativepath]
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresource type]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
Queries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasapi32[enablefiletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasapi32[filetracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasapi32[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasapi32[consoletracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasapi32[maxfilesize]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasapi32[filedirectory]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasmancs[enablefiletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasmancs[filetracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasmancs[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasmancs[consoletracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasmancs[maxfilesize]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\iexplore_rasmancs[filedirectory]
Queries value: HKLM\system\currentcontrolset\control\sqmclientlist[sqmclientlist]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[74dd1fc8]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodiald11]
Queries value: HKCU\software\microsoft\internet explorer\main>window_min_width
Queries value: HKCU\software\microsoft\internet explorer\main>window_min_height
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
Queries value:

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\com3[gipactivitybypass]
Queries value: HKCR\wow6432node\interface\{ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKCR\wow6432node\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[groups]
Queries value: HKCU\software\microsoft\internet explorer\main\windowssearch[enabledscopes]
Queries value: HKLM\software\wow6432node\microsoft\windows search[currentversion]
Queries value: HKLM\system\currentcontrolset\control\ntp\local[00000409]
Queries value: HKLM\system\currentcontrolset\control\ntp\language groups[1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0[disable]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane12]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[flags]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[iexplore.exe]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablefixsecuritysettings]
Queries value: HKCU\software\microsoft\internet explorer\security[disablefixsecuritysettings]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\security[disablefixsecuritysettings]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-08002b30309d}]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}[generation]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
Queries value: HKCR\drive\shellex\folderextensions\{fbef8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}[generation]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]

Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[icononly]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
Queries value: HKCR\directory[docobject]
Queries value: HKCR\folder[docobject]
Queries value: HKCR\allfilesystemobjects[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\folder[browseinplace]
Queries value: HKCR\allfilesystemobjects[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\folder[isshortcut]
Queries value: HKCR\allfilesystemobjects[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKCR\folder[nevershowext]
Queries value: HKCR\allfilesystemobjects[nevershowext]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
Queries value: HKCR\.html[]
Queries value: HKCR\htmlfile\shellex\iconhandler[]
Queries value: HKCR\htmlfile[docobject]
Queries value: HKCR\systemfileassociations\.html[docobject]
Queries value: HKCR\htmlfile[browseinplace]
Queries value: HKCR\systemfileassociations\.html[browseinplace]
Queries value: HKCR\.html[content_type]
Queries value: HKCR\htmlfile\clsid[]
Queries value: HKCR\htmlfile[isshortcut]
Queries value: HKCR\systemfileassociations\.html[isshortcut]
Queries value: HKCR\htmlfile[alwaysshowext]
Queries value: HKCR\systemfileassociations\.html[alwaysshowext]
Queries value: HKCR\htmlfile[nevershowext]
Queries value: HKCR\systemfileassociations\.html[nevershowext]
Queries value: HKCU\software\microsoft\internet explorer\main>window_placement]
Queries value: HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbar7position]
Queries value: HKCU\software\microsoft\internet explorer\main[fullscreen]
Queries value: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}[]
Queries value: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\internet explorer\main[useie7autocomplete]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
Queries value: HKCU\software\microsoft\internet explorer\main[searchcontrolwidth]
Queries value: HKCU\software\microsoft\internet explorer\main[searchmigrated]
Queries value: HKCU\software\microsoft\internet explorer\main[searchmigratedinstalled]
Queries value: HKCU\software\microsoft\internet
explorer\main[searchmigrateddefaultname]
Queries value: HKCU\software\microsoft\internet explorer\main[searchmigrateddefaulturl]
Queries value: HKCU\software\microsoft\internet explorer\searchurl[provider]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[defaultscope]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[deleted]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[url]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[displayname]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]
Queries value: HKCU\software\microsoft\internet
explorer\searchscopes[showsearchsuggestionsglobal]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\searchscopes[showsearchsuggestionsglobal]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[suggestionsurl_json]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl_json]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[suggestionsurl_jsonfallback]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl_jsonfallback]

Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurlfallback]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[previewurl]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[previewurl]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[previewurlfallback]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[previewurlfallback]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[faviconurl]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[faviconurl]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[faviconurlfallback]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[faviconpath]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[codepage]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[codepage]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[sortindex]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddlversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddlversionhigh]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[enabled]
Queries value: HKCU\software\microsoft\internet explorer\toolbar[locked]
Queries value: HKCU\software\microsoft\internet explorer\linksbar[enabled]
Queries value: HKCU\software\microsoft\internet explorer\linksbar[testhandler]
Queries value: HKCU\software\microsoft\internet explorer\linksbar[linksfoldermigrate]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\migration[ie installed date]
Queries value: HKCU\software\microsoft\internet explorer\linksbar[marketinglinksmigrate]
Queries value: HKCU\software\microsoft\internet explorer\linksbar\itemcache\0[path]
Queries value: HKCU\software\microsoft\internet explorer\linksbar\itemcache\0[handler]
Queries value: HKCU\software\microsoft\internet explorer\linksbar\itemcache\0[feedurl]
Queries value: HKCU\software\microsoft\internet explorer\linksbar\itemcache\1[path]
Queries value: HKCU\software\microsoft\internet explorer\linksbar\itemcache\1[handler]
Queries value: HKCU\software\microsoft\internet explorer\linksbar\itemcache\1[feedurl]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[cascadefolderbands]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\advanced[cascadefolderbands]
Queries value: HKCU\software\microsoft\internet explorer\linksbar[defaultitemwidth]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[activitymetertimerinterval]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[activitymeterdisable]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\[]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[quicktabsthreshold]
Queries value: HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[thumbnailbehavior]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localizedname]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[security]
Queries value: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}[]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]type
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]
Queries value: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[streamresource]type
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-

4901-4acc-8648-d5d44b04ef8f}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[initfolderhandler]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-5595fe6b30ee}]
Queries value: HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbar7height]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[streamresource type]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-

ab48-4ec1-ba1f-a1ef4146fc19}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menu]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}[initfolderhandler]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\user shell folders[common start menu]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[category]
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[streamresource]
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[initfolderhandler]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[initfolderhandler]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[name]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[streamresourcetype]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}[initfolderhandler]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\wow6432node\microsoft\ctf\enableanchorcontext]
Queries value: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\progid[]
Queries value: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}[]
Queries value: HKCR\wow6432node\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{25336920-03f9-11cf-8fd0-00aa00686f13}]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url_history[daystokeep]
Queries value: HKCR\wow6432node\interface\{9ec704ba-e1d4-45c5-9b59-bfae07d9f04e}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{f704b7e0-4760-46ff-bbdb-7439e0a2a814}\proxystubclsid32[]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites\links[order]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nostrcmptlogical]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[8c50fa6e-394e-4b47-b6d1-a880a5f225a2]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[2b240425-3141-43ee-931f-ec9f997c7d7e]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[acredir]
Queries value: HKCU\software\microsoft\internet explorer\main[tabshutdowndelay]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[tabshutdowndelay]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[displayname]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[displaymask]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[expiration]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[errorstate]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[displayname]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[displaymask]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[expiration]
Queries value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[errorstate]
Queries value: HKLM\hardware\devicemap\video[\device\video3]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.bitsperpel]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.xresolution]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.yresolution]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.vrefresh]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.flags]

Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.xpanning]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.ypanning]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.orientation]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.fixedoutput]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[attach.relativevex]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[attach.relativev]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[attach.todesktop]
Queries value: HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[defaultsettings.driverextra]
Queries value: HKLM\software\microsoft\windows\currentversion\app
paths\iexplore.exe[dontusedesktopchangerouter]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}[]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance[clsid]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance[loadwithoutcom]
Queries value: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-d3202aaa02da}[]
Queries value: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}[]
Queries value: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}[]
Queries value: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}\2[section]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}[section]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}\2[key]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{5cbf2787-48cf-4208-b90e-ee5e5d420294}\2[vartype]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\8[section]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}[section]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\8[key]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\8[vartype]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\9[section]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\9[key]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\9[vartype]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2[section]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2[key]
Queries value: HKCR\wow6432node\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2[vartype]
Queries value: HKCU\software\microsoft\internet explorer\main[enableprebiding]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
Queries value: HKCU\software\microsoft\internet explorer\main>window title]
Queries value: HKCU\software\microsoft\internet explorer\main>statusbarweb]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[statusbarweb]
Queries value: HKCU\software\microsoft\internet explorer\main[enable browser
extensions]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nobandcustomize]
Queries value: HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbar7layout]
Queries value: HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbarlayout]
Queries value: HKCU\software\microsoft\internet explorer\main[alwaysshowmenus]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[alwaysshowmenus]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_addon_management[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_addon_management[*]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[count]
Queries value: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\progid[]
Queries value: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[]
Queries value: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-
fa578c2ebdc3}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-
fa578c2ebdc3}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-
784b7d6be0b3}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\progid[]
Queries value: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}[]
Queries value: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-
784b7d6be0b3}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-
784b7d6be0b3}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}\iexplore[count]
Queries value: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}[]
Queries value: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-
9c25c1c588a9}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-
9c25c1c588a9}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\javasoft\java plug-in\10.2.0[usenewjavaplugin]
Queries value: HKLM\software\wow6432node\javasoft\java runtime
environment\1.7.0_02[javahome]
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32[]
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32[]
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32[]
Queries value: HKCU\software\classes\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32[]
Queries value: HKLM\software\wow6432node\microsoft\feeds[urlcacheversion]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]
Queries value: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\win32[]
Queries value: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-
00aa004ae837}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-
00aa004ae837}\inprocserver32[loadwithoutcom]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{e7e4bc40-e76a-11ce-a9bb-00aa004ae837} {000214e6-0000-0000-c000-000000000046}
0xffff]
Queries value: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}[]
Queries value: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-
00aa004ae837}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-
00aa004ae837}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d95-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\lockdown_zones\0[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\lockdown_zones\0[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[icon]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[currentlevel]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
Queries value: HKCR\protocols\handler\about\clsid]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[iexplore.exe]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-91a2-7b624e0e7244]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility[iexplore.exe]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
Queries value: HKCU\software\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[iexplore.exe]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[iexplore.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2100]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[iexplore.exe]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
Queries value: HKCU\software\microsoft\windows

```

nt\currentversion\windows[dragscrollldelay]
  Queries value: HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[iexplore.exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
  Queries value: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\[]
  Queries value: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32[threadingmodel]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
  Queries value: HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
  Queries value: HKCU\software\microsoft\internet explorer\zoom[resettextsizeonstartup]
  Queries value: HKCU\software\microsoft\internet explorer\zoom[resettextsizeonzoom]
  Queries value: HKCU\software\microsoft\internet explorer\zoom[resetzoomonstartup2]
  Queries value: HKCU\software\microsoft\internet explorer\zoom[zoomfactor]
  Queries value: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
  Queries value: HKLM\software\policies\microsoft\internet explorer[smartdithering]
  Queries value: HKCU\software\microsoft\internet explorer[smartdithering]
  Queries value: HKCU\software\microsoft\internet explorer[rtfconverterflags]
  Queries value: HKCU\software\microsoft\internet explorer\main[usecleartype]
  Queries value: HKCU\software\microsoft\internet explorer\main[page_transitions]
  Queries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
  Queries value: HKCU\software\microsoft\internet explorer\main[anchor_underline]
  Queries value: HKCU\software\microsoft\internet explorer\main[css_compat]
  Queries value: HKCU\software\microsoft\internet explorer\main[expand alt text]
  Queries value: HKCU\software\microsoft\internet explorer\main[display inline images]
  Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos]
  Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[display
inline_videos]
  Queries value: HKCU\software\microsoft\internet explorer\main[play_background_sounds]
  Queries value: HKCU\software\microsoft\internet explorer\main[play_animations]
  Queries value: HKCU\software\microsoft\internet explorer\main[print_background]
  Queries value: HKCU\software\microsoft\internet explorer\main[use_stylesheets]
  Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll]
  Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp]
  Queries value: HKCU\software\microsoft\internet explorer\main[show_image_placeholders]
  Queries value: HKCU\software\microsoft\internet explorer\main[disable_script_debugger]
  Queries value: HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
  Queries value: HKCU\software\microsoft\internet explorer\main[move_system_caret]
  Queries value: HKCU\software\microsoft\internet explorer\main[force_offscreen
composition]
  Queries value: HKCU\software\microsoft\internet explorer\main[enable_autoimageresize]
  Queries value: HKCU\software\microsoft\internet explorer\main[usethemes]
  Queries value: HKCU\software\microsoft\internet explorer\main[usehr]
  Queries value: HKCU\software\microsoft\internet explorer\main[q300829]
  Queries value: HKCU\software\microsoft\internet explorer\main[cleanup htcs]
  Queries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[xdomainrequest]
  Queries value: HKCU\software\microsoft\internet explorer\main[domstorage]
  Queries value: HKCU\software\microsoft\internet
explorer\international[default_codepage]
  Queries value: HKCU\software\microsoft\internet explorer\international[autodetect]
  Queries value: HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
  Queries value: HKCU\software\microsoft\internet explorer\settings[anchor_color]
  Queries value: HKCU\software\microsoft\internet explorer\settings[anchor_color visited]
  Queries value: HKCU\software\microsoft\internet explorer\settings[anchor_color hover]
  Queries value: HKCU\software\microsoft\internet explorer\settings[always use my colors]
  Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font
size]
  Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font
face]
  Queries value: HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
  Queries value: HKCU\software\microsoft\internet explorer\settings[use anchor hover
color]
  Queries value: HKCU\software\microsoft\internet explorer\settings[miscflags]
  Queries value: HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic_cut_copy_paste]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value: HKCU\software\microsoft\internet explorer\pagesetup[print_background]
  Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
  Queries value: HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsize]
  Queries value: HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
  Queries value: HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
  Queries value: HKCU\software\microsoft\internet
explorer\international\scripts\3[iefixedfontname]
  Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage]
  Queries value: HKCR\wow6432node\interface\{48a98a1f-5cdd-47ee-9286-

