Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 54, Task ID: 204

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: FakelE [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 \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex Creates mutex: \Sessions\1\BaseNamedObjects\!IECompat!Mutex \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex Creates mutex: \Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x000004FC) Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069} \Sessions\1\BaseNamedObjects\http://www.baidu.com/ Creates mutex: $\verb|\Sessions|| 1 \\| BaseNamedObjects\\| InternetExplorerDOMStoreQuotally | A linear learning and the context of the context of$ Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects_!SHMSFTHISTORY!_

Creates mutex: \Sessions\1\BaseNamedObjects_!SHMSFTH1STC
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\TVGA1500.txt
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TDSMCW0I.txt
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

 $Files \verb|\Content.IE5| QGCS3SK2 \verb|\index[1].htm| \\$

 $\label{lem:creates:C:Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet} In ternet$

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\G0L00AON\nuomi_510f7472[1].png

 $\label{lem:creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet Files\Content.IE5\QGCS3SK2\icons_0e814c16[1].png} \\$

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

```
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates
Files\Content.IE5\LOWEYQNT\every_cookie_aa168cb4[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Internet
 Creates:
Explorer\DOMStore\NRKAPV8T\www.baidu[1].xml
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\G0L00A0N\nu_instant_search_ebeb5baa[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates
Files\Content.IE5\QGCS3SK2\env_beb83b45[1].swf
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Creates:
Player\#SharedObjects\Q9PEB75U
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Creates:
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
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Creates:
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com
 Creates:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                         C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Creates:
Explorer\UserData\3L1D4SUG\userDataBIDUPSID[1].xml
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\LOWEYQNT\bdsug_async_dac7ea02[1].js
 Creates:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\quickdelete_9c14b01a[1].png
                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
Files\Content.IE5\G0L00AON\his[1].htm
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
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
                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
Files\Content.IE5\3XGK55F6\JSocket_9a52fc3e[1].swf
                         {\tt C:\Windows\Temporary\ Internet}
 Creates
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
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\LOWEYQNT\favicon[1].ico
                         \verb|C:\USers\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico| \\
 Creates:
                         C:\Windows\Prefetch\1AF5338669EFABE0A984147839687-7F9632B6.pf
 Opens:
 Opens:
                         C:\Windows
                         C:\Windows\System32\wow64.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64
 Opens:
                         C:\Windows\SysWOW64\apphelp.dll
                         C:\Windows\Temp\1af5338669efabe0a9841478396871b1.exe
 Opens:
 Opens:
                         C:\Windows\SysWOW64\ntdll.dll
                         C:\Windows\SysWOW64\kernel32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\KernelBase.dll
 Opens:
                         C:\Windows\apppatch\sysmain.sdb
                         C:\Windows\WinSxS\x86 microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
                         C:\Windows\SysWOW64\msimg32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\version.dll
 Opens:
                         C:\Windows\SysWOW64\sechost.dll
                         C:\Windows\SysWOW64\combase.dll
 Opens:
 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
                         C:\Windows\SysWOW64\sspicli.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
                         C:\Windows\SysWOW64\advapi32.dll
                         C:\Windows\SysWOW64\shlwapi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
                         C:\Windows\SysWOW64\oleaut32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\iertutil.dll
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\urlmon.dll
 Opens:
                         C:\Windows\SysWOW64\nsi.dll
                         C:\Windows\SysWOW64\ws2_32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\psapi.dll
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
                         C:\Windows\SysWOW64\msctf.dll
 Opens:
 Opens:
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\program files\fve31bb\zxz63d\Log.dat
                         C:\Windows\SvsWOW64\uxtheme.dll
 Opens:
```

C:\Users\Admin\AppData\Local\Temp\restart.dat

Opens:

```
C:\Windows\SysWOW64\dwmapi.dll
                         C:\Windows\Fonts\StaticCache.dat
 Opens:
                         C:\Windows\Fonts\micross.ttf
 Opens:
 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\msvh.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
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
 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
                         C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TVGA1500.txt|
 Opens:
 Opens:
                         C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TDSMCW0I.txt|
 Opens:
                         C:\Windows\SysWOW64\mlang.dll
                         \verb|C:\USers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet|\\
 Opens:
Files\Content.IE5\QGCS3SK2\index[1].htm
                         C:\Windows\SysWOW64\jscript9.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\urlmon.dll.mui
 Opens:
 Opens:
                         C:\Windows\SysWOW64\en-US\mshtml.dll.mui
 Opens:
                         C:\Windows\SysWOW64\msimtf.dll
                         C:\Windows\SysWOW64\powrprof.dll
 Opens:
 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
                         C:\Windows\SysWOW64\msls31.dll
 Opens:
 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
                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
 Opens:
 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
                         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\08IATE7C.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
                         C:\Windows\SysWOW64\winmm.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dsound.dll
 Opens:
                         C:\Windows\SysWOW64\UIAutomationCore.dll
 Opens:
                         C:\Windows\SysWOW64\mscms.dll
                         C:\Windows\SysWOW64\winmmbase.dll
 Opens:
 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:
  Opens:
                                   C:\Windows\SysWOW64\Macromed\Flash\ss.sgn
  Opens:
                                   C:\Windows\SysWOW64\Macromed\Flash
  Opens:
                                   C:\Windows\SysWOW64\Macromed\Flash\ss.cfg
                                   C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
  Opens:
                                   C:\Windows\SysWOW64\Macromed\Flash\oem.cfg
  Opens:
  Opens:
                                   C:\Windows\SysWOW64\oem.cfg
                                   C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
  Opens:
                                   C:\Windows\SysWOW64\stdole2.tlb
  Opens:
                                   C:\Windows\SysWOW64\iepeers.dll
                                   C:\Windows\SysWOW64\xmllite.dll
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\NRKAPV8T\www.baidu[1].xml
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\G0L00A0N\nu_instant_search_ebeb5baa[1].js
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\env_beb83b45[1].swf
                                   C:\Windows\SysWOW64\msxml3.dll
  Opens:
                                   C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
  Opens:
                                   C:\Windows\SysWOW64\msxml3r.dll
  Opens:
  Opens:
                                   C:\Windows\SysWOW64\en-US\msxml3r.dll.mui
  Opens:
                                   C:\Windows\SysWOW64\schannel.dll
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
  Opens:
  Opens:
                                   C: \verb|\USers\Admin\AppData\Roaming\Macromedia\Flash\ Player| \\
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\#SharedObjects\Q9PEB75U
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\macromedia.com\support\flashplayer\sys\settings.sol
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
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
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\s1.bdstatic.com\
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\*Shared0bjects\Q9PEB75U\*macromedia.com\support\flashplayer\sys\*s1.bdstatic.com\support\flashplayer\sys\sys\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibared0bjects\graphibar
                                   Opens:
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\
                                   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
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\#AppContainer\s1.bdstatic.com\
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com
                                   {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
  Opens:
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\3L1D4SUG\userDataBIDUPSID[1].xml
  Opens:
                                   C:\Windows\SysWOW64\MMDevAPI.dll
                                   C:\Windows\SysWOW64\cfgmgr32.dll
  Opens:
                                   C:\Windows\SysWOW64\devobj.dll
  Opens:
  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
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\baiduia_b45d552b[1].js
  Opens:
                                   C:\Windows\SysWOW64\netmsg.dll
                                   C:\Windows\SysWOW64\en-US\netmsg.dll.mui
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\3XGK55F6\JSocket_9a52fc3e[1].swf
  Opens:
                                   4C77-AF34-C647E37CA0D9}.1.ver0x000000000000010.db
  Opens:
                                   C:\Users\desktop.ini
```

```
C:\Windows\SysWOW64\setupapi.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens:
 Opens:
                         C:\Users
                         C:\Users\Admin
 Opens:
 Opens:
                         C:\Users\Admin\AppData
 Opens:
                         C:\Users\Admin\AppData\Local
                         C:\Users\Admin\AppData\Local\Microsoft
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens:
                         C:\Windows\SysWOW64\en-US\shell32.dll.mui
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\LOWEYQNT\favicon[1].ico
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\AATKOXA4.txt
 Writes to:
 Writes to:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TVGA1500.txt
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\TDSMCW0I.txt
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\QGCS3SK2\index[1].htm
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Content.IE5|| 3XGK55F6 \verb|\baidu_jgylogo3[1].gif|
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\LOWEYQNT\jquery-1.10.2.min_f2fb5194[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\G0L00AON\nuomi_510f7472[1].png
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\QGCS3SK2\icons_0e814c16[1].png
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\3XGK55F6\all_async_search_641293e1[1].js
                         {\tt C:\Windows\Temporary\ Internet}
 Writes to:
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
                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
 Writes to:
Files\Content.IE5\L0WEYQNT\every_cookie_aa168cb4[1].js
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Internet}
 Writes to:
Explorer\DOMStore\NRKAPV8T\www.baidu[1].xml
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\G0L00A0N\nu_instant_search_ebeb5baa[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\QGCS3SK2\env_beb83b45[1].swf
                         Writes to:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Writes to:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Writes to:
Player\#SharedObjects\Q9PEB75U\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
 Writes to:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\3L1D4SUG\userDataBIDUPSID[1].xml
                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
 Writes to:
Files\Content.IE5\LOWEYQNT\bdsug_async_dac7ea02[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\GOLOOAON\his[1].htm
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\G0L00AON\quickdelete_9c14b01a[1].png
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\QGCS3SK2\error[1].htm
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\QGCS3SK2\baiduia_b45d552b[1].js
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Writes to:
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
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\LOWEYQNT\favicon[1].ico
                         C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
 Writes to:
 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\LOWEYQNT\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\LOWEYQNT\every_cookie_aa168cb4[1].js
 Reads from:
                         C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
                         C:\Windows\SysWOW64\Macromed\Flash\Flash.ocx
 Reads from:
 Reads from:
                         C:\Windows\SysWOW64\stdole2.tlb
                         C:\Windows\SysWOW64\iepeers.dll
 Reads from:
 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\LOWEYQNT\bdsug_async_dac7ea02[1].js

Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

 $Files \verb|\Content.IE5| QGCS3SK2 \verb|\baiduia_b45d552b[1].js \\$

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\LOWEYQNT\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

Connects to:

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: www.a.shifen.com \Rightarrow 103.235.46.39 DNS response: wwwstatic1.gshifen.com \Rightarrow 103.235.44.90 DNS response: s.a.shifen.com \Rightarrow 123.125.115.95 DNS response: formi.baidu.com \Rightarrow 61.135.169.120 DNS response: formi.baidu.com \Rightarrow 180.149.131.55

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:
 8.8.8.8:53

 Sends data to:
 127.0.0.1:63162

 Sends data to:
 www.a.shifen.com

 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

 $\label{lem:condition} Creates \ key: \\ HKCU \ software \ microsoft \ windows \ current version \ internet \ settings$

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:

 $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$

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

 $Opens\ key: \\ HKLM \ system \ current control \ mui \ uilanguages \ pending delete$

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\currentcontrol\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:

 $HKLM \label{limits} LLM \label{limits} HKLM \label{limits} LM \label{limits} LM \label{limits} HKLM \label{limits} LM \label{limits} LM$

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\

 $Opens~key: \\ HKLM \ software \ wow 6432 node \ microsoft \ windows~nt \ current version \ windows~nt \ current version \ windows~nt \ current \ version \ vers$

Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

Opens key: HKLM\system\currentcontrol\lsa

Opens key:

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \configuration \\ \begin{tabular}{ll} HKLM \end{tabular} system \configuration \\ \begin{tabular}{ll} HKLM \end{tabular} system \configuration \\ \begin{tabular}{ll} HKLM \end{tabular} system \e$

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\currentcontrol\set\control\nls\locale

 Opens key:
 HKLM\system\currentcontrol\set\control\nls\locale\alternate sorts

 Opens key:
 HKLM\system\currentcontrol\set\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

 $\label{thm:local-prop} Opens \ key: \\ HKLM\ software\ microsoft\ windows \\ nt\ current version\ language pack\ surrogate fallback$

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ 1af 5338669e fabe 0a9841478396871b1. exemple \ description \ description$

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 kev: HKCR\activatableclasses\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2} Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8856f961 - 340a - 11d0 - a96b - a96b$

00c04fd705a2}

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\treatas

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8856f961 - 340a - 11d0 - a96b - a96b$

00c04fd705a2}\inprocserver32

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

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

HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

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}

HKCR\activatableclasses\clsid\{889d2feb-5411-4565-8998-1dd2c5261283} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{889d2feb-5411-4565-8998-

1dd2c5261283}

HKCR\wow6432node\clsid\{889d2feb-5411-4565-8998-1dd2c5261283} Opens kev: 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}

HKCU\software\policies\microsoft\windows\app management Opens key:

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\app management

Opens key: HKLM\software\policies\microsoft\windows\app management

 $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{004b0726 - a010 - 4abf - 8556 - a010 - a0$ Opens key:

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} HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e} Opens key:

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\

HKLM\software\wow6432node\microsoft\ctf\knownclasses Opens kev: Opens key:

 $HKLM \verb|\software| wow 6432 node \verb|\policies| microsoft| windows \verb|\currentversion| internet settings | setti$ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

settings

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

settings

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

explorer\main\featurecontrol

Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\internet\ explorer\mbox{\tt main\featurecontrol}} \\$

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

explorer\main\featurecontrol

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \ internet explorer \ \verb+main \ \verb+feature control+ \ explorer \ \verb+main \ \verb+feature \ explorer \ explorer \ \verb+main \ explorer \ explorer$ Opens key:

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 kev: 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 kev:

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:

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}

08002b30309d}

 $\label{lem:continuous} \begin{tabular}{lll} Opens key: & HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d} \\ Opens key: & HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d} \\ \end{tabular}$

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}\treatas

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

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:

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:

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

 $\label{lem:control} explorer \ends of the control explorer \ends$

Opens key: HKCU\software\microsoft\internet

 $\label{lem:control} explorer\mbox{$main\featurecontrol\retry_headeronlypost_onconnection} \\ Opens key: $HKLM\software\wow6432node\mbox{$microsoft\internet}$ \\ explorer\mbox{$main\featurecontrol\retry_headeronlypost_onconnection} \\ \\ \end{array}$

Opens key: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_mime_handling
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_mime_handling
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
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
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
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
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer \verb|\main| featurecontrol| feature\_enable\_passport\_session\_store\_kb948608
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
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 \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
                         HKLM\software\wow6432node\policies
 Opens kev:
                         HKCU\software\policies
 Opens key:
 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
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
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 HKCU\software\microsoft\internet Opens kev: 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 HKLM\software\wow6432node\microsoft\internet Opens kev: 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: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol_catalog 9 \setminus 00000005$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens kev: Opens kev: Opens kev: Opens kev: Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001 Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006 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 HKLM\system\currentcontrolset\services\winsock\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens key: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock$ Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers Opens key: HKLM\svstem\currentcontrolset\services\winsock\setup migration\providers\tcpip6 HKLM\software\wow6432node\microsoft\internet explorer\mediatypeclass Opens kev: 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

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ratings
Opens key: HKLM\software\microsoft\windows\currentversion\policies\rating
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\
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
     Opens key:
settings\zonemap\domains
     Opens key:
                                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap\domains\
                                                                       HKLM\zonemap\ranges\
     Opens key:
     Opens key:
                                                                        HKCU\zonemap\ranges\
                                                                        HKCU\software\microsoft\internet
     Opens key:
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
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
     Opens key:
 settings\zonemap
     Opens key:
                                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap
                                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
    Opens key:
 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\
                                                                        \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
     Opens key:
 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\
                                                                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
    Opens key:
 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
                                                                       HKCU\software\microsoft\internet
    Opens key:
 explorer\main\featurecontrol\feature_browser_emulation
                                                                       HKLM\software\wow6432node\microsoft\internet
     Opens key:
 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:
                                                                        \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl} zones \end{\tt 0}
     Opens kev:
                                                                        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
                                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
     Opens key:
     Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ zones \ \ windows \ construction \ the settings \ before \ the settings \ the settings \ before \ the settings \ t
    Opens key:
                                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zones
                                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
     Opens key:
 settings\zones\
     Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
    Opens key:
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zones\0
                                                                        \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
     Opens key:
settings\zones\0
     Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet settings \setminus zones \setminus 1 \\ note that the policies \setminus microsoft \setminus version \setminus internet settings \setminus zones \setminus 1 \\ note that the policies \setminus microsoft \setminus version \setminus version
    Opens key:
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zones\1
     Opens key:
                                                                        \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Soft \end{tabular} windows \current version \current versi
settings\zones\1
     Opens key:
                                                                        HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap\
    Opens kev:
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 kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
```

