

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 4, Task ID: 13	
Task ID:	13
Risk Level:	4
Date Processed:	2016-03-29 03:27:45 (UTC)
Processing Time:	61.32 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:	1b7e0322a81be961ebce33aaeb395124544cfb01a3ab54f23cf64400fb2b04c7
Description:	None

## Pattern Matching Results

- 1 YARA score 1
- 2 ZIP archive format
- 4 Reads process memory

## 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\Internet Explorer\IEXPLORE.EXE ["C:\Program Files\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:1740 CREDAT:209921 /prefetch:2]
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=10945206438 -D__applet_launched=10945141997 -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_pid1744_pipe3,read_pipe_name=jpi2_pid1744_pipe2]
Creates process:	C:\Program Files (x86)\Java\jre7\bin\java.exe ["C:\Program Files (x86)\Java\jre7\bin\java.exe" -D__jvm_launched=10945206438 -D__applet_launched=10945141997 "-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_pid1744_pipe3,read_pipe_name=jpi2_pid1744_pipe2]
Creates process:	\SystemRoot\System32\Conhost.exe [??C:\Windows\system32\conhost.exe 0xffffffff]
Reads from process:	PID:1740 C:\Program Files\Internet Explorer\iexplore.exe
Writes to process:	PID:1740 C:\Program Files\Internet Explorer\iexplore.exe
Terminates process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\!BrowserEmulation!SharedMemory!Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_IE_EarlyTabStart_0x650_Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_ConnHashTable<1740>_HashTable_Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects\!PrivacIE!SharedMem!Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_IESQMMUTEX_0_303
Creates mutex:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_IESQMMUTEX_0_331
Creates mutex:	\Sessions\1\BaseNamedObjects\!IECompat!Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_IESQMMUTEX_0_274
Creates mutex:	\Sessions\1\BaseNamedObjects\!SHMSFTHISTORY!_
Creates mutex:	\Sessions\1\BaseNamedObjects\__DDrawExclMode__
Creates mutex:	\Sessions\1\BaseNamedObjects\__DDrawCheckExclMode__
Creates event:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_iso_sm_e_6cc_1401_7d
Creates event:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_IE_EarlyTabStart_0x650
Creates event:	\Sessions\1\BaseNamedObjects\0leDfRoot1AD15B0E8E6AC65
Creates event:	\Sessions\1\BaseNamedObjects\0leDfRootFDfC26A2CE701147
Creates event:	\Sessions\1\BaseNamedObjects\0leDfRootC5E47F2E00B50F60
Creates event:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_iso_sm_e_6cc_11401_7d
Creates event:	\Sessions\1\BaseNamedObjects\IEFrame.EventCheckDefaultBrowser
Creates event:	\Sessions\1\BaseNamedObjects\jpi2_pid1744_evt1
Creates semaphore:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_IEFrame!GetAsyncKeyStateQuery
Creates semaphore:	\Sessions\1\BaseNamedObjects\IsoScope_6cc_IEFrame!GetAsyncKeyStateReply

## File System Events

Creates:	C:\Users\Admin
----------	----------------

Creates: C:\Users\Admin\Favorites  
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\AppData\Roaming\Microsoft\Windows\PrivacIE  
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache  
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatUACache  
Creates: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Active  
Creates: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Active\RecoveryStore.{3A6B4AD6-F55E-11E5-BE82-080027FAC36D}.dat  
Creates: C:\Users\Admin\AppData\Local\Temp\~DF4F3B8B06DE69A3C7.TMP  
Creates: C:\Users\Admin\AppData\Local\Temp\~DFC49DAE6B11C5A7A6.TMP  
Creates: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Active\{3A6B4AD7-F55E-11E5-BE82-080027FAC36D}.dat  
Creates: C:\Users\Admin\AppData\Local\Temp\~DFCE93E6AE6B3AD232.TMP  
Creates: C:\Users\Admin\AppData\Local\Temp\hsperfdata\_Admin  
Creates: C:\Users\Admin\AppData\Local\Temp\hsperfdata\_Admin\1744  
Creates: C:\Users\Admin\AppData\Local\Temp\hsperfdata\_Admin\1976  
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\SysWow64  
Opens: C:\Windows\SysWow64\apphelp.dll  
Opens: C:\Program Files (x86)\Internet Explorer\iexplore.exe  
Opens: C:\Windows\SysWow64\ntdll.dll

Opens: C:\Windows\SysWOW64\kernel32.dll  
Opens: C:\Windows\SysWOW64\KernelBase.dll  
Opens: C:\Windows\apppatch\sysmain.sdb  
Opens: C:\Windows\SysWOW64\msvcrt.dll  
Opens: C:\Windows\SysWOW64\iertutil.dll  
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls  
Opens: C:\Windows\SysWOW64\imm32.dll  
Opens: C:\Program Files (x86)\Internet Explorer\en-US\iexplore.exe.mui  
Opens: C:\Windows\SysWOW64\SHCore.dll  
Opens: C:\Windows\SysWOW64\combase.dll  
Opens: C:\Windows\SysWOW64\sechost.dll  
Opens: C:\Program Files\Internet Explorer\iexplore.exe  
Opens: C:\Windows\apppatch\apppatch64\sysmain.sdb  
Opens: C:\Windows\Prefetch\IEXPLORE.EXE-908C99F8.pf  
Opens: C:  
Opens: C:\\$Extend  
Opens: C:\Program Files  
Opens: C:\Program Files (x86)  
Opens: C:\Program Files (x86)\Internet Explorer  
Opens: C:\Program Files\Internet Explorer  
Opens: C:\Program Files\Internet Explorer\en-US  
Opens: C:\ProgramData  
Opens: C:\ProgramData\Microsoft  
Opens: C:\ProgramData\Microsoft\Windows  
Opens: C:\ProgramData\Microsoft\Windows\Caches  
Opens: C:\Users  
Opens: C:\Users\Admin  
Opens: C:\Users\Admin\AppData  
Opens: C:\Users\Admin\AppData\Local  
Opens: C:\Users\Admin\AppData\Local\Microsoft  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files  
Opens: C:\Users\Admin\AppData\Roaming  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows  
Opens: C:\Users\Admin\Desktop  
Opens: C:\Users\Admin\Favorites  
Opens: C:\Windows\apppatch  
Opens: C:\Windows\apppatch\apppatch64  
Opens: C:\Windows\Fonts  
Opens: C:\Windows\Globalization  
Opens: C:\Windows\Globalization\Sorting  
Opens: C:\Windows\System32  
Opens: C:\Windows\System32\en-US  
Opens: C:\Windows\System32\Macromed  
Opens: C:\Windows\System32\Macromed\Flash  
Opens: C:\Windows\WinSxS\amd64\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_418c2a697189c07f  
Opens: C:\Windows\System32\ntdll.dll  
Opens: C:\Windows\System32\kernel32.dll  
Opens: C:\Windows\System32\KernelBase.dll  
Opens: C:\Windows\System32\locale.nls  
Opens: C:\Windows\System32\apphelp.dll  
Opens: C:\Windows\System32\msvcrt.dll  
Opens: C:\Windows\System32\iertutil.dll  
Opens: C:\Windows\System32\user32.dll  
Opens: C:\Windows\System32\gdi32.dll  
Opens: C:\Windows\System32\imm32.dll  
Opens: C:\Windows\System32\msctf.dll  
Opens: C:\Program Files\Internet Explorer\en-US\iexplore.exe.mui  
Opens: C:\Windows\System32\SHCore.dll  
Opens: C:\Windows\System32\combase.dll  
Opens: C:\Windows\System32\rpcrt4.dll  
Opens: C:\Windows\System32\ieframe.dll  
Opens: C:\Windows\System32\shlwapi.dll  
Opens: C:\Windows\System32\sechost.dll  
Opens: C:\Windows\System32\ole32.dll  
Opens: C:\Windows\System32\oleaut32.dll  
Opens: C:\Windows\System32\shell32.dll  
Opens: C:\Windows\WinSxS\amd64\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_418c2a697189c07f\comctl32.dll  
Opens: C:\Windows\WindowsShell.Manifest  
Opens: C:\Program Files\Internet Explorer\IEShims.dll  
Opens: C:\Windows\System32\comctl32.dll  
Opens: C:\Windows\System32\comdlg32.dll  
Opens: C:\Windows\System32\rpcss.dll  
Opens: C:\Windows\System32\cryptbase.dll  
Opens: C:\Windows\System32\bcryptprimitives.dll  
Opens: C:\Windows\System32\uxtheme.dll  
Opens: C:\Windows\System32\urlmon.dll  
Opens: C:\Windows\System32\wininet.dll  
Opens: C:\Windows\System32\advapi32.dll  
Opens: C:\Windows\System32\dwapi.dll  
Opens: C:\Program Files\Internet Explorer\sqmapi.dll  
Opens: C:\Windows\System32\secur32.dll  
Opens: C:\Windows\System32\sspicli.dll  
Opens: C:\Windows\System32\profapi.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\counters.dat  
Opens: C:\Windows\System32\ws2\_32.dll  
Opens: C:\Windows\System32\ansi.dll  
Opens: C:\Windows\System32\winhttp.dll  
Opens: C:\Windows\System32\IPHLPAPI.DLL  
Opens: C:\Windows\System32\winnsi.dll  
Opens: C:\Windows\System32\mswsock.dll  
Opens: C:\Windows\System32\en-US\ieframe.dll.mui  
Opens: C:\Windows\System32\ieui.dll  
Opens: C:\Windows\System32\cryptsp.dll  
Opens: C:\Windows\System32\rsaenh.dll  
Opens: C:\Windows\System32\clbcatq.dll  
Opens: C:\Program Files\Internet Explorer\ieproxy.dll  
Opens: C:\Windows\System32\oleacc.dll  
Opens: C:\Windows\System32\oleaccrc.dll  
Opens: C:\Windows\Fonts\StaticCache.dat  
Opens: C:\Windows\System32\xmlite.dll  
Opens: C:\Windows\System32\ExplorerFrame.dll  
Opens: C:\Windows\System32\duser.dll  
Opens: C:\Windows\System32\dui70.dll  
Opens: C:\Windows\System32\msimg32.dll  
Opens: C:\Windows\System32\actxprxy.dll  
Opens: C:\Windows\System32\mlang.dll  
Opens: C:\Windows\System32\propsys.dll  
Opens: C:\Windows\System32\mshhtml.dll  
Opens: C:\Windows\System32\setupapi.dll  
Opens: C:\Windows\System32\cfgmgr32.dll  
Opens: C:\Windows\System32\devobj.dll  
Opens: C:\Windows\System32\en-US\setupapi.dll.mui  
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.VER0X0000000000000004.DB  
Opens: C:\Users\desktop.ini  
Opens: C:\Users\Admin\Favorites\desktop.ini  
Opens: C:\Users\Admin\Desktop\desktop.ini  
Opens: C:\Windows\System32\Macromed\Flash\Flash.ocx  
Opens: C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db  
Opens: C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000003.db  
Opens: C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000001.db  
Opens: C:\Windows\System32\Wpc.dll  
Opens: C:\Windows\System32\wevtapi.dll  
Opens: C:\Windows\System32\en-US\oleaccrc.dll.mui  
Opens: C:\Windows\System32\crypt32.dll  
Opens: C:\Windows\System32\msasn1.dll  
Opens: C:\Windows\WinSxS\amd64\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.9200.16384\_none\_7762d5fd3178b04e  
Opens: C:\Windows\WinSxS\amd64\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.9200.16384\_none\_7762d5fd3178b04e\comctl32.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low  
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\Adobe\Flash Player\NativeCache  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Tracking  
Protection  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Feeds  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacyIE\Low  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatUACache\Low  
Opens: C:\Users\Admin\AppData\Local\Temp\Low  
Opens: C:\  
Opens: C:\Windows\Temp  
Opens: C:\Windows\System32\en-US\propsys.dll.mui  
Opens: C:\Windows\Prefetch\IEXPLORE.EXE-4B6C9215.pf  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active  
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)\Common Files\Adobe\Acrobat\ActiveX  
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\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Last Active  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Last Active\RecoveryStore.{28A948A4-AAE6-11E3-BE72-0800275A72F1}.dat  
Opens: C:\Users\Admin\AppData\LocalLow  
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft  
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache  
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content  
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History  
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\41101FRQ

Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies  
Opens: C:\Windows\ServiceProfiles  
Opens: C:\Windows\ServiceProfiles\LocalService  
Opens: C:\Windows\ServiceProfiles\LocalService\AppData  
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local  
Opens: C:\Windows\SysWOW64\en-US  
Opens: C:\Windows\SysWOW64\Macromed  
Opens: C:\Windows\SysWOW64\Macromed\Flash  
Opens:  
C:\Windows\WinSxS\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.6910\_none\_d089c358442de345  
Opens: C:\Windows\WinSxS\x86\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985  
Opens: C:\Windows\System32\wow64win.dll  
Opens: C:\Windows\System32\wow64cpu.dll  
Opens: C:\Windows\SysWOW64\user32.dll  
Opens: C:\Windows\SysWOW64\gdi32.dll  
Opens: C:\Windows\SysWOW64\msctf.dll  
Opens: C:\Windows\SysWOW64\rpcrt4.dll  
Opens: C:\Windows\SysWOW64\sspicli.dll  
Opens: C:\Windows\SysWOW64\cryptbase.dll  
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll  
Opens: C:\Windows\SysWOW64\ieframe.dll  
Opens: C:\Windows\SysWOW64\shlwapi.dll  
Opens: C:\Windows\SysWOW64\ole32.dll  
Opens: C:\Windows\SysWOW64\oleaut32.dll  
Opens: C:\Windows\SysWOW64\shell32.dll  
Opens: C:\Windows\WinSxS\x86\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985\comctl32.dll  
Opens: C:\Program Files (x86)\Internet Explorer\IEShims.dll  
Opens: C:\Windows\SysWOW64\advapi32.dll  
Opens: C:\Windows\SysWOW64\comctl32.dll  
Opens: C:\Windows\SysWOW64\comdlg32.dll  
Opens: C:\Windows\SysWOW64\uxtheme.dll  
Opens: C:\Windows\SysWOW64\wininet.dll  
Opens: C:\Windows\SysWOW64\secur32.dll  
Opens: C:\Windows\SysWOW64\profapi.dll  
Opens: C:\Windows\SysWOW64\urlmon.dll  
Opens: C:\Windows\SysWOW64\ws2\_32.dll  
Opens: C:\Windows\SysWOW64\nsi.dll  
Opens: C:\Windows\SysWOW64\winhttp.dll  
Opens: C:\Windows\SysWOW64\mswsock.dll  
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL  
Opens: C:\Windows\SysWOW64\winnsi.dll  
Opens: C:\Windows\SysWOW64\dwmapi.dll  
Opens: C:\Windows\SysWOW64\cryptsp.dll  
Opens: C:\Windows\SysWOW64\rsaenh.dll  
Opens: C:\Windows\SysWOW64\clbcatq.dll  
Opens: C:\Program Files (x86)\Internet Explorer\ieproxy.dll  
Opens: C:\Program Files (x86)\Internet Explorer\sqmapi.dll  
Opens: C:\Windows\SysWOW64\mshtml.dll  
Opens: C:\Windows\SysWOW64\d2d1.dll  
Opens: C:\Windows\SysWOW64\DWrite.dll  
Opens: C:\Windows\SysWOW64\dxgi.dll  
Opens: C:\Windows\SysWOW64\mlang.dll  
Opens: C:\Windows\SysWOW64\propsys.dll  
Opens: C:\Windows\SysWOW64\dnsapi.dll  
Opens: C:\Program Files (x86)\Common  
Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll  
Opens:  
C:\Windows\WinSxS\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.6910\_none\_d089c358442de345\msvcr80.dll  
Opens:  
C:\Windows\WinSxS\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.6910\_none\_d089c358442de345\msvcp80.dll  
Opens: C:\Program Files (x86)\Common  
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll  
Opens: C:\Program Files (x86)\Java\jre7\bin\jp2ssv.dll  
Opens: C:\Program Files (x86)\Java\jre7\bin\msvcr100.dll  
Opens: C:\Windows\SysWOW64\sxs.dll  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\EKQRWULQ.TXT  
Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL  
Opens: C:\Windows\SysWOW64\stdole2.tlb  
Opens: C:\Windows\SysWOW64\rasadhlp.dll  
Opens: C:\Windows\SysWOW64\actxprxy.dll  
Opens: C:\Windows\SysWOW64\ieui.dll  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\CPSID\_83708[1].HTM  
Opens: C:\Windows\SysWOW64\ninput.dll  
Opens: C:\Windows\SysWOW64\jscript9.dll  
Opens: C:\Windows\SysWOW64\en-US\urlmon.dll.mui  
Opens: C:\Windows\System32\en-US\mshtml.dll.mui  
Opens: C:\Windows\SysWOW64\msimtf.dll  
Opens: C:\Windows\SysWOW64\powrprof.dll  
Opens: C:\Windows\SysWOW64\dcomp.dll  
Opens: C:\Windows\SysWOW64\d3d11.dll  
Opens: C:\Windows\SysWOW64\d3d10warp.dll  
Opens: C:\Windows\SysWOW64\tzres.dll  
Opens: C:\Windows\System32\en-US\tzres.dll.mui

Opens: C:\Windows\SysWOW64\oleacc.dll  
Opens: C:\Windows\SysWOW64\oleaccrc.dll  
Opens: C:\Windows\SysWOW64\vaultcli.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini  
Opens: C:\Windows\System32\en-US\shell32.dll.mui  
Opens: C:\Windows\SysWOW64\setupapi.dll  
Opens: C:\Windows\SysWOW64\cfgmgr32.dll  
Opens: C:\Windows\SysWOW64\devobj.dll  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\RELEASE-NOTES-ACROBAT-READER[1].HTM  
Opens: C:\Windows\SysWOW64\UIAutomationCore.dll  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R\ADOBE-LIGHT-COMPRESSED[1].CSS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R\COMPRESSED[1].CSS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R\ADOBE-CONFIGURATOR-COMPRESSED[1].CSS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\VISITORAPI[2].JS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\MBOX[1].JS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\CHLIMS[1].JS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\HELPPAGE[1].JS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\STATIC[2].CSS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\HELPPAGE[1].CSS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\LOCALE-SPECIFIC[1].CSS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\HELP-SUPPORT[1].CSS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\TYPEKIT-COMPRESSED[2].JS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\S\_CHL\_CODE[2].JS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\0[1].GIF  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R\CC[1].PNG  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT  
Opens: C:\Windows\SysWOW64\WindowsCodecs.dll  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\FAVICON[1].ICO  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\COMPRESSED[1].JS  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\CLIENTLIBS[1].CSS  
Opens: C:\Windows\SysWOW64\Macromed\Flash\Flash.ocx  
Opens: C:\Windows\SysWOW64\version.dll  
Opens: C:\Windows\SysWOW64\winmm.dll  
Opens: C:\Windows\SysWOW64\crypt32.dll  
Opens: C:\Windows\SysWOW64\dsound.dll  
Opens: C:\Windows\SysWOW64\msimg32.dll  
Opens: C:\Windows\SysWOW64\mscms.dll  
Opens: C:\Windows\SysWOW64\winmmbase.dll  
Opens: C:\Windows\SysWOW64\msasn1.dll  
Opens: C:\Windows\SysWOW64\userenv.dll  
Opens: C:\Windows\System32\en-US\KernelBase.dll.mui  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\TV60UTUN.TXT  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\OBPL89B7.TXT  
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\~FontCache-  
System.dat  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\TILE[1].PNG  
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\~FontCache-  
FontFace.dat  
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\~FontCache-S-1-5-  
21-1923240461-1905901954-2556564120-1001.dat  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R\CHL[1].JS  
Opens: C:\Windows\SysWOW64\en-US\jscript9.dll.mui  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\S\_CODE\_CHL[1].JS  
Opens: C:\Windows\Fonts\arial.ttf  
Opens: C:\Windows\SysWOW64\msls31.dll  
Opens: C:\Windows\Fonts\ariali.ttf  
Opens: C:\Windows\Fonts\arialbd.ttf  
Opens: C:\Windows\SysWOW64\iepeers.dll  
Opens: C:\Windows\SysWOW64\mshtml.tlb  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\ZNHTA2NB.TXT  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\COMMUNITYHELP[1].JS  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\17TE3KQ3.TXT  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\BJQC4YWQ.TXT  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\RNOAFXQF.TXT  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\WQVMK9ZX.TXT  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\20UEE020.TXT  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\LOGO[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET

FILES\CONTENT.IE5\41101FRQ\NEW\_WINDOW\_ICON\_BLUE[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R\ICON\_SEARCH\_MOBILE[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\ARROW\_LIGHT[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\CART\_LIGHT[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\P8S8Q01R\TOTHE TOP[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\LXTB75Y0\FOLD-ORANGE[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\SEARCH\_BUTTON[1].PNG  
Opens: C:\Windows\SysWOW64\schannel.dll  
Opens: C:\Windows\SysWOW64\ncrypt.dll  
Opens: C:\Windows\SysWOW64\bcrypt.dll  
Opens: C:\Windows\SysWOW64\ntasn1.dll  
Opens: C:\Windows\SysWOW64\ncryptsslp.dll  
Opens: C:\Windows\SysWOW64\wintrust.dll  
Opens: C:\Windows\SysWOW64\gpapi.dll  
Opens: C:\Windows\System32\en-US\crypt32.dll.mui  
Opens: C:\Windows\SysWOW64\cryptnet.dll  
Opens: C:\Windows\SysWOW64\Wldap32.dll  
Opens:  
C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\FB788E090BC1F3AA2FBC9E8FB2859601  
Opens:  
C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\FB788E090BC1F3AA2FBC9E8FB2859601  
Opens:  
C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1DAF2884EC4DFA96BA4A58D4DBC9C406  
Opens:  
C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1DAF2884EC4DFA96BA4A58D4DBC9C406  
Opens:  
C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D1F03728133589A90656A87E482B21F  
Opens:  
C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D1F03728133589A90656A87E482B21F  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\REGION\_BLUE[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\EVIDON[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\REGION\_BLACK[1].PNG  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\41101FRQ\SSOCHECK[1].TXT  
Opens: C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\YTTZKXT8.TXT  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET  
FILES\CONTENT.IE5\T2095MVJ\PDF[1].GIF  
Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll  
Opens: C:\Windows\SysWOW64\dhcpcsvc.dll  
Opens: C:\Windows\SysWOW64\en-US\mshtml.dll.mui  
Opens: C:\Windows\System32\en-US\urlmon.dll.mui  
Opens: C:\Windows\WinSxS\x86\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_5.82.9200.16384\_none\_bf100cd445f4d954  
Opens: C:\Windows\WinSxS\x86\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_5.82.9200.16384\_none\_bf100cd445f4d954\comctl32.dll  
Opens: C:\Windows\SysWOW64\en-US\ieframe.dll.mui  
Opens: C:\Windows\SysWOW64\en-US\propsys.dll.mui  
Opens: C:\Windows\Temp\test12.jar.html  
Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui  
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui  
Opens: C:\Program Files (x86)\Java\jre7\bin\jp2iexp.dll  
Opens: C:\Program Files (x86)\Java\jre7\bin\client  
Opens: C:\Program Files (x86)\Java\jre7\bin\client\jvm.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-  
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000010.db  
Opens: C:\Windows\SysWOW64\en-US\shell32.dll.mui  
Opens: C:\Windows\System32\url.dll  
Opens: C:\Windows\SysWOW64\wsock32.dll  
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:\Users\Admin\AppData\Local\Temp\hsperfdata\_Admin  
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:\Program Files (x86)\Java\jre7\bin\client\classes.jsa  
Opens: C:\Program Files (x86)\Java\jre7\lib\rt.jar  
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:\Program Files (x86)\Java\jre7\bin\deploy.dll  
Opens: C:\Program Files (x86)\Java\jre7\bin\jp2native.dll  
Opens:  
C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\deployment.properties  
Opens: C:\Program Files (x86)\Java\jre7\bin\net.dll  
Opens: C:\Program Files (x86)\Java\jre7\bin\nio.dll  
Opens: C:\Program Files\Java  
Opens: C:\Program Files\Java\jre7  
Opens: C:\Program Files\Java\jre7\bin  
Opens: C:\Program Files (x86)\Java\jre7\lib\security\java.security