```

db04a3eb7ce1}\proxystubclsid32[]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version
vector[vm1]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version vector[ie]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version
vector[windowsedition]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_sslux[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_sslux[*]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[*]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[allsitescompatibilitymode]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[intranetcompatibilitymode]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[localmachinecompatibilitymode]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user agent]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2700]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[iexplore.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones[securitysafe]
Queries value: HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\1[2500]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\2[2500]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\3[2500]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\4[2500]
Queries value: HKCR\wow6432node\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}[]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
Queries value: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}[]
Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
Queries value: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
Queries value: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0[2301]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\lockdown_zones\0[2301]
Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]
Queries value: HKCU\software\microsoft\internet explorer\toolbar[menuuserexpanded]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Queries value: HKCR\wow6432node\interface\{9d973e3b-f610-4f03-8d3d-aed90c3237ac}\synchronousinterface[]
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}[]
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1c00]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1207]
Queries value: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[appid]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[compatibility flags]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[miscstatus flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[120b]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1208]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2201]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall[iexplore.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall[*]
Queries value: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas[]
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdfeffedcbb}[]
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdfeffedcbb}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdfeffedcbb}\inprocserver32[inprocserver32]
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdfeffedcbb}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\javasoft\java runtime environment\1.7.0_02[eula]
Queries value: HKLM\software\wow6432node\javasoft\java plugin\10.2.0[usejava2iexplorer]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[count]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1201]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.html]
Queries value: HKCR\htmlfile[nostaticdefaultverb]
Queries value: HKCR\htmlfile\shell[]
Queries value: HKCR\htmlfile\shell\opennew[neverdefault]
Queries value: HKCR\htmlfile\shell\edit\command[]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default.html
editor[stubs]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default.html
editor[description]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default.html
editor\shell\edit[friendlyappname]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.htm]
Queries value: HKCR*.htm[]
Queries value: HKCR\applications\notepad.exe\shell\edit\command[]
Queries value: HKCU\software\microsoft\internet explorer\main[checkdocumentforprogid]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[checkdocumentforprogid]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\feed discovery[enabled]

Queries value: HKCU\software\microsoft\ftp[use web based ftp]
Queries value: HKCU\software\microsoft\internet explorer\services[selectionactivitybuttondisable]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[loadwithoutcom]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046} 0xffff]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016032920160330[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016032920160330[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016032920160330[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016032920160330[cacheolimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016032920160330[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
Queries value: HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\typelib[]
Queries value: HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\typelib[version]
Queries value: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\internet explorer\main[use formsuggest]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[use formsuggest]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[maxrenderline]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[parentfolder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[infotip]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[localizedname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[security]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[streamresource]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[streamresource type]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[localredirectonly]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[roamable]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[precreate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[stream]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[initfolderhandler]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}[sortorderindex]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[type]
Queries value: HKCU\software\microsoft\internet explorer\caretbrowsing[enableonstartup]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[migrationtime]
Queries value: HKCU\software\microsoft\internet explorer\main[ie8runonceperinstallcompleted]
Queries value: HKCU\software\microsoft\internet explorer\main[ie8runoncecompletiontime]
Queries value: HKCU\software\microsoft\internet explorer\main[check_associations]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[check_associations]
Queries value:
HKLM\software\clients\startmenuinternet\iexplore.exe\installinfo[showiconscommand]
Queries value:
HKLM\software\clients\startmenuinternet\iexplore.exe\installinfo[iconsvisible]
Queries value: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}[]
Queries value: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-

