Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 54, Task ID: 206

Task ID: 206 Risk Level:

Date Processed: 2016-04-22 06:01:56 (UTC)

Processing Time: 61.21 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1af5338669efabe0a9841478396871b1.exe"

Sample ID: Type: basic admin Owner:

1af5338669efabe0a9841478396871b1 Label:

2016-04-22 06:01:55 (UTC) Date Added:

PE32:win32:gui File Type: File Size: 939520 bytes

1af5338669efabe0a9841478396871b1 MD5:

98511820966946e5c2c543c720816047a808816f674bc8525016f362785c8b3e SHA256:

Description: None

Pattern Matching Results

Creates malicious events: FakeIE [PUA , Downware]

2 ECMA Script

3 Connects to local host

5 JavaScript: Writes a string of text to a document stream

4 JavaScript: Eval method

3 HTTP connection - response code 200 (success)

3 Long sleep detected

4 Checks whether debugger is present

2 HTML file 1 YARA score 1

Static Events

YARA rule hit:

YARA rule hit: Nonexecutable

Process/Thread Events

Creates process: C:\windows\temp\1af5338669efabe0a9841478396871b1.exe

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

jscript.dll:eval Calls function: Calls function: mshtml.dll:document.write

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1 Creates mutex:

\Sessions\1\BaseNamedObjects\!IETld!Mutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCounterMutex

\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex: $\verb|\Sessions|1\BaseNamedObjects|\ZonesCacheCounterMutex|$ Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex

\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_ Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!

\Sessions\1\BaseNamedObjects\WininetStartupMutex Creates mutex: $\verb|\Sessions|| 1 \\| BaseNamedObjects|| WininetConnectionMutex||$ Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex Creates mutex:

Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile $\verb|\Sessions|1| BaseNamedObjects| IESQMMUTEX_0_208$ Creates mutex:

Creates mutex: \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex

 $\verb|\Sessions|1| BaseNamedObjects|_DDrawExclMode|$ Creates mutex: \Sessions\1\BaseNamedObjects__DDrawCheckExclMode_ Creates mutex: \Sessions\1\BaseNamedObjects\DDrawWindowListMutex Creates mutex: \Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex Creates mutex:

 $\verb|\Sessions|1| BaseNamedObjects| DirectSound DllMain mutex (0x000008B0)|$ Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069}

\Sessions\1\BaseNamedObjects\http://www.baidu.com/ Creates mutex:

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!internet explorer!domstore! Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!internet explorer!userdata!

Creates mutex: \Sessions\1\BaseNamedObjects\InternetExplorerDOMStoreQuota Creates mutex: \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex
Creates mutex: \Sessions\1\BaseNamedObjects_!SHMSFTHISTORY!_

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!mshist012016042220160423!

 $\label{lem:condition} \textit{Creates event:} \qquad \textit{$$ \ensuremath{\backslash}$ KernelObjects$$$ MaximumCommitCondition}$

Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

Creates event: \BaseNamedObjects\BFE_Notify_Event_{f5c68d00-9867-462b-8ad1-

67dd82817101}

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:

Creates:

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

 $Files \verb|\Content.IE5\BX3UL1G0\index[1].php|$

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\KQ5TVCON\bd_logo1[1].png

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\X3IPB3Z1\baidu_jgylogo3[1].gif

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\BX3UL1G0\zbios_62c636fe[1].png

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\KQ5TVCON\nuomi_510f7472[1].png

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\X3IPB3Z1\icons_0e814c16[1].png

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\X3IPB3Z1\all_async_search_641293e1[1].js

Treates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\BX3UL1G0\every_cookie_aa168cb4[1].js

Creates: C:\Users\Admin\AppData\Local\Microsoft\Internet

Explorer\DOMStore\6K541L89\www.baidu[1].xml

Creates:

Creates:

Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet

Explorer\UserData\index.dat

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet

Explorer\UserData\Y0GL1THK

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet

Explorer\UserData\09XN329K

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet

Explorer\UserData\UB8D11YC

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet

Explorer\UserData\73C6DRQW

 ${\tt Creates:} \qquad {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}$

Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js

Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash

 ${\tt Player\macromedia.com\support\flashplayer\sys\mbox{\$s1.bdstatic.com}}$

Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash

Player\macromedia.com\support\flashplayer\sys\settings.sxx

Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash

Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com

Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet

 ${\tt Explorer \backslash UserData \backslash YOGL1THK \backslash userDataBIDUPSID[1].xml}$

Files\Content.IE5\BX3UL1G0\JSocket_9a52fc3e[1].swf

```
Creates:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\error[1].htm
  Creates:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\union[1].gif
  Creates:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
  Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423
  Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\index.dat
                                        C:\Users\Admin\Favorites
  Creates:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
                                        C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
                                        \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
  Creates:
Files\Content.IE5\WG2VLW5Y\bdbri_icons_2e35e84b[1].png
                                        C:\Windows\Prefetch\1AF5338669EFABE0A984147839687-7F9632B6.pf
  Opens:
                                        C:\Windows\System32
  Opens:
  Opens:
                                        C:\Windows\System32\sechost.dll
  Opens:
                                        C:\windows\temp\1af5338669efabe0a9841478396871b1.exe.Local\
  Opens:
                                        C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                                        C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:
                                        C:\windows\temp\MSIMG32.dll
  Opens:
                                        C:\Windows\System32\msimg32.dll
  Opens:
                                        C:\windows\temp\VERSION.dll
  Opens:
                                        C:\Windows\System32\version.dll
  Opens:
                                        C:\Windows\System32\imm32.dll
  Opens:
                                        C:\Windows\WindowsShell.Manifest
  Opens:
                                        C:\windows\temp\msdialg100_D.dll
  Opens:
                                        C:\Windows\system32\msdialg100_D.dll
  Opens:
                                        C:\Windows\system\msdialg100_D.dll
  Opens:
                                        C:\Windows\msdialg100_D.dll
  Opens:
                                        C:\Windows\System32\Wbem\msdialg100_D.dll
  Opens:
                                        C:\Windows\System32\WindowsPowerShell\v1.0\msdialg100_D.dll
  Opens:
                                        C:\windows\temp\MFC90ENut.dll
  Opens:
                                        C:\Windows\system32\MFC90ENut.dll
  Opens:
                                        C:\Windows\system\MFC90ENut.dll
  Opens:
                                        C:\Windows\MFC90ENut.dll
  Opens:
                                        C:\Windows\System32\Wbem\MFC90ENut.dll
                                        C: \verb|\windows| System32\\ | Windows Power Shell \verb|\v1.0\\ | MFC90ENut.dll | C: \verb|\windows| System32\\ | Windows | Windows | System32\\ | Windows | System32\\ | Windows | Windows | System32\\ | Windows | Windows
  Opens:
  Opens:
                                        C:\windows\temp\Afx100net.dll
  Opens:
                                        C:\Windows\system32\Afx100net.dll
                                        C:\Windows\system\Afx100net.dll
  Opens:
  Opens:
                                        C:\Windows\Afx100net.dll
  Opens:
                                        C:\Windows\System32\Wbem\Afx100net.dll
                                        C:\Windows\System32\WindowsPowerShell\v1.0\Afx100net.dll
  Opens:
  Opens:
                                        C:\program files\fve31bb\zxz63d\Log.dat
  Opens:
                                        C:\Program Files\FVe31bb\ZXz63d\BLr11610Ho64.dll
  Opens:
                                        C:\Windows\System32\rpcss.dl1
  Opens:
                                        C:\windows\temp\CRYPTBASE.dll
                                        C:\Windows\System32\cryptbase.dll
  Opens:
  Opens:
                                        C:\Windows\System32\uxtheme.dll
  Opens:
                                        C:\Users\Admin\AppData\Local\Temp\restart.dat
  Opens:
                                        C:\windows\temp\dwmapi.dll
  Opens:
                                        C:\Windows\System32\dwmapi.dl1
  Opens:
                                        C:\Windows\Fonts\StaticCache.dat
  Opens:
                                        C:\Windows\Fonts\tahoma.ttf
                                        C:\Windows\Fonts\meiryo.ttc
  Opens:
  Opens:
                                        C:\Windows\Fonts\msgothic.ttc
  Opens:
                                        C:\Windows\Fonts\msjh.ttf
  Opens:
                                        C:\Windows\Fonts\msyh.ttf
  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\System32\en-US\user32.dll.mui
  Opens:
                                        {\tt C:\Windows\Globalization\Sorting\SortDefault.nls}
  Opens:
                                        C:\Windows\system32\uxtheme.dll.Config
  Opens:
                                        C:\program files\fve31bb\zxz63d\log.dat
  Opens:
                                        C:\Windows\System32\ieframe.dll
  Opens:
                                        C:\Windows\System32\oleacc.dll
  Opens:
                                        C:\windows\temp\OLEACCRC.DLL
  Opens:
                                        C:\Windows\System32\oleaccrc.dll
  Opens:
                                        C:\Windows\Temp\1af5338669efabe0a9841478396871b1.exe
                                        C:\windows\temp\ntmarta.dll
  Opens:
  Opens:
                                        C:\Windows\System32\ntmarta.dll
  Opens:
                                        C:\Windows\System32\en-US\urlmon.dll.mui
```