Opens: C:\Program Files (x86)\Java\jre7\bin\jp2launcher.exe  
Opens: C:\Windows\Prefetch\JP2LAUNCHER.EXE-6240744E.pf  
Opens: C:\Windows\apppatch\AcLayers.dll  
Opens: C:\Windows\SysWOW64\mpr.dll  
Opens: C:\Windows\SysWOW64\sfc.dll  
Opens: C:\Windows\SysWOW64\winspool.drv  
Opens: C:\Windows\SysWOW64\sfc\_os.dll  
Opens: C:\Program Files (x86)\Java\jre7\bin\java.exe  
Opens: C:\Program Files (x86)\Java\jre7\bin\jpishare.dll  
Opens: C:\Windows\Prefetch\JAVA.EXE-07FE5A9A.pf  
Opens: C:\Program Files (x86)\Java\jre7\lib\i386  
Opens: C:\Program Files (x86)\Java\jre7\lib\security  
Opens: C:\Users\Admin\AppData\LocalLow\Sun  
Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java  
Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment  
Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\cache  
Opens: C:\Users\Admin\AppData\Local\Temp  
Opens: C:\Program Files (x86)\Java\jre7\lib\i386\jvm.cfg  
Opens: C:\Windows\SysWOW64\psapi.dll  
Opens: C:\Program Files (x86)\Java\jre7\bin\awt.dll  
Opens: C:\Windows\apppatch\AcGeneral.dll  
Opens: C:\Windows\SysWOW64\samcli.dll  
Opens: C:\Windows\SysWOW64\msacm32.dll  
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\TEMP\HSPERFDATA\_ADMIN\2456  
Opens: C:\Windows\SysWOW64\d3d9.dll  
Opens: C:\Program Files (x86)\Java\jre7\lib\net.properties  
Opens: C:\Program Files (x86)\Java\jre7\lib\security\java.policy  
Opens: C:\Program Files (x86)\Java\jre7\bin\fontmanager.dll  
Opens: C:\Program Files (x86)\Java\jre7\lib\fontconfig.bfc  
Opens: C:\Windows\System32\dpapi.dll  
Opens: C:\Windows\System32\conhost.exe  
Opens: C:\Windows\System32\en-US\conhost.exe.mui  
Opens: C:\Windows\System32\java.exe  
Opens: C:\Users\Admin\accessibility.properties  
Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui  
Opens: C:\Program Files (x86)\Java\jre7\lib\accessibility.properties  
Opens: C:\Windows\Sun  
Opens: C:\Windows\Sun\Java  
Opens: C:\Users\Admin\java.policy  
Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\security\java.policy  
Opens: C:\Program Files (x86)\Java\jre7\lib\management  
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\fonts  
Opens: C:\Program Files (x86)\Java\jre7\lib\applet  
Opens: C:\Windows\Sun\Java\Deployment  
Opens: C:\Program Files (x86)\Java\jre7\lib\currency.data  
Opens: C:\Windows\Temp\test12.jar.exe  
Opens: C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\security  
Opens: C:\Program Files (x86)\Java\jre7\lib\security\blacklist  
Opens: C:\Program Files (x86)\Java\jre7\lib\security\trusted.libraries  
Opens: C:\Program Files (x86)\Java\jre7\lib\jsse.jar  
Opens: C:\Program Files (x86)\Java\jre7\bin\t2k.dll  
Opens: C:\Windows\Fonts\wingding.ttf  
Opens: C:\Windows\Fonts\symbol.ttf  
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Active\RecoveryStore.{3A6B4AD6-F55E-11E5-BE82-080027FAC36D}.dat  
Writes to: C:\Users\Admin\AppData\Local\Temp\~DF4F3B8B06DE69A3C7.TMP  
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Active\{3A6B4AD7-F55E-11E5-BE82-080027FAC36D}.dat  
Writes to: C:\Users\Admin\AppData\Local\Temp\~DFCE93E6AE6B3AD232.TMP  
Reads from: C:\Windows\Prefetch\IEXPLORE.EXE-908C99F8.pf  
Reads from: C:\Windows\Prefetch\IEXPLORE.EXE-4B6C9215.pf  
Reads from: C:\Windows\Fonts\StaticCache.dat  
Reads from: C:\Users\Admin\AppData\Local\Temp\~DF4F3B8B06DE69A3C7.TMP  
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Active\RecoveryStore.{3A6B4AD6-F55E-11E5-BE82-080027FAC36D}.dat  
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Last Active\RecoveryStore.{28A948A4-AAE6-11E3-BE72-0800275A72F1}.dat  
Reads from: C:\Users\Admin\AppData\Local\Temp\~DFCE93E6AE6B3AD232.TMP  
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Internet  
Explorer\Recovery\High\Active\{3A6B4AD7-F55E-11E5-BE82-080027FAC36D}.dat  
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:\Users\desktop.ini  
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini  
Reads from: C:\Users\Admin\Favorites\desktop.ini  
Reads from: C:\Users\Admin\Desktop\desktop.ini  
Reads from: C:\Program Files (x86)\Java\jre7\lib\meta-index  
Reads from: C:\Program Files (x86)\Java\jre7\bin\client\classes.jsa  
Reads from: C:\Program Files (x86)\Java\jre7\lib\rt.jar  
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:\Windows\Prefetch\JP2LAUNCHER.EXE-6240744E.pf
Reads from:	C:\Program Files (x86)\Java\jre7\bin\java.exe
Reads from:	C:\Windows\Prefetch\JAVA.EXE-07FE5A9A.pf
Reads from:	C:\Program Files (x86)\Java\jre7\lib\i386\jvm.cfg
Reads from:	C:\Program Files (x86)\Java\jre7\bin\awt.dll
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\appdata\low\software\microsoft\internet explorer
Creates key:	HKCU\software\appdata\low\software\microsoft\repsservice
Creates key:	HKCU\software\microsoft\feeds
Creates key:	HKCU\software\microsoft\internet explorer\browseremulation\lowmic
Creates key:	HKCU\software\microsoft\internet explorer\gpu
Creates key:	HKCU\software\microsoft\internet explorer\ieltld\lowmic
Creates key:	HKCU\software\microsoft\internet explorer\intelliforms
Creates key:	HKCU\software\microsoft\internet explorer\internetregistry
Creates key:	HKCU\software\microsoft\internet explorer\lowregistry
Creates key:	HKCU\software\microsoft\internet explorer\lowregistry\domstorage
Creates key:	HKCU\software\microsoft\internet explorer\lowregistry\dontshowmethisdialogagain
Creates key:	HKCU\software\microsoft\internet explorer\pagesetup
Creates key:	HKCU\software\microsoft\internet explorer\toolbar
Creates key:	HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Creates key:	HKCU\software\microsoft\internet explorer\zoom
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
Creates key:	HKCU\software\microsoft\windows\currentversion\ext
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache
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\internet settings\zones
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\zonemap\
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:	HKLM\system\currentcontrolset\services\tcpip\parameters
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKLM\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
Deletes value:	HKLM\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
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[autoconfigur1]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[autodetect]
Deletes value:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\iexplore.exe
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\software\microsoft\windows nt\currentversion\appcompatflags\dbglog  
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dllexportoptions  
Opens key: HKLM\  
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\windows\currentversion\internet settings  
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings  
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  
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\system\currentcontrolset\control\nls\extendedlocale  
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids  
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 compatibility  
Opens key: HKLM\system\currentcontrolset\control\lsa\lipsalgorithmpolicy  
Opens key: HKLM\system\currentcontrolset\control\lsa  
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration  
Opens key: HKLM\software\wow6432node\microsoft\ole  
Opens key: HKLM\software\microsoft\ole  
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing  
Opens key: HKLM\software\microsoft\ole\tracing  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe\perfoptions  
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: HKLM\software\microsoft\windows\currentversion\sidebyside  
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol  
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_enablesafesearchpath\_kb963027  
Opens key: HKLM\system\currentcontrolset\control\error message instrument\  
Opens key: HKLM\system\currentcontrolset\control\error message instrument  
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize  
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32  
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility  
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows  
Opens key: HKLM\software\policies  
Opens key: HKCU\software\policies  
Opens key: HKCU\software  
Opens key: HKLM\software  
Opens key: HKLM\software\wow6432node  
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\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\microsoft\internet explorer\main  
Opens key: HKLM\software\microsoft\windows\currentversion\policies\system  
Opens key: HKCU\software\microsoft\internet explorer\setup  
Opens key: HKLM\system\currentcontrolset\control\session manager  
Opens key: HKLM\software\microsoft\oleaut  
Opens key:  
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\msinternal\_metro\_allow\_tpg\_zero  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\msinternal\_metro\_allow\_tpg\_zero  
Opens key: HKLM\software\microsoft\rpc  
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername  
Opens key: HKLM\system\setup  
Opens key: HKLM\software\policies\microsoft\windows nt\rpc  
Opens key: HKLM\software\policies\microsoft\sqmclient\windows  
Opens key: HKLM\software\microsoft\sqmclient\windows  
Opens key: HKLM\software\policies\microsoft\internet explorer\safety\privacie  
Opens key: HKCU\software\policies\microsoft\internet explorer\safety\privacie  
Opens key: HKCU\software\microsoft\internet explorer\safety\privacie  
Opens key: HKLM\software\microsoft\internet explorer\safety\privacie  
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation  
Opens key: HKCU\software\microsoft\internet explorer\sqm  
Opens key: HKLM\software\microsoft\internet explorer\sqm  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}\propertybag  
Opens key: HKLM\software\microsoft\windows\currentversion  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\knownfolderssettings  
Opens key: HKCU\software\microsoft\internet explorer  
Opens key: HKLM\software\microsoft\internet explorer  
Opens key: HKLM\software\microsoft\windows\currentversion\internet  
settings\5.0\cache  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}  
Opens key:  
HKLM\software\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: HKU\  
Opens key: HKU\default  
Opens key: HKU\default\software\microsoft\windows\currentversion\explorer\user  
shell folders  
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_bypass\_cache\_for\_credpolicy\_kb936611  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_bypass\_cache\_for\_credpolicy\_kb936611  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_ignore\_mappings\_for\_credpolicy  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_ignore\_mappings\_for\_credpolicy  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_bufferbreaking\_818408  
Opens key: HKLM\software\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\microsoft\internet  
explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954

Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289  
Opens key: HKLM\software\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\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_allow\_long\_international\_filenames  
Opens key: HKLM\software\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\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\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\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\microsoft\internet  
explorer\main\featurecontrol\feature\_digest\_no\_extras\_in\_uri  
Opens key: HKLM\software\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\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\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_utf8\_for\_basic\_auth\_kb967545  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_preserve\_spaces\_in\_filenames\_kb952730  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_preserve\_spaces\_in\_filenames\_kb952730  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings  
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings  
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\_disable\_notify\_unverified\_spn\_kb2385266  
Opens key: HKLM\software\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\microsoft\internet  
explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_sch\_send\_aux\_record\_kb\_2618444  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_sch\_send\_aux\_record\_kb\_2618444  
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\29bc6c5a-15708810  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\29bc6c5a  
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\_entries64  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000001  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000002  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000003  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000004  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000005  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000006  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000007

Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000008  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000009  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000010  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000014  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000001  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000002  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000003  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000004  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000005  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000006  
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock  
Opens key: HKLM\software\policies\microsoft\internet explorer\searchscopes  
Opens key: HKCU\software\microsoft\internet explorer\searchscopes  
Opens key: HKLM\software\microsoft\internet explorer\searchscopes  
Opens key: HKCU\software\microsoft\internet  
explorer\browseremulation\clearablelistdata  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip6  
Opens key: HKCU\software\microsoft\internet explorer\browseremulation  
Opens key: HKLM\software\microsoft\internet explorer\browseremulation  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}\propertybag  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\propertybag  
Opens key: HKLM\software\policies\microsoft\windows\explorer  
Opens key: HKCU\software\policies\microsoft\windows\explorer  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag  
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag  
Opens key: HKCU\software\classes\  
Opens key: HKCU\software\classes\appid\iexplore.exe  
Opens key: HKCR\appid\iexplore.exe  
Opens key: HKLM\software\microsoft\ole\appcompat  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}  
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong  
cryptographic provider  
Opens key: HKLM\software\policies\microsoft\cryptography  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}  
Opens key: HKLM\software\microsoft\cryptography  
Opens key: HKLM\software\microsoft\cryptography\offload  
Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}  
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32  
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32  
Opens key: HKLM\software\microsoft\rpc\extensions  
Opens key: HKCU\software\classes\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}  
Opens key: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}  
Opens key: HKCU\software\classes\interface\{1ac7516e-e6bb-4a69-b63f-

e841904dc5a6}\proxystubclsid32  
Opens key: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32  
Opens key: HKLM\software\microsoft\com3  
Opens key: HKLM\software\microsoft\windowsruntime\clsid  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}  
e4fddd701cba}  
Opens key: HKCR\activatableclasses\clsid  
Opens key: HKCR\activatableclasses\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}  
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}\treatas  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag  
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas  
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32  
e4fddd701cba}\inprocserver32  
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32  
e4fddd701cba}\inprochandler32  
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler  
e4fddd701cba}\inprochandler  
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag  
Opens key: HKLM\software\policies\microsoft\internet explorer\toolbars\restrictions  
Opens key: HKCU\software\microsoft\internet explorer\toolbars\restrictions  
Opens key: HKLM\software\microsoft\internet explorer\toolbars\restrictions  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\toolbar  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\discordable\postsetup\component categories\{00021493-0000-0000-c000-000000000046}\enum  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\discordable\postsetup\component categories64\{00021493-0000-0000-c000-000000000046}\enum  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\discordable\postsetup\component categories\{00021494-0000-0000-c000-000000000046}\enum  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\discordable\postsetup\component categories64\{00021494-0000-0000-c000-000000000046}\enum  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\browser helper objects\{18df081c-e8ad-4283-a596-fa578c2ebdc3}  
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\browser helper objects\{dbc80044-a445-435b-bc74-9c25c1c588a9}  
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\browser helper objects  
Opens key: HKCU\software\microsoft\internet explorer\approvedextensionsmigration  
Opens key: HKLM\software\microsoft\internet explorer\migration  
Opens key: HKLM\software\microsoft\internet explorer\extension compatibility\{18df081c-e8ad-4283-a596-fa578c2ebdc3}  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\extension compatibility\{18df081c-e8ad-4283-a596-fa578c2ebdc3}  
Opens key: HKLM\software\microsoft\internet explorer\extension compatibility\{dbc80044-a445-435b-bc74-9c25c1c588a9}  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\extension compatibility\{dbc80044-a445-435b-bc74-9c25c1c588a9}  
Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation  
Opens key: HKLM\software\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\microsoft\internet explorer\main\featurecontrol\feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915  
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\zonemap\ranges\  
Opens key: HKCU\zonemap\ranges\  
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\policies\microsoft\windows\currentversion\internet settings\zones\  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

