Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	204
Risk Level:	7
Date Processed:	2016-04-22 06:01:55 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1af5338669efabe0a9841478396871b1.exe"

Sample ID:	54
Type:	basic
Owner:	admin
Label:	1af5338669efabe0a9841478396871b1
Date Added:	2016-04-22 06:01:55 (UTC)
File Type:	PE32:win32:gui
File Size:	939520 bytes
MD5:	1af5338669efabe0a9841478396871b1
SHA256:	98511820966946e5c2c543c720816047a808816f674bc8525016f362785c8b3e
Description:	None

Pattern Matching Results

7	Creates malicious events: FakeIE [PUA , Downware]
2	ECMA Script
3	Connects to local host
3	HTTP connection - response code 200 (success)
4	Checks whether debugger is present
2	HTML file
1	YARA score 1

Static Events

YARA rule hit:	SWF
YARA rule hit:	Nonexecutable

Process/Thread Events

Creates process:	C:\windows\temp\1af5338669efabe0a9841478396871b1.exe ["C:\windows\temp\1af5338669efabe0a9841478396871b1.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\!IECompat!Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x000004FC)
Creates mutex:	\Sessions\1\BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069}
Creates mutex:	\Sessions\1\BaseNamedObjects\http://www.baidu.com/
Creates mutex:	\Sessions\1\BaseNamedObjects\InternetExplorerDOMStoreQuota
Creates mutex:	\Sessions\1\BaseNamedObjects_!SHMSFTHISTORY!_
Creates event:	\Sessions\1\BaseNamedObjects\DINPUTWINMM

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\AATKOXA4.txt
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TVGA15OO.txt
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TDSMCWOI.txt
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QGCS3SK2\index[1].htm
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\3XGK55F6\baidu_jgylogo3[1].gif
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\LOWEYQNT\jquery-1.10.2.min_f2fb5194[1].js
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\GOLOOAON\nuomi_510f7472[1].png
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QGCS3SK2\icons_0e814c16[1].png
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\3XGK55F6\all_async_search_641293e1[1].js
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\3XGK55F6\bd_logo1[1].png
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\08IATE7C.txt
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\2JLA8H3S.txt

```
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\every_cookie_aa168cb4[1].js
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\NRKAPV8T\www.baidu[1].xml
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\nu_instant_search_ebeb5baa[1].js
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\env_beb83b45[1].swf
  Creates:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U
  Creates:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
  Creates:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Creates:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Creates:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com
  Creates:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Creates:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\3L1D4SUG\userDataBIDUPSID[1].xml
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\bdsug_async_dac7ea02[1].js
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\quickdelete_9c14b01a[1].png
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\his[1].htm
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\baiduia_b45d552b[1].js
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\error[1].htm
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\JSocket_9a52fc3e[1].swf
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\union[1].gif
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\zbios_62c636fe[1].png
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\favicon[1].ico
  Creates:                 C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Opens:                   C:\Windows\Prefetch\1AF5338669EFABE0A984147839687-7F9632B6.pf
  Opens:                   C:\Windows
  Opens:                   C:\Windows\System32\wow64.dll
  Opens:                   C:\Windows\SysWOW64
  Opens:                   C:\Windows\SysWOW64\apphelp.dll
  Opens:                   C:\Windows\Temp\1af5338669efabe0a9841478396871b1.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\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
  Opens:                   C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
  Opens:                   C:\Windows\SysWOW64\msimg32.dll
  Opens:                   C:\Windows\SysWOW64\version.dll
  Opens:                   C:\Windows\SysWOW64\sechost.dll
  Opens:                   C:\Windows\SysWOW64\combase.dll
  Opens:                   C:\Windows\SysWOW64\gdi32.dll
  Opens:                   C:\Windows\SysWOW64\user32.dll
  Opens:                   C:\Windows\SysWOW64\msvcrt.dll
  Opens:                   C:\Windows\SysWOW64\bcryptprimitives.dll
  Opens:                   C:\Windows\SysWOW64\cryptbase.dll
  Opens:                   C:\Windows\SysWOW64\sspicli.dll
  Opens:                   C:\Windows\SysWOW64\rpcrt4.dll
  Opens:                   C:\Windows\SysWOW64\advapi32.dll
  Opens:                   C:\Windows\SysWOW64\shlwapi.dll
  Opens:                   C:\Windows\SysWOW64\shell32.dll
  Opens:                   C:\Windows\SysWOW64\ole32.dll
  Opens:                   C:\Windows\SysWOW64\oleaut32.dll
  Opens:                   C:\Windows\SysWOW64\iertutil.dll
  Opens:                   C:\Windows\SysWOW64\wininet.dll
  Opens:                   C:\Windows\SysWOW64\urlmon.dll
  Opens:                   C:\Windows\SysWOW64\nsi.dll
  Opens:                   C:\Windows\SysWOW64\ws2_32.dll
  Opens:                   C:\Windows\SysWOW64\psapi.dll
  Opens:                   C:\Windows\SysWOW64\imm32.dll
  Opens:                   C:\Windows\SysWOW64\msctf.dll
  Opens:                   C:\Windows\WindowsShell.Manifest
  Opens:                   C:\program files\fve31bb\zxz63d\Log.dat
  Opens:                   C:\Windows\SysWOW64\uxtheme.dll
  Opens:                   C:\Users\Admin\AppData\Local\Temp\restart.dat
  Opens:                    C:\Windows\SysWOW64\dwmapi.dll
  Opens:                    C:\Windows\Fonts\StaticCache.dat
  Opens:                    C:\Windows\Fonts\micross.ttf
  Opens:                    C:\Windows\Fonts\tahoma.ttf
  Opens:                    C:\Windows\Fonts\meiryo.ttc
  Opens:                    C:\Windows\Fonts\msgothic.ttc
  Opens:                    C:\Windows\Fonts\msjh.ttc
  Opens:                    C:\Windows\Fonts\msyh.ttc
  Opens:                    C:\Windows\Fonts\malgun.ttf
  Opens:                    C:\Windows\Fonts\mingliu.ttc
  Opens:                    C:\Windows\Fonts\simsun.ttc
  Opens:                    C:\Windows\Fonts\gulim.ttc
  Opens:                    C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                    C:\Windows\SysWOW64\uxtheme.dll.Config
  Opens:                    C:\program files\fve31bb\zxz63d\log.dat
  Opens:                    C:\Windows\SysWOW64\clbcatq.dll
  Opens:                    C:\Windows\SysWOW64\ieframe.dll
  Opens:                    C:\Windows\SysWOW64\SHCore.dll
  Opens:                    C:\Windows\SysWOW64\propsys.dll
  Opens:                    C:\Windows\SysWOW64\secur32.dll
  Opens:                    C:\Windows\SysWOW64\profapi.dll
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\counters.dat
  Opens:                    C:\WINDOWS\Temp\MJPGC.TMP
  Opens:                    C:\Windows\SysWOW64\winhttp.dll
  Opens:                    C:\Windows\SysWOW64\mswsock.dll
  Opens:                    C:\Windows\SysWOW64\en-US\ieframe.dll.mui
  Opens:                    C:\Windows\SysWOW64\IPHLPAPI.DLL
  Opens:                    C:\Windows\SysWOW64\winnsi.dll
  Opens:                    C:\Windows\SysWOW64\dnsapi.dll
  Opens:                    C:\Windows\SysWOW64\cryptsp.dll
  Opens:                    C:\Windows\SysWOW64\rsaenh.dll
  Opens:                    C:\Windows\SysWOW64\mshtml.dll
  Opens:                    C:\Windows\SysWOW64\dhcpcsvc6.dll
  Opens:                    C:\Windows\SysWOW64\dhcpcsvc.dll
  Opens:                    C:\Windows\SysWOW64\rasadhlp.dll
  Opens:                    C:\Windows\System32\Drivers\etc\hosts
  Opens:                    C:\Windows\SysWOW64\FWPUCLNT.DLL
  Opens:                    C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\tiptsf.dll
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\AATKOXA4.txt
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TVGA15OO.txt
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TDSMCW0I.txt
  Opens:                    C:\Windows\SysWOW64\mlang.dll
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\index[1].htm
  Opens:                    C:\Windows\SysWOW64\jscript9.dll
  Opens:                    C:\Windows\SysWOW64\en-US\urlmon.dll.mui
  Opens:                    C:\Windows\SysWOW64\en-US\mshtml.dll.mui
  Opens:                    C:\Windows\SysWOW64\msimtf.dll
  Opens:                    C:\Windows\SysWOW64\powrprof.dll
  Opens:                    C:\Windows\SysWOW64\tzres.dll
  Opens:                    C:\Windows\SysWOW64\en-US\tzres.dll.mui
  Opens:                    C:\Windows\SysWOW64\dxgi.dll
  Opens:                    C:\Windows\SysWOW64\d2d1.dll
  Opens:                    C:\Windows\SysWOW64\DWrite.dll
  Opens:                    C:\Windows\SysWOW64\d3d11.dll
  Opens:                    C:\Windows\SysWOW64\d3d10warp.dll
  Opens:                    C:\Windows\Fonts\arial.ttf
  Opens:                    C:\Windows\SysWOW64\msls31.dll
  Opens:                    C:\Windows\SysWOW64\en-US\mlang.dll.mui
  Opens:                    C:\Windows\Fonts\arialbd.ttf
  Opens:                    C:\Windows\SysWOW64\oleacc.dll
  Opens:                    C:\Windows\SysWOW64\oleaccrc.dll
  Opens:                    C:\Windows\SysWOW64\sxs.dll
  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\LOWEYQNT\jquery-1.10.2.min_f2fb5194[1].js
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\all_async_search_641293e1[1].js
  Opens:                    C:\Windows\SysWOW64\en-US\jscript9.dll.mui
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\O8IATE7C.txt
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\2JLA8H3S.txt
  Opens:                    C:\
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\LOWEYQNT\every_cookie_aa168cb4[1].js
  Opens:                    C:\Windows\SysWOW64\Macromed\Flash\Flash.ocx
  Opens:                    C:\Windows\SysWOW64\winmm.dll
  Opens:                    C:\Windows\SysWOW64\dsound.dll
  Opens:                    C:\Windows\SysWOW64\UIAutomationCore.dll
  Opens:                    C:\Windows\SysWOW64\mscms.dll