C:\Windows\System32\shell32.dll

C:\Windows\System32\apphelp.dll

C:\Windows\System32\en-US\ieframe.dll.mui

C:\windows\temp\apphelp.dll

C:\WINDOWS\Temp\MJPGC.TMP

Opens:

Opens:

Opens:

Opens:

```
C:\windows\temp\SspiCli.dll
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
 Opens:
                         C:\Windows\System32\wininet.dll
 Opens:
                         C:\windows\temp\profapi.dll
 Opens:
                         C:\Windows\System32\profapi.dll
 Opens:
                         C:\Users\Admin
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
                         C:\windows\temp\dnsapi.DLL
 Opens:
 Opens:
                         C:\Windows\System32\dnsapi.dll
 Opens:
                         C:\windows\temp\iphlpapi.DLL
 Opens:
                         C:\Windows\System32\IPHLPAPI.DLL
 Opens:
                         C:\windows\temp\WINNSI.DLL
 Opens:
                         C:\Windows\System32\winnsi.dll
 Opens:
                         C:\windows\temp\RASAPI32.dll
 Opens:
                         C:\Windows\System32\rasapi32.dll
 Opens:
                         C:\windows\temp\rasman.dll
 Opens:
                         C:\Windows\System32\rasman.dll
 Opens:
                         C:\windows\temp\rtutils.dll
 Opens:
                         C:\Windows\System32\rtutils.dll
 Opens:
                         C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\Windows\System32\ras
                         C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk| \\
 Opens:
 Opens:
                         C:\windows\temp\sensapi.dll
 Opens:
                         C:\Windows\System32\SensApi.dll
 Opens:
                         C:\Windows\System32\nlaapi.dll
 Opens:
                         C:\windows\temp\rasadhlp.dll
 Opens:
                         C:\Windows\System32\rasadhlp.dll
 Opens:
                         C:\Windows\System32\NapiNSP.dll
 Opens:
                         C:\Windows\System32\pnrpnsp.dll
                         C:\Windows\System32\mswsock.dll
 Opens:
 Opens:
                         C:\Windows\System32\winrnr.dll
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\Windows\System32\wship6.dll
 Opens:
                         C:\windows\temp\dhcpcsvc6.DLL
 Opens:
                         C:\Windows\System32\dhcpcsvc6.dll
 Opens:
                         C:\windows\temp\MLANG.dll
 Opens:
                         C:\Windows\System32\mlang.dll
 Opens:
                         C:\Program Files\Common Files\microsoft shared\ink\tiptsf.dll
 Opens:
                         C:\windows\temp\dhcpcsvc.DLL
                         C:\Windows\System32\dhcpcsvc.dll
 Opens:
 Opens:
                         C:\Windows\System32\drivers\etc\hosts
 Opens:
                         C:\Windows\System32\FWPUCLNT.DLL
 Opens:
                         C:\Windows\System32\netprofm.dll
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\windows\temp\RpcRtRemote.dll
 Opens:
 Opens:
                         C:\Windows\System32\RpcRtRemote.dll
 Opens:
                         C:\Windows\System32\npmproxy.dll
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
 Opens:
                         C:\Windows\Svstem32\C 20127.NLS
 Opens:
                         C:\Windows\System32\mshtml.dll
 Opens:
                         C:\Windows\System32\msls31.dll
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\BX3UL1G0\index[1].php
                         C:\Windows\System32\msimtf.dll
 Opens:
 Opens:
                         C:\Windows\System32\jscript.dll
 Opens:
                         C:\Windows\System32\iepeers.dll
 Opens:
                         C:\Windows\System32\winspool.drv
                         C:\Windows\System32\dxtrans.dll
 Opens:
 Opens:
                         C:\Windows\System32\atl.dll
```

```
Opens:
                         C:\Windows\Svstem32\ddraw.dll
                         C:\Windows\System32\dciman32.dll
 Opens:
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Windows\win.ini
 Opens:
                         C:\Windows\System32\en-US\ddraw.dll.mui
                         C:\Windows\System32\dxtmsft.dll
 Opens:
                         C:\windows\temp\SXS.DLL
 Opens:
 Opens:
                         C:\Windows\System32\sxs.dll
 Opens:
                         C:\Windows\Fonts\arial.ttf
 Opens:
                         C:\Windows\System32\en-US\mlang.dll.mui
 Opens:
                         C:\Windows\System32\C_1250.NLS
 Opens:
                         C:\Windows\System32\C_1251.NLS
                         C:\Windows\System32\C_1253.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_1254.NLS
 Opens:
                         C:\Windows\System32\C_1255.NLS
                         C:\Windows\System32\C_1256.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_1257.NLS
 Opens:
                         C:\Windows\System32\C_1258.NLS
                         C:\Windows\System32\C_874.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_932.NLS
 Opens:
                         C:\Windows\System32\C_936.NLS
                         C:\Windows\System32\C_949.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_950.NLS
 Opens:
                         C:\Windows\System32\C_1361.NLS
 Opens:
                         C:\Windows\Fonts\arialbd.ttf
 Opens:
                         C:\Windows\Fonts\ariali.ttf
 Opens:
                         C:\Windows\System32\en-US\mshtml.dll.mui
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js
 Opens:
                         C:\windows\temp\ImgUtil.dll
 Opens:
                         C:\Windows\System32\imgutil.dll
 Opens:
                         C:\Windows\System32\pngfilt.dll
 Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
                         C:\windows\temp\D3DIM700.DLL
 Opens:
 Opens:
                         C:\Windows\System32\d3dim700.dll
 Opens:
                         C:\Windows\System32\tzres.dll
 Opens:
                         C:\Windows\System32\en-US\tzres.dll.mui
 Opens:
                         C:\Windows\System32\en-US\jscript.dll.mui
 Opens:
                         C:\Windows\System32\en-US\KernelBase.dll.mui
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\all_async_search_641293e1[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\BX3UL1G0\every_cookie_aa168cb4[1].js
 Opens:
                         C:\Windows\System32\Macromed\Flash\Flash10h.ocx
                         C:\Windows\system32\Macromed\Flash\WINMM.dll
 Opens:
 Opens:
                         C:\Windows\System32\winmm.dll
 Opens:
                         C:\Windows\system32\Macromed\Flash\DSOUND.dll
 Opens:
                         C:\Windows\System32\dsound.dll
 Opens:
                         C:\Windows\system32\Macromed\Flash\POWRPROF.dll
 Opens:
                         C:\Windows\System32\powrprof.dll
 Opens:
                         C:\Windows\system32\Macromed\Flash\mscms.dll
 Opens:
                         C:\Windows\System32\mscms.dll
 Opens:
                         C:\Windows\system32\Macromed\Flash\USERENV.dll
 Opens:
                         C:\Windows\System32\userenv.dll
 Opens:
 Opens:
                         C:\Windows\system32\Macromed\Flash\ss.sgn
 Opens:
                         C:\Windows\System32\Macromed\Flash
 Opens:
                         C:\Windows\system32\Macromed\Flash\ss.cfg
 Opens:
                         C:\Windows\System32\Macromed\Flash\mms.cfg
 Opens:
                         C:\Windows\system32\Macromed\Flash\oem.cfg
 Opens:
                         C:\Windows\system32\oem.cfg
 Opens:
                         C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
                         C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
 Opens:
 Opens:
                         C:\Windows\System32\stdole2.tlb
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\index.dat
                         C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\6K541L89\www.baidu[1].xml
 Opens:
                         C:\windows\temp\XmlLite.dll
 Opens:
                         C:\Windows\System32\xmllite.dll
 Opens:
                         C:\Windows\System32\mshtml.tlb
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
 Opens:
                         C:\Windows\System32\urlmon.dll
                         C:\Windows
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

C:\Windows\System32\ddrawex.dll

Opens:

```
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
                                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
                                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js
  Opens:
                                    C:\windows\temp\MMDevAPI.DLL
                                    C:\Windows\System32\MMDevAPI.dll
  Opens:
                                    C:\windows\temp\PROPSYS.dll
  Opens:
  Opens:
                                    C:\Windows\System32\propsys.dll
                                    C:\Windows\System32\msxml3.dll
  Opens:
  Opens:
                                    C:\Windows\System32\msxml3r.dll
  Opens:
                                    C:\Windows\System32\en-US\msxml3r.dll.mui
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData\
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\index.dat
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\Y0GL1THK
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\09XN329K
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UB8D11YC
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\73C6DRQW
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\*.*09XN329K\desktop.ini
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\73C6DRQW\desktop.ini
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\UB8D11YC\desktop.ini
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\YOGL1THK\desktop.ini
  Opens:
                                    C:\windows\temp\Secur32.dll
  Opens:
                                    C:\Windows\System32\secur32.dll
                                    C:\windows\temp\credssp.dll
  Opens:
  Opens:
                                    C:\Windows\System32\credssp.dll
  Opens:
                                    C:\Windows\System32\schannel.dll
                                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\settings.sol
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sol
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\s1.bdstatic.com\
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\* Shared Objects\* HA2GV3VL\* macromedia.com\* support\* flashplayer\* sys\* \#s1.bdstatic.com\* com\* Support\* flashplayer\* sys\* \#s1.bdstatic.com\* Support\* sys\* \#s1.bdstatic.com\* Support\* sys\* \#s1.bdstatic.com\* Support\* sys\* \#s1.bdstatic.com\* Support\* Support\* Support\* sys\* \#s1.bdstatic.com\* Support\* sys\* \#s1.bdstatic.com\* Support\* 
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  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:
Player\macromedia.com\support\flashplayer\sys
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK\userDataBIDUPSID[1].xml
  Opens:
                                    C:\Program Files\Internet Explorer\ieproxy.dll
                                    C:\Users\Admin\AppData\Local\Microsoft
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
```

```
Opens:
                                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5\BX3UL1G0\union[1].gif
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\JSocket_9a52fc3e[1].swf
   Opens:
                                         C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db|
                                         Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000006.db
   Opens:
                                         C:\Users\desktop.ini
   Opens:
                                         C:\Users
                                         C:\Users\Admin\AppData
   Opens:
   Opens:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows
   Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\
   Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423
   Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\index.dat
   Opens:
                                         C:\Windows\System32\en-US\shell32.dll.mui
   Opens:
                                         C:\Users\Admin\Favorites
   Opens:
                                         C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
   Opens:
                                         C:\windows\temp\netmsg.dll
                                         C:\Windows\System32\netmsg.dll
   Opens:
   Opens:
                                         C:\Windows\System32\en-US\netmsg.dll.mui
   Opens:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
   Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
   Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\BX3UL1G0\index[1].php
                                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
   Writes to:
Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\KQ5TVCON\bd_logo1[1].png
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\X3IPB3Z1\baidu_jgylogo3[1].gif
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\BX3UL1G0\zbios_62c636fe[1].png
   Writes to:
                                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\KQ5TVCON\nuomi_510f7472[1].png
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\X3IPB3Z1\icons_0e814c16[1].png
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\X3IPB3Z1\all_async_search_641293e1[1].js
   Writes to:
                                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\BX3UL1G0\every_cookie_aa168cb4[1].js
                                         C:\Users\Admin\AppData\Local\Microsoft\Internet
  Writes to:
Explorer\DOMStore\6K541L89\www.baidu[1].xml
Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
  Writes to:
                                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js
                                         C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Writes to:
Explorer\UserData\index.dat
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
  Writes to:
                                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Writes to:
                                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Writes to:
                                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Writes to:
                                        C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK\userDataBIDUPSID[1].xml
   Writes to:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\JSocket_9a52fc3e[1].swf
   Writes to:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\error[1].htm
  Writes to:
C: \ \ Users \land Admin \land App Data \land Local \land Microsoft \land Windows \land History \land History . IE5 \land MSH ist 012016042220160423 \land IE5 \land MSH ist 01201604220160423 \land IE5 \land MSH ist 012016042220160423 \land IE5 \land MSH ist 01201604220160423 \land IE5 \land MSH ist 0120160423 \land IE5 \land MSH ist 0120160423 \land IE5 \land MSH ist 012016042220160423 \land IE5 \land MSH ist 01201604220160423 \land IE5 \land IE5 \land MSH ist 0120160423 \land IE5 \land IE5 \land MSH ist 0120160423 \land IE5 \land IE
   Writes to:
                                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\KQ5TVCON\favicon[1].ico
```

C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico

Writes to:

```
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\WG2VLW5Y\bdbri_icons_2e35e84b[1].png
 Reads from:
                        C:\Windows\Fonts\StaticCache.dat
                        C:\Windows\Temp\1af5338669efabe0a9841478396871b1.exe
 Reads from:
 Reads from:
                        C:\Windows\System32\drivers\etc\hosts
 Reads from:
                        C:\Windows\win.ini
                        C:\Windows\System32\dxtmsft.dll
 Reads from:
 Reads from:
                        C:\Windows\System32\dxtrans.dll
 Reads from:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Reads from:
Files\Content.IE5\BX3UL1G0\every_cookie_aa168cb4[1].js
                        C:\Windows\System32\Macromed\Flash\mms.cfg
 Reads from:
                        C:\Windows\System32\Macromed\Flash\Flash10h.ocx
 Reads from:
                        C:\Windows\System32\stdole2.tlb
 Reads from:
                        C:\Windows\System32\iepeers.dll
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Reads from:
Files\Content.IE5\X3IPB3Z1\all_async_search_641293e1[1].js
 Reads from:
                        C:\Windows\System32\mshtml.tlb
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Reads from:
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
 Reads from:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
 Reads from:
                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Reads from:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
 Reads from:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js
 Reads from:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
 Reads from:
                        C:\Windows\System32\ieframe.dll
 Reads from:
                        Player\macromedia.com\support\flashplayer\sys\settings.sxx
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Reads from:
Files\Content.IE5\BX3UL1G0\JSocket_9a52fc3e[1].swf
 Reads from:
                        C:\Users\desktop.ini
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Reads from:
 Reads from:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
 Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
 Deletes:
                        C: \verb|\USers\Admin\AppData\Roaming\Macromedia\Flash|
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Deletes:
Player\macromedia.com\support\flashplayer\sys\settings.sol
                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                        Deletes:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
Network Events
```

NEWON EVENS	
DNS query:	wpad
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.static1.gshifen.com ⇒ 103.235.44.90
DNS response:	s.a.shifen.com ⇒ 123.125.115.95
DNS response:	formi.baidu.com ⇒ 180.149.131.55
DNS response:	formi.baidu.com ⇒ 61.135.169.120
Connects to:	224.0.0.252:5355
Connects to:	8.8.8.8:53
Connects to:	103.235.46.39:80
Connects to:	127.0.0.1:52894
Connects to:	103.235.44.90:80
Connects to:	123.125.115.95:80
Connects to:	180.149.131.55:843
Connects to:	180.149.131.55:8843
Sends data to:	224.0.0.252:5355
Sends data to:	8.8.8.8:53
Sends data to:	127.0.0.1:52894
Sends data to:	www.a.shifen.com:80 (103.235.46.39)
Sends data to:	www.static1.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:	127.0.0.1:52894

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

HKCU\software\explore Creates key:

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings

Creates key: HKLM\software\microsoft\tracing

Creates key:

HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32

Creates kev:

HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs

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

settings\connections

Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location

awareness

Creates kev: HKLM\system\currentcontrolset\services\tcpip\parameters Creates key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ runmru$

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\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}

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

settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}\0a-23-64-39-4c-b7

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

settings\wpad\0a-23-64-39-4c-b7

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

settings\p3p\history

HKI M\software\microsoft\directdraw\mostrecentapplication Creates kev:

Creates key: HKCU\software\microsoft\windows script\settings

Creates key: HKLM\software\microsoft\direct3d\mostrecentapplication Creates key: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$

settings\5.0\cache\extensible cache\userdata

Creates key: HKLM\system\currentcontrolset\control\securityproviders\schannel HKCU\software\microsoft\internet explorer\domstorage\total Creates key: Creates key: HKCU\software\microsoft\internet explorer\domstorage\baidu.com HKCU\software\macromedia\flashplayer

Creates key:

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

settings\5.0\cache\extensible cache\mshist012016042220160423

Creates key: HKCU\software\microsoft\internet explorer\main\windowssearch

HKLM\software\microsoft\downloadmanager Creates key:

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

settings\zonemap[proxybypass]

HKLM\software\microsoft\windows\currentversion\internet Deletes value:

settings\zonemap[proxybypass]

Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]

Deletes value:

HKLM\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]

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

settings[proxyserver]

Deletes value:

HKCU\software\microsoft\windows\currentversion\internet

settings[proxyoverride]

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

settings[autoconfigurl]

Opens kev: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

Opens key: HKLM\software\policies\microsoft\mui\settings

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

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

HKLM\system\currentcontrolset\control\error message instrument\ Opens key: Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKI M\

HKLM\software\microsoft\windows nt\currentversion\windows Opens kev: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key:

Opens key: HKLM\software\microsoft\ole

Opens key: HKLM\software\microsoft\ole\tracing Opens kev: HKLM\software\microsoft\oleaut

```
HKLM\system\currentcontrolset\services\crypt32
Opens key:
```

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

settings

Opens kev: HKCU\software\microsoft\internet explorer\main $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows\windows\ error\ reporting\sc wmr} \\$ Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key:

Opens key: HKLM\system\currentcontrolset\control\nls\locale Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink Opens key:

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens key: HKLM\system\currentcontrolset\control\cmf\config

Opens key: $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hklm}\software\mbox{$\mbox{microsoft}\windows nt\currentversion}\sline{\mbox{$\mbox{hklm}\software}\sline{\mbox{$\mbox{hklm}\software}\sline{\mbox{\mbox{$$

Opens key:

HKLM\software\microsoft\ctf\compatibility\1af5338669efabe0a9841478396871b1.exe

Opens kev: HKI M\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg

Opens key: HKCU\software\explore HKCU\software\classes\ Opens key: Opens key: HKLM\software\microsoft\com3

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

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

00c04fd705a2}\treatas

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

00c04fd705a2}\progid

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

00c04fd705a2}\inprocserver32

 $HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver 32$ Opens key:

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

00c04fd705a2}\inprochandler32

Opens key: $HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler 32$

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

00c04fd705a2}\inprochandler

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler Opens key:

Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

HKLM\system\setup Opens key:

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\policies\microsoft\sqmclient\windows

HKLM\software\microsoft\sqmclient\windows Opens key:

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

Opens key: HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283} HKCU\software\policies\microsoft\windows\app management Opens key: Opens key: HKLM\software\policies\microsoft\windows\app management

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

HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e} Opens key: Opens key: $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b$ Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

Opens key: HKLM\software\microsoft\ctf\

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

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

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

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

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562 HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination $HKLM \setminus system \setminus current control \setminus lsa \setminus access providers$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\ldap HKCU\software\microsoft\internet explorer\ietld Opens kev: Opens key: HKLM\software\microsoft\internet explorer\main

Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKCU\software\policies\microsoft\internet explorer\main

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

Opens key:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version's hell compatibility \ 'applications' \ '1 af 5338669 ef abe 0 a 9841478396871b1. exemple the software \ 'microsoft' \ 'mic$

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\shellfolder

Opens key: HKCR\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\microsoft\windows\currentversion\policies\nonenum

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKLM\software\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\policies\microsoft\windows\appcompat

Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\treatas

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprochandler32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprochandler

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler

Opens key:

a2ea-08002b30309d}

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol

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

Opens key: HKLM\software\microsoft\internet explorer\mediatypeclass
Opens key: HKLM\software\microsoft\windows\currentversion\internet

settings\accepted documents

Opens key: HKLM\software\microsoft\windows\currentversion\policies\ratings

Opens key: HKCU\software\microsoft\internet

 $\label{lem:control} explorer $$\max \operatorname{led}_{\operatorname{connect_content_kb942615}}$$ Opens key: $$HKLM\software\microsoft\internet$$$

explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615

Opens key: HKLM\software\policies
Opens key: HKCU\software\policies

Opens key: HKCU\software
Opens key: HKLM\software

 $Opens \ key: \\ HKLM \ software \ policies \ microsoft \ windows \ current version \ internet$

settings\

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\domains\

 $Opens~key: \\ HKCU \ software \ policies \ microsoft \ windows \ current version \ internet$

settings\zonemap\domains\

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

settings\zonemap\ranges\

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

settings\zonemap\ranges\

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck

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

settings\zonemap\

Opens key: HKCU\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_zones_check_zonemap_policy_kb941001$

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

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

settings\zonemap

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