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

settings\zones\0  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\0  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zones\1  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\1  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap\  
 Opens key: HKLM\software\microsoft\windows\currentversion\internet

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

settings\zones\2  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\2  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zones\3  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\3  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zones\4  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\4  
 Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_localmachine\_lockdown  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\lockdown\_zones\  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\lockdown\_zones\0  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\0  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\0  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\lockdown\_zones\1  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\1  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\1  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\lockdown\_zones\2  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\2  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\2  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\lockdown\_zones\3  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\3  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\3  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\lockdown\_zones\4  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\4  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\lockdown\_zones\4  
 Opens key: HKCU\software\microsoft\internet explorer\security

Opens key: HKLM\software\microsoft\internet explorer\security

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562  
 Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562  
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\iexplore.exe  
 Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key: HKCR\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\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key: HKCU\software\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\{d5291c64-7c88-11e3-be65-806e6f6e963}\

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\advanced
Opens key: HKCU\software\classes\directory
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: HKLM\software\microsoft\windows\currentversion\explorer\kindmap
Opens key: HKCU\software\classes\.html
Opens key: HKCR\.html
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
Opens key: HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
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}\treatas
Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr
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\microsoft\windows\shell\associations
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\systemfileassociations\document\docobject
Opens key: HKCR\systemfileassociations\document\docobject
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\systemfileassociations\document\browseinplace
Opens key: HKCR\systemfileassociations\document\browseinplace
Opens key: HKCU\software\classes\htmlfile\clsid
Opens key: HKCR\htmlfile\clsid
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented

```



categories\{00021490-0000-0000-c000-000000000046}  
Opens key: HKLM\software\microsoft\windows\currentversion\setup  
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}  
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\properties  
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags  
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\iexplore.exe  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-11e3-be65-806e6f6e6963}\  
Opens key: HKLM\software\microsoft\directui  
Opens key: HKCU\software\microsoft\authcookies\live\default\caw  
Opens key: HKCU\software\microsoft\authcookies\live\default\didc  
Opens key: HKCU\software\classes\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}  
Opens key: HKCR\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}  
Opens key: HKCU\software\classes\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32  
Opens key: HKCR\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32  
Opens key: HKLM\software\policies\microsoft\internet explorer\tabbedbrowsing  
Opens key: HKCU\software\microsoft\internet explorer\tabbedbrowsing  
Opens key: HKLM\software\microsoft\internet explorer\tabbedbrowsing  
Opens key: HKCU\software\microsoft\internet explorer\main\windowssearch  
Opens key: HKLM\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\microsoft\internet explorer\feeds  
Opens key: HKLM\software\microsoft\windows search  
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist  
Opens key: HKLM\software\policies\microsoft\internet explorer\minie  
Opens key: HKCU\software\microsoft\internet explorer\minie  
Opens key: HKLM\software\microsoft\internet explorer\minie  
Opens key: HKCU\software\microsoft\windows\currentversion\policies\ieak  
Opens key: HKLM\software\microsoft\windows\currentversion\policies\ieak  
Opens key: HKLM\software\policies\microsoft\internet explorer\commandbar  
Opens key: HKCU\software\microsoft\internet explorer\commandbar  
Opens key: HKLM\software\microsoft\internet explorer\commandbar  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}  
Opens key: HKCR\activatableclasses\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}  
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}\treatas  
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\treatas  
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32  
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler32  
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler  
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler  
Opens key: HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32  
Opens key: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32  
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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_zones\_check\_zonemap\_policy\_kb941001  
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_zones\_check\_zonemap\_policy\_kb941001  
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\policies\microsoft\windows\currentversion\internet settings\zonemap\  
Opens key: HKLM\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\microsoft\windows\currentversion\internet settings\zonemap\domains\  
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes  
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: HKCU\software\microsoft\internet explorer\searchurl  
Opens key: HKLM\software\policies\microsoft\internet explorer\infodelivery\restrictions

Opens key: HKCU\software\policies\microsoft\internet  
explorer\infodelivery\restrictions  
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\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}  
Opens key: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}  
Opens key: HKLM\software\policies\microsoft\internet explorer\toolbar  
Opens key: HKCU\software\microsoft\internet explorer\toolbar  
Opens key: HKCU\software\policies\microsoft\internet explorer\toolbars\restrictions  
Opens key: HKLM\software\policies\microsoft\internet explorer\linksbar  
Opens key: HKCU\software\microsoft\internet explorer\linksexplorer  
Opens key: HKLM\software\microsoft\internet explorer\linksexplorer  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}  
Opens key: HKCR\activatableclasses\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}  
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}\treatas  
Opens key: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\treatas  
Opens key: HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32  
Opens key: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprochandler32  
Opens key: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprochandler  
Opens key: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprochandler  
Opens key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser  
Opens key: HKLM\software\microsoft\internet explorer\setup\flashupdated  
Opens key: HKLM\software\microsoft\ctf\compatibility\iexplore.exe  
Opens key: HKLM\software\microsoft\ctf\  
Opens key: HKLM\software\microsoft\ctf\knownclasses  
Opens key: HKLM\software\wow6432node\policies  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\low rights  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0002df01-0000-0000-c000-000000000046}  
Opens key: HKCR\activatableclasses\clsid\{0002df01-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}  
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}\treatas  
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\treatas  
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}\inprocserver32  
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}\inprochandler32  
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}\inprochandler  
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\inprochandler  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}  
Opens key: HKCR\activatableclasses\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}  
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}\treatas  
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\treatas  
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprocserver32  
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler32  
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler  
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler  
Opens key: HKCU\software\microsoft\internet explorer\recovery\admininactive  
Opens key: HKLM\software\policies\microsoft\internet explorer\iedevtools  
Opens key: HKCU\software\microsoft\internet explorer\iedevtools  
Opens key: HKLM\software\microsoft\internet explorer\iedevtools  
Opens key: HKLM\software\policies\microsoft\internet explorer\continuousbrowsing  
Opens key: HKCU\software\microsoft\internet explorer\continuousbrowsing  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\content  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\cookies  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\history  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\system  
Opens key: HKCU\software\classes\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}  
Opens key: HKCR\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}  
Opens key: HKCU\software\classes\interface\{a168aad-1674-49da-ad4f-

4f27df8760d0}\proxystubclsid32  
Opens key: HKCR\interface\{a168aad0-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}  
60ce2149e33c}  
Opens key: HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}  
Opens key: HKCU\software\classes\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}  
Opens key: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}  
Opens key: HKCU\software\classes\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas  
Opens key: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas  
Opens key: HKCU\software\classes\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32  
Opens key: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler32  
Opens key: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler  
Opens key: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler  
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file  
execution options\iexplore.exe  
Opens key: HKCU\software\classes\htmlfile\shellex\{000214f9-0000-0000-c000-000000000046}  
000000000046}  
Opens key: HKCR\htmlfile\shellex\{000214f9-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\.html\shellex\{000214f9-0000-0000-c000-000000000046}  
000000000046}  
Opens key: HKCR\.html\shellex\{000214f9-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\systemfileassociations\.html\shellex\{000214f9-0000-0000-c000-000000000046}  
000000000046}  
Opens key: HKCR\systemfileassociations\.html\shellex\{000214f9-0000-0000-c000-000000000046}  
000000000046}  
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\shellfolder  
00aa00686f13}\shellfolder  
Opens key: HKCR\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\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}  
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\microsoft\windows\currentversion\internet settings\url  
history  
Opens key: HKCU\software\classes\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}  
Opens key: HKCR\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}  
Opens key: HKCU\software\classes\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}\proxystubclsid32  
Opens key: HKCR\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{036438a5-d9ac-4353-a567-69298fdaa990}  
Opens key: HKCR\interface\{036438a5-d9ac-4353-a567-69298fdaa990}  
Opens key: HKCU\software\classes\interface\{036438a5-d9ac-4353-a567-69298fdaa990}\proxystubclsid32  
Opens key: HKCR\interface\{036438a5-d9ac-4353-a567-69298fdaa990}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}  
Opens key: HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}  
Opens key: HKCU\software\classes\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32  
Opens key: HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}  
Opens key: HKCR\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}  
Opens key: HKCU\software\classes\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}\proxystubclsid32  
Opens key: HKCR\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}\proxystubclsid32  
Opens key: HKLM\software\wow6432node\microsoft\oleaut  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\msinternal\_metro\_allow\_tpg\_zero  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings  
Opens key: HKLM\software\wow6432node\microsoft\rpc  
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\cache  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedc9d}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-

33be-4251-ba85-6007caedcf9d)\propertybag  
Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\profilelist  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_bypass\_cache\_for\_credpolicy\_kb936611  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_ignore\_mappings\_for\_credpolicy  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_bufferbreaking\_818408  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_allow\_long\_international\_filenames  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_permit\_cache\_for\_authenticated\_ftp\_kb910274  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disallow\_null\_in\_response\_headers  
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: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_exclude\_invalid\_client\_cert\_kb929477  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_utf8\_for\_basic\_auth\_kb967545  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_preserve\_spaces\_in\_filenames\_kb952730  
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_sch\_send\_aux\_record\_kb\_2618444  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\1a677c0f-1473d5b3  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\1a677c0f  
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\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: HKLM\software\wow6432node\microsoft\ole\appcompat

Opens key:  
HKLM\software\wow6432node\microsoft\cryptographic\defaults\provider\microsoft strong cryptographic provider  
Opens key: HKLM\software\wow6432node\microsoft\cryptographic\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\rpc\extensions  
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}\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: 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:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_gpu\_rendering  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_gpu\_rendering  
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\_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: HKCU\software\microsoft\windows\currentversion\settingsync\namespace\browsersettings\wininet-internet-explorer  
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\internet  
explorer\main\featurecontrol\feature\_download\_initiator\_http\_header  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_download\_initiator\_http\_header  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mobile\_customizations  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mobile\_customizations  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_high\_resolution\_aware  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_high\_resolution\_aware  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_force\_disable\_untrustedprotocol  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_force\_disable\_untrustedprotocol  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_weboc\_omnavigator\_implementation  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_weboc\_omnavigator\_implementation  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_security\_thunks  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_security\_thunks  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_deferred\_image\_download  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_deferred\_image\_download  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_lazy\_image\_decoding  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_lazy\_image\_decoding  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_allow\_intranet\_css\_mime\_mismatch  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_allow\_intranet\_css\_mime\_mismatch  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_clipchildren\_optimization  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_clipchildren\_optimization  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_larger\_hit\_test  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_larger\_hit\_test  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_legacy\_jscript  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_legacy\_jscript  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mobile\_viewport\_width\_restrictions  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mobile\_viewport\_width\_restrictions  
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: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_xdomainrequest  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_xdomainrequest  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_websocket  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_websocket

Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_uniscribe  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_uniscribe  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_ninput\_legacymode  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_ninput\_legacymode  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_direct\_composition  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_direct\_composition  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_hang\_recovery\_touch\_mitigation  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_hang\_recovery\_touch\_mitigation  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_paint\_inside\_wmpaint  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_paint\_inside\_wmpaint  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_software\_filter\_rendering  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_software\_filter\_rendering  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_spellchecking  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_spellchecking  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_structure\_node\_child\_count  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_structure\_node\_child\_count  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_tune\_hang\_recovery\_touch\_mitigation  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_tune\_hang\_recovery\_touch\_mitigation  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_force\_natural\_text\_metrics  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_force\_natural\_text\_metrics  
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\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\policies\microsoft\internet explorer\persistance  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\persistance  
Opens key: HKLM\software\policies\microsoft\internet explorer\persistance  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\safety\privacie  
Opens key: HKCU\software\microsoft\internet explorer\safety\privacie\lists  
Opens key: HKLM\system\currentcontrolset\services\fontcache\parameters  
Opens key: HKCU\software\microsoft\direct3d  
Opens key: HKLM\software\wow6432node\microsoft\direct3d  
Opens key: HKLM\software\wow6432node\microsoft\direct3d\drivers  
Opens key: HKCU\software\classes\wow6432node\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}  
Opens key: HKCR\wow6432node\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}  
Opens key: HKCU\software\classes\wow6432node\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}\proxystubclsid32  
Opens key: HKCR\wow6432node\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}\proxystubclsid32  
Opens key: HKCU\software\classes\wow6432node\interface\{036438a5-d9ac-4353-a567-69298fdaa990}  
Opens key: HKCR\wow6432node\interface\{036438a5-d9ac-4353-a567-69298fdaa990}  
Opens key: HKCU\software\classes\wow6432node\interface\{036438a5-d9ac-4353-a567-69298fdaa990}\proxystubclsid32  
Opens key: HKCR\wow6432node\interface\{036438a5-d9ac-4353-a567-69298fdaa990}\proxystubclsid32  
Opens key: HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist  
Opens key: HKCU\software\microsoft\dxgi  
Opens key: HKLM\software\wow6432node\microsoft\dxgi  
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: HKLM\software\wow6432node\microsoft\ole\appcompat\inputmessages  
Opens key: HKLM\software\microsoft\ole\appcompat\inputmessages  
Opens key: HKCU\software\classes\wow6432node\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}  
Opens key: HKCR\wow6432node\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}

Opens key: HKCU\software\classes\wow6432node\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}\proxystubclsid32

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

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

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\iexplore.exe

Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key: HKCR\wow6432node\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: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum

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

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}\inprocserver32

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

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\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\restrictions

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

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

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

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

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects\{18df081c-e8ad-4283-a596-fa578c2ebdc3}

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: HKCU\software\microsoft\windows\currentversion\policies\ext

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

Opens key: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}

Opens key: HKCR\activatableclasses\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}

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: 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: HKLM\software\microsoft\windowsruntime\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}

Opens key: HKCR\activatableclasses\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}