 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

Opens key:

settings\zones\3
Opens key:

```
settings\zones\3
   Opens kev:
HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet settings \setminus version \setminus internet settings \setminus version \setminus internet settings \setminus version \setminus versi
   Opens key:
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
   Opens key:
                                               \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\4
                                               HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                                               HKLM\software\wow6432node\microsoft\internet
   Opens key:
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
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\
  Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                               HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\0
   Opens kev:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\0
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\0
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\0
                                               HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\1
   Opens key:
settings\lockdown_zones\1
                                               \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\lockdown_zones\1
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\1
                                               HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown zones\2
   Opens key:
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
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
                                               \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\lockdown_zones\4
   Opens key:
settings\lockdown_zones\4
                                               \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\lockdown_zones\4
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\4
                                               HKLM\system\currentcontrolset\control\sqmservicelist
   Opens kev:
   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
                                               HKLM\system\currentcontrolset\services\dns
   Opens kev:
   Opens key:
                                               HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
                                               HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
   Opens kev:
   Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   Opens kev:
                                               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

 $Opens \ key: \\ HKCU \ software \ microsoft \ internet \\ explorer \ main \ feature control \ feature _max connections perserver \\$

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

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver

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:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-66ba-4fcf-9d55-7b8e7f157091\}$

Opens key:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fi1b32785-6fba-4fcf-9d55-7b8e7f157091\propertybag$

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-

00000000046}

 Opens key:
 HKCR\activatableclasses\clsid\{00000323-0000-0000-c000-00000000046}

 Opens key:
 HKCU\software\classes\ww6432node\clsid\{00000323-0000-0000-c000

000000000046}

 Opens key:
 HKCR\wow6432node\clsid\{00000323-0000-0000-c000-00000000046}

 Opens key:
 HKCU\software\classes\clsid\{00000323-0000-0000-c000-000000000046}

Opens key: HKCR\clsid\{00000323-0000-0000-0000-000000000046}

Opens key: HKCU\software\classes\activatableclasses\clsid\{00000323-0000-0000-c000-

000000000046}

Opens key: HKCU\software\classes\appid\1af5338669efabe0a9841478396871b1.exe

Opens key: HKLM\software\microsoft\ole\appcompat

Opens key:

 $HKLM \label{lem:hklm} Wow 6432 node \verb|microsoft| cryptography \verb|defaults| provider \verb|microsoft| strong cryptographic | for the provider \verb|microsoft| cryptographic | for the provider | for the provide$

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-

00000000046}

00000000046}\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}

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\ww6432node\clsid\{057eee47-2572-4aa1-88d7-

60ce2149e33c}

 $\label{lem:continuous} Opens key: $$ HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}$$ Opens key: $$ HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}$$ Opens key: $$ HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}$$ Opens key: $$ HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}$$ Opens key: $$ HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}$$ Opens key: $$ HKCU\software\classes\wow6432node\clsid\close\clsid\close\clsid\close\clsid\close\clsid\close\clsid\cls$

60ce2149e33c}\treatas

Opens key: $\begin{tabular}{ll} HKCR\wow6432node\clsid\end{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\end{057eee47-2572-4aa1-88d7-} \\ \end{tabular}$

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

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:

 $\label{thm:local-state} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescri$

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:

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies

Opens key:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe9-4171$

Opens key:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}$

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ property bag$

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history

Opens key:

 $\label{local-bound} HKLM \software \wow 6432 node \windows \current version \explorer \folder descriptions \explorer \folder descriptions \folder \f$

Opens kev:

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

Opens key: HKCU\software\microsoft\interneexplorer\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

```
HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature private font setting
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_private_font_setting
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature css show hide events
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens kev:
                         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
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
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
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_object_caching
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_object_caching
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                         HKCU\software\microsoft\internet
 Opens kev:
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 kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_download_initiator_http_header
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature download initiator http header
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mobile_customizations
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mobile_customizations
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature high resolution aware
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_high_resolution_aware
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_force_disable_untrustedprotocol
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_force_disable_untrustedprotocol
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_weboc_omnavigator_implementation
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_use\_weboc\_omnavigator\_implementation
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_security_thunks
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
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
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_clipchildren_optimization
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_larger_hit_test
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_larger_hit_test
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_legacy_jscript
 Opens key:
                        HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature_use_legacy_jscript
                        HKCU\software\microsoft\internet
 Opens key:
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
                        HKCU\software\microsoft\internet
 Opens key:
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
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
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
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_hang_recovery_touch_mitigation
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_hang_recovery_touch_mitigation
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_paint_inside_wmpaint
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_paint_inside_wmpaint
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_software_filter_rendering
                        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
                        HKCU\software\microsoft\internet
 Opens key:
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
                        HKLM\software\wow6432node\microsoft\internet
 Opens kev:
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:
paths\outlook.exe
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
                         HKLM\software\wow6432node\microsoft\internet explorer\application
 Opens key:
compatibility
                         HKLM\software\wow6432node\policies\microsoft\internet
 Opens kev:
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
                         HKCU\software\policies\microsoft\internet explorer\persistence
 Opens kev:
```

HKLM\software\wow6432node\policies\microsoft\internet

Opens key:

```
explorer\persistence
                         HKLM\software\policies\microsoft\internet explorer\persistence
 Opens key:
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\explorer\travellog
 Opens key:
```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\travellog

Opens key: $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| system\\| dnsclient$

HKLM\software\policies\microsoft\system\dnsclient Opens kev:

Opens key:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-4054, b5105d63-74c6-4dc1-87b7-4054, b5105d63-87b7-4054, b5105d63-87b7-4054, b5105d64-87b7-4054, b5105d64-87b7-4054, b5105d64-87b7-4054, b5105d64-87b7-4054, b5105d64-87b7-4054, b5105d64-87b7-4054,$ 55779daa70e9}

Opens kev:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-

806e6f6e6963}

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}

Opens key:

25b8d56dd1d8}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-

8a6dc56e0da93

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

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

Opens key:

HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ \ autocomplete$

Opens key:

00c04fd7d062}

Opens key: HKCR\activatableclasses\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key: 00c04fd7d062}

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2765 - 6a77 - 11d0 - a535 - 6a77 - 11d0 - a550 - 6a77$ Opens key:

00c04fd7d062}\treatas

HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas Opens kev: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprocserver32

HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprocserver32

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2765 - 6a77 - 11d0 - a535 - 6a77 - 11d0 - a550 - 6a77$

00c04fd7d062}\inprochandler32

 $HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl$ Opens key:

00c04fd7d062}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprochandler

HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprochandler

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}

HKCR\activatableclasses\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a} Opens key: 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

HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas Opens kev: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens key:

9fe3c77a297a}\inprocserver32

HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens key:

9fe3c77a297a}\inprocserver32

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{6935 \\ db93-21e8-4ccc-beb9-16432 \\ node \setminus clsid \setminus \{6935 \\ db93-21e8-4cc-beb9-16422 \\ node \setminus \{6935 \\ db93-21e8-4cc-beb9-16422 \\ node \setminus \{605 \\ db93-$

9fe3c77a297a}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens kev:

9fe3c77a297a}\inprochandler

Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\inprochandler

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 11d0 - a555 - 11d0 - a5$

00c04fd7d062}

Opens key: HKCR\activatableclasses\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-

00c04fd7d062}

HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062} Opens kev: Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 12d0 - 12d0$ 00c04fd7d062}\treatas

Opens key: $\begin{tabular}{ll} HKCR\wow6432node\clsid\end{tabular} HKCR\wow6432node\clsid\end{tabular} \label{tabular} HKCU\software\classes\wow6432node\clsid\end{tabular} \label{tabular} HKCU\software\classes\wow6432node\clsid\end{tabular} \label{tabular}$

00c04fd7d062}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-

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:

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}

b61bb7cdd997}

Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\treatas

 $\label{lem:continuous} Opens~key: $$ HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas$$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}$$$

b61bb7cdd997}\inprocserver32 Opens key: HKCF

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

 $\verb|settings\p3p\history\baidu.com||$

 $Opens~key: \\ HKLM \software \wow 6432 node \microsoft \cryptography \defaults \provider \end{tikzpicture} \\$

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

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: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 11cf - 11$ 00aa00686f13} HKCR\activatableclasses\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-Opens key: 00aa00686f13} Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-Opens key: 00aa00686f13}\treatas HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-Opens key: 00aa00686f13}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-Opens key: 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 HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-Opens key: 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 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_topmost_gwnd HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_topmost_gwnd Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_aligned_timers HKLM\software\wow6432node\microsoft\internet Opens key: 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 HKCU\software\microsoft\internet explorer\flipahead Opens key: Opens key: HKLM\software\wow6432node\microsoft\internet explorer\security\floppy access Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof detection HKLM\software\wow6432node\microsoft\internet explorer\security\adv Opens key: addrbar spoof detection Opens key: HKCU\software\classes\protocols\name-space handler\about\ Opens key: HKCR\protocols\name-space handler\about HKCU\software\classes\protocols\handler\about Opens key: HKCR\protocols\handler\about Opens kev: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{3050f406 - 98b5 - 11cf - bb82 - bb$ Opens key: 00aa00bdce0b} HKCR\activatableclasses\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens kev: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandler32 HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 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

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_weboc_document_zoom

Opens key: HKLM\sortware\wow6432node\microsott\internet

explorer\main\featurecontrol\feature_vsync_watchdog

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

HKLM\software\wow6432node\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_allow_highfreq_timers

Opens kev: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\progid

 $HKCR\wow6432 node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\ \ progid$ Opens key: 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: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\currentversion\currentvers$

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

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

explorer\international\scripts

Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts HKCU\software\policies\microsoft\internet explorer\international\scripts Opens kev:

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

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: $\label{lem:hkcu} \verb+KKCU \software \microsoft \microso$ Opens key: HKLM\system\currentcontrolset\control\nls\codepage

HKCU\software\microsoft\internet explorer\international\scripts\3 Opens key:

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

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

explorer\main\featurecontrol\feature_restrict_filedownload

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}

Opens key: $HKCR \ activatable classes \ \ clsid \ \{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}$ Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}

Opens key: $HKCR\wow6432 node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}$ Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\treatas

 $HKCR\wow6432 node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\\treat as$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\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

HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-Opens kev:

fd2b31b3eefd}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandler

HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-Opens key:

fd2b31b3eefd}\inprochandler

HKLM\software\wow6432node\microsoft\internet explorer\version vector Opens kev:

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 HKCU\software\policies\microsoft\internet explorer\iedevtools\options Opens kev:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ shell \ associations \ mimeassociations \ text/xml \ userchoice$ HKCU\software\classes\mime\database\content type\text/xml

Opens key: Opens key: HKCR\mime\database\content type\text/xml

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter

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

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 kev: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-

0ff4dc41e755}

Opens key: $HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{16d51579 - a30b - 4c8b - a276 - 0ff4dc41e755\}$ Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-

Off4dc41e755}\treatas

Opens key: $HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\$ treatas Opens kev: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-

Off4dc41e755}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-

Off4dc41e755}\inprocserver32

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{16d51579 - a30b - 4c8b - a276 - a276$

Off4dc41e755}\inprochandler32

HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Opens kev:

Off4dc41e755}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Opens kev:

Off4dc41e755}\inprochandler

HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Opens key:

Off4dc41e755}\inprochandler

HKCU\software\microsoft\internet explorer\jscript9 Opens key:

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{842a1268-6e6a-465c-868f-

8bc445b9828f}

HKCR\activatableclasses\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f} Opens key: Opens key: 8bc445b9828f}

HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-

8bc445b9828f}\treatas

 $\label{localized} HKCR \land 6432 node \ clsid \ \{842a1268-6e6a-465c-868f-8bc445b9828f\} \land treat as$ Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-Opens kev:

8bc445b9828f}\inprocserver32

HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-Opens key:

8bc445b9828f}\inprocserver32

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

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

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:

8bc445b9828f}\inprochandler32

HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-Opens key:

8bc445b9828f}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-

8bc445b9828f}\inprochandler

HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-Opens key:

8bc445b9828f}\inprochandler

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl}} zones$ Opens key:

Opens key: HKLM\software\policies\microsoft\internet explorer\low rights

Opens key: HKCU\software\policies\microsoft\internet explorer Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\internet explorer\low rights}}$

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\low rights Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\0

HKCU\software\microsoft\internet Opens kev:

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:

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

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

explorer\main\featurecontrol\feature_mshtml_autoload_ieframe

Opens kev: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_block_paint_for_page_enter Opens kev: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_block_paint_for_page_enter

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

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

settings\

HKCU\software\microsoft\windows\currentversion\internet settings\ Opens key: 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: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d2$

f4ceaaf59cfc}

Opens key: HKCR\activatableclasses\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d278$

f4ceaaf59cfc}

HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-Opens kev:

f4ceaaf59cfc}\treatas

Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 -$

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

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

f4ceaaf59cfc}\inprochandler32

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

f4ceaaf59cfc}\inprochandler

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

f4ceaaf59cfc}\inprochandler

Opens key:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens key: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_disable_layout9_partial Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_disable_layout9_partial HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_force_layout9_partialdebug HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_force_layout9_partialdebug HKCU\software\policies\microsoft\internet explorer\control panel Opens key:

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 kev: HKCU\software\microsoft\direct3d

HKLM\software\wow6432node\microsoft\direct3d Opens key: Opens key: HKLM\software\wow6432node\microsoft\direct3d\drivers

Opens key: HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist

Opens kev: 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

HKCU\software\microsoft\internet Opens key: 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

HKCU\software\microsoft\internet explorer\gpu Opens kev:

HKCU\software\microsoft\internet Opens key:

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 kev: HKCU\eudc\ HKCU\eudc\1252 Opens key: Opens kev: 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} HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas Opens key: $HKCR \setminus wow6432 \\ node \\ clsid \\ \{275c23e2-3747-11d0-9fea-00aa003f8646\} \\ \setminus treatas$ Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-1444\} \\ node \setminus clsid \setminus \{275c23e2-3744-11d0-9fea-1444\} \\ node \setminus clsid \setminus \{275c23e2-3744\} \\ node \setminus clsid \setminus clsid \setminus clsid \setminus clsid \setminus clsid \setminus clsid \setminus clsid$ 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 HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-Opens key: 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 HKCU\software\microsoft\internet explorer\international\scripts\26 Opens key: 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 HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-Opens key: 00c04fd90119} Opens key: HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119} HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-Opens key: 00c04fd90119}\proxystubclsid32 HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-Opens kev: 00c04fd90119}\proxystubclsid32 Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{00020424-0000-0000-c000-c000-c000-c0000-c00-c000-c000-c000-c000-c000-c00-c000-c000-c000-c00-c00-c00-c00-c00-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c000-c00-$ 00000000046} Opens key: HKCR\activatableclasses\clsid\{00020424-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-00000000046} HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-Opens key: 00000000046}\inprochandler32 HKCR\wow6432node\clsid\{00020424-0000-0000-c000-Opens key: 00000000046}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}\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 HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows Opens key: Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm HKLM\software\microsoft\telemetryclient\throttlestore Opens key: Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} is observed that the limit of the local property of the loc$ Opens key: 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 kev: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784

 $\label{lem:hklmsoftwaremicrosoft} \\ HKLM\software\microsoft\telemetryclient\telestore\sqm\windows\winsqm8\13238784 \\ Opens key: \\ HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784 \\ Opens key: \\ HKLM\software\microsoft\tef\tip\tolestore\telest$