  Opens:                    C:\Windows\SysWOW64\winmmbase.dll
  Opens:                    C:\Windows\SysWOW64\userenv.dll
  Opens:                  C:\Windows\SysWOW64\msasn1.dll
  Opens:                  C:\Windows\SysWOW64\crypt32.dll
  Opens:                  C:\Windows\SysWOW64\comdlg32.dll
  Opens:                  C:\Windows\SysWOW64\Macromed\Flash\ss.sgn
  Opens:                  C:\Windows\SysWOW64\Macromed\Flash
  Opens:                  C:\Windows\SysWOW64\Macromed\Flash\ss.cfg
  Opens:                  C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
  Opens:                  C:\Windows\SysWOW64\Macromed\Flash\oem.cfg
  Opens:                  C:\Windows\SysWOW64\oem.cfg
  Opens:                  C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
  Opens:                  C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
  Opens:                  C:\Windows\SysWOW64\stdole2.tlb
  Opens:                  C:\Windows\SysWOW64\iepeers.dll
  Opens:                  C:\Windows\SysWOW64\xmllite.dll
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\NRKAPV8T\www.baidu[1].xml
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\nu_instant_search_ebeb5baa[1].js
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\env_beb83b45[1].swf
  Opens:                  C:\Windows\SysWOW64\msxml3.dll
  Opens:                  C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
  Opens:                  C:\Windows\SysWOW64\msxml3r.dll
  Opens:                  C:\Windows\SysWOW64\en-US\msxml3r.dll.mui
  Opens:                  C:\Windows\SysWOW64\schannel.dll
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\macromedia.com\support\flashplayer\sys\settings.sol
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\macromedia.com\support\flashplayer\sys\
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sol
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\s1.bdstatic.com\
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\#AppContainer\s1.bdstatic.com\
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com
  Opens:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\3L1D4SUG\userDataBIDUPSID[1].xml
  Opens:                  C:\Windows\SysWOW64\MMDevAPI.dll
  Opens:                  C:\Windows\SysWOW64\cfgmgr32.dll
  Opens:                  C:\Windows\SysWOW64\devobj.dll
  Opens:                  C:\Windows\SysWOW64\actxprxy.dll
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\bdsug_async_dac7ea02[1].js
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\baiduia_b45d552b[1].js
  Opens:                  C:\Windows\SysWOW64\netmsg.dll
  Opens:                  C:\Windows\SysWOW64\en-US\netmsg.dll.mui
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\JSocket_9a52fc3e[1].swf
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000010.db
  Opens:                  C:\Users\desktop.ini
  Opens:                    C:\Windows\SysWOW64\setupapi.dll
  Opens:                    C:\Windows\SysWOW64\en-US\setupapi.dll.mui
  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\Windows
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Opens:                    C:\Windows\SysWOW64\en-US\shell32.dll.mui
  Opens:                    C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\favicon[1].ico
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\AATKOXA4.txt
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TVGA15OO.txt
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TDSMCW0I.txt
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\index[1].htm
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\baidu_jgylogo3[1].gif
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\jquery-1.10.2.min_f2fb5194[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\nuomi_510f7472[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\icons_0e814c16[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\all_async_search_641293e1[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\bd_logo1[1].png
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\08IATE7C.txt
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\2JLA8H3S.txt
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\every_cookie_aa168cb4[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\NRKAPV8T\www.baidu[1].xml
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\nu_instant_search_ebeb5baa[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\env_beb83b45[1].swf
  Writes to:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Writes to:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Writes to:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\3L1D4SUG\userDataBIDUPSID[1].xml
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\bdsug_async_dac7ea02[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\his[1].htm
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\quickdelete_9c14b01a[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\error[1].htm
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\baiduia_b45d552b[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\JSocket_9a52fc3e[1].swf
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\zbios_62c636fe[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\favicon[1].ico
  Writes to:                C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Reads from:               C:\Windows\Fonts\StaticCache.dat
  Reads from:               C:\Windows\Temp\1af5338669efabe0a9841478396871b1.exe
  Reads from:               C:\Windows\System32\Drivers\etc\hosts
  Reads from:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\jquery-1.10.2.min_f2fb5194[1].js
  Reads from:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\all_async_search_641293e1[1].js
  Reads from:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\every_cookie_aa168cb4[1].js
  Reads from:               C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
  Reads from:               C:\Windows\SysWOW64\Macromed\Flash\Flash.ocx
  Reads from:               C:\Windows\SysWOW64\stdole2.tlb
  Reads from:               C:\Windows\SysWOW64\iepeers.dll
  Reads from:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\nu_instant_search_ebeb5baa[1].js
  Reads from:               C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
  Reads from:               C:\Users\Admin\AppData\Roaming\Macromedia\Flash
```

```
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Reads from:             C:\Windows\SysWOW64\ieframe.dll
  Reads from:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\bdsug_async_dac7ea02[1].js
  Reads from:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\baiduia_b45d552b[1].js
  Reads from:             C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Reads from:             C:\Users\desktop.ini
  Reads from:             C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Reads from:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\L0WEYQNT\favicon[1].ico
  Deletes:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Deletes:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
  Deletes:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Deletes:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
```

Network Events

```
  DNS query:              www.baidu.com
  DNS query:              s1.bdstatic.com
  DNS query:              sclick.baidu.com
  DNS query:              formi.baidu.com
  DNS response:           www.a.shifen.com ⇒ 103.235.46.39
  DNS response:           wwwstatic1.gshifen.com ⇒ 103.235.44.90
  DNS response:           s.a.shifen.com ⇒ 123.125.115.95
  DNS response:           formi.baidu.com ⇒ 61.135.169.120
  DNS response:           formi.baidu.com ⇒ 180.149.131.55
  Connects to:            8.8.8.8:53
  Connects to:            103.235.46.39:80
  Connects to:            127.0.0.1:63162
  Connects to:            103.235.44.90:80
  Connects to:            123.125.115.95:80
  Connects to:            61.135.169.120:843
  Connects to:            61.135.169.120:8843
  Sends data to:          8.8.8.8:53
  Sends data to:          127.0.0.1:63162
  Sends data to:          www.a.shifen.com:80 (103.235.46.39)
  Sends data to:          wwwstatic1.gshifen.com:80 (103.235.44.90)
  Sends data to:          s.a.shifen.com:80 (123.125.115.95)
  Receives data from:     8.8.8.8:53
  Receives data from:     127.0.0.1:63162
  Receives data from:     www.a.shifen.com:80 (103.235.46.39)
  Receives data from:     wwwstatic1.gshifen.com:80 (103.235.44.90)
  Receives data from:     s.a.shifen.com:80 (123.125.115.95)
```

Windows Registry Events

```
  Creates key:            HKCU\software\explore
  Creates key:            HKCU\software\microsoft\windows\currentversion\internet settings
  Creates key:            HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Creates key:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Creates key:            HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:            HKCU\software\microsoft\windows\currentversion\explorer\runmru
  Creates key:            HKCU\software\microsoft\internet explorer\typedurls
  Creates key:            HKCU\software\microsoft\windows\currentversion\explorer\typedpaths
  Creates key:            HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
  Creates key:            HKCU\software\microsoft\internet explorer\main
  Creates key:            HKLM\system\currentcontrolset\control\securityproviders\schannel
  Creates key:            HKCU\software\microsoft\internet explorer\domstorage\total
  Creates key:            HKCU\software\microsoft\internet explorer\domstorage\baidu.com
  Creates key:            HKCU\software\macromedia\flashplayer
  Creates key:            HKCU\software\microsoft\internet explorer\main\windowssearch
  Creates key:            HKLM\software\wow6432node\microsoft\downloadmanager
  Deletes value:          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
  Deletes value:          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
  Deletes value:          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
  Deletes value:          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
  Deletes value:          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Deletes value:          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Deletes value:          HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[autoconfigurl]
  Deletes value:          HKCU\software\microsoft\windows\currentversion\internet
settings[autodetect]
  Opens key:              HKLM\software\microsoft\wow64
  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\appcompatflags\disable8and16bitmitigation
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  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\