```

Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}
784b7d6be0b3}
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\treatas
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}\inprochandler32
784b7d6be0b3}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler32
784b7d6be0b3}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler
784b7d6be0b3}\inprochandler
Opens key: HKCR\wow6432node\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler
784b7d6be0b3}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32
9c25c1c588a9}\inprocserver32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
9c25c1c588a9}
Opens key: HKCR\activatableclasses\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
9c25c1c588a9}
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\treatas
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
9c25c1c588a9}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
9c25c1c588a9}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
9c25c1c588a9}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler
9c25c1c588a9}\inprochandler
Opens key: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler
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: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore
4283-a596-fa578c2ebdc3}\iexplore
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
abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbcb}\inprocserver32
abcdeffedcbcb}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbcb}\inprocserver32
abcdeffedcbcb}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
00805f499d93}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}\inprocserver32
abcdeffedcba}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbcb}\inprocserver32
abcdeffedcbcb}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbcb}\inprocserver32
abcdeffedcbcb}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
00805f499d93}\inprocserver32
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore
435b-bc74-9c25c1c588a9}\iexplore
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKCU\software\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\classes\typelib
Opens key: HKCU\software\microsoft\internet explorer\mao settings
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
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
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
explorer\main\featurecontrol\feature_iedde_register_protocol
Opens key: HKCR\wow6432node\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}\inprocserver32
00aa004ae837}\inprocserver32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shell
extensions\blocked
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
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: HKLM\software\microsoft\windowsruntime\clsid\{e7e4bc40-e76a-11ce-a9bb-  
00aa004ae837}  
Opens key: HKCR\activatableclasses\clsid\{e7e4bc40-e76a-11ce-a9bb-00aa004ae837}  
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}\inprocserver32  
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:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{e7e4bc40-  
e76a-11ce-a9bb-00aa004ae837}  
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:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\  
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: 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\wow6432node\microsoft\windows\currentversion\internet  
settings\zonemap\  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zonemap\domains\  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_browser\_compatdata  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_browser\_compatdata  
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:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\  
Opens key: HKLM\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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet  
settings\lockdown\_zones\  
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings\lockdown\_zones  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet  
settings\lockdown\_zones\0  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet  
settings\lockdown\_zones\1  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet  
settings\lockdown\_zones\2  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet  
settings\lockdown\_zones\3  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet  
settings\lockdown\_zones\4

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:  
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: 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: HKLM\software\microsoft\windowsruntime\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}  
Opens key: HKCR\activatableclasses\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}  
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}\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\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\classes\protocols\name-space handler\file\  
Opens key: HKCR\protocols\name-space handler\file  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_fileprotocol\_nofindfirst\_kb947853  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_fileprotocol\_nofindfirst\_kb947853  
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: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\3  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}  
Opens key: HKCR\activatableclasses\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}  
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}\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\_olealias\_gwnd  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_olealias\_gwnd  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_topmost\_gwnd  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_topmost\_gwnd  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_aligned\_timers

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_aligned\_timers  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap  
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\flipahead  
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\_use\_qme\_for\_toplevel\_docs  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_use\_qme\_for\_toplevel\_docs  
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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_weboc\_document\_zoom  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_weboc\_document\_zoom  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_vsync\_watchdog  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_vsync\_watchdog  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_allow\_highfreq\_timers  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_allow\_highfreq\_timers  
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\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\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\internet explorer\text scaling  
Opens key: HKCU\software\microsoft\internet explorer\viewport  
Opens key: HKCU\software\microsoft\internet explorer\larger hit test  
Opens key: HKCU\software\microsoft\internet explorer\script  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\advancedoptions\disambiguation  
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: HKLM\system\currentcontrolset\control\nls\codepage  
Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3  
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: HKLM\software\microsoft\windowsruntime\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}  
Opens key: HKCR\activatableclasses\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}  
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}\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: HKCU\software\microsoft\windows\currentversion\explorer\travellog  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\travellog  
Opens key: HKCU\software\classes\interface\{d3e09618-273f-4a13-a7d2-29f90ed68e8a}  
Opens key: HKCR\interface\{d3e09618-273f-4a13-a7d2-29f90ed68e8a}  
Opens key: HKCU\software\classes\interface\{d3e09618-273f-4a13-a7d2-

29f90ed68e8a}\proxystubclsid32  
Opens key: HKCR\interface\{d3e09618-273f-4a13-a7d2-29f90ed68e8a}\proxystubclsid32  
Opens key: HKCU\software\classes\wow6432node\interface\{d3e09618-273f-4a13-a7d2-  
29f90ed68e8a}  
Opens key: HKCR\wow6432node\interface\{d3e09618-273f-4a13-a7d2-29f90ed68e8a}  
Opens key: HKCU\software\classes\wow6432node\interface\{d3e09618-273f-4a13-a7d2-  
29f90ed68e8a}\proxystubclsid32  
Opens key: HKCR\wow6432node\interface\{d3e09618-273f-4a13-a7d2-  
29f90ed68e8a}\proxystubclsid32  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}  
Opens key: HKCR\activatableclasses\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}  
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}  
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}  
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}\treatas  
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
fd2b31b3eefd}\inprochandler  
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\_disable\_navigation\_sounds  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_navigation\_sounds  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\iedevtools\options  
Opens key: HKLM\software\policies\microsoft\internet explorer\iedevtools\options  
Opens key: HKCU\software\microsoft\internet explorer\iedevtools\options  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\iedevtools\options  
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\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\tablet pc\  
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\_always\_send\_extended\_ua\_string  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_always\_send\_extended\_ua\_string  
Opens key: HKCU\software\microsoft\windows\shell\associations\mimeassociations\text/xml\userchoice  
Opens key: HKCU\software\classes\mime\database\content type\text/xml  
Opens key: HKCR\mime\database\content type\text/xml  
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\internet  
explorer\main\featurecontrol\feature\_process\_xml\_as\_html  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_process\_xml\_as\_html  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{16d51579-a30b-4c8b-a276-  
0ff4dc41e755}  
Opens key: HKCR\activatableclasses\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}  
Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-  
0ff4dc41e755}  
Opens key: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}  
Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-  
0ff4dc41e755}\treatas  
Opens key: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-  
0ff4dc41e755}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-  
0ff4dc41e755}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-  
0ff4dc41e755}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\inprochandler  
Opens key: HKCU\software\microsoft\internet explorer\jscript9  
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: HKLM\software\microsoft\windowsruntime\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}  
Opens key: HKCR\activatableclasses\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}  
Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}  
Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}  
Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\treatas  
Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprochandler  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\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\4  
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: HKLM\software\microsoft\windowsruntime\clsid\{00020420-0000-0000-c000-000000000046}  
Opens key: HKCR\activatableclasses\clsid\{00020420-0000-0000-c000-000000000046}  
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}\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: HKLM\software\microsoft\sqlclient\windows\disabledprocesses\  
Opens key: HKLM\software\microsoft\telemetryclient\throttlemore\sql\windows\winsqm8  
Opens key: HKLM\software\microsoft\telemetryclient\throttlemore\sql\windows  
Opens key: HKLM\software\microsoft\telemetryclient\throttlemore\sql  
Opens key: HKLM\software\microsoft\telemetryclient\throttlemore  
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sql\windows\winsqm8  
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sql\windows  
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sql  
Opens key: HKLM\software\microsoft\telemetryclient\throttlemore\sql\windows\winsqm8\13238528  
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sql\windows\winsqm8\13238528  
Opens key: HKLM\software\microsoft\telemetryclient\throttlemore\sql\windows\winsqm8\13238784  
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sql\windows\winsqm8\13238784  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\tabbedbrowsing  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}  
Opens key: HKCR\activatableclasses\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{3cb169b3-17d9-4e47-8b93-  
2878998f69a2}  
Opens key: HKCR\activatableclasses\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}  
Opens key: HKCU\software\classes\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}  
Opens key: HKCR\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}  
Opens key: HKCU\software\classes\clsid\{3cb169b3-17d9-4e47-8b93-  
2878998f69a2}\treatas  
Opens key: HKCR\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\treatas  
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}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-  
00a0c90a8f39}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{3cb169b3-17d9-4e47-8b93-  
2878998f69a2}\inprocserver32  
Opens key: HKCR\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{3cb169b3-17d9-4e47-8b93-  
2878998f69a2}\inprochandler32  
Opens key: HKCR\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{3cb169b3-17d9-4e47-8b93-  
2878998f69a2}\inprochandler  
Opens key: HKCR\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler  
Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}  
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-  
000000000046}\proxystubclsid32  
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32  
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\clsid\{00020420-0000-0000-c000-000000000046}  
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}  
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: HKLM\software\microsoft\windowsruntime\clsid\{00020424-0000-0000-c000-  
000000000046}  
Opens key: HKCR\activatableclasses\clsid\{00020424-0000-0000-c000-000000000046}  
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\clsid\{00020420-0000-0000-c000-  
000000000046}\treatas  
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas  
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-  
000000000046}\inprocserver32  
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32  
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}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-  
000000000046}\inprochandler32  
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-  
000000000046}\inprochandler  
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler  
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: HKCU\software\classes\wow6432node\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}  
Opens key: HKCR\wow6432node\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}  
Opens key: HKCU\software\classes\wow6432node\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}\proxystubclsid32  
Opens key: HKCR\wow6432node\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}  
Opens key: HKCR\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}  
Opens key: HKCU\software\classes\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}\proxystubclsid32  
Opens key: HKCR\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}\proxystubclsid32  
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: HKLM\software\wow6432node\policies\microsoft\internet explorer\safety\activexfiltering  
Opens key: HKLM\software\policies\microsoft\internet explorer\safety\activexfiltering  
Opens key: HKCU\software\microsoft\internet explorer\safety\activexfiltering  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\safety\activexfiltering  
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: 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: 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: 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: HKLM\software\wow6432node\microsoft\windows\currentversion\setup  
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: HKLM\software\wow6432node\policies\microsoft\windows\explorer  
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32  
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\windows\currentversion\internet settings\  
Opens key: HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}  
Opens key: HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}  
Opens key: HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\treatas  
Opens key: HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\treatas  
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: HKLM\software\microsoft\windowsruntime\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}  
Opens key: HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler32  
Opens key: HKCR\activatableclasses\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}\treatas  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler



Opens key: HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler  
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: 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\microsoft\windowsruntime\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}  
Opens key: HKCR\activatableclasses\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}  
Opens key: HKCU\software\classes\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}  
Opens key: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\treatas  
Opens key: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprochandler  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}  
Opens key: HKCR\activatableclasses\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}  
Opens key: HKCU\software\classes\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}  
Opens key: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}  
Opens key: HKCU\software\classes\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\treatas  
Opens key: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprochandler32  
Opens key: HKLM\software\wow6432node\microsoft\com3  
Opens key: HKCU\software\classes\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprochandler  
Opens key: HKLM\system\currentcontrolset\control\graphicsdrivers  
Opens key: HKLM\system\currentcontrolset\control\graphicsdrivers\scheduler  
Opens key: HKCU\software\microsoft\internet explorer\gpu  
Opens key: HKLM\hardware\devicemap\video  
Opens key: HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000  
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000  
Opens key: HKLM\system\currentcontrolset\enum\pci\ven\_80ee&dev\_beef&subsys\_00000000&rev\_00\3&267a616a&1&10  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_layout9\_partial  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_disable\_layout9\_partial  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_force\_layout9\_partialdebug  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_force\_layout9\_partialdebug  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\manipulation  
Opens key: HKCU\euadc\  
Opens key: HKCU\euadc\1252  
Opens key: HKCU\software\policies\microsoft\internet explorer\control panel  
Opens key: HKLM\software\microsoft\windowsruntime\activatableclassid  
Opens key: HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{61fd2c0b-c8d4-48c1-a54f-bc5a64205af2}  
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\policies\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}  
Opens key: HKLM\software\policies\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}  
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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_alloweddomainlist  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_alloweddomainlist  
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  
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: HKLM\software\microsoft\windowsruntime\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}  
Opens key: HKCR\activatableclasses\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}  
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: 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: HKLM\software\microsoft\windowsruntime\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}  
Opens key: HKCR\activatableclasses\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}  
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: 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\ctf\compatibility\iexplore.exe  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\url history  
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: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\infodelivery\restrictions  
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-1-5-21-1923240461-1905901954-2556564120-1001  
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:  
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\classes\wow6432node\interface\{a168aad-1674-49da-ad4f-  
4f27df8760d0}  
Opens key: HKCR\wow6432node\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}  
Opens key: HKCU\software\classes\wow6432node\interface\{a168aad-1674-49da-ad4f-  
4f27df8760d0}\proxystubclsid32  
Opens key: HKCR\wow6432node\interface\{a168aad-1674-49da-ad4f-  
4f27df8760d0}\proxystubclsid32  
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}  
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}  
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}\treatas  
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-  
60ce2149e33c}\inprochandler  
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-  
444553540000}  
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}  
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: HKLM\software\microsoft\windowsruntime\clsid\{ff393560-c2a7-11cf-bff4-  
444553540000}  
Opens key: HKCR\activatableclasses\clsid\{ff393560-c2a7-11cf-bff4-444553540000}  
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}\inprocserver32  
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\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: 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: HKLM\software\wow6432node\microsoft\internet\_explorer\main\windowssearch  
Opens key: HKLM\software\wow6432node\microsoft\internet\_explorer\feeds  
Opens key: HKLM\software\wow6432node\microsoft\windows\_search  
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: HKLM\software\microsoft\windowsruntime\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}  
Opens key: HKCR\activatableclasses\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}  
Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}  
Opens key: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}  
Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas  
Opens key: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler  
Opens key: HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}  
Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}  
Opens key: HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32  
Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32  
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}  
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}  
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas  
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas  
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32  
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32  
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler  
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler  
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: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}  
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}  
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32  
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32  
Opens key: HKCU\software\microsoft\internet\_explorer\main\featurecontrol\feature\_enable\_web\_control\_visuals  
Opens key: HKLM\software\wow6432node\microsoft\internet\_explorer\main\featurecontrol\feature\_enable\_web\_control\_visuals  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}\propertybag  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}\propertybag  
Opens key: HKCU\software\classes\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder  
Opens key: HKCR\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\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder  
Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32  
Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}\propertybag  
Opens key: HKCU\software\classes\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}  
Opens key: HKCR\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}  
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}  
Opens key: HKLM\software\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\policies\microsoft\internet explorer\caretbrowsing  
Opens key: HKCU\software\microsoft\internet explorer\caretbrowsing  
Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites  
Opens key: HKLM\software\policies\microsoft\internet explorer\flipahead  
Opens key: HKCU\software\microsoft\internet explorer\tabbedbrowsing\newtabpage  
Opens key: HKLM\software\clients\startmenuinternet\iexplore.exe\installinfo  
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}  
Opens key: HKCR\activatableclasses\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}  
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}\treatas  
Opens key: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\treatas  
Opens key: HKCU\software\classes\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32  
Opens key: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler32  
Opens key: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler  
Opens key: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprochandler  
Opens key: HKCU\software\classes\http  
Opens key: HKCR\http  
Opens key: HKCU\software\microsoft\windows\shell\associations\urlassociations\http  
Opens key: HKCU\software\microsoft\windows\shell\associations\urlassociations\http\userchoice  
Opens key: HKCU\software\classes\ie.http  
Opens key: HKCR\ie.http  
Opens key: HKCR\ie.http\  
Opens key: HKCU\software\classes\ie.http\shell\open  
Opens key: HKCR\ie.http\shell\open  
Opens key: HKCU\software\classes\ie.http\shell\open\command  
Opens key: HKCR\ie.http\shell\open\command  
Opens key: HKCU\software\classes\ie.http\curver  
Opens key: HKCR\ie.http\curver  
Opens key: HKCU\software\classes\ie.http\progid  
Opens key: HKCR\ie.http\progid  
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\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\cryptography\defaults\provider types\type 001  
Opens key: HKCU\software\microsoft\internet explorer\user preferences  
Opens key: HKLM\system\currentcontrolset\services\crypt32  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\conhost.exe  
Opens key: HKLM\software\microsoft\windows nt\currentversion\console\truetypefont

Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen  
Opens key: HKCU\console  
Opens key: HKCU\console\  
Opens key: HKCU\console\c:\program files (x86)\java\jre7\bin\java.exe  
Opens key: HKCU\console\c:\program files (x86)\java\jre7\bin\java.exe  
Opens key: HKLM\system\currentcontrolset\control\nls\codepage\euclcodepage  
Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\appcompatflags\custom\awt.dll  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\awt.dll  
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\ram emulation  
Opens key: HKLM\software\wow6432node\microsoft\direct3d\drivers\rgb emulation  
Opens key: HKCU\system\currentcontrolset\control\graphicsdrivers\scheduler  
Opens key: HKLM\software\wow6432node\microsoft\direct3d\shims  
Opens key: HKCU\software\microsoft\direct3d\shims\maximizedwindowedmode  
Opens key: HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator  
Opens key: HKLM\software\wow6432node\microsoft\directdraw  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\1a3e7dae-123fffde  
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: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\fontsubstitutes  
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip  
Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters  
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient  
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient  
Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient  
Opens key: HKLM\software\policies\microsoft\system\dnsclient  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[usefilter]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[disableheaplookaside]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[frontenddebugoptions]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[shutdownflags]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[unloadeventtracedepth]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[tracingflags]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[minimumstackcommitinbytes]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[breakoninitializeprocessfailure]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[keepactivationcontextsalive]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[trackactivationcontextreleases]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[maxdeadactivationcontexts]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[globalflag]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[cwdillegalindllsearch]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[debugprocessheaponly]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[executeoptions]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[disableexceptionchainvalidation]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[searchpathmode]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]  
Queries value:  
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]  
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]  
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-  
us[alternatecodepage]  
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: HKCU\software\microsoft\windows  
nt\currentversion\appcompatflags[showdebuginfo]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dxoptions[usefilter]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dxoptions[iexplore.exe]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5c8bb950-959e-4309-

8908-67961a1205d5]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[depoﬀ]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[security\_hkln\_only]  
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]  
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\system\currentcontrolset\control\lsa\lipsalgorithmpolicy[enabled]  
Queries value: HKLM\system\currentcontrolset\control\lsa\lipsalgorithmpolicy]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]  
Queries value: HKLM\software\microsoft\ole[aggressivemtestesting]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[debugger]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[uselargepages]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[nodeoptions]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[disablewakecharge]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[mitigationoptions]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\compatibility32[iexplore]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\internet explorer\low  
rights[protectedmodeoffforallzones]  
Queries value: HKCU\software\microsoft\internet explorer\main[tabprocgrowth]  
Queries value: HKLM\software\microsoft\internet explorer\main[tabprocgrowth]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]  
Queries value: HKLM\software\microsoft\internet explorer\low rights[luaoﬄorleon]  
Queries value: HKCU\software\microsoft\internet  
explorer\setup[havecreatedquicklaunchitems]  
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
Queries value: HKCU\software\microsoft\internet explorer\main[frametabwindow]  
Queries value: HKLM\software\microsoft\internet explorer\main[frametabwindow]  
Queries value: HKCU\software\microsoft\internet explorer\main[framemerging]  
Queries value: HKLM\software\microsoft\internet explorer\main[framemerging]  
Queries value: HKCU\software\microsoft\internet explorer\main[sessionmerging]  
Queries value: HKLM\software\microsoft\internet explorer\main[sessionmerging]  
Queries value: HKCU\software\microsoft\internet explorer\main[admintabprocs]  
Queries value: HKLM\software\microsoft\internet explorer\main[admintabprocs]  
Queries value: HKCU\software\microsoft\internet explorer\main[hangrecovery]  
Queries value: HKLM\software\microsoft\internet explorer\main[hangrecovery]  
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: HKLM\software\microsoft\rpc[idletimerwindow]  
Queries value: HKCU\software\microsoft\internet explorer\main[compatibilityflags]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\appcompatflags[acredir]  
Queries value: HKCU\software\microsoft\internet explorer\sql[serverfreezeonupload]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-  
b29c-65b732d3d21a}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-  
b29c-65b732d3d21a}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-  
b29c-65b732d3d21a}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-  
b29c-65b732d3d21a}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-  
b29c-65b732d3d21a}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-  
b29c-65b732d3d21a}[parsingname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-  
b29c-65b732d3d21a}[infotip]  
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[foldertypeid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]  
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[syncmode5]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings\5.0\cache[sessionstarttimedefaultdeltasecs]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]  
Queries value:



HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]  
Queries value: HKU\default\software\microsoft\windows\currentversion\explorer\user  
shell folders[cache]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[cache]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[mbscapiforcrack]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable[iexplore.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable[\*]  
Queries value: HKCU\software\microsoft\internet  
explorer\main\featurecontrol[feature\_clientauthcertfilter]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol[feature\_clientauthcertfilter]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[iexplore.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[iexplore.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[\*]  
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[idnenabled]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[preconnectlimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[preresolverlimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[sqmhttpstreamrandomuploadpoolsize]  
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\windows\currentversion\internet  
settings[clientauthbuiltinui]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[enableautoproxycache]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[displayscriptdownloadfailureui]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[mbscservername]  
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\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\microsoft\windows\currentversion\internet  
settings[maxconnectionsperserver]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[maxconnectionsper1\_0server]  
Queries value: HKLM\software\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\microsoft\windows\currentversion\internet  
settings[connecttimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[connectretries]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[connectretries]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[sendtimeout]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[sendtimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[receivetimeout]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[receivetimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[disablentlmpreauth]  
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\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: HKCU\software\microsoft\windows\currentversion\internet  
settings[disablecachingofsslpages]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[leashlegacycookies]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[dialupuselansettings]  
Queries value: HKLM\software\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\microsoft\windows\currentversion\internet  
settings[bypasshttnocachecheck]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[bypasssslnocachecheck]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[bypasssslnocachecheck]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[enablehttptrace]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[nocheckautodialoverride]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[nocheckautodialoverride]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[dontusednsloadbalancing]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[dontusednsloadbalancing]  
Queries value: HKLM\software\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]

[illegible]

[illegible]

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[autodetect]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\connections[savedlegacysettings]  
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\connections[defaultconnectionsettings]  
Queries value: HKCU\software\microsoft\internet  
explorer\searchscopes[showsearchsuggestionsinaddressglobal]  
Queries value: HKLM\software\microsoft\internet  
explorer\searchscopes[showsearchsuggestionsinaddressglobal]  
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: HKCU\software\microsoft\internet  
explorer\browseremulation[unattendloaded]  
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[tldupdates]  
Queries value: HKLM\software\microsoft\internet explorer\browseremulation[tldupdates]  
Queries value: HKCU\software\microsoft\internet explorer\main[operationaldata]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[category]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[name]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parentfolder]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[description]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[relativepath]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parsingname]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[infotip]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localizedname]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[icon]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[security]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresource]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localredirectonly]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[roamable]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[precreate]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[stream]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[attributes]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[foldertypeid]

Queries value:  
HKLM\software\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:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]  
Queries value:  
HKLM\software\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\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]  
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]  
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]  
Queries value:  
HKLM\software\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\microsoft\ole\appcompat[raisedefaultauthnlevel]  
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]  
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]  
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong  
cryptographic provider[type]  
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong  
cryptographic provider[image path]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]  
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\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\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]  
Queries value: HKLM\software\microsoft\cryptography[machineguid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-



a03a-e3ef65729f3d}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]  
Queries value: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]  
Queries value: HKLM\software\microsoft\rpc\extensions\ndroleextdll  
Queries value: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32[]  
Queries value: HKLM\software\microsoft\com3\com+enabled  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]  
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]  
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[inprocserver32]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[appdata]  
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]  
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[security]

Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]  
Queries value:  
HKLM\software\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\explorer\discardable\postsetup\component categories\{00021493-0000-0000-c000-000000000046}\enum[implementing]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup\component categories64\{00021493-0000-0000-c000-000000000046}\enum[implementing]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup\component categories\{00021494-0000-0000-c000-000000000046}\enum[implementing]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup\component categories64\{00021494-0000-0000-c000-000000000046}\enum[implementing]  
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[flags]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\browser helper objects\{dbc80044-a445-435b-bc74-9c25c1c588a9}[nointernetexplorer]  
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}[flags]  
Queries value: HKCU\software\microsoft\internet explorer\approvedextensionsmigration[timestamp]  
Queries value: HKLM\software\microsoft\internet explorer\migration[ie installed date]  
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[mscompatibilitymode]  
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\microsoft\internet explorer\security[disablefixsecuritysettings]  
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\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\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\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes]
  Queries value:
    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[callforattributes]
  Queries value:
    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[restrictedattributes]
  Queries value:
    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[foldervalueflags]
  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\{d5291c64-7c88-11e3-be65-806e6f6e6963}[data]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-11e3-be65-806e6f6e6963}[generation]
  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\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[iconsonly]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
  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:
    HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.html]
  Queries value:
    HKCR\.html[content type]
  Queries value:
    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
  Queries value:
    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[inprocserver32]
  Queries value:
    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
  Queries value:
    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[threadingmodel]

```

Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
Queries value: HKCR\.html[]  
Queries value: HKCU\software\microsoft\windows\shell\associations[isconnectedatlogon]  
Queries value: HKCR\htmlfile\shellex\iconhandler[]  
Queries value: HKCR\htmlfile[docobject]  
Queries value: HKCR\systemfileassociations\.html[docobject]  
Queries value: HKCR\systemfileassociations\document[docobject]  
Queries value: HKCR\htmlfile[browseinplace]  
Queries value: HKCR\systemfileassociations\.html[browseinplace]  
Queries value: HKCR\systemfileassociations\document[browseinplace]  
Queries value: HKCR\htmlfile\clsid[]  
Queries value: HKCR\htmlfile[isshortcut]  
Queries value: HKCR\systemfileassociations\.html[isshortcut]  
Queries value: HKCR\systemfileassociations\document[isshortcut]  
Queries value: HKCR\htmlfile[alwaysshowext]  
Queries value: HKCR\systemfileassociations\.html[alwaysshowext]  
Queries value: HKCR\systemfileassociations\document[alwaysshowext]  
Queries value: HKCR\htmlfile[nevershowext]  
Queries value: HKCR\systemfileassociations\.html[nevershowext]  
Queries value: HKCR\systemfileassociations\document[nevershowext]  
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]  
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]  
Queries value: HKLM\software\microsoft\internet explorer\main[x86apppath]  
Queries value: HKCU\software\microsoft\internet explorer\main>window\_min\_width  
Queries value: HKCU\software\microsoft\internet explorer\main>window\_min\_height  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-11e3-be65-806e6f6e6963}[data]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-11e3-be65-806e6f6e6963}[generation]  
Queries value: HKCR\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\microsoft\windows search[currentversion]  
Queries value: HKLM\system\currentcontrolset\control\smservicelist[smservicelist]  
Queries value: HKCU\software\microsoft\internet explorer\main>window\_placement  
Queries value: HKCU\software\microsoft\internet explorer\main[fullscreen]  
Queries value: HKCU\software\microsoft\internet explorer\minie[showtabsbelowaddressbar]  
Queries value: HKCU\software\microsoft\internet explorer\main[autosearch]  
Queries value: HKLM\software\microsoft\internet explorer\main[autosearch]  
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}[]  
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32[inprocserver32]  
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32[]  
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32[threadingmodel]  
Queries value: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]  
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]  
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]  
Queries value: HKCU\software\microsoft\internet explorer\main[useie7autocomplete]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe ui]  
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: HKCU\software\microsoft\internet explorer\tabbedbrowsing[enabled]  
Queries value: HKCU\software\microsoft\internet

explorer\tabbedbrowsing[activitymetertimerinterval]  
Queries value: HKCU\software\microsoft\internet  
explorer\tabbedbrowsing[activitymeterdisable]  
Queries value: HKCU\software\microsoft\internet explorer\minie[tabbandwidth]  
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\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: HKLM\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}[showtopresult]  
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[showtopresult]  
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[topresult]  
Queries value: HKLM\software\microsoft\internet explorer\searchscopes[topresult]  
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[topresulturl]  
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[topresulturl]  
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[topresulturlfallback]  
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]  
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]  
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[showsearchsuggestionsglobal]  
Queries value: HKLM\software\microsoft\internet explorer\searchscopes[showsearchsuggestionsglobal]  
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl\_json]  
Queries value: HKLM\software\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\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\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\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\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\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\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\toolbar[locked]  
Queries value: HKCU\software\microsoft\internet explorer\minie[commandbarenable]  
Queries value: HKCU\software\microsoft\internet explorer\minie[linksbandenable]  
Queries value: HKCU\software\microsoft\internet  
explorer\tabbedbrowsing[thumbnailbehavior]  
Queries value: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}[]  
Queries value: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32[inprocserver32]  
Queries value: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32[]  
Queries value: HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32[threadingmodel]  
Queries value: HKCU\software\microsoft\internet  
explorer\toolbar\webbrowser[itbar7height64]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]  
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\low  
rights[protectedmodeoffforallzones]

Queries value: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}[]  
Queries value: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}[]  
Queries value: HKCU\software\microsoft\internet explorer\continuousbrowsing[enabled]  
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[cache\limit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\history[cache\limit]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[tabproc\growth]  
Queries value: HKCR\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32[]  
Queries value: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]  
Queries value: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[inprocserver32]  
Queries value: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[]  
Queries value: HKCR\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\low  
rights[luaoff\lorieon]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\iexplore.exe[terminateonshutdown]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{25336920-03f9-11cf-8fd0-00aa00686f13}]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[url  
history[daystokeep]  
Queries value: HKCR\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}\proxystubclsid32[]  
Queries value: HKCR\interface\{036438a5-d9ac-4353-a567-69298fdaa990}\proxystubclsid32[]  
Queries value: HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32[]  
Queries value: HKCR\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}\proxystubclsid32[]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[frame\window]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[frame\merging]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[session\merging]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[admin\procs]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[background\connections]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[background\connections]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\cache[session\start\time\default\delta\secs]  
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}[parent\folder]  
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}[relative\path]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsing\name]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[info\tip]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localized\name]  
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}[stream\resource]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream\resource\type]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[local\redirect\only]  
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: 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: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol[feature\_clientauthcertfilter]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[iexplore.exe]  
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: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[disableworkerthreadhibernation]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[maxconnectionsperserver]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[maxconnectionsper1\_0server]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[connecttimeout]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[connectretries]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[sendtimeout]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[receivetimeout]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\cache[scavengecachefilelimit]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[dialupuselansettings]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[bypasshttptocachecheck]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[bypasssslnocheck]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[enablehttptrace]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[nocheckautodialoverride]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[dontusednsloadbalancing]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[sharecredswithwinhttp]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[tcpautotuning]  
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[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]

[illegible]



Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storiesserviceclassinfo]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[disablebranchcache]  
Queries value: HKCU\software\microsoft\internet explorer\main[tabshuttdowndelay]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[tabshuttdowndelay]  
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: HKCR\wow6432node\interface\{00000134-0000-0000-c000-  
000000000046}\proxystubclsid32[]  
Queries value: HKCR\wow6432node\interface\{1ac7516e-e6bb-4a69-b63f-  
e841904dc5a6}\proxystubclsid32[]  
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\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}[parsingname]  
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}[streamresource type]  
 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: 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: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_document\_compatible\_mode[iexplore.exe]  
 Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_document\_compatible\_mode[\*]  
 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\system\currentcontrolset\control\wmi\security[7f8e35ca-68e8-41b9-86fe-d6adc5b327e7]  
 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\main[useswrender]  
 Queries value:  
 HKLM\system\currentcontrolset\services\fontcache\parameters[clientcachesize]  
 Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers[size]  
 Queries value: HKCR\wow6432node\interface\{bfb070ce-95f2-4edb-bab5-4dad9e6a2905}\proxystubclsid32[]  
 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: HKCR\wow6432node\interface\{036438a5-d9ac-4353-a567-69298fdaa990}\proxystubclsid32[]  
 Queries value: HKCR\wow6432node\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32[]  
 Queries value: HKCR\wow6432node\interface\{49296cad-92e6-43b2-abe1-5d73d71d7ac9}\proxystubclsid32[]

Queries value: HKLM\software\wow6432node\microsoft\windows\windows error  
reporting\wmr[disable]  
Queries value: HKCU\software\microsoft\internet explorer\main[enableprebinding]  
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[foldervalueflags]  
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]  
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: 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\minie[showstatusbar]  
Queries value: HKCU\software\microsoft\internet explorer\main[enable browser extensions]  
Queries value: HKCU\software\microsoft\internet explorer\toolbar\webbrowser[itbar7layout]  
Queries value: HKCU\software\microsoft\internet explorer\minie[alwaysshowmenus]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nobandcustomize]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[nointernetexplorer]  
Queries value: HKLM\software\policies\microsoft\internet explorer[disableflashinie]  
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\internet explorer\approved extensions[\{18df081c-e8ad-4283-a596-fa578c2ebdc3}]  
Queries value: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[]  
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}\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}[]  
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: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects\{dbc80044-a445-435b-bc74-9c25c1c588a9}[nointernetexplorer]  
Queries value: HKCU\software\microsoft\internet explorer\approved extensions[\{dbc80044-a445-435b-bc74-9c25c1c588a9}]  
Queries value: HKCR\wow6432node\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32[]  
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: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore[loadtimearray]  
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: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore[loadtimearray]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[createuricachesize]  
Queries value: HKCU\software\microsoft\internet explorer\suggested  
sites[datastreamenabledstate]  
Queries value: HKCU\software\microsoft\internet explorer\mao settings[discardloadtimes]  
Queries value: HKCU\software\microsoft\internet explorer\mao  
settings[suppressperfbaruntil]  
Queries value: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32[]  
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-  
4283-a596-fa578c2ebdc3}\iexplore[navtimearray]  
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\internet explorer\mao  
settings[addonloadtimethreshold]  
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: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]  
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: HKLM\software\wow6432node\microsoft\internet  
explorer\browseremulation[allsitescompatibilitymode]  
Queries value: HKCU\software\microsoft\internet  
explorer\browseremulation[intranetcompatibilitymode]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\browseremulation[intranetcompatibilitymode]  
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\microsoft\windows\currentversion\internet  
settings[specialfolderscachesize]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[specialfolderscachesize]  
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}[parentfolder]  
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}[parsiname]  
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}[streamresourcetype]  
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: 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: HKCU\software\microsoft\internet explorer\browseremulation[localmachinecompatibilitymode]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\browseremulation[localmachinecompatibilitymode]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding]  
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\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\zones\3[2703]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\3[2703]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[istextplainhonored]  
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[dragscrolldelay]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrollinterval]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[ieharden]  
Queries value: HKCU\software\microsoft\internet explorer\flipahead[notificationdelay]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2106]  
Queries value: HKLM\software\wow6432node\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: HKLM\system\currentcontrolset\control\wmi\security[2c3e6d9f-8298-450f-8e5d-49b724f1216f]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[954cc269-9c80-41b9-a2cd-ce4c8ccf59a2]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[8a8b5246-6eb6-4339-8b59-b0085b9f4890]  
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[naturalinputhandler]  
Queries value: HKCU\software\microsoft\internet explorer\main[minimumsystemtimerresolution]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[minimumsystemtimerresolution]  
Queries value: HKCU\software\microsoft\internet explorer\main[renderingloopmaxtime]  
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_safe\_bindtoobject[iexplore.exe]  
Queries value: HKCU\software\microsoft\internet explorer[rtfconverterflags]  
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: HKLM\software\wow6432node\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[disablescripdebuggerie]  
 Queries value: HKCU\software\microsoft\internet explorer\main[disable\_diagnostics\_mode]  
 Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[disable  
 diagnostics\_mode]  
 Queries value: HKCU\software\microsoft\internet explorer\main[move\_system\_caret]  
 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\main[jscripuprofilecacheeventdelay]  
 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\ntp\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: 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: HKCR\interface\{d3e09618-273f-4a13-a7d2-29f90ed68e8a}\proxystubclsid32[]  
 Queries value: HKCR\wow6432node\interface\{d3e09618-273f-4a13-a7d2-  
 29f90ed68e8a}\proxystubclsid32[]  
 Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\[]  
 Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
 fd2b31b3eefd}\inprocserver32[inprocserver32]  
 Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
 fd2b31b3eefd}\inprocserver32[]  
 Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-  
 fd2b31b3eefd}\inprocserver32[threadingmodel]  
 Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version  
 vector[vml]  
 Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version vector[ie]  
 Queries value: HKLM\software\wow6432node\microsoft\internet  
 explorer\main\featurecontrol\feature\_zone\_elevation[iexplore.exe]  
 Queries value: HKCU\software\microsoft\internet explorer\main[donottrack]

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\5.0\user agent[platform]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent[platform]  
Queries value: HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]  
Queries value: HKCR\mime\database\content type\text/xml[clsid]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[2700]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\3[2700]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_xssfilter[iexplore.exe]  
Queries value: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}[]  