```
Opens key:
                                                                                                                         74a569205c16}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
        Opens key:
                                                                                                                         960e8fcdc732}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
                                                                                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
        Opens kev:
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:
                                                                                                                         1dd2563286bc}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
                                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{a028ae76-01b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c2-99c4-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0-1b1-46c0
        Opens kev:
acd9858ae02f}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
        Opens key:
                                                                                                                         8a820df7190f}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
        Opens key:
                                                                                                                         HKLM\software\microsoft\ctf\tip\{ae6be008-07fb-400d-8beb-equiv}
337a64f7051f}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
                                                                                                                         HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
        Opens kev:
e988c088ec82}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
        Opens key:
                                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143
00c04fc324a1}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
                                                                                                                         Opens key:
Oc608477e3a1}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
                                                                                                                         HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{f25e9f57-2fc8-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3-a41a-4eb3
        Opens kev:
cce5f08541e6}\category\item\{b2c7f219-68fb-47d8-9881-aa681d0944f0}
                                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2
        Opens key:
Of816cO9f4ee}\category\item\{b2c7f219-68fb-47d8-9881-aa681dO944f0}
                                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
        Opens key:
Ofb58b01c4a4}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{03b5835f - f03c - 411b - 9ce2 - formula + formul
        Opens key:
aa23e1171e36}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         HKLM\software\microsoft\ctf\tip\{07eb03d6-b001-41df-9192-
       Opens kev:
bf9b841ee71f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         Opens key:
74a569205c16}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         Opens key:
960e8fcdc732}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
       Opens kev:
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{81d4e9c9-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e6c-1d3b-41bc-9e
        Opens key:
4b40bf79e35e}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
        Opens key:
                                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{8613e14c-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c0-4161-ac0f-d0c
1dd2563286bc}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         HKLM\software\microsoft\ctf\tip\{a028ae76-01b1-46c2-99c4-
       Opens kev:
acd9858ae02f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         Opens kev:
8a820df7190f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
        Opens key:
                                                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{ae6be008-07fb-400d-8beb-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-12006-120
337a64f7051f}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                                         HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
       Opens kev:
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
        Opens kev:
                                                                                                                         HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-14d}
00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
        Opens key:
                                                                                                                         Oc608477e3a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
        Opens kev:
                                                                                                                         HKLM\software\microsoft\ctf\tip\{f25e9f57-2fc8-4eb3-a41a-
cce5f08541e6}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
        Opens kev:
                                                                                                                         Of816c09f4ee}\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}
                                                                                                                         HKCR\activatableclasses\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
        Opens key:
                                                                                                                         HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
        Opens kev:
79ce68d8abc2}
                                                                                                                         HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
        Opens kev:
        Opens key:
                                                                                                                         HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\treatas
        Opens key:
                                                                                                                         HKCR \setminus wow 6432 \\ node \\ clsid \\ \{317d06e8-5f24-433d-bdf7-79ce68d8abc2\} \\ \setminus treat \\ as
                                                                                                                         HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
        Opens kev
79ce68d8abc2}\inprocserver32
                                                                                                                         HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
        Opens key:
79ce68d8abc2}\inprocserver32
        Opens key:
                                                                                                                         79ce68d8abc2}\inprochandler32
        Opens kev:
                                                                                                                         HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler32
        Opens key:
                                                                                                                         HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler
                                                                                                                        HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{317d06e8-5f24-433d-bdf7-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-14434-1444-14434-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-1444-144-1444-144-144-144-144-144-144-144-144-144-144-144-144-144-144-144
        Opens key:
79ce68d8abc2}\inprochandler
                                                                                                                         HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-
        Opens kev:
c6b61110b681}\instance
```

Opens key: $HKCR\wow6432 node \clsid \fae3d380-fea4-4623-8c75-c6b61110b681 \hinstance$ HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-Opens key: c6b61110b681}\instance\disabled HKCR\wow6432node\clsid\{fae3d380-fea4-4623-8c75-Opens key: c6b61110b681}\instance\disabled Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561 HKLM\software\wow6432node\microsoft\internet Opens key: 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: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet$ 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 HKLM\software\wow6432node\microsoft\internet Opens key: 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 HKLM\software\wow6432node\microsoft\internet Opens key: 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 HKCU\software\classes\wow6432node\clsid\{7835eae8-bf14-49d1-93ce-Opens key: 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} HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserv er32 HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key: 00c04fb6bfc4}\inprocserver32 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{7b8a2d94 - 0ac9 - 11d1 - 896c - 12d1 - 12d1$ Opens key: 00c04fb6bfc4}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key: 00c04fb6bfc4}\inprochandler HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key: 00c04fb6bfc4}\inprochandler Opens key: HKCU\software\microsoft\internet explorer\feed discovery $\label{lem:hklm} \mbox{HKLM\software\wow6432} node\mbox{\sware\s$ Opens key: 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}

HKCR\activatableclasses\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000} Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-Opens kev:

444553540000}

HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000} Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{d27cdb6e-ae6d-11cf-96b8-$

444553540000}\treatas

 $HKCR \verb|\wow6432| node \verb|\clsid| \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \verb|\treatas| \} treatas$ Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-Opens key:

444553540000}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\inprocserver32

Opens kev: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\inprochandler32

 $HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{d27cdb6e-ae6d-11cf-96b8-ae6d-1$ Opens key:

444553540000}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\inprochandler

HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-Opens kev:

444553540000}\inprochandler

Opens key: HKLM\system\currentcontrolset\services\crypt32 Opens key: HKLM\hardware\description\system\centralprocessor\0 Opens kev: 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: HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0 Opens key: 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 HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9 Opens key: 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 HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32 Opens key: Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046} HKCR\typelib\{00020430-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-0000-000000000046}\2.0 Opens key: Opens key: HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0 Opens key: HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0 HKCU\software\classes\typelib\{00020430-0000-0000-c000-Opens key: 00000000046}\2.0\0\win32 Opens key: HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32 Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4} HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4} Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus typelib \setminus \{7e8bc440 - aeff-11d1 - 89c2 - 00c04fb6bfc4\} \setminus 1.0$ Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0 $HKCU \setminus software \setminus classes \setminus typelib \setminus \{7e8bc440 - aeff-11d1 - 89c2 - aeff-11d1 - aef$ Opens key: 00c04fb6bfc4}\1.0\0 Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0 $HKCU \setminus software \setminus classes \setminus typelib \setminus \{7e8bc440 - aeff-11d1 - 89c2 - aeff-11d1 -$ Opens key: 00c04fb6bfc4}\1.0\0\win32 HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\time Opens key: zones\w. europe standard time\dynamic dst Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe standard time\dynamic dst HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_activex_repurposedetection Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection Opens kev: HKLM\software\wow6432node\policies\microsoft\internet explorer\activex compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000} HKLM\software\policies\microsoft\internet explorer\activex Opens kev: compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000} Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000} HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_addon_management HKLM\software\wow6432node\microsoft\internet Opens key: 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 HKLM\software\wow6432node\microsoft\internet explorer\extension Opens key: compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000} $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{aaf8c6ce-f972-11d0-97eb-f872-11d0-97eb-$ Opens key: 00aa00615333} Opens key: HKCR\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333} Opens key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\code} store \ database\distribution \ units}$ Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ code \ store \ database \ distribution$ units Opens key: HKLM\software\wow6432node\microsoft\code store database\distribution units\{d27cdb6e-ae6d-11cf-96b8-444553540000} HKCU\software\classes\wow6432node\clsid Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion Opens kev: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion

Opens key: 444553540000}\installedversion

HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-

 $HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-a$ Opens key:

444553540000}\installedversion

Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\appid

Opens key: $\begin{tabular}{ll} HKCR\wow6432node\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\appid \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\d27cdb6e-ae6d-11cf-96b8- \\ \end{tabular}$

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

 $Opens~key: \\ HKCR\\wow6432\\node\\clsid\\\{d27cdb6e-ae6d-11cf-96b8-444553540000\\\}\\miscstatus$

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

00c04f990bb4}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-

00c04f990bb4}\inprocserver32

 $Opens~key: \\ HKCU\software\classes\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-11d3-b$

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

00c04f990bb4}\inprochandler

Opens key: HKLM\software\wow6432node\microsoft\msxml30

Opens key: HKLM\system\currentcontrolset\control\securityproviders
Opens key: HKLM\system\currentcontrol\set\control\lsa\sspicache

Opens key: HKLM\system\currentcontrol\set\control\lsa\sspicache\credssp.dll
Opens key: HKLM\system\currentcontrol\securityproviders\saslprofiles
Opens key:

 $\label{thm:local-continuous} HKLM \software \wow6432 node \mbox{\currentversion} \explorer \folder descriptions \folder \fol$

Opens key

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder descriptions \folder \folder$

Opens key: HKCU\software\microsoft\internet explorer\domstorage\total

Opens key:

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} wow 6432 node \end{tabular} node \end{tabular} wow 6432 node \end{tabular} wow 64$

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}

00a0c90a8f39}\treatas

Opens key: $\begin{tabular}{ll} HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas \\ HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas \\ HKCU\software\classes\wow6432node\clsid\closebox{0.5}{loop} \closebox{0.5}{loop} \closebox$

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-

0000000000463