```
settings\zonemap
                          HKCU\software\microsoft\windows\currentversion\internet
 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\
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\security
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens kev:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 Opens key:
settings\zones\
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\zones\1
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\1
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                          HKLM\software\microsoft\internet
 Opens key:
\verb|explorer\main\featurecontrol\feature_localmachine_lockdown|
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                          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:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
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
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
```

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\content Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions Opens kev: ba85-6007caedcf9d} Opens key: ba85-6007caedcf9d}\propertybag HKCU\software\microsoft\windows\currentversion\explorer Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1 Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens kev: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer Opens key: 9d55-7b8e7f157091} Opens key: 9d55-7b8e7f157091}\propertybag Opens kev: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173} Opens key: 9afe-ea3317b67173}\propertybag HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Opens kev: 2160590473-689474908-1361669368-1002 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\cookies Opens key: 908e-08a611b84ff6} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag Opens kev: a03a-e3ef65729f3d} Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}\propertybag Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet$ Opens key: settings\5.0\cache\history Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963} Opens kev: a781-5a1130a75963}\propertybag HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache Opens key: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\5.0\cache\extensible cache\domstore Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\iecompat Opens key: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\5.0\cache\extensible cache\ietld Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\privacie:

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key:

Opens key:

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
                       HKLM\software\microsoft\internet
 Opens kev:
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\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache
 Opens key:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                       HKLM\software\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\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                       HKLM\software\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\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
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                       HKLM\software\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
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                       HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 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 kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
Opens kev:
```

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000011 \parameters \end{substitute} Opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000014 \parameters \end{subarray} Opens \ key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \0000000000017 \parameters \end{substitute} Opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004

Opens key:

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens kev:

HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\

Opens key: HKU\

Opens key: HKLM\system\currentcontrolset\control\sqmservicelist

Opens key:

HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs

Opens key: HKCU\software\classes\autoproxytypes

Opens key: HKCR\autoproxytypes

 $Opens~key: \\ \qquad \qquad \text{HKCU} software \verb|\classes| autoproxytypes| application/x-internet-signup| }$

Opens key: ${\tt HKCR} \verb| autoproxytypes \verb| application/x-internet-signup \\$

Opens key: HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig

Opens key: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

Opens key: HKLM\system\currentcontrolset\services\dns

 $Opens\ key: \\ HKLM\software\policies\microsoft\windows\ nt\dnsclient\dnspolicyconfig$

Opens key:

 ${\tt HKLM} \ system \verb|\currentcontrolset\ services\ dnscache\ parameters\ dnspolicy config}$

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling

Opens key: HKCU\software\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*\

HKCR\protocols\name-space handler* Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_enable_compat_logging

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

agent

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

agent

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

settings\5.0\user agent

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

settings\5.0\user agent

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

settings\user agent

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

settings\user agent

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

agent\ua tokens

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

agent\pre platform

Opens key: HKLM\software\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

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

agent\post platform

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

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_browser_emulation Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_maxconnectionsperserver Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver

HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_maxconnectionsper1_0server

HKLM\software\policies\microsoft\system\dnsclient Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock Opens key: $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ psched \+ parameters \+ winsock$

Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens kev: HKLM\svstem\currentcontrolset\services\winsock\setup

migration\providers\psched

 $\label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip \parameters \winsock \end{tabular}$ Opens kev:

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

HKLM\system\currentcontrolset\services\winsock\setup Opens key:

migration\providers\tcpip6

Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache

c19ce8a73253}

Opens key: HKCU\software\microsoft\windows\currentversion\urlmon settings

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_legacy_compression Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_legacy_compression

Opens kev: HKCU\software\classes\protocols\name-space handler

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

Opens key:

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

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

Opens kev:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus autocomplete$

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\autocomplete Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}

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

00c04fd7d062}\treatas

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

00c04fd7d062}\progid

 Opens key:
 HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid

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

00c04fd7d062}\inprocserver32

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprochandler32

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062\}\inprochandler32}} \mbox{$$ \mbox{HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062\}\inprochandler32}$} \mbox{$$ \mbox{$$$ \mbox{$$ \mbox{$$ \mbox{$$$ \mbox{$$ \mbox{$$$ \mbox{$$ \mbox{$$$ \mbox{$$$ \mbox{$$$ \mbox{$$$ \mbox{$$$ \mbox{$$$ \mbox{$$$ \mbox{$$$ \mbox{$$$$ \mbox{$$$ \mbox{$$$$}$}$}}$}}}} \mbox{$$ \mbox{$\mbox{$$ \mbox{$$$ \mbox{$$$ \mbox{$$$$}$}$}}$}}}} \mbox{$$ \mbox{$\mbox{$$ \mbox{$$$$}$}$}}}} \mbox{$$ \mbox{$\mbox{$$$$}$}$}}$} \mbox{$$ \mbox{$$ \mbox{$$$$}$}$}}$} \mbox{$$ \mbox{$$ \mbox{$$$$}$}$}}$} \mbox{$$ \mbox{$$ \mbox{$$$$}$}$}}$} \mbox{$$ \mbox{$$ \mbox{$$$$}$}$}}$} \mbox{$$ \mbox{$$$$$}$}$} \mbox{$$ \mbox{$$$$$}$}$} \mbox{$$ \mbox{$$$$$}$}$}} \mbox{$$ \mbox{$$$$}$}$} \mbox{$$\mbox{$$$$}$}$} \mbox{$$\mbox{$$$}$}$}} \mbox{$$\mbox{$$$$}$}$} \mbox{$$\mbox{$$$$}$}$}} \mbox{$$\mbox{$$$}$}$}} \mbox{$$\mbox{$$$$}$}$} \mbox{$$\mbox{$$$$}$}$} \mbox{$$\mbox{$$$}$}$} \mbox{$\mbox{$$$}$} \mbox{$\mbox{$$$}$}$} \mbox{$\mbox{$$$}$}$} \mbox{$\mbox{$$\mbox{$$}$}$} \mbox{$\mbox{$$}$}$} \mbox{$\mbox{$$$

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

00c04fd7d062}\inprochandler

Opens key: $\begin{tabular}{ll} HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler \\ Opens key: \\ HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a} \end{tabular}$

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

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

9fe3c77a297a}\treatas

Opens key: $\label{eq:hcclsid} \mbox{HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas}$ Opens key: $\mbox{HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-}}$

9fe3c77a297a}\progid

 $\label{lem:continuous} \begin{tabular}{lll} Opens~key: & HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid\\ Opens~key: & HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-1e8-4cc-beb9-1e8-4cc-beb9-1e8-4cc-beb9$