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  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\wow6432node\microsoft\oleaut
  Opens key:              HKCU\software\microsoft\internet explorer\main
  Opens key:              HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:              HKLM\software\microsoft\sqmclient\windows
  Opens key:              HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:              HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:              HKLM\system\currentcontrolset\control\nls\locale
  Opens key:              HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:              HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\1af5338669efabe0a9841478396871b1.exe
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
  Opens key:              HKCU\software\explore
  Opens key:              HKCU\software\classes\
  Opens key:              HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}
  Opens key:                HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
  Opens key:                HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{889d2feb-5411-4565-8998-
1dd2c5261283}
  Opens key:                HKCR\activatableclasses\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{889d2feb-5411-4565-8998-
1dd2c5261283}
  Opens key:                HKCR\wow6432node\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key:                HKCU\software\classes\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key:                HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key:                HKCU\software\classes\activatableclasses\clsid
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{889d2feb-5411-4565-8998-
1dd2c5261283}
  Opens key:                HKCU\software\policies\microsoft\windows\app management
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows\app management
  Opens key:                HKLM\software\policies\microsoft\windows\app management
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{004b0726-a010-4abf-8556-
fcdb7f1fca1e}
  Opens key:                HKCR\activatableclasses\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{004b0726-a010-4abf-8556-
fcdb7f1fca1e}
  Opens key:                HKCR\wow6432node\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  Opens key:                HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  Opens key:                HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{004b0726-a010-4abf-8556-
fcdb7f1fca1e}
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\knownclasses
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  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:                HKLM\software\wow6432node\policies\microsoft\internet
explorer\main\featurecontrol
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer\main
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet explorer\main
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\msinternal_metro_allow_tpg_zero
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\msinternal_metro_allow_tpg_zero
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\1af5338669efabe0a9841478396871b1.exe
```

```
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder
  Opens key:                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
  Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\shell
extensions\blocked
  Opens key:                 HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
  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\currentversion\shell extensions\cached
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}
  Opens key:                 HKCR\activatableclasses\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}
  Opens key:                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-
42a0-1069-a2ea-08002b30309d}
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
  Opens key:                 HKLM\software\wow6432node\microsoft\rpc
  Opens key:                 HKLM\software\microsoft\rpc
  Opens key:                 HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                 HKLM\system\setup
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  Opens key:                 HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                 HKLM\software\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-ba85-6007caedcf9d}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}\propertybag
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  Opens key:                 HKU\
  Opens key:                 HKU\.default
  Opens key:                 HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
  Opens key:                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                 HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                 HKLM\software\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                 HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
  Opens key:                 HKLM\software\wow6432node\policies
  Opens key:                 HKCU\software\policies
  Opens key:                 HKCU\software
  Opens key:                 HKLM\software\wow6432node
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\internet explorer
  Opens key:                 HKLM\software\policies\microsoft\internet explorer
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
```

```
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
  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
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\024bd1a1
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
  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\policies\microsoft\internet
explorer\browseremulation
  Opens key:                HKLM\software\policies\microsoft\internet explorer\browseremulation
  Opens key:                HKCU\software\policies\microsoft\internet explorer\browseremulation
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  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\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  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:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
```

```
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\zonemap\ranges\
  Opens key:                HKCU\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                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:                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:                HKLM\software\policies\microsoft\internet explorer\security
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
  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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
  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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
  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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
  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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  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:                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\wow6432node\policies\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\wow6432node\policies\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\wow6432node\policies\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\wow6432node\policies\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\wow6432node\policies\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:                HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\system\currentcontrolset\services\dns
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp
  Opens key:                HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters
  Opens key:                HKCU\software\microsoft\internet explorer
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer
  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\http\
  Opens key:                 HKCR\protocols\name-space handler\http
  Opens key:                 HKCU\software\classes\protocols\name-space handler\*\
  Opens key:                 HKCR\protocols\name-space handler\*
  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_maxconnectionsperserver
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
  Opens key:                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:                 HKLM\software\policies\microsoft\peerdist\service
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\peerdist\service
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_urlmon_iqda_size
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_urlmon_iqda_size
  Opens key:                 HKCU\software\microsoft\windows\currentversion\urlmon settings
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\internet
explorer\browserstorage\appcache
  Opens key:                 HKLM\software\policies\microsoft\internet
explorer\browserstorage\appcache
  Opens key:                 HKCU\software\policies\microsoft\internet
explorer\browserstorage\appcache
  Opens key:                 HKCU\software\microsoft\internet explorer\browserstorage\appcache
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\browserstorage\appcache
  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\rpc\extensions
  Opens key:                 HKLM\software\microsoft\rpc\extensions
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{00000323-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\activatableclasses\clsid\{00000323-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00000323-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\wow6432node\clsid\{00000323-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\clsid\{00000323-0000-0000-c000-000000000046}
  Opens key:                 HKCR\clsid\{00000323-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\activatableclasses\clsid\{00000323-0000-0000-c000-
000000000046}
  Opens key:                 HKCU\software\classes\appid\1af5338669efabe0a9841478396871b1.exe
  Opens key:                 HKCR\appid\1af5338669efabe0a9841478396871b1.exe
  Opens key:                 HKLM\software\wow6432node\microsoft\ole\appcompat
  Opens key:                 HKLM\software\microsoft\ole\appcompat
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
  Opens key:                 HKLM\software\policies\microsoft\cryptography
  Opens key:                 HKLM\software\microsoft\cryptography
  Opens key:                 HKLM\software\wow6432node\microsoft\cryptography\offload
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}
```

```
  Opens key:                HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}