44ee4615f2c7}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32[threadingmodel]
44ee4615f2c7}\inprocserver32[threadingmodel]
Queries value: HKCR\.url[]
Queries value: HKCR\internetshortcut\shellex\iconhandler[]
Queries value: HKCR\internetshortcut[docobject]
Queries value: HKCR\.url[perceivedtype]
Queries value: HKCR\internetshortcut[browseinplace]
Queries value: HKCR\.url[content type]
Queries value: HKCR\internetshortcut\clsid[]
Queries value: HKCR\internetshortcut[isshortcut]
Queries value: HKCR\internetshortcut[alwaysshowext]
Queries value: HKCR\internetshortcut[nevershowext]
Queries value: HKLM\software\registeredapplications[internet explorer]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\fileassociations[.mht]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\fileassociations[.html]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\fileassociations[.htm]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\fileassociations[.url]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\fileassociations[.mhtml]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\urlassociations[https]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\urlassociations[ftp]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\urlassociations[http]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\mimeassociations[message/rfc822]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\capabilities\mimeassociations[text/html]
Queries value: HKCR\http[editflags]
Queries value: HKCR\http[url protocol]
Queries value: HKCR\http[webnavigableclsid]
Queries value: HKCR\https[editflags]
Queries value: HKCR\https[url protocol]
Queries value: HKCR\ftp[editflags]
Queries value: HKCR\ftp[url protocol]
Queries value: HKCR\internetshortcut[editflags]
Queries value: HKCR\internetshortcut\defaulticon[]
Queries value: HKCR\.htm[content type]
Queries value: HKCR\http\shell\open\command[]
Queries value: HKCR\http\shell\open\ddeexec[]
Queries value: HKCR\http\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\http\shell\open\ddeexec\application[]
Queries value: HKCR\http\shell\open\ddeexec\topic[]
Queries value: HKCR\https\shell\open\command[]
Queries value: HKCR\https\shell\open\ddeexec[]
Queries value: HKCR\https\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\https\shell\open\ddeexec\application[]
Queries value: HKCR\https\shell\open\ddeexec\topic[]
Queries value: HKCR\ftp\shell\open\command[]
Queries value: HKCR\ftp\shell\open\ddeexec[]
Queries value: HKCR\ftp\shell\open\ddeexec\ifexec[]
Queries value: HKCR\ftp\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\ftp\shell\open\ddeexec\application[]
Queries value: HKCR\ftp\shell\open\ddeexec\topic[]
Queries value: HKCR\htmlfile\shell\open[]
Queries value: HKCR\htmlfile\shell\open[muiverb]
Queries value: HKCR\htmlfile\shell\open\command[]
Queries value: HKCR\htmlfile\shell\open\ddeexec[]
Queries value: HKCR\htmlfile\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\htmlfile\shell\open\ddeexec\application[]
Queries value: HKCR\htmlfile\shell\open\ddeexec\topic[]
Queries value: HKCR\mhtmlfile\shell[]
Queries value: HKCR\htmlfile\shell\opennew[]
Queries value: HKCR\htmlfile\shell\opennew[muiverb]
Queries value: HKCR\htmlfile\shell\opennew\command[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec\ifexec[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec[noactivatehandler]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec\application[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec\topic[]
Queries value: HKCR\.mht[]
Queries value: HKCR\.mht[content type]
Queries value: HKCR\.mhtml[]
Queries value: HKCR\.mhtml[content type]
Queries value: HKCR\mhtmlfile\shell\open[]
Queries value: HKCR\mhtmlfile\shell\open[muiverb]
Queries value: HKCR\mhtmlfile\shell\open\command[]
Queries value: HKCR\mhtmlfile\shell\open\ddeexec[]
Queries value: HKCR\mhtmlfile\shell\open\ddeexec\application[]
Queries value: HKCR\mhtmlfile\shell\open\ddeexec\topic[]
Queries value: HKCR\mhtmlfile\shell\opennew[]
Queries value: HKCR\mhtmlfile\shell\opennew[muiverb]
Queries value: HKCR\mhtmlfile\shell\opennew\command[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec\ifexec[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec[noactivatehandler]

Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec\application[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec\topic[]
Queries value: HKCR\internetshortcut\shell\open[clsid]
Queries value: HKCR\internetshortcut\shell\open[legacydisable]
Queries value: HKCR\internetshortcut\shell\open\command[]
Queries value: HKCR\wow6432node\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}[]
Queries value: HKCR\wow6432node\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}[friendlytypename]
Queries value: HKCR\applications\iexplore.exe\shell\open\command[]
Queries value: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32[]
Queries value: HKCU\software\microsoft\internet explorer\suggested
sites[objectscreated]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[sliceath]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[version]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[upgradetime]
Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001[name]
Queries value: HKCU\software\microsoft\internet explorer\user
preferences[2d53cffc5c1a3dd2e97b7979ac2a92bd59bc839e81]
Queries value: HKCU\software\microsoft\internet explorer\user
preferences[88d7d0879dab32e14de5b3a805a34f98aff34f5977]
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\progid[]
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}[]
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\feeds[syncstatus]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
Queries value: HKCU\software\microsoft\internet
explorer\tabbedbrowsing[quicktabslastused]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[parentfolder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[infotip]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[localizedname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[security]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[streamresource]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[streamresourcetype]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[localredirectonly]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[roamable]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[precreate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[stream]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[publishexpandedpath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[attributes]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[foldertypeid]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{a520a1a4-1780-4ff6-bd18-167343c5af16}]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Queries value: HKLM\software\wow6432node\javasoft\java runtime
environment\1.7[javahome]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[jp2launcher]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{22624cac-fe50-451e-9261-e7f22aab93ec}]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{22624cac-fe50-451e-9261-e7f22aab93ec}]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[java]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[gdiobjecthandlequota]
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video0]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video1]
Queries value: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video2]
Queries value: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000[pruningmode]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[65cd4c8a-0848-4583-92a0-31c0fbaf00c0]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers[size]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers[name]
Queries value:
HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist[size]
Queries value:
HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist[name]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers\direct3d_hal[size]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers\direct3d_hal[name]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers\ramp
emulation[size]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers\ramp
emulation[name]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers\rgb_emulation[size]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers\rgb_emulation[name]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[loaddebugruntime]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[forcedriverflagsoff]
Queries value:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode1]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode2]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode3]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode4]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode5]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode6]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode7]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode8]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0000\modes\640,480[mode9]
Queries value:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02\device
parameters[edid]
Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers[softwareonly]
Queries value: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[installeddisplaydrivers]
Queries value: HKLM\software\wow6432node\javasoft\java
update\policy[promptautoupdatecheck]

Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[java.exe]
Queries value: HKCU\control panel\desktop\fontsmoothingorientation
Queries value: HKCU\control panel\desktop\windowmetrics[shell icon bpp]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[themeactive]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[dllname]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[sizename]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[colorname]
Sets/Creates value: HKCU\software\microsoft\internet
explorer\recovery\adminactive[{3f2112f4-f55e-11e5-a3b1-080027b54693}]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cache\path]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cache\prefix]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cache\limit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cache\options]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cache\repair]
Sets/Creates value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[expiration]
Sets/Creates value: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[expiration]
Value changes: HKLM\software\microsoft\rpc[uuidsequencenumber]
Value changes: HKCU\software\microsoft\internet explorer\main[compatibilityflags]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
Value changes: HKCU\software\microsoft\internet explorer\main[fullscreen]
Value changes: HKCU\software\microsoft\internet explorer\main>window_placement]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites\links[order]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[time]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[loadtime]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}\iexplore[time]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}\iexplore[loadtime]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
11cf-aaa5-00401c608501}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
11cf-aaa5-00401c608501}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
11cf-aaa5-00401c608501}\iexplore[time]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cache\path]
Value changes: HKCU\software\microsoft\internet explorer\linksbar\itemcache\0[path]
Value changes: HKCU\software\microsoft\internet explorer\linksbar\itemcache\0[handler]
Value changes: HKCU\software\microsoft\internet explorer\linksbar\itemcache\0[feedurl]
Value changes: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[displayname]
Value changes: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[errorstate]
Value changes: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\0[displaymask]
Value changes: HKCU\software\microsoft\internet explorer\linksbar\itemcache\1[path]
Value changes: HKCU\software\microsoft\internet explorer\linksbar\itemcache\1[handler]
Value changes: HKCU\software\microsoft\internet explorer\linksbar\itemcache\1[feedurl]
Value changes: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[displayname]
Value changes: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[errorstate]
Value changes: HKCU\software\microsoft\internet
explorer\linksbar\itemcache\1[displaymask]
Value changes: HKCU\software\microsoft\direct3d\mostrecentapplication[name]