```
HKCR\activatableclasses\clsid\{0000032a-0000-0000-c000-00000000046}
  Opens key:
                                  HKCU\software\classes\wow6432node\clsid\{0000032a-0000-0000-c000-
  Opens key:
00000000046}
                                  HKCR\wow6432node\clsid\{0000032a-0000-0000-c000-00000000046}
  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{0000032a-0000-0000-c000-00000000046}
                                  \label{local-equation} \mbox{HKCR\clsid} $$ \{0000032a - 0000 - 0000 - c000 - 0000000000046 \} $$ $$
  Opens key:
                                  Opens key:
000000000046}
                                  Opens key:
000000000046}
  Opens kev:
                                  HKCR\activatableclasses\clsid\{00000339-0000-0000-c000-00000000046}
  Opens key:
                                  HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00000339-0000-0000-c000-c000-c000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c000-c000-c0000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c
000000000046}
                                  HKCR\wow6432node\clsid\{00000339-0000-0000-c000-00000000046}
  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{00000339-0000-0000-c000-00000000046}
  Opens key:
                                  HKCR\clsid\{00000339-0000-0000-c000-00000000046}
                                  HKCU\software\classes\activatableclasses\clsid\{00000339-0000-0000-c000-
  Opens key:
00000000046}
  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
                                  HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
  Opens key:
0080c7f4ee85}\proxystubclsid32
                                  HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
  Opens key:
c4579291692e}\inprocserver32
                                  HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
  Opens kev:
c4579291692e}\inprocserver32
                                  HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
  Opens key:
0080c7f4ee85}\forward
  Opens key:
                                  HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
                                  HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
  Opens kev:
0080c7f4ee85}\forward
                                  HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
  Opens kev:
  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
                                  HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
  Opens key:
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}
                                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
  Opens key:
  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
                                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
  Opens kev:
  Opens key:
                                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
  Opens key:
                                  Opens key:
                                  Opens key:
                                  00000000046}
                                  Opens key:
  Opens key:
                                  HKCR\wow6432node\interface\{00020400-0000-0000-c000-00000000046}
  Opens key:
                                  HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
00000000046}\proxystubclsid32
  Opens key:
                                  HKCR\wow6432node\interface\{00020400-0000-0000-c000-
00000000046}\proxystubclsid32
  Opens key:
                                  000000000046}
  Opens key:
                                  HKCR\activatableclasses\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:
                                  HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
```

000000000046}

000000000046}\treatas

HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-

000000000046}\inprocserver32

HKCR\wow6432node\clsid\{00020420-0000-0000-c000-Opens kev:

000000000046}\inprocserver32

Opens key:

Opens key: HKLM\software\microsoft\windows\currentversion\mmdevices\audio\capture\ Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-

a3cc-00a0c9223196}

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00020420-0000-0000-c000-c000-c000-c000-c00-c00-c000-c00-c00-c00-c00-c00-c000-c000-c00$

000000000046}\inprochandler32

HKCR\wow6432node\clsid\{00020420-0000-0000-c000-Opens key:

00000000046}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-

00000000046}\inprochandler

Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-

000000000046}\inprochandler

HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-Opens key:

00aa006009fa}

Opens key: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa} Opens kev: HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-

00aa006009fa}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-

00aa006009fa}\proxystubclsid32

Opens key:

a5c5bc1c2ae6}

Opens key: HKCR\activatableclasses\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6} Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-

a5c5bc1c2ae6}

HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6} Opens key: Opens key:

a5c5bc1c2ae6}\treatas

HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-

a5c5bc1c2ae6}\inprocserver32

HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-Opens key:

a5c5bc1c2ae6}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-Opens key:

a5c5bc1c2ae6}\inprochandler32

HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-Opens key:

a5c5bc1c2ae6}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-

a5c5bc1c2ae6}\inprochandler

HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-Opens key:

a5c5bc1c2ae6}\inprochandler

Opens key: HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-

000000000046}

Opens key: HKCR\wow6432node\interface\{00020404-0000-0000-c000-00000000046} HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-Opens kev:

000000000046}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{00020404-0000-0000-c000-

000000000046}\proxystubclsid32

HKLM\software\microsoft\windowsruntime\clsid\{00020421-0000-0000-c000-Opens kev:

000000000046}

HKCR\activatableclasses\clsid\{00020421-0000-0000-c000-000000000046} Opens key: HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-Opens key:

000000000046}

Opens key: $HKCR \setminus wow6432 node \setminus clsid \setminus \{00020421-0000-0000-c000-0000000000046\}$ Opens key: HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\treatas

Opens key:

HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}\treatas HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-Opens kev:

00000000046}\inprocserver32

HKCR\wow6432node\clsid\{00020421-0000-0000-c000-Opens kev:

00000000046}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-Opens key:

000000000046}\inprochandler32

HKCR\wow6432node\clsid\{00020421-0000-0000-c000-Opens kev:

00000000046}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-Opens kev:

00000000046}\inprochandler

HKCR\wow6432node\clsid\{00020421-0000-0000-c000-Opens key:

000000000046}\inprochandler

Opens kev: HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-

00c04fc9e26e}

 $HKCR \setminus wow6432 node \setminus interface \setminus \{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e\}$ Opens key: Opens key: HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-

00c04fc9e26e}\proxystubclsid32 Opens key:

 $HKCR \setminus wow 6432 \\ node \setminus interface \setminus \{d30c1661 - cdaf - 11d0 - 8a3e - 12d0 -$

00c04fc9e26e}\proxystubclsid32

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{d30c1661 - cdaf - 11d0 - 8a3e - 12d - 12d$ 00c04fc9e26e}\forward

HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-Opens kev

00c04fc9e26e}\forward

Opens key:

HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-

00c04fc9e26e}\forward

Opens key: Opens key: HKCU\software\classes\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-

00c04fc9e26e}\typelib

Opens key: $HKCR \setminus wow 6432 \\ node \setminus interface \setminus \{d30c1661 - cdaf - 11d0 - 8a3e - 11d0 -$

00c04fc9e26e}\typelib

HKCU\software\classes\shockwaveflash.shockwaveflash.7 Opens key:

Opens key: ${\tt HKCR \ } shock wave flash. shock wave flash. 7$

Opens key: HKCU\software\classes\shockwaveflash.shockwaveflash.7\clsid

Opens key: HKCR\shockwaveflash.shockwaveflash.7\clsid

Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7ed96837 - 96f0 - 4812 - b211 - b211$

f13c24117ed3}\instance

HKCR\wow6432node\clsid\{7ed96837-96f0-4812-b211-f13c24117ed3}\instance Opens kev:

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

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

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

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

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

Opens kev: HKLM\software\wow6432node\policies\microsoft\internet

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

08002b30309d}\shellfolder

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens kev:

08002b30309d}\shellfolder

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-theoryte \} + theoryte \setminus foreign + theoryte \}$ Opens key:

3aea-1069-a2d8-08002b30309d}\shellfolder

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-3aea-1069-1044fe0-3aea-1046fe0-3aea$

a2d8-08002b30309d}\shellfolder

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key:

08002b30309d}\inprocserver32

Opens key: Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ mountpoints \ 2 \ cpc \ \ \ volume$

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-

11e3-be65-806e6f6e6963}\

HKCU\software\classes\drive\shellex\folderextensions Opens kev:

HKCR\drive\shellex\folderextensions Opens key:

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Opens kev:

409d6c4515e9}

HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-Opens key: a6bb2164fbd0}\inprocserver32

Opens key:

b8dc300d9f9d}

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

b8dc300d9f9d}

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ Opens key:

b8dc300d9f9d}\treatas

 $HKCR\wow6432 node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens kev

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

Opens key: $HKCR\wow6432 node\clsid\{a07034fd-6caa-4954-ac3f-407034-ac3f-4070707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3$

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directorv

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

```
HKCR\folder\shellex\iconhandler
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\allfilesystemobjects
     Opens kev:
                                                                        HKCR\allfilesystemobjects
                                                                        HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
     Opens key:
     Opens key:
                                                                        HKCR\allfilesystemobjects\shellex\iconhandler
     Opens key:
                                                                        HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ setup
     Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\setup
                                                                        HKLM\software\wow6432node\microsoft\windows\currentversion
     Opens key:
     Opens key:
                                                                        HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
 94f2-00a0c91efb8b}
                                                                        HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f5630d-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6b
     Opens kev:
 94f2-00a0c91efb8b}\properties
     Opens key:
                                                                        HKCU\software\classes\directory\docobject
                                                                        HKCR\directory\docobject
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\folder\docobject
     Opens key:
                                                                        HKCR\folder\docobject
                                                                        HKCU\software\classes\allfilesystemobjects\docobject
     Opens kev:
     Opens key:
                                                                        HKCR\allfilesystemobjects\docobject
     Opens key:
11e3-be65-806e6f6e6963}\
     Opens key:
                                                                        HKCU\software\classes\directory\browseinplace
                                                                        HKCR\directory\browseinplace
     Opens kev:
     Opens key:
                                                                        HKCU\software\classes\folder\browseinplace
     Opens key:
                                                                        HKCR\folder\browseinplace
     Opens key:
                                                                        HKCU\software\classes\allfilesystemobjects\browseinplace
     Opens key:
                                                                        {\tt HKCR\ left} lesystemobjects \ browsein place
     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
                                                                        HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c2a7
     Opens key:
444553540000}\shellfolder
                                                                       HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-
     Opens key:
 444553540000}\shellfolder
    Opens key:
                                                                       HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c1aff - c1a
444553540000}
                                                                        HKCR\activatableclasses\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
     Opens kev:
     Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\treatas
     Opens key:
                                                                        HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\
                                                                        HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
     Opens kev:
444553540000}\inprocserver32
                                                                        HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
     Opens key:
444553540000}\inprochandler32
                                                                        Opens key:
444553540000}\inprochandler32
                                                                       HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
    Opens kev:
444553540000}\inprochandler
                                                                       HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-
     Opens key:
444553540000}\inprochandler
     Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ objects
c2a7-11cf-bff4-444553540000}
                                                                       HKCU\software\microsoft\windows\currentversion\app
     Opens key:
paths\1af5338669efabe0a9841478396871b1.exe
                                                                       HKLM\software\wow6432node\microsoft\windows\currentversion\app
     Opens kev:
paths\1af5338669efabe0a9841478396871b1.exe
                                                                        {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus app}
     Opens kev:
paths\1af5338669efabe0a9841478396871b1.exe
     Opens key:
                                                                       3aea-1069-a2d8-08002b30309d}
     Opens kev:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session info \ 1 \ desktop \ names pace \ name \ customizations
     Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}
                                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
     Opens key:
     Opens key:
                                                                        \label{lem:hkcu} \verb+KKCU\software\microsoft\ internet\ explorer\main\windowssearch
                                                                        HKLM\software\wow6432node\microsoft\internet explorer\main\windowssearch
     Opens kev:
     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 kev:
                                                                        HKCR\protocols\filter\image/x-icon
     Opens key:
                                                                        HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
                           HKLM\software\wow6432node\microsoft\internet
 Opens kev:
\verb|explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative| \\
  Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:
                           HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
                           HKLM\system\currentcontrolset\control\mui\uilanguages\en-
  Oueries value:
us[alternatecodepage]
  Queries value:
                           HKCU\control panel\desktop[preferreduilanguages]
  Oueries value:
                           HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]] \ details a software \ wow 6432 node \ microsoft \ windows \ current \ version \ side by side \ preferex \ ternal \ manifest]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                           HKCU\software\microsoft\windows
  Oueries value:
nt\currentversion\appcompatflags[showdebuginfo]
  Oueries value:
                           HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Oueries 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]
                           HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[1af5338669efabe0a9841478396871b1]
                           HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\windows[loadappinit dlls]
                           HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
                           HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Oueries value:
  Queries value:
                           \label{locator} \verb+HKLM\+ software \verb+\microsoft\+ ole[pageallocatorsystem+ eapisprivate]
  Queries value:
                           HKLM\software\microsoft\ole[aggressivemtatesting]
                           HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
  Queries value:
                           HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
                           HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Oueries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\language groups[1]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
                           HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane8]|
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
                           HKLM\software\microsoft\windows
  Oueries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\current version \verb|\languagepack\surrogatefallback[plane14]|
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                           HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Oueries value:
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
```

ui1

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms

```
shell dlg]
                                      HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Oueries value:
  Oueries value:
                                      HKLM\software\microsoft\com3[com+enabled]
                                      HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
  Oueries value:
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]
                                     HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
  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]
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[createuricachesize]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[createuricachesize]
                                      Queries value:
settings[createuricachesize]
  Oueries value:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
                                     \label{lem:hklm} \verb+Kklm/software/policies/microsoft/windows/currentversion/internet \\
  Oueries value:
settings[security_hklm_only]
                                     HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Oueries value:
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main[frametabwindow]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[framemerging]
  Oueries value:
                                     HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]
                                      HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main[sessionmerging]
                                      HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main[admintabprocs]
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ internet explorer \verb+ main[tabprocgrowth]+ \\
  Queries value:
                                      HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main[tabprocgrowth]
                                      HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main[navigationdelay]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Oueries value:
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Queries value:
08002b30309d}\shellfolder[callforattributes]
  Queries value:
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[restrictedattributes]
  Oueries value:
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[foldervalueflags]
                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\clsid| \{871c5380-microsoft| and the substitution of the subs
  Queries value:
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}1
                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[1
  Queries value:
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                                     HKCU\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xffff1
                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
  Oueries value:
  Queries value:
                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
```

HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

Oueries value:

08002b30309d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Oueries 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]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caedcf9d \ [name]$

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \eqref{352481e8-33be-4251-ba85-6007} (parent folder)$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [description]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsingname]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value:

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{352481e8-33be-4251-ba85-6007} [streamresourcetype]$

Queries value:

 $\label{thm:local_ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folde$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caed \ comable]$

Queries value:

 $\label{thm:local-base-equal} HKLM \software \wow 6432 node \mbox{352481e8-33be-4251-ba85-6007} caed cf9d \cite{Continuous and the continuous and$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caed \ folder \ basis \ folder \ f$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]$

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]

```
Oueries value:
                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Oueries value:
                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[1af5338669efabe0a9841478396871b1.exe]
                              HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_mime_handling[*]
  Oueries value:
                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[1af5338669efabe0a9841478396871b1.exe]
  Oueries value:
                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                              HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
                              HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[secureprotocols]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[certificaterevocation]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablekeepalive]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[idnenabled]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[preconnectlimit]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[preresolvelimit]
                              \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[sqmhttpstreamrandomuploadpoolsize]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[cachemode]
                              HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttp1_1]
  Queries value:
                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
                              HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyhttp1.1]
  Queries value:
                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
settings[proxyhttp1.1]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablenegotiate]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablebasicoverclearchannel]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[clientauthbuiltinui]
  Oueries value:
                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Queries value:
                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
                              HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[mbcsservername]
  Queries value:
                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings[disableworkerthreadhibernation]
                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[disableworkerthreadhibernation]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablereadrange]
                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Queries value:
settings[socketsendbufferlength]
                              HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
  Queries value:
                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[keepalivetimeout]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
  Queries value:
                              HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings[maxconnectionsperserver]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
  Queries value:
                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[maxconnectionsperproxy]
```

 $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$

Queries value:

```
settings[serverinfotimeout]
 Oueries 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]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
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]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirytimesecs]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[wpadsearchalldomains]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Queries value:
                         settings[bypasshttpnocachecheck]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                         HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[bypasssslnocachecheck]
 Queries value:
                         HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[enablehttptrace]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
                         HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings[nocheckautodialoverride]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[headerexclusionlistforcache]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonzonecrossing]
```

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertrecving] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpostredirect] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[alwaysdrainonredirect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect] Queries value: settings[tcpautotuning] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] Oueries 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\00000000001[packedcatalogitem] Oueries 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\000000000004[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath] Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000001[displaystring])$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily] Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space _ catalog 5 \ (catalog_entries \ 000000000001 [supported name space]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 1000000000001 \ [storesservice classinfo]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value: 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\0000000000002[supportednamespace] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 00000000000002 [version]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog_catalog_entries \ (000000000003[library path])$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000003 \ [displaystring]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
  Queries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000003 [version]$

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[librarypath] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog S \setminus catalog_entries \setminus 0000000000004 [providerid]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily] Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000004 [enabled]$ Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ set alog_entries \ 0000000000004 \ [version]$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[storesserviceclassinfo] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog \\ \setminus catalog_entries \setminus 0000000000004 [provider info]]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[displaystring] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ name space_catalog \ name spac$ Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000005 \ [address family]$

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_catalog_entries\00000000005[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000006[displaystring]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[addressfamily]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space _ catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[enabled] Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000006 [storesservice class info]$ Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Oueries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[proxysettingsperuser]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[badproxyexpirestime]

HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings[enableautodial]

Oueries value:

Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings[nonetautodial]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[globaluseroffline]

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value:

settings[disablebranchcache]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[usefirstavailable] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[combinefalsestartdata] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[disablefalsestartblacklist] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enforcep3pvalidity] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu] HKLM\system\currentcontrolset\control\cmf\config[system] Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries 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] HKLM\software\microsoft\windows\currentversion\policies\ratings[key] Queries value: HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_browser_emulation[1af5338669efabe0a9841478396871b1.exe] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_browser_emulation[*] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding] HKLM\software\policies\microsoft\internet Oueries value: explorer\security[disablesecuritysettingscheck] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\0[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\1[flags] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[flags] HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe] HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature localmachine lockdown[*] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[defaultconnectionsettings] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyenable] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyoverride] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autodetect] $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu$ Queries value: settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zonemap[autodetect] Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]

 $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]$ Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Oueries 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] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution] HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [query net bt fqdn]$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]

```
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries 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]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
                          HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [resolver registration only]
HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns query time outs]
 Oueries 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[autoproxydetecttype]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\winhttp[disablebranchcache]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[winhttplowercasehost]
 Queries value:
                          HKCU\software\microsoft\internet explorer[no3dborder]
                          HKLM\software\wow6432node\microsoft\internet explorer[no3dborder]
 Oueries value:
 Queries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[urlencoding]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings\5.0\user agent[]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[compatible]
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings\5.0\user agent[compatible]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\5.0\user agent[version]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[version]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
 Queries value:
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings\5.0\user agent[platform]
                          HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]
 Oueries value:
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[1af5338669efabe0a9841478396871b1.exe]
                          HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
 Oueries value:
                          HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
```

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

Oueries value:

Queries value:

Queries value: HKLM\software\microsoft\windows

nt\currentversion\peerdist\service[enable]

Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet

settings[enableutf8]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parent folder]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [description]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [relative path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parsing name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [infotip]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [localized name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [icon]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [stream resource]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource type]$

Queries value:

 $\label{thm:local_ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fills 2785-65 ba-4fcf-9d55-7b8e7f157091 \cite{thm:local_redirectonly} \end{substitute}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [roamable]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [precreate]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[stream]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$157091 $$[publish \end{fiba} $$157091 $$[publish \end{fiba} $$157091 \end{fi$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[attributes]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [folder typeid]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[initfolder handler]$

Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{\sc microsoft \windows \current version \explorer \sc while} \end{tabular}$

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\currentcontrol\sa[everyoneincludesanonymous]

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\cryptography\defaults\provider\microsoft\ strong\ cryptographic provider[type]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic \ microsoft \ microsoft$

provider[image path]

Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Oueries 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-

00000000046}\proxystubclsid32[]

Queries value: HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-

4f27df8760d0}\proxystubclsid32[]

Queries value: HKCR\www6432node\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]

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [name]$

Queries value:

 $\label{local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folde$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} Idescription \end{array} The substitution \end{a$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In the constant of the$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [parsing name]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[infotip]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [localized name]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $\label{local-prop} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[security]$}$

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \current \folder \fol$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} exclaim \end{substitute} Hklm \end{substitute} exclaim \end{substitute} Hklm \end{substitute} exclaim \end{substitute} e$

Queries value:

 $\label{localization} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder descriptions \folder \folder$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[stream]$

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[publishexpandedpath]}$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescri$

Queries value:

 $\label{thm:local-bound} $HKLM \cdot software \cdot wow 6432 node : in the constant of the constant o$

Oueries value:

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]

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot \$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [parent folder]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [description]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescription\explorer\fold$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [infotip]$

Oueries value

 $\label{localized-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe12ed name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[icon]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [stream resource]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream resource type]$

Queries value:

 $\label{localization} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\cdo$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \ \ coe9-4171-908e-08a611b84ff6 \ [roamable]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot$

Oueries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[publishexpandedpath]$

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{align*.} Hklk \end{align*.} Which is a substitution \end{align*.} The substitution \end{$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]$

Queries value: folders[cookies]

HKCU\software\microsoft\windows\currentversion\explorer\user shell

rolders[cookies]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [category]$

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[parent folder]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [description]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[relative path]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cal{lem:hklmsoftware} \end{substitute} folderdescriptions\cal{lem:hklmsoftware} \end{substitute} folderdescriptions\cal{lem:hklmsoftware} \end{substitute} folderdescriptions\cal{lem:hklmsoftware} \end{substitute} \begin{substitute} \begin{substitute}(1,0) \put(0,0) \pu$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [infotip]$

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[localized name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[icon]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream resource]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream resource type]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [local redirect on \ v]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [roamable]$

Oueries value

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [precreate]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [publish \ expanded \ path]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [attributes]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [folder type id]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [initfolder \ handler]$

Queries value: folders[appdata]

HKCU\software\microsoft\windows\currentversion\explorer\user shell

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit]

Oueries value:

Queries value:

 $\label{limit} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[name]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [parent folder]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescription\folderdescri$

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [localized name]$

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder b784-432e-a781-5a1130a75963\folder\fol$

Queries value:

 $HKLM \\ software \\ \\ wow 6432 \\ node \\ microsoft \\ \\ windows \\ \\ current \\ version \\ \\ explorer \\ \\ folder descriptions \\ \\ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \\ [security]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[streamresource]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} [stream resource type]$

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[local redirectonly]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-descriptions\} \ description \ descrip$

b784-432e-a781-5a1130a75963}[roamable] Oueries value: b784-432e-a781-5a1130a75963}[precreate] Oueries value: b784-432e-a781-5a1130a75963}[stream] Oueries value: b784-432e-a781-5a1130a75963}[publishexpandedpath] Oueries value: b784-432e-a781-5a1130a75963}[attributes] Oueries value: b784-432e-a781-5a1130a75963}[foldertypeid] Queries value: b784-432e-a781-5a1130a75963}[initfolderhandler] HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value: folders[history] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cachelimit] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_legacy_dispparams[1af5338669efabe0a9841478396871b1.exe] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_legacy_dispparams[*] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_object_caching[1af5338669efabe0a9841478396871b1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_object_caching[*] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[1a10] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode[1af5338669efabe0a9841478396871b1.exe] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_document_compatible_mode[*] HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay] Queries value: HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-Queries value: 91a2-7b624e0e7244] Queries value: HKLM\system\currentcontrolset\control\wmi\security[7f8e35ca-68e8-41b9-86fe-d6adc5b327e7] HKLM\software\wow6432node\microsoft\internet explorer\application Oueries value: compatibility[1af5338669efabe0a9841478396871b1.exe] HKCU\software\microsoft\internet explorer\domstorage[totallimit] Oueries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations] HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: Oueries value: 55779daa70e9}[searchlist] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationenabled] Queries value: 55779daa70e9}[registeradaptername] Oueries value: 55779daa70e9}[domain] Queries value: $HKLM \land system \land current control set \land services \land tcpip \land parameters \land interfaces \land \{b5105d63-74c6-4dc1-87b7-487b1, and the system \land tcpip \land$ 55779daa70e9}[dhcpdomain] Oueries value: $HKLM \land system \land current control set \land services \land tcpip6 \land parameters \land terfaces \land \{b5105d63-74c6-4dc1-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-800-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c$ 55779daa70e9}[dhcpv6domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

55779daa70e9}[dhcpnameserver]

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

HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]

 $HKCR \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 00c04fd7d062\}[]$

Oueries value:

```
Queries value:
                                                 HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                                 HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
   Oueries value:
00c04fd7d062}\inprocserver32[]
                                                HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
   Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                                                 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
   Oueries value:
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]
                                                HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
   Oueries value:
00aa005b4383}\inprocserver32[]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
                                                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Queries value:
b61bb7cdd997}\inprocserver32[inprocserver32]
                                                 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Queries value:
b61bb7cdd997}\inprocserver32[]
                                                HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Oueries value:
b61bb7cdd997}\inprocserver32[threadingmodel]
                                                HKCU\control panel\desktop[smoothscroll]
   Queries value:
   Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [enable balloon tips]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
   Queries value:
Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced \ [used ouble click timer]
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
                                                 HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ micro
   Queries value:
types\type 001[name]
                                                 HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
   Queries value:
explorer\main\featurecontrol\feature_mime_sniffing[1af5338669efabe0a9841478396871b1.exe]
   Queries value:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
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[*]
                                                HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_protocol_lockdown[1af5338669efabe0a9841478396871b1.exe]
                                                HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature protocol lockdown[*]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2703]
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\3[2703]
                                                 HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Queries value:
00aa00686f13}\inprocserver32[inprocserver32]
                                                 HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Queries value:
00aa00686f13}\inprocserver32[1
                                                 HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 03f9 - 11cf - 11cf
   Queries value:
00aa00686f13}\inprocserver32[threadingmodel]
                                                HKCU\software\microsoft\windows
   Queries value:
nt\currentversion\windows[dragscrollinset]
   Queries value:
                                                {\tt HKCU \backslash software \backslash microsoft \backslash windows}
nt\currentversion\windows[dragscrolldelay]
   Queries value:
                                                HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zonemap[ieharden]
   Queries value:
                                                 HKCU\software\microsoft\internet explorer\flipahead[notificationdelay]
   Oueries value:
                                                 HKCR\protocols\handler\about[clsid]
                                                 HKCR \setminus wow6432 node \\ clsid \\ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\}[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                                                HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
   Oueries value:
00aa00bdce0b}\inprocserver32[]
                                                 HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
   Oueries value:
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]

HKCU\software\microsoft\internet explorer\zoom[zoomdisabled] Oueries value:

Queries value: HKCU\software\microsoft\internet

explorer\main[minimumsystemtimerresolution]

HKLM\software\wow6432node\microsoft\internet Oueries value:

explorer\main[minimumsvstemtimerresolution]

Queries value: HKCU\software\microsoft\internet explorer\main[renderingloopmaxtime] Oueries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[] Queries value:

settings\url history[daystokeep]

HKLM\software\wow6432node\microsoft\internet Oueries value:

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] Oueries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main[anchor underline]}} \mbox{\sc microsoft\sc main[anchor underline]} \mbox{\sc microsoft\sc microsoft\sc main[anchor underline]} \mbox{\sc microsoft\sc mic$ Oueries value: Queries value: HKCU\software\microsoft\internet explorer\main[css_compat] Queries value: HKCU\software\microsoft\internet explorer\main[expand alt text] HKCU\software\microsoft\internet explorer\main[display inline images] Oueries value: 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] HKCU\software\microsoft\internet explorer\main[print_background] Oueries value:

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main[print_background]

HKCU\software\microsoft\internet explorer\main[smoothscroll] Queries value: Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp]

Queries value: HKCU\software\microsoft\internet explorer\main[show image placeholders] Oueries 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] Oueries value:

diagnostics mode]

Queries value: HKCU\software\microsoft\internet explorer\main[move system caret] Oueries 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] $\label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc microsoft\sc micro$ Oueries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest] Oueries value:

HKLM\software\wow6432node\microsoft\internet Queries value:

explorer\main[xdomainrequest]

Queries value: HKCU\software\microsoft\internet explorer\main[domstorage]

HKCU\software\microsoft\internet Oueries value: explorer\main[jscriptprofilecacheeventdelay]

HKCU\software\microsoft\internet Oueries value:

explorer\international[default_codepage]

Oueries value: HKCU\software\microsoft\internet explorer\international[autodetect]

HKCU\software\microsoft\internet Queries value: explorer\international\scripts[default_iefontsizeprivate]

Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color] HKCU\software\microsoft\internet explorer\settings[anchor color visited] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color hover] Oueries 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 face1

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]

Oueries value: HKCU\software\policies\microsoft\windows\currentversion\internet

settings[disablecachingofsslpages]

Queries value: HKCU\software\microsoft\internet explorer\pagesetup[print_background]

HKLM\system\currentcontrolset\control\nls\codepage[950] Oueries value:

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefontsize]

HKCU\software\microsoft\internet Oueries value: 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]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
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}\[]
 Oueries value:
                         HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
 Oueries value:
                         HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[]
                         HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
 Oueries value:
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]
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_zone_elevation[*]
                         HKCR\mime\database\content type\text/xml[clsid]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_xssfilter[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_xssfilter[*]
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}[]
 Queries value:
 Queries value:
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-
Off4dc41e755}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-
 Queries value:
Off4dc41e755}\inprocserver32[]
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-
 Queries value:
Off4dc41e755}\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}[]
 Oueries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[cointernetcombineiuricachesize]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                         HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-
 Oueries value:
8bc445b9828f}\inprocserver32[inprocserver32]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_subdownload_lockdown[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
                         HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-
 Oueries value:
8bc445b9828f}\inprocserver32[]
 Oueries value:
                         HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-
8bc445b9828f}\inprocserver32[threadingmodel1
 Queries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[securityidiuricachesize]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones[securitysafe]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet explorer\low
rights[protectedmodeoffforallzones]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\0[icon]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0[minlevel]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\0[recommendedlevel]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings\zones\0[currentlevel1
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[icon]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\1[minlevel]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1[recommendedlevell
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[currentlevel]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[minlevel] Queries value: settings\zones\2[recommendedlevel] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[currentlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[2500] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\zones\2[2500] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[icon] HKI M\software\wow6432node\microsoft\windows\currentyersion\internet Oueries value: settings\zones\3[minlevel] $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$ Queries value: settings\zones\3[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[currentlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[2500] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\zones\3[2500] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\4[icon] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[minlevel] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\4[currentlevel] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[2500] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[2500] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[1af5338669efabe0a9841478396871b1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*] Oueries value: HKCU\software\microsoft\internet explorer\main[operationaldata] Queries value: HKCU\software\microsoft\internet explorer\browseremulation[cvlistxmlversionlow] HKCU\software\microsoft\internet Queries value: explorer\browseremulation[cvlistxmlversionhigh] $\label{local-objective} \verb|HKCU| software \verb|microsoft| internet| \\$ Queries value: explorer\browseremulation[iecompatversionlow] Queries value: HKCU\software\microsoft\internet explorer\browseremulation[iecompatversionhigh] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[warnonintranet] Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[warnonintranet] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonintranet] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[warnonintranet] HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[] Queries value: Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprocserver32[inprocserver32] HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-Queries value: f4ceaaf59cfc}\inprocserver32[] HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-Queries value: f4ceaaf59cfc}\inprocserver32[threadingmodel] HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-Queries value: $0 fb 58b 01c 4a 4 \\ language profile \\ 0 x 00000000 \\ \{0001 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} [enable]$ Queries value: HKLM\software\wow6432node\microsoft\direct3d\drivers[size] Oueries value: HKLM\software\wow6432node\microsoft\direct3d\drivers[name] Queries value: HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist[size] Oueries value: HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist[name] Queries value: HKCU\software\microsoft\internet explorer\recovery[autorecover] Oueries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_img[1af5338669efabe0a9841478396871b1.exe] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_block_lmz_img[*] Oueries value:

Queries value: HKLM\software\wow6432node\microsoft\internet

Oueries value:

HKLM\system\currentcontrolset\services\fontcache\parameters[clientcachesize]