  Opens key:                HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}
  Opens key:                HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
  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\microsoft\internet explorer\international
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows\explorer
  Opens key:                HKLM\software\policies\microsoft\windows\explorer
  Opens key:                HKCU\software\policies\microsoft\windows\explorer
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{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\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}\propertybag
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\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\protocols\name-space handler
  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:                  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_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_fls
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\outlook.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet
explorer\domstorage
  Opens key:                HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:                HKCU\software\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\persistence
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet
```

```
explorer\persistence
  Opens key:                HKLM\software\policies\microsoft\internet explorer\persistence
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\travellog
  Opens key:                HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key:                HKLM\software\policies\microsoft\system\dnsclient
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-
25b8d56dd1d8}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:
HKCU\software\policies\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:
HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}
  Opens key:                HKCR\activatableclasses\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}
  Opens key:                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\treatas
  Opens key:                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}
  Opens key:                HKCR\activatableclasses\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}
  Opens key:                HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\treatas
  Opens key:                HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}
  Opens key:                HKCR\activatableclasses\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}
  Opens key:                HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}
  Opens key:                 HKCR\activatableclasses\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}
  Opens key:                 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client\
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}
  Opens key:                 HKCR\activatableclasses\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}
  Opens key:                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\baidu.com
  Opens key:                 HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
  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_feeds
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds
  Opens key:                 HKCU\software\classes\mime\database\content type\text/html
  Opens key:                 HKCR\mime\database\content type\text/html
  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\classes\protocols\name-space handler\about\
  Opens key:                 HKCR\protocols\name-space handler\about
  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:                 HKLM\software\wow6432node\policies\microsoft\internet explorer\zoom
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\zoom
  Opens key:                 HKCU\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:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\url history
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\url history
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\url
history
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url history
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\internet
explorer\international\scripts
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\international\scripts
  Opens key:                 HKCU\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\wow6432node\policies\microsoft\internet explorer\settings
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\settings
  Opens key:                 HKCU\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\{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\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\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:                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\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_use_builtin_accept_headers
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_use_builtin_accept_headers
  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\policies\microsoft\internet explorer\low rights
  Opens key:                HKCU\software\policies\microsoft\internet explorer
  Opens key:                HKCU\software\microsoft\internet explorer\low rights
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer\low rights
  Opens key:                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\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
```

```
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_paint_for_page_enter
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_paint_for_page_enter
  Opens key:                HKCU\software\microsoft\internet explorer\browseremulation
  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:                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\microsoft\windowsruntime\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}
  Opens key:                HKCR\activatableclasses\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}
  Opens key:                HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\treatas
  Opens key:                HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler
  Opens key:                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:                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:                HKCU\software\policies\microsoft\internet explorer\control panel
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:                HKCU\software\microsoft\direct3d
  Opens key:                HKLM\software\wow6432node\microsoft\direct3d
  Opens key:                HKLM\software\wow6432node\microsoft\direct3d\drivers
  Opens key:                HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist
  Opens key:                HKCU\software\microsoft\dxgi
  Opens key:                HKLM\software\wow6432node\microsoft\dxgi
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet explorer\recovery
  Opens key:                HKLM\software\policies\microsoft\internet explorer\recovery
  Opens key:                HKCU\software\policies\microsoft\internet explorer\recovery
  Opens key:                HKCU\software\microsoft\internet explorer\recovery
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key:                HKLM\system\currentcontrolset\services\fontcache\parameters
  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:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer\default behaviors
  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\eudc\
  Opens key:                 HKCU\eudc\1252
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}
  Opens key:                 HKCR\activatableclasses\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}
  Opens key:                 HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler
  Opens key:                 HKCU\software\microsoft\internet explorer\international\scripts\26
  Opens key:                 HKLM\software\wow6432node\microsoft\avalon.graphics
  Opens key:                 HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
  Opens key:                 HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}
  Opens key:                 HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\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\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\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:                 HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
  Opens key:                 HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows
  Opens key:                 HKLM\software\microsoft\telemetryclient\throttlestore\sqm
  Opens key:                 HKLM\software\microsoft\telemetryclient\throttlestore
  Opens key:                 HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
  Opens key:                 HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
  Opens key:                 HKLM\software\microsoft\telemetryclient\samplestore\sqm
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238528
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
  Opens key:                 HKLM\software\wow6432node\microsoft\ctf\tip\
  Opens key:                 HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{03b5835f-f03c-411b-9ce2-
aa23e1171e36}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{07eb03d6-b001-41df-9192-
bf9b841ee71f}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
```

```
  Opens key:                  HKLM\software\microsoft\ctf\tip\{3697c5fa-60dd-4b56-92d4-
74a569205c16}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{531fdebf-9b4c-4a43-a2aa-
960e8fcdc732}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{81d4e9c9-1d3b-41bc-9e6c-
4b40bf79e35e}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{8613e14c-d0c0-4161-ac0f-
1dd2563286bc}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{a028ae76-01b1-46c2-99c4-
acd9858ae02f}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{a1e2b86b-924a-4d43-80f6-
8a820df7190f}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{ae6be008-07fb-400d-8beb-
337a64f7051f}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{e429b25a-e5d3-4d1f-9be3-
0c608477e3a1}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{f25e9f57-2fc8-4eb3-a41a-
cce5f08541e6}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{03b5835f-f03c-411b-9ce2-
aa23e1171e36}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{07eb03d6-b001-41df-9192-
bf9b841ee71f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{3697c5fa-60dd-4b56-92d4-
74a569205c16}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{531fdebf-9b4c-4a43-a2aa-