9fe3c77a297a}\inprocserver32

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32

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

9fe3c77a297a}\inprochandler32

Opens key: HKCR\clsid\\6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler32

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

9fe3c77a297a}\inprochandler

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler
Opens key: HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}

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

00c04fd7d062}\treatas

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

00c04fd7d062}\progid

 $\label{thm:continuous} Opens~key: $$ HKCR\clsid_{00bb2764-6a77-11d0-a535-00c04fd7d062}\right\ Opens~key: $$ HKCU_software_classes_clsid_{00bb2764-6a77-11d0-a535-}$$

00c04fd7d062}\inprocserver32

Opens key: HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32

Opens key: HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\nprochandler 32 and $100b2764-6a77-11d0-a535-00c04fd7d062}. \end{tabular}$

Opens key: HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-

 $00c04fd7d062 \\ \verb|\inprochandler| \\$

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\treatas

Opens key: $\begin{tabular}{ll} HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas \\ HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas \\ HKCU\software\classes\clsid$

00c04fd7d062}\progid

 $\label{thm:continuous} Opens~key: $$ HKCR\clsid_{00bb2763-6a77-11d0-a535-00c04fd7d062}\right\cdot Opens~key: $$ HKCU_software_classes_clsid_{00bb2763-6a77-11d0-a535-} $$$

00c04fd7d062}\inprocserver32

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062\}\inprocserver32}} \\$

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler

Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprocserver32

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32

Opens key:

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

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

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

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

b61bb7cdd997}\treatas

Opens key: $\label{eq:hkcnlsid} \begin{tabular}{ll} HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas \\ HKCU\software\classes\clsid\clsi$

b61bb7cdd997}\progid

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

b61bb7cdd997}\inprocserver32

 $Opens~key: \\ HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\ \ \ inprocserver 32$

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

b61bb7cdd997}\inprochandler32

Opens key: HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprochandler32

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

```
b61bb7cdd997}\inprochandler
                                                         HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprochandler
    Opens key:
    Opens key:
                                                          HKLM\software\microsoft\rpc\extensions
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\advanced
    Opens key:
                                                         HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
    Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
    Opens kev:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
    Opens key:
806e6f6e6963}
    Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
    Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
    Opens key:
                                                         HKLM\system\currentcontrolset\services\tcpip\linkage
                                                          HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
    Opens key:
    Opens key:
                                                         HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
    Opens key:
                                                         HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\treatas
                                                         HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
    Opens key:
    Opens key:
                                                          HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\progid
                                                          HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid
    Opens kev:
    Opens key:
                                                         HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
                                                         HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32
    Opens key:
    Opens key:
                                                          HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler32
    Opens key:
                                                         HKCR\clsid\dcb00c01-570f-4a9b-8d69-199fdba5723b\\inprochandler32
    Opens key:
                                                          HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
                                                         HKCR\clsid\\\{dcb00c01-570f-4a9b-8d69-199fdba5723b\\\}\inprochandler
    Opens key:
    Opens key:
                                                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{a47979d2-c419-11d9-a5b4-001185ad2b89\}
    Opens key:
                                                         HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
    Opens key:
                                                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{a47979d2 - c419 - 11d9 - a5b4 - c419 - c
001185ad2b89}\treatas
    Opens key:
                                                          HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
    Opens key:
                                                          HKCU \setminus software \setminus classes \setminus clsid \setminus \{a47979d2 - c419 - 11d9 - a5b4 - c419 - c
001185ad2b89}\progid
    Opens key:
                                                          HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
                                                         HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
    Opens key:
001185ad2b89}\inprocserver32
                                                         HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32
    Opens kev:
    Opens key:
                                                         HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
                                                         HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32
    Opens key:
    Opens key:
                                                         HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
    Opens kev:
                                                         HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler
                                                         HKCU \setminus software \setminus classes \setminus appid \setminus 1af5338669efabe0a9841478396871b1.exe
    Opens key:
    Opens key:
                                                          HKCR\appid\1af5338669efabe0a9841478396871b1.exe
    Opens key:
                                                          HKLM\software\microsoft\ole\appcompat
                                                         HKLM\system\currentcontrolset\control\lsa
    Opens key:
    Opens key:
                                                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
```

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

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

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

Opens key: HKLM\software\microsoft\cryptography

Opens key: HKLM\software\microsoft\cryptography\offload $\label{local-eq:hkcu} \mbox{HKCU\software\classes\interface} \ \{00000134-0000-0000-c000-000000000046\} \ \mbox{HKCU\software\classes\$ Opens key:

Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046}

Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-

00000000046}\proxystubclsid32

Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32

Opens key: HKLM\system\currentcontrolset\services\bfe

 $HKCU \setminus software \setminus classes \setminus interface \setminus \{d0074ffd-570f-4a9b-8d69-199fdba5723b\}$ Opens key:

Opens key: $HKCR\interface { d0074ffd-570f-4a9b-8d69-199fdba5723b }$ Opens key: HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-

199fdba5723b}\proxystubclsid32

Opens key: $HKCR\ interface \\ \{d0074ffd-570f-4a9b-8d69-199fdba5723b\} \\ \ proxystubclsid32$ Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}

HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27} Opens key: Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\treatas

Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas

```
HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
    Opens key:
2299f0398e27}\progid
                                                                       HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
    Opens key:
                                                                       HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
    Opens key:
2299f0398e27}\inprocserver32
                                                                       Opens key:
                                                                       HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
    Opens key:
2299f0398e27}\inprochandler32
                                                                       HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
    Opens key:
                                                                       HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
    Opens key:
2299f0398e27}\inprochandler
                                                                       \label{lem:hkcr} $$ HKCR\clsid_{1299cf18-c4f5-4b6a-bb0f-2299f0398e27} \in \cline{1.000} $$ here. $$ The property of the content of the conten
    Opens key:
    Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus interface \setminus \{26656eaa - 54eb - 4e6f - 8f85 - 4f0ef901a406\}
                                                                       HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
    Opens key:
                                                                       HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-
    Opens key:
4f0ef901a406}\proxystubclsid32
                                                                       HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32
    Opens key:
    Opens key:
                                                                       HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
    Opens key:
                                                                       HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
                                                                       Opens key:
6d613e2ceaec}\proxystubclsid32
    Opens key:
                                                                       HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32
                                                                       HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
    Opens kev:
    Opens key:
                                                                       HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
    Opens key:
                                                                       HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-
00aa004bb851}\proxystubclsid32
    Opens key:
                                                                       HKCR \land (55272a00-42cb-11ce-8135-00aa004bb851) \land (55272a0a00-42cb-11ce-8135-00aa004bb851) \land (55272a0a00-42cb-11ce-8135-00aa004bb851) \land (55272a0a00-42cb-11ce-8135-00aa004bb851) \land (55272a0a00-42cb-11ce-8135-00aa004bb851) \land (55272a0a00-42cb-11ce-8135-00aa004bb851) \land (55272a0a00-42cb-11ce-8135-00aa004bb851) \land (55272a000-42cb-11ce-8135-00aa004b851) \land (55272a000-42cb-11ce-8135-00aa004b851) \land (55272a000-42cb-11ce-8135-00aa004b851) \land (55272a000-42cb-11ce-8135-00aa004b851) \land (55272a000-42cb-11ce-8135-00aa004b851) \land (55272a000-42cb-11ce-8135-00aa004b851) \land (55272a000-42cb-
    Opens key:
                                                                       HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
    Opens key:
                                                                       HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
    Opens key:
                                                                       HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\treatas
                                                                       HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
    Opens key:
    Opens key:
                                                                       HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\progid
    Opens key:
                                                                       HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
    Opens key:
                                                                       HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32
                                                                       HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
    Opens key:
    Opens key:
                                                                       HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler32
    Opens key:
                                                                       HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\
    Opens key:
                                                                       HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
                                                                      HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\
    Opens key:
    Opens key:
                                                                       HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
    Opens key:
                                                                       HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
                                                                       HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-
    Opens key:
4a74e101f8c1}\proxystubclsid32
                                                                       HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32
    Opens kev:
                                                                       Opens key:
    Opens key:
                                                                       HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
    Opens key:
                                                                       HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-
63278fcb8037}\proxystubclsid32
                                                                       HKCR \verb|\interface| \{ 2a1c9eb2-df62-4154-b800-63278fcb8037 \} \verb|\proxystubclsid32| \} | Although the statement of the statemen
    Opens key:
    Opens key:
                                                                       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}
                                                                       HKLM\system\currentcontrolset\services\netbt\linkage
    Opens key:
                                                                       HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\p3p\history\baidu.com
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\text/html; charset=utf-
8
                                                                       \label{local-hammel} \mbox{HKCR} $$ \mbox{HKCR} \mbox{mime} \mbox{database} \mbox{content type} \mbox{type} \mbox{text/html}; $$ \mbox{charset=utf-8} $$ \mbox{database} \mb
    Opens key:
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\text/html
    Opens key:
                                                                       HKCR\mime\database\content type\text/html
                                                                       HKCU\software\classes\protocols\filter\text/html; charset=utf-8
    Opens key:
    Opens key:
                                                                       HKCR\protocols\filter\text/html; charset=utf-8
    Opens key:
                                                                       HKCU\software\classes\protocols\filter\text/html
                                                                       HKCR\protocols\filter\text/html
    Opens key:
    Opens key:
                                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                                                                       HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
    Opens key:
                                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
    Opens key:
                                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
```

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} Opens kev:

Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd000aa00686f13}\treatas HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas Opens kev: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-Opens key: 00aa00686f13}\progid Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32 HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32 Opens kev: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-Opens key: 00aa00686f13}\inprochandler32 Opens kev: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32 Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131 Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_aria_support Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_aria_support HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_legacy_dispparams HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_legacy_dispparams Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_private_font_setting HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_private_font_setting HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_css_show_hide_events Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_css_show_hide_events HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_display_node_advise_kb833311 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_display_node_advise_kb833311 HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_allow_expanduri_bypass HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_allow_expanduri_bypass Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245 Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245 HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature databinding support Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_databinding_support Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enforce_bstr HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature enforce bstr HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_enable_dynamic_object_caching Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_dynamic_object_caching HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_object_caching HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_object_caching Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_tostring_in_compatview Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_tostring_in_compatview Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454

explorer\main\featurecontrol\feature_cleanup_at_fls

explorer\main\featurecontrol\feature_cleanup_at_fls

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

HKCU\software\microsoft\windows nt\currentversion\windows

Opens key:

Opens key:

Opens key:

Opens key:

```
HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
   Opens key:
                                               HKLM\software\microsoft\internet explorer\application compatibility
   Opens key:
                                               HKLM\software\policies\microsoft\internet explorer\domstorage
   Opens kev:
   Opens key:
                                               HKCU\software\policies\microsoft\internet explorer\domstorage
   Opens kev:
                                               HKCU\software\microsoft\internet explorer\domstorage
                                               \label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{$\mbox{$}$} \mbox{$\mbox{$}$} \mbox{$\mb
   Opens key:
                                               HKLM\software\policies\microsoft\internet explorer\safety\privacie
   Opens key:
   Opens key:
                                               HKCU\software\policies\microsoft\internet explorer\safety\privacie
   Opens key:
                                               HKCU\software\microsoft\internet explorer\safety\privacie
   Opens key:
                                               HKLM\software\microsoft\internet explorer\safety\privacie
   Opens kev:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
   Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
                                              HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_restrict_filedownload
   Opens key:
                                               HKLM\software\microsoft\internet explorer\security\floppy access
   Opens key:
                                               HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
                                               HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
   Opens key:
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:
   Opens key:
                                               HKCR\protocols\handler\about
                                               HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
   Opens key:
                                               HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
   Opens kev:
   Opens key:
                                               HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                               HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
   Opens key:
   Opens key:
                                               HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
                                               HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
   Opens key:
   Opens key:
                                               HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                                               HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
   Opens key:
   Opens key:
                                               HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
   Opens key:
                                               HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
   Opens key:
                                               HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
                                              HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
                                               HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_document_compatible_mode
                                              HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_protocol_lockdown
                                              HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature protocol lockdown
                                               HKLM\software\policies\microsoft\internet explorer\zoom
   Opens key:
   Opens key:
                                               HKCU\software\policies\microsoft\internet explorer\zoom
   Opens kev:
                                               HKCU\software\microsoft\internet explorer\zoom
   Opens key:
                                               HKLM\software\microsoft\internet explorer\zoom
                                               HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_weboc_document_zoom
                                               HKLM\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_weboc_document_zoom
  Opens key:
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\url history
   Opens key:
                                               \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\url history
                                               \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentvers
   Opens key:
history
  Opens key:
                                               HKLM\software\microsoft\windows\currentversion\internet settings\url
history
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
                                               HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
   Opens key:
                                               HKCU\software\policies\microsoft\internet explorer
                                               \label{lem:hklmsoftware policies microsoft internet explorer international scripts \\
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\international\scripts
   Opens key:
                                               HKLM\software\microsoft\internet explorer\international\scripts
                                               HKLM\software\policies\microsoft\internet explorer\settings
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\settings
   Opens key:
                                               HKLM\software\microsoft\internet explorer\settings
   Opens key:
                                               HKCU\software\microsoft\internet explorer\styles
   Opens key:
                                               HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus active desktop
   Opens kev:
                                               HKCU\software\microsoft\windows\currentversion\policies
   Opens key:
                                               HKCU\software\microsoft\internet explorer\pagesetup
```

Opens key: HKCU\software\microsoft\internet explorer\menuext
Opens key: HKCU\software\microsoft\internet explorer\menuext\%s
Opens key: HKLM\system\currentcontrol\set\control\nls\codepage

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

Opens key: HKLM\software\microsoft\internet explorer\version vector

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mshtml_autoload_ieframe Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mshtml_autoload_ieframe

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

Opens key: HKCU\software\microsoft\internet explorer\dxtrans
Opens key: HKLM\software\microsoft\internet explorer\dxtrans

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_sslux

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_sslux

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

settings\

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

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

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

settings\zonemap\

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

settings\zonemap\

Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}

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

f4ceaaf59cfc}\treatas

 Opens key:
 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas

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

f4ceaaf59cfc}\progid

 Opens key:
 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\progid

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

f4ceaaf59cfc}\inprocserver32

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32

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

f4ceaaf59cfc}\inprochandler32

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32

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

f4ceaaf59cfc}\inprochandler

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\clsid\space{2.5cm} HKCR\clsid\space{2.5cm} HKCU\software\policies\microsoft\internet\ explorer\control\ panel \end{tabular}$