HKCU\software\microsoft\internet explorer\gpu[adapterinfo]

```
explorer\main\featurecontrol\feature_behaviors[1af5338669efabe0a9841478396871b1.exe]
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_behaviors[*]
                                     HKLM\software\wow6432node\microsoft\internet explorer\default
  Queries value:
behaviors[homepage]
  Queries value:
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[]
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[threadingmodel]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1250]
                                     HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Oueries value:
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1254]
                                     HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Oueries 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]
  Oueries value:
                                     HKLM\svstem\currentcontrolset\control\nls\codepage[936]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1361]
                                     HKCU\software\microsoft\internet
  Queries value:
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]
                                     HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\26[iefixedfontname]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
                                     Oueries value:
                                     HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
  Queries value:
00aa00389b71}\proxystubclsid32[]
                                     HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
  Oueries value:
00c04fd90119}\proxystubclsid32[]
                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}[]
  Queries value:
  Oueries value:
                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[]
                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
                                     HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \texttt{[a5ea4f8e]}
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\sqmclient\windows[studyid]
                                     HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
  Oueries value:
                                     HKCR \setminus wow 6432 \\ node \\ clsid \\ \{317d06e8-5f24-433d-bdf7-79ce68d8abc2\}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
  Oueries value:
79ce68d8abc2}\inprocserver32[inprocserver32]
                                     HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
  Queries value:
79ce68d8abc2}\inprocserver32[]
                                     HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
  Oueries value:
79ce68d8abc2}\inprocserver32[threadingmodel]
                                    HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_block_lmz_script[1af5338669efabe0a9841478396871b1.exe]
  Oueries 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]
                                     HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
  Queries value:
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}[]
                                     HKCR\wow6432 node\clsid\{7b8a2d94-0ac9-11d1-896c-1}
  Oueries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
  Oueries value:
00c04fb6bfc4}\inprocserver32[]
                                     HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
  Oueries value:
00c04fb6bfc4}\inprocserver32[threadingmodel1
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
  Oueries value:
                                     HKLM\software\wow6432node\microsoft\internet explorer\feed
discovery[sound]
  Queries value:
                                     HKCU\software\microsoft\ftp[use web based ftp]
  Oueries value:
                                     HKCR\shockwaveflash.shockwaveflash\clsid[]
  Oueries 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[] Oueries value: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[threadingmodel] HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Queries value: HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-Oueries value: bc58-54c27d745f8f] Queries value: HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-958a-dad20c90073c1 Queries value: HKLM\hardware\description\system\centralprocessor\0[~mhz] HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[] Oueries value: HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[] Oueries value: Queries value: behaviors[userdata] HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[] Oueries value: Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection[1af5338669efabe0a9841478396871b1.exe] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_activex_repurposedetection[*] Queries value: HKLM\software\policies\microsoft\internet explorer[disableflashinie] HKLM\software\wow6432node\microsoft\internet Queries value: 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] HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-Queries value: 444553540000}\miscstatus\1[] Queries value: HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}[] HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-Oueries value: 00c04f990bb4}\inprocserver32[inprocserver32] Queries value: HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprocserver32[] HKCR\wow6432node\clsid\{f6d90f11-9c73-11d3-b32e-Queries value: 00c04f990bb4}\inprocserver32[threadingmodel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[1606] Oueries value: HKLM\system\currentcontrolset\control\securityproviders[securityproviders] HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name] HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment] Queries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize] HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount] Queries value: HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount] Oueries value: 02e7-4e5d-b744-2eb1ae5198b7}[category] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1ac14e77-1$ 02e7-4e5d-b744-2eb1ae5198b7}[name] Oueries value: 02e7-4e5d-b744-2eb1ae5198b7}[parentfolder] Queries value: 02e7-4e5d-b744-2eb1ae5198b7}[description] Oueries value: 02e7-4e5d-b744-2eb1ae5198b7}[relativepath] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1ac14e77-1$ 02e7-4e5d-b744-2eb1ae5198b7}[parsingname] Oueries value: 02e7-4e5d-b744-2eb1ae5198b7}[infotip] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1ac14e77-1ac14e77$ 02e7-4e5d-b744-2eb1ae5198b7}[localizedname] Oueries value: 02e7-4e5d-b744-2eb1ae5198b7}[icon]

Queries value: $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{1ac14e77-1ac1$

Oueries value:

02e7-4e5d-b744-2eb1ae5198b7}[security]

```
02e7-4e5d-b744-2eb1ae5198b7}[streamresource]
  Oueries value:
02e7-4e5d-b744-2eb1ae5198b7}[streamresourcetype]
  Oueries value:
02e7-4e5d-b744-2eb1ae5198b7}[localredirectonly]
  Oueries value:
02e7-4e5d-b744-2eb1ae5198b7}[roamable]
  Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77-1ac14e77
02e7-4e5d-b744-2eb1ae5198b7}[precreate]
  Oueries value:
02e7-4e5d-b744-2eb1ae5198b7}[stream]
  Oueries value:
02e7-4e5d-b744-2eb1ae5198b7}[publishexpandedpath]
  Oueries value:
02e7-4e5d-b744-2eb1ae5198b7}[attributes]
  Oueries value:
02e7-4e5d-b744-2eb1ae5198b7}[foldertypeid]
  Queries value:
02e7-4e5d-b744-2eb1ae5198b7}[initfolderhandler]
                                 HKCU\software\microsoft\internet explorer\domstorage\total[]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
                                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[]
                                 HKCU\software\macromedia\flashplayer[flashplayerversion]
                                 HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
  Oueries value:
c4579291692e}\inprocserver32[inprocserver32]
                                 HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
  Queries value:
c4579291692e}\inprocserver32[]
  Queries value:
                                 HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib[]
                                HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
  Oueries value:
c4579291692e}\inprocserver32[threadingmodel]
                                HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
  Oueries value:
0080c7f4ee85}\typelib[version]
  Queries value:
                                HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
  Queries value:
                                 HKLM\software\microsoft\rpc[udtalignmentpolicy]
                                 HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\drivers32[wave]
                                 HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\drivers32[wave1]
  Queries value:
                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave2]
                                 HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\drivers32[wave3]
  Oueries value:
                                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave4]
  Oueries value:
                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave5]
                                HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\drivers32[wave6]
                                 HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\drivers32[wave7]
  Queries value:
                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave81
                                HKCR\wow6432node\interface\{00020400-0000-0000-c000-
  Queries value:
00000000046}\proxystubclsid32[]
  Queries value:
                                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32\lambda wave91
  Queries value:
                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi]
                                HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\drivers32[midi1]
                                HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\drivers32[midi2]
  Queries value:
                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi3]
                                HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\drivers32[midi4]
                                HKLM\software\wow6432node\microsoft\windows
  Queries value:
```

HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[midi5]

```
nt\currentversion\drivers32[midi6]
                                                 HKLM\software\wow6432node\microsoft\windows
   Oueries value:
nt\currentversion\drivers32[midi7]
   Queries value:
                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi8]
                                                 HKCR \setminus \{00020420-0000-0000-000000000000046\}[]
   Queries value:
   Oueries value:
                                                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
   Oueries value:
                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi9]
   Oueries value:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
                                                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
   Oueries value:
000000000046}\inprocserver32[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
                                                 HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-
   Oueries value:
00aa006009fa}\proxystubclsid32[]
                                                 HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-
   Queries value:
a5c5bc1c2ae6}\inprocserver32[inprocserver32]
                                                 HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-
   Queries value:
a5c5bc1c2ae6}\inprocserver32[]
                                                 HKCR\wow6432node\clsid\{c90250f3-4d7d-4991-9b69-
   Queries value:
a5c5bc1c2ae6}\inprocserver32[threadingmodel]
                                                HKCR\wow6432node\interface\{00020404-0000-0000-c000-
   Queries value:
00000000046}\proxystubclsid32[]
                                                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
   Oueries value:
00000000046}\inprocserver32[inprocserver32]
                                                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
   Oueries value:
000000000046}\inprocserver32[]
                                                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
   Queries value:
00000000046}\inprocserver32[threadingmodel]
   Oueries value:
                                                 HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
00c04fc9e26e}\proxystubclsid32[]
                                                 HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
   Oueries value:
00c04fc9e26e}\typelib[]
                                                 HKCR\wow6432node\interface\{d30c1661-cdaf-11d0-8a3e-
   Queries value:
00c04fc9e26e}\typelib[version]
   Oueries value:
                                                 HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
                                                 HKCR\shockwaveflash.shockwaveflash.7\clsid[]
   Queries value:
                                                 HKCU\software\microsoft\internet
   Oueries value:
explorer\browseremulation[mscompatibilitymode]
                                                 HKCU\software\microsoft\internet
   Oueries value:
explorer\services[selectionactivitybuttondisable]
   Queries value:
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[foldervalueflags]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[data]
   Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-five a content version \setminus cpc \setminus cpc \setminus volume \setminus cpc \setminus cpc
11e3-be65-806e6f6e6963}[generation]
                                                 HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
   Oueries value:
409d6c4515e9}[drivemask]
   Queries value:
                                                 HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
                                                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
   Oueries value:
   Queries value:
                                                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Oueries value:
b8dc300d9f9d}\inprocserver32[]
   Queries value:
                                                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                                                 HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Oueries value:
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[classicshell]
```

Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced [filter] \end{tabular}$ Oueries value:

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]

HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-Oueries value:

97a27216f98a}\inprocserver32[]

HKCR\directorv[docobject] Oueries value:

HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] Queries value:

Queries value: HKCR\folder[docobject]

Queries value: HKCR\allfilesystemobjects[docobject]

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus cpc \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus cpc$

11e3-be65-806e6f6e6963}[data]

HKCR\directory[browseinplace] Oueries value: Queries value: HKCR\folder[browseinplace]

Oueries value: HKCR\allfilesystemobjects[browseinplace]

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-

11e3-be65-806e6f6e6963}[generation]

HKCR\directory[isshortcut] Oueries value: Oueries value: HKCR\folder[isshortcut]

Queries value: HKCR\allfilesystemobjects[isshortcut] Queries value: HKCR\directory[alwaysshowext] HKCR\directory[nevershowext] Oueries value: Queries value: HKCR\folder[nevershowext]

Queries value: HKCR\allfilesystemobjects[nevershowext]

Oueries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprocserver32[]

HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-Queries value:

444553540000}\inprocserver32[loadwithoutcom]

Oueries value: HKCU\software\microsoft\windows\currentversion\shell

extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046}}

0xffff1

HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[] Queries value:

HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-Oueries value:

444553540000}\inprocserver32[inprocserver32]

Queries value: $HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-$

444553540000}\inprocserver32[threadingmodel]

HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-Oueries value:

3aea-1069-a2d8-08002b30309d}[]

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value:

08002b30309d}[localizedstring]

Queries value: HKCU\software\microsoft\internet

explorer\main\windowssearch[enabledscopes]

Oueries 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[] HKCU\software\microsoft\internet explorer\main[disable script debugger] Value changes:

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[uncasintranet]

HKCU\software\microsoft\windows\currentversion\internet Value changes:

settings\zonemap[autodetect]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyenable]

 $\label{thm:condition} Value\ changes: \\ HKCU\ software\ microsoft\ windows\ current version\ internet$

settings\connections[savedlegacysettings]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cacheprefix]

 $\label{thm:condition} \begin{tabular}{ll} \b$

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]