960e8fcdc732}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{81d4e9c9-1d3b-41bc-9e6c-
4b40bf79e35e}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{8613e14c-d0c0-4161-ac0f-
1dd2563286bc}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{a028ae76-01b1-46c2-99c4-
acd9858ae02f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{a1e2b86b-924a-4d43-80f6-
8a820df7190f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{ae6be008-07fb-400d-8beb-
337a64f7051f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{e429b25a-e5d3-4d1f-9be3-
0c608477e3a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{f25e9f57-2fc8-4eb3-a41a-
cce5f08541e6}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                  HKCU\software\microsoft\ctf\cuas
  Opens key:                  HKCU\software\microsoft\avalon.graphics
  Opens key:                  HKLM\software\microsoft\windowsruntime\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}
  Opens key:                  HKCR\activatableclasses\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}
  Opens key:                  HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\treatas
  Opens key:                  HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\treatas
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32
  Opens key:                  HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler32
  Opens key:                  HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler
  Opens key:                  HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-
c6b61110b681}\instance
```

```
  Opens key:                 HKCR\wow6432node\clsid\{fae3d380-fea4-4623-8c75-c6b61110b681}\instance
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-
c6b61110b681}\instance\disabled
  Opens key:                 HKCR\wow6432node\clsid\{fae3d380-fea4-4623-8c75-
c6b61110b681}\instance\disabled
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
  Opens key:                 HKCU\software\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:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
  Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
  Opens key:                 HKCU\software\microsoft\internet explorer\new windows
  Opens key:                 HKLM\software\wow6432node\microsoft\internet explorer\new windows
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{7835eae8-bf14-49d1-93ce-
533a407b2248}\instance
  Opens key:                 HKCR\wow6432node\clsid\{7835eae8-bf14-49d1-93ce-533a407b2248}\instance
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}
  Opens key:                 HKCR\activatableclasses\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}
  Opens key:                 HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
  Opens key:                 HKCU\software\microsoft\internet explorer\feed discovery
  Opens key:                 HKLM\software\wow6432node\microsoft\internet explorer\feed discovery
  Opens key:                 HKCU\software\microsoft\ftp
  Opens key:                 HKCU\software\classes\shockwaveflash.shockwaveflash
  Opens key:                 HKCR\shockwaveflash.shockwaveflash
  Opens key:                 HKCU\software\classes\shockwaveflash.shockwaveflash\clsid
  Opens key:                 HKCR\shockwaveflash.shockwaveflash\clsid
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}
  Opens key:                 HKCR\activatableclasses\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}
  Opens key:                 HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler
```

```
  Opens key:              HKLM\system\currentcontrolset\services\crypt32
  Opens key:              HKLM\hardware\description\system\centralprocessor\0
  Opens key:              HKCU\software\classes\typelib
  Opens key:              HKCR\typelib
  Opens key:              HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
  Opens key:              HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
  Opens key:              HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
  Opens key:              HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
  Opens key:              HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\409
  Opens key:              HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\409
  Opens key:              HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\9
  Opens key:              HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9
  Opens key:              HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0
  Opens key:              HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0
  Opens key:              HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0\win32
  Opens key:              HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32
  Opens key:              HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:              HKCR\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:              HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:              HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:              HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
  Opens key:              HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
  Opens key:              HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
  Opens key:              HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
  Opens key:              HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
  Opens key:              HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
  Opens key:              HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens key:              HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens key:              HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0
  Opens key:              HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0
  Opens key:              HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0\win32
  Opens key:              HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\time
zones\w. europe standard time\dynamic dst
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe
standard time\dynamic dst
  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:              HKLM\software\wow6432node\policies\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:              HKLM\software\policies\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:              HKLM\software\wow6432node\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  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:              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\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  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\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:              HKCU\software\classes\wow6432node\clsid
  Opens key:              HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
  Opens key:              HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
  Opens key:              HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
  Opens key:              HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
  Opens key:              HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\appid
```

```
  Opens key:                HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
  Opens key:                HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\languagecheckperiod
  Opens key:                HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\languagecheckperiod
  Opens key:                HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus
  Opens key:                HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus
  Opens key:                HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus\1
  Opens key:                HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus\1
  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:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\disablefcm
  Opens key:                HKCU\software\microsoft\internet explorer\domstorage\baidu.com
  Opens key:                HKCU\software\classes\protocols\filter\application/x-shockwave-flash
  Opens key:                HKCR\protocols\filter\application/x-shockwave-flash
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}
  Opens key:                HKCR\activatableclasses\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}
  Opens key:                HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\treatas
  Opens key:                HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprochandler
  Opens key:                HKLM\software\wow6432node\microsoft\msxml30
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}\propertybag
  Opens key:                HKCU\software\microsoft\internet explorer\domstorage\total
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\system
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\system
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}
  Opens key:                HKCR\activatableclasses\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  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\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:                HKLM\software\microsoft\windowsruntime\clsid\{0000032a-0000-0000-c000-
000000000046}
```

```
   Opens key:                 HKCR\activatableclasses\clsid\{0000032a-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{0000032a-0000-0000-c000-
000000000046}
   Opens key:                 HKCR\wow6432node\clsid\{0000032a-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\clsid\{0000032a-0000-0000-c000-000000000046}
   Opens key:                 HKCR\clsid\{0000032a-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\activatableclasses\clsid\{0000032a-0000-0000-c000-
000000000046}
   Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{00000339-0000-0000-c000-
000000000046}
   Opens key:                 HKCR\activatableclasses\clsid\{00000339-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00000339-0000-0000-c000-
000000000046}
   Opens key:                 HKCR\wow6432node\clsid\{00000339-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\clsid\{00000339-0000-0000-c000-000000000046}
   Opens key:                 HKCR\clsid\{00000339-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\activatableclasses\clsid\{00000339-0000-0000-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:                 HKLM\software\microsoft\windowsruntime\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}
   Opens key:                 HKCR\activatableclasses\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}