Queries value: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\inprocserver32[threadingmodel]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[57277741-3638-4a4b-bdba-0ac6e45da56c]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[1201]  
Queries value: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}[]  
Queries value: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprocserver32[threadingmodel]  
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\0[icon]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[minlevel]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[recommendedlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[currentlevel]  
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\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[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\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[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\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[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: 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: HKLM\software\microsoft\sqlclient\windows\disabledprocesses[74dd1fc8]  
Queries value: HKLM\software\microsoft\sqlclient\windows\studyid  
Queries value: HKLM\software\microsoft\telemetryclient\samplstore\sam[sampledout]  
Queries value: HKCR\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}[]  
Queries value: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]  
Queries value: HKCR\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler32[]  
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]  
Queries value: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]  
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}[]  
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]  
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\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]  
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]  
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\{5f568e3e-317c-402e-a883-546b0f7673a4}\proxystubclsid32[]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mshhtml\_autoload\_ieframe[iexplore.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mshhtml\_autoload\_ieframe[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[1400]  
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\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}\proxystubclsid32[]  
Queries value: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv9]  
Queries value: HKCU\software\microsoft\internet  
explorer\browseremulation[cvlistxmlversionlow]  
Queries value: HKCU\software\microsoft\internet  
explorer\browseremulation[cvlistxmlversionhigh]  
Queries value: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]  
Queries value: HKCU\software\microsoft\internet  
explorer\browseremulation[iecompatversionlow]  
Queries value: HKCU\software\microsoft\internet  
explorer\browseremulation[iecompatversionhigh]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]  
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]  
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: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[warnonintranet]  
Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]  
Queries value: HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}[]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zonemap[autodetect]  
Queries value: HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\inprochandler32[]  
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: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]  
Queries value: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}[]  
Queries value: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-



fa359598e1c5}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{54e211b6-3650-4f75-8334-fa359598e1c5}\inprocserver32[threadingmodel]  
fa359598e1c5}\inprocserver32[threadingmodel]  
Queries value: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}[]  
Queries value: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprocserver32[inprocserver32]  
6900b9299126}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprocserver32[]  
6900b9299126}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{79dea627-a08a-43ac-8ef5-6900b9299126}\inprocserver32[threadingmodel]  
6900b9299126}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\microsoft\com3[gipactivitybypass]  
Queries value: HKCU\software\microsoft\internet explorer\gpu[adapterinfo]  
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]  
Queries value: HKLM\hardware\devicemap\video[\device\video0]  
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000[pruningmode]  
08002be10318}\0000[pruningmode]  
Queries value: HKCU\software\microsoft\internet explorer\main[predictedviewexpansion]  
Queries value: HKCU\software\microsoft\internet explorer\main[contentlayercacheexpansion]  
explorer\main[contentlayercacheexpansion]  
Queries value: HKCU\software\microsoft\internet explorer\main[predictedviewchangethreshold]  
explorer\main[predictedviewchangethreshold]  
Queries value: HKCU\software\microsoft\internet explorer\main[predictedviewchangethresholdpaint]  
explorer\main[predictedviewchangethresholdpaint]  
Queries value: HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[clsid]  
HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[clsid]  
Queries value: HKLM\software\microsoft\windowsruntime\clsid\{61fd2c0b-c8d4-48c1-a54f-bc5a64205af2}[activatableclassid]  
bc5a64205af2}[activatableclassid]  
Queries value: HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[activationtype]  
HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[activationtype]  
Queries value: HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[threading]  
HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[threading]  
Queries value: HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[trustlevel]  
HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[trustlevel]  
Queries value: HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[dllpath]  
HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[dllpath]  
Queries value: HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[server]  
HKLM\software\microsoft\windowsruntime\activatableclassid\windows.security.credentials.passwordvault[server]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[7fdd167c-79e5-4403-8c84-b7c0bb9923a1]  
8c84-b7c0bb9923a1]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e6c92fb8-89d7-4d1f-be46-d56e59804783]  
be46-d56e59804783]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1c00]  
settings\zones\3[1c00]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\3[1c00]  
settings\zones\3[1c00]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_activex\_repurposedetection[iexplore.exe]  
explorer\main\featurecontrol\feature\_activex\_repurposedetection[iexplore.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_activex\_repurposedetection[\*]  
explorer\main\featurecontrol\feature\_activex\_repurposedetection[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1207]  
settings\zones\3[1207]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\3[1207]  
settings\zones\3[1207]  
Queries value: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[appid]  
HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[appid]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]  
settings[cointernetcombineiuricachesize]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]  
settings[cointernetcombineiuricachesize]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]  
settings[cointernetcombineiuricachesize]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]  
settings[cointernetcombineiuricachesize]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[compatibility flags]  
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]  
compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[miscstatus flags]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[120b]  
settings\zones\3[120b]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1208]  
settings\zones\3[1208]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2201]  
settings\zones\3[2201]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_restrict\_activexinstall[iexplore.exe]  
explorer\main\featurecontrol\feature\_restrict\_activexinstall[iexplore.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_restrict\_activexinstall[\*]  
explorer\main\featurecontrol\feature\_restrict\_activexinstall[\*]  
Queries value: HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas[]  
HKCR\wow6432node\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas[]  
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}[]  
abcdeffedcbb}[]  
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32[inprocserver32]  
abcdeffedcbb}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32[inprocserver32]  
abcdeffedcbb}\inprocserver32[inprocserver32]  
Queries value: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32[threadingmodel]  
abcdeffedcbb}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\wow6432node\javasoft\java runtime environment\1.7.0\_02[eula]  
environment\1.7.0\_02[eula]  
Queries value: HKLM\software\wow6432node\javasoft\java plug-in\10.2.0[usejava2iexplorer]  
in\10.2.0[usejava2iexplorer]  
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[count]  
11cf-aaa5-00401c608501}\iexplore[count]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\3[2000]  
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\url\_history[daystokeep]  
    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:  
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}[streamresource type]  
    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:  
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]

[illegible]

65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]  
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: HKCR\wow6432node\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32[]  
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]  
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[threadingmodel]  
Queries value: HKU\.\default\software\microsoft\windows\currentversion\explorer\user  
shell folders[local appdata]  
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: HKLM\software\microsoft\windows\currentversion\app  
paths\iexplore.exe[dontusedesktopchangerouter]  
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: HKLM\software\wow6432node\microsoft\windows\_search[currentversion]  
Queries value: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]  
00aa006009fa}\proxystubclsid32[]  
Queries value: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}[]  
Queries value: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[threadingmodel]  
Queries value: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]  
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}[]  
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[inprocserver32]  
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[]  
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[threadingmodel]  
Queries value: HKCR\wow6432node\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]  
00aa00404770}\proxystubclsid32[]  
Queries value: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[foldertypeid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user\_shell\_folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[parentfolder]

Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[foldertypeid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[initfolderhandler]  
Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[attributes]  
Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[callforattributes]  
Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[restrictedattributes]  
Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[foldervalueflags]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-5595fe6b30ee}]  
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[quicktabsthreshold]  
Queries value: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-44453540000}\inprocserver32[]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[parsiname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[icon]

Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[foldertypeid]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}[initfolderhandler]  
Queries value: HKCR\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}[sortorderindex]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[category]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[name]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[parentfolder]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[description]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[relativepath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[parsingname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[infotip]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[localizedname]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[icon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[security]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[streamresource]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[streamresourcetype]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[localredirectonly]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[roamable]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[precreate]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[stream]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[publishexpandedpath]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[attributes]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}[foldertypeid]  
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}\initfolderhandler]  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[safeprocesssearchmode]  
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[type]  
Queries value: HKCU\software\microsoft\internet explorer\setup[urlhistorymigrationtime]  
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\suggested sites[enabled]  
Queries value: HKCU\software\microsoft\internet explorer\main[disablefirsttruncustomize]  
Queries value: HKLM\software\microsoft\internet explorer\main[disablefirsttruncustomize]  
Queries value: HKCU\software\microsoft\internet explorer\main[ie10recommendedsettingsno]  
Queries value: HKLM\software\microsoft\internet explorer\main[ie10recommendedsettingsno]  
Queries value: HKCU\software\microsoft\internet explorer\main[ie10runonceperinstallcompleted]  
Queries value: HKCU\software\microsoft\internet explorer\main[ie10runoncecompletiontime]  
Queries value: HKCU\software\microsoft\internet explorer\flipahead[enabled]  
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[sliceath]  
Queries value: HKCU\software\microsoft\internet explorer\main[check\_associations]  
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing\newtabpage[schedule]  
Queries value:  
HKLM\software\clients\startmenuinternet\iexplore.exe\installinfo[showiconscommand]  
Queries value:  
HKLM\software\clients\startmenuinternet\iexplore.exe\installinfo[iconsvisible]  
Queries value: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}[]  
Queries value: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32[inprocserver32]  
Queries value: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32[]  
Queries value: HKCR\clsid\{591209c7-767b-42b2-9fba-44ee4615f2c7}\inprocserver32[threadingmodel]  
Queries value:  
HKCU\software\microsoft\windows\shell\associations\urlassociations\http\userchoice[progid]  
Queries value:  
HKCU\software\microsoft\windows\shell\associations\urlassociations\http\userchoice[hash]  
Queries value: HKCR\ie.http\shell\open\command[]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[desktop]  
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\software\wow6432node\javasoft\java runtime
environment\1.7[javahome]
  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[{2262cac-fe50-451e-9261-e7f22aab93ec}]
  Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{2262cac-fe50-451e-9261-e7f22aab93ec}]
  Queries value: HKCU\software\microsoft\internet explorer\searchscopes[version]
  Queries value: HKCU\software\microsoft\internet explorer\searchscopes[upgradetime]
  Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
  Queries value: HKCU\software\microsoft\internet explorer\user
preferences[2d53cffc5c1a3dd2e97b7979ac2a92bd59bc839e81]
  Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value: HKCU\software\microsoft\internet explorer\user
preferences[88d7d0879dab32e14de5b3a805a34f98aff34f5977]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
  Queries value: HKCU\console[screencolors]
  Queries value: HKCU\console[popupcolors]
  Queries value: HKCU\console[insertmode]
  Queries value: HKCU\console[quickedit]
  Queries value: HKCU\console[codepage]
  Queries value: HKCU\console[screenbuffersize]
  Queries value: HKCU\console[windowsize]
  Queries value: HKCU\console>windowposition]
  Queries value: HKCU\console[fontsize]
  Queries value: HKCU\console[fontfamily]
  Queries value: HKCU\console[fontweight]
  Queries value: HKCU\console[facename]
  Queries value: HKCU\console[cursorsize]
  Queries value: HKCU\console[historybuffersize]
  Queries value: HKCU\console[numberofhistorybuffers]
  Queries value: HKCU\console[historynodup]
  Queries value: HKCU\console[colortable00]
  Queries value: HKCU\console[colortable01]
  Queries value: HKCU\console[colortable02]
  Queries value: HKCU\console[colortable03]
  Queries value: HKCU\console[colortable04]
  Queries value: HKCU\console[colortable05]
  Queries value: HKCU\console[colortable06]
  Queries value: HKCU\console[colortable07]
  Queries value: HKCU\console[colortable08]
  Queries value: HKCU\console[colortable09]
  Queries value: HKCU\console[colortable10]
  Queries value: HKCU\console[colortable11]
  Queries value: HKCU\console[colortable12]
  Queries value: HKCU\console[colortable13]
  Queries value: HKCU\console[colortable14]
  Queries value: HKCU\console[colortable15]
  Queries value: HKCU\console[loadconime]
  Queries value: HKCU\console[extendededitkey]
  Queries value: HKCU\console[extendededitkeycustom]
  Queries value: HKCU\console[worddelimiters]
  Queries value: HKCU\console[trimleadingzeros]
  Queries value: HKCU\console[enablecolorselection]
  Queries value: HKCU\console[scrollscale]
  Queries value: HKLM\system\currentcontrolset\control\ls\codepage\euiccoderange[1252]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[java]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{f94f19e0-d5f7-4bf7-8a29-351593054411}]
  Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{f94f19e0-d5f7-4bf7-8a29-351593054411}]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[gdiprocesshandlequota]
  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[minimumlocalvidmem]
  Queries value: HKLM\software\wow6432node\microsoft\direct3d[forcedriverflagsoff]
  Queries value: HKLM\software\wow6432node\microsoft\direct3d[dd_runtime_version]

```

Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers[softwareonly]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[usevsconverter]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[usepsconverter]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disabledm]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablest]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[showframerate]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[flipnovsync]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw[forcerefreshrate]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablevbfailovers]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablevidmemvbs]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[fulldebug]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[emulatestateblocks]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablestripvfvf]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablegb]  
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablepsgp]  
Queries value: HKLM\software\wow6432node\javasoft\java  
update\policy[promptautoupdatecheck]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable[java.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[java.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[\*]  
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]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip[winsock 2.0 provider id]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]  
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]  
Sets/Creates value: HKCU\software\microsoft\internet  
explorer\recovery\adminactive[{3a6b4ad6-f55e-11e5-be82-080027fac36d}]  
Value changes: HKCU\software\microsoft\internet explorer\main[compatibilityflags]  
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\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\internet explorer\main[fullscreen]  
Value changes: HKCU\software\microsoft\internet explorer\main>window\_placement]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\content[cacheprefix]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\cookies[cacheprefix]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\history[cacheprefix]  
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\{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\{18df081c-e8ad-  
4283-a596-fa578c2ebdc3}\iexplore[loadtimearray]  
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-  
435b-bc74-9c25c1c588a9}\iexplore[loadtimearray]  
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]