   Opens key:                 HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\treatas
   Opens key:                 HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}\treatas
   Opens key:                 HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
   Opens key:                 HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32
   Opens key:                 HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
   Opens key:                 HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
   Opens key:                 HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
   Opens key:                 HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
   Opens key:                 HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
   Opens key:                 HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler32
   Opens key:                 HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler
   Opens key:                 HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler
   Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
   Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
   Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
   Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
   Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
   Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
   Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
   Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
   Opens key:                 HKLM\software\microsoft\windows\currentversion\mmdevices\audio\render\
   Opens key:                 HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}
   Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32
   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\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
   Opens key:                 HKLM\software\microsoft\windows\currentversion\mmdevices\audio\capture\
   Opens key:                 HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-
a3cc-00a0c9223196}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
   Opens key:                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
   Opens key:                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
   Opens key:                 HKCU\software\classes\wow6432node\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\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}
   Opens key:                 HKCR\wow6432node\interface\{00020404-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
   Opens key:                 HKCR\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
   Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{00020421-0000-0000-c000-
000000000046}
   Opens key:                 HKCR\activatableclasses\clsid\{00020421-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}
   Opens key:                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\treatas
   Opens key:                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\treatas
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32
   Opens key:                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler32
   Opens key:                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler
   Opens key:                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler
   Opens key:                 HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}
   Opens key:                 HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}
   Opens key:                 HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\proxystubclsid32
   Opens key:                 HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\proxystubclsid32
   Opens key:                 HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
```

```
00c04fc9e26e}\forward
  Opens key:                 HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\forward
  Opens key:                 HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\forward
  Opens key:                 HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\forward
  Opens key:                 HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\typelib
  Opens key:                 HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\typelib
  Opens key:                 HKCU\software\classes\shockwaveflash.shockwaveflash.7
  Opens key:                 HKCR\shockwaveflash.shockwaveflash.7
  Opens key:                 HKCU\software\classes\shockwaveflash.shockwaveflash.7\clsid
  Opens key:                 HKCR\shockwaveflash.shockwaveflash.7\clsid
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{7ed96837-96f0-4812-b211-
f13c24117ed3}\instance
  Opens key:                 HKCR\wow6432node\clsid\{7ed96837-96f0-4812-b211-f13c24117ed3}\instance
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\services
  Opens key:                 HKCU\software\microsoft\internet explorer\services
  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\policies\microsoft\internet
explorer\infodelivery\restrictions
  Opens key:                 HKCU\software\policies\microsoft\internet
explorer\infodelivery\restrictions
  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:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-
a2d8-08002b30309d}\shellfolder
  Opens key:                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
  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-be65-806e6f6e6963}\
  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:                 HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32
  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\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\microsoft\windows\currentversion\explorer\
  Opens key:                 HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32
  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:                HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion
  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:                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\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}\
  Opens key:                HKCU\software\classes\directory\browseinplace
  Opens key:                HKCR\directory\browseinplace
  Opens key:                HKCU\software\classes\folder\browseinplace
  Opens key:                HKCR\folder\browseinplace
  Opens key:                HKCU\software\classes\allfilesystemobjects\browseinplace
  Opens key:                HKCR\allfilesystemobjects\browseinplace
  Opens key:                HKCU\software\classes\directory\clsid
  Opens key:                HKCR\directory\clsid
  Opens key:                HKCU\software\classes\folder\clsid
  Opens key:                HKCR\folder\clsid
  Opens key:                HKCU\software\classes\allfilesystemobjects\clsid
  Opens key:                HKCR\allfilesystemobjects\clsid
  Opens key:                HKCU\software\classes\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\1af5338669efabe0a9841478396871b1.exe
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\1af5338669efabe0a9841478396871b1.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\app
paths\1af5338669efabe0a9841478396871b1.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:                HKCU\software\microsoft\internet explorer\main\windowssearch
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer\main\windowssearch
  Opens key:                HKLM\software\policies\microsoft\internet explorer\feeds
  Opens key:                HKCU\software\microsoft\internet explorer\feeds
  Opens key:                HKLM\software\wow6432node\microsoft\internet explorer\feeds
  Opens key:                HKLM\software\wow6432node\microsoft\windows search
  Opens key:                HKCU\software\classes\protocols\filter\image/x-icon
  Opens key:                HKCR\protocols\filter\image/x-icon
  Opens key:                HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
  Opens key:               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
  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\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
  Queries value:           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[1af5338669efabe0a9841478396871b1.exe]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:           HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[1af5338669efabe0a9841478396871b1]
  Queries value:           HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:           HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:           HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:           HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:           HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:           HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:           HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:           HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  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\locale[00000409]
  Queries value:           HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:           HKLM\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\fontsubstitutes[segoe
ui]
  Queries value:           HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
  Queries value:              HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:              HKLM\software\microsoft\com3[com+enabled]
  Queries value:              HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
  Queries value:              HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[5c8bb950-959e-4309-
8908-67961a1205d5]
  Queries value:              HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  Queries value:              HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main[frametabwindow]
  Queries value:              HKCU\software\microsoft\internet explorer\main[framemerging]
  Queries value:              HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]
  Queries value:              HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main[sessionmerging]
  Queries value:              HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main[admintabprocs]
  Queries value:              HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main[tabprocgrowth]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main[navigationdelay]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[foldervalueflags]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
  Queries value:              HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xffff]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
```

```
  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\rpc[idletimerwindow]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
  Queries value:              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[mbcsapiforcrack]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[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[preresolvelimit]
  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[enableautoproxyresultcache]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[serverinfotimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:              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\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
```

```
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
```

```
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[usefirstavailable]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[combinefalsestartdata]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablefalsestartblacklist]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enforcep3pvalidity]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
  Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:              HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Queries value:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
  Queries value:              HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
  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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autodetect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
  Queries value:              HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
```

```
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
  Queries value:
HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[winhttplowercasehost]
  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:              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:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
  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\software\microsoft\windows
nt\currentversion\peerdist\service[enable]
  Queries value:            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
  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}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
  Queries value:            HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:            HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:            HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:            HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
```

```
provider[image path]
   Queries value:             HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
   Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
   Queries value:             HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
   Queries value:             HKLM\software\microsoft\cryptography[machineguid]
   Queries value:             HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
   Queries value:             HKCR\wow6432node\interface\{a168aadc-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:             HKCU\software\microsoft\internet explorer\international[acceptlanguage]
   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}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
   Queries value:             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001[profileimagepath]
   Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
   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}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[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:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[infotip]
   Queries value:
```

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

```
b784-432e-a781-5a1130a75963}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[initfolderhandler]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
   Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.exe]
   Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
   Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.exe]
   Queries value:              HKCU\software\microsoft\internet explorer\domstorage[totallimit]
   Queries value:              HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
   Queries value:              HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
```

```
806e6f6e6963}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpnameserver]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[enablemulticast]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enableadapterdomainnameregistration]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enablemulticast]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
   Queries value:              HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
   Queries value:              HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
   Queries value:              HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
   Queries value:              HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[threadingmodel]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[mrulist]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
   Queries value:              HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
```

```
  Queries value:               HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:               HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[]
  Queries value:               HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:               HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
  Queries value:               HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:               HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[]
  Queries value:               HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:               HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
  Queries value:               HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
  Queries value:               HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
  Queries value:               HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[]
  Queries value:               HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
  Queries value:               HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
  Queries value:               HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001[name]
  Queries value:               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[1af5338669efabe0a9841478396871b1.exe]
  Queries value:               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
  Queries value:               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds[1af5338669efabe0a9841478396871b1.exe]
  Queries value:               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds[*]
  Queries value:               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[1af5338669efabe0a9841478396871b1.exe]
  Queries value:               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  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:               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:               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\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\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\windows\currentversion\internet
settings\url history[daystokeep]
  Queries value:            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[1af5338669efabe0a9841478396871b1.exe]
  Queries value:            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
  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[smoothscroll]
  Queries value:            HKCU\software\microsoft\internet explorer\main[xmlhttp]
  Queries value:            HKCU\software\microsoft\internet explorer\main[show image placeholders]
  Queries value:            HKCU\software\microsoft\internet explorer\main[disable script debugger]
  Queries value:            HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
  Queries value:            HKCU\software\microsoft\internet explorer\main[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[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[jscriptprofilecacheeventdelay]
  Queries value:            HKCU\software\microsoft\internet
explorer\international[default_codepage]
  Queries value:            HKCU\software\microsoft\internet explorer\international[autodetect]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[anchor color]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[anchor color visited]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[anchor color hover]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[always use my colors]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[always use my font
size]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[always use my font
face]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[use anchor hover
color]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[miscflags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
  Queries value:            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:            HKCU\software\microsoft\internet explorer\pagesetup[print_background]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[950]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsize]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
  Queries value:            HKCU\software\microsoft\internet
```

```
explorer\international\scripts\3[iefixedfontname]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
  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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[*]
  Queries value:              HKCR\mime\database\content type\text/xml[clsid]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[*]
  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:              HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}[]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:              HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-
8bc445b9828f}\inprocserver32[inprocserver32]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
  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:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
  Queries value:              HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
  Queries value:              HKLM\software\wow6432node\microsoft\internet explorer\low
rights[protectedmodeoffforallzones]
  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:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
  Queries value:              HKCU\software\microsoft\internet explorer\main[operationaldata]
  Queries value:              HKCU\software\microsoft\internet
explorer\browseremulation[cvlistxmlversionlow]
  Queries value:              HKCU\software\microsoft\internet
explorer\browseremulation[cvlistxmlversionhigh]
  Queries value:              HKCU\software\microsoft\internet
explorer\browseremulation[iecompatversionlow]
  Queries value:              HKCU\software\microsoft\internet
explorer\browseremulation[iecompatversionhigh]
  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:              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
  Queries value:              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:              HKLM\software\wow6432node\microsoft\direct3d\drivers[size]
  Queries value:              HKLM\software\wow6432node\microsoft\direct3d\drivers[name]
  Queries value:
HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist[size]
  Queries value:
HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist[name]
  Queries value:              HKCU\software\microsoft\internet explorer\recovery[autorecover]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
  Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[clientcachesize]
  Queries value:              HKCU\software\microsoft\internet explorer\gpu[adapterinfo]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
```

```
explorer\main\featurecontrol\feature_behaviors[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[*]
  Queries value:              HKLM\software\wow6432node\microsoft\internet explorer\default
behaviors[homepage]
  Queries value:              HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
  Queries value:              HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[threadingmodel]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[874]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1361]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsize]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsizeprivate]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iepropfontname]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iefixedfontname]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-cn]
  Queries value:              HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32[]
  Queries value:              HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32[]
  Queries value:              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a5ea4f8e]
  Queries value:              HKLM\software\microsoft\sqmclient\windows[studyid]
  Queries value:              HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
  Queries value:              HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}[]
  Queries value:              HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[*]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
  Queries value:              HKCU\software\microsoft\internet explorer\new
windows[accuserinitonclick]
  Queries value:              HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
  Queries value:              HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
  Queries value:              HKLM\software\wow6432node\microsoft\internet explorer\feed
discovery[sound]
  Queries value:              HKCU\software\microsoft\ftp[use web based ftp]
  Queries value:              HKCR\shockwaveflash.shockwaveflash\clsid[]
  Queries value:              HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
  Queries value:              HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
```

```
444553540000}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32[threadingmodel]
  Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
bc58-54c27d745f8f]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
958a-dad20c90073c]
  Queries value:              HKLM\hardware\description\system\centralprocessor\0[~mhz]
  Queries value:              HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
  Queries value:              HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
  Queries value:              HKLM\software\wow6432node\microsoft\internet explorer\default
behaviors[userdata]
  Queries value:              HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection[*]
  Queries value:              HKLM\software\policies\microsoft\internet explorer[disableflashinie]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_addon_management[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_addon_management[*]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:              HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus\1[]
  Queries value:              HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}[]
  Queries value:              HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32[threadingmodel]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1606]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
```

```
02e7-4e5d-b744-2eb1ae5198b7}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-
02e7-4e5d-b744-2eb1ae5198b7}[initfolderhandler]
   Queries value:              HKCU\software\microsoft\internet explorer\domstorage\total[]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
   Queries value:              HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
   Queries value:              HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}[]
   Queries value:              HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32[]
   Queries value:              HKCU\software\macromedia\flashplayer[flashplayerversion]
   Queries value:              HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32[]
   Queries value:              HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib[]
   Queries value:              HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32[threadingmodel]
   Queries value:              HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib[version]
   Queries value:              HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
   Queries value:              HKLM\software\microsoft\rpc[udtalignmentpolicy]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave1]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave2]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave3]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave4]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave5]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave6]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave7]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave8]
   Queries value:              HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32[]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave9]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi1]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi2]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi3]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi4]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi5]
   Queries value:              HKLM\software\wow6432node\microsoft\windows
```

```
nt\currentversion\drivers32[midi6]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi7]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi8]
  Queries value:              HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi9]
  Queries value:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:              HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-
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\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value:              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\proxystubclsid32[]
  Queries value:              HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\typelib[]
  Queries value:              HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\typelib[version]
  Queries value:              HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Queries value:              HKCR\shockwaveflash.shockwaveflash.7\clsid[]
  Queries value:              HKCU\software\microsoft\internet
explorer\browseremulation[mscompatibilitymode]
  Queries value:              HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
  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:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
  Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
  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\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:              HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
  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[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\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
   Queries value:              HKCR\directory[docobject]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   Queries value:              HKCR\folder[docobject]
   Queries value:              HKCR\allfilesystemobjects[docobject]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[data]
   Queries value:              HKCR\directory[browseinplace]
   Queries value:              HKCR\folder[browseinplace]
   Queries value:              HKCR\allfilesystemobjects[browseinplace]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[generation]
   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:              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[loadwithoutcom]
   Queries value:              HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046}
0xffff]
   Queries value:              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]
   Queries value:              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[threadingmodel]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}[]
   Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}[localizedstring]
   Queries value:              HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
   Queries value:              HKLM\software\wow6432node\microsoft\windows search[currentversion]
   Queries value:              HKLM\software\wow6432node\microsoft\downloadmanager[cacheok]
   Sets/Creates value:         HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
   Value changes:              HKCU\software\microsoft\internet explorer\main[disable script debugger]
   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[proxyenable]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  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\internet explorer\domstorage\total[]
  Value changes:            HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Value changes:            HKCU\software\microsoft\internet explorer\main\windowssearch[version]
```