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

Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}

Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\treatas

 $\label{lem:continuous} Opens \; key: & HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\treatas \\ Opens \; key: & HKCU\software\classes\clsid\f414c260-6ac0-11cf-b6d1- \\ \end{tabular}$

00aa00bbbb58}\progid

00aa00bbbb58}\inprocserver32

00aa00bbbb58}\inprochandler32

Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32

Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprochandler

Opens key: HKLM\software\microsoft\windows script\features

Opens key: ${\tt HKLM\backslash software\backslash policies\backslash microsoft\backslash internet\ explorer\backslash recovery}$

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_scripturl_mitigation Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_img HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_block_lmz_img Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_behaviors HKLM\software\microsoft\internet explorer\default behaviors Opens key: Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas $HKCR \clsid \ \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\} \ treat as$ Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\progid Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandler32 $HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\ \ in prochandler 32$ Opens key: Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler Opens key: $HKCR \verb|\clsid|{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprochandler| \\$ Opens key: HKCU\software\policies\microsoft\internet explorer\persistence HKLM\software\policies\microsoft\internet explorer\persistence Opens kev: Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-dc030521aabd} Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd} HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-Opens key: dc030521aabd}\treatas Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas $HKCU \setminus software \setminus classes \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - f51a - 6d7b - f$ Opens kev: dc030521aabd}\progid Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7bdc030521aabd}\inprocserver32 Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32 Opens kev: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7bdc030521aabd}\inprochandler32 Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler32 HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-Opens key: dc030521aabd}\inprochandler HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000} Opens key: Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000} HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-Opens kev: 3c8b00c10000}\treatas HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32 $HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\\\\inprocserver32$ Opens key: Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler32 Opens key: Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler $HKCR\clsid\d1fe6762-fc48-11d0-883a-3c8b00c10000\)\inprochandler$ Opens key: Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d} Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d} Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid Opens key: Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32

HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32 Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-Opens key: 00c04fd9189d}\inprochandler

HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler Opens key:

Opens key: HKLM\software\microsoft\windows\currentversion\setup HKLM\software\microsoft\windows\currentversion Opens kev:

Opens key: HKLM\hardware\devicemap\video

```
Opens key:
                          HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
 Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
                          HKLM\svstem\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
 Opens kev:
9dd4432fa2e9}\0000
 Opens key:
                          HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000
 Opens key:
                          HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000
                          HKLM\software\microsoft\directdraw\compatibility
 Opens kev:
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\bug!
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
                          HKLM\software\microsoft\directdraw\compatibility\diablo
 Opens key:
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\mortalkombat3
                          HKLM\software\microsoft\directdraw\compatibility\msgolf98
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
 Opens kev:
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\rogue squadron
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\savage
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\silentthunder
                          HKLM\software\microsoft\directdraw\compatibility\starcraft100
 Opens kev:
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\starcraft115
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\starcraftdemo
 Opens key:
                          {\tt HKLM \backslash software \backslash microsoft \backslash direct draw \backslash compatibility \backslash terracide}
 Opens key:
                          HKLM\software\microsoft\directdraw\compatibility\thirddimension
 Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
 Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
                          HKLM\software\microsoft\directdraw\gammacalibrator
 Opens key:
 Opens key:
                          HKLM\software\microsoft\directdraw
 Opens key:
                          HKLM\software\microsoft\direct3d
                          HKLM\software\microsoft\windows nt\currentversion\msasn1
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
 Opens key:
                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
                          HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key:
f941e9b7e1fe}\treatas
                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
 Opens key:
```

HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-Opens key:

f941e9b7e1fe}\progid

HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid Opens kev: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-Opens key:

f941e9b7e1fe}\inprocserver32

HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-

f941e9b7e1fe}\inprochandler32

 $HKCR\clsid\arrowantered$ +34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32 Opens kev:

Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-

f941e9b7e1fe}\inprochandler

 $HKCR\clsid$ {a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler Opens key:

Opens key: HKCU\software\classes\dximagetransform.microsoft.shadow

HKCR\dximagetransform.microsoft.shadow Opens key:

Opens kev: HKCU\software\classes\dximagetransform.microsoft.shadow\clsid

Opens key: HKCR\dximagetransform.microsoft.shadow\clsid

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{e71b4063-3e59-11d2-952a-00c04fa34f05\}$

Opens key: HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05} HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-Opens key:

00c04fa34f05}\treatas

Opens key: HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas Opens key: HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-

00c04fa34f05}\progid

HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid Opens kev: Opens key: HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-

00c04fa34f05}\inprocserver32

Opens key: HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32 Opens key:

00c04fa34f05}\inprochandler32

HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler32 Opens kev:

Opens key: HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-

00c04fa34f05}\inprochandler

Opens key: HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler Opens key: HKLM\software\microsoft\internet explorer\activex compatibility

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

compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{4cb26c03-ff93-11d0-817e-0000f87557db\}$ Opens key:

HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db} Opens kev: Opens key:

0000f87557db}\treatas

Opens key: $HKCR \c1sid \end{4cb26c03-ff93-11d0-817e-0000f87557db} \treat as$ HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-Opens key:

0000f87557db}\progid

HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-Opens key:

0000f87557db}\inprocserver32

HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32 Opens key:

Opens kev: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\inprochandler32

Opens key:

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\inprochandler

 $HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler$ Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd} Opens key:

Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd} Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-

f4fc1e6ca1bd}\treatas

Opens key: $HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas$ HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-Opens key:

f4fc1e6ca1bd}\progid

Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-

f4fc1e6ca1bd}\inprocserver32

Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-

f4fc1e6ca1bd}\inprochandler32

Opens key: $HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\ \ inprochandler 32$

Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-

f4fc1e6ca1bd}\inprochandler

Opens key: $HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler$

Opens key: HKCU\software\classes\typelib

HKCR\typelib Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus typelib \setminus \{5e77eb03-937c-11d1-b047-00aa003b6061\}$

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}

 $\label{local-bound} HKCU \software \classes \typelib \{5e77eb03-937c-11d1-b047-00aa003b6061\} \label{local-bound} 1.1 \end{constraints} \\$ Opens key:

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-

00aa003b6061}\1.1\409

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-

00aa003b6061}\1.1\9

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-

00aa003b6061}\1.1\0

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-

00aa003b6061}\1.1\0\win32

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}

HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db} Opens key:

Opens key: $HKCU \setminus software \\ classes \\ typelib \\ \{54314d1d-35fe-11d1-81a1-0000f87557db\} \\ \\ 1.1 \\ 1.2 \\ 1.2 \\ 1.3 \\ 1.3 \\ 1.4 \\ 1.3 \\ 1.4 \\ 1$

HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409

HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1 Opens kev: Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409

Opens key:

Opens key:

HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9 Opens kev: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9

Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0

Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-

0000f87557db}\1.1\0\win32

Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}

Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-1864\} + (275c23e2-3747-11d0-9fea-1864) + (275c23e2-364) + (275c256) + ($ Opens key: 00aa003f8646}\treatas

Opens kev:

HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid

Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-Opens key:

00aa003f8646}\inprocserver32

HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-

00aa003f8646}\inprochandler32

Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32

Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-

00aa003f8646}\inprochandler

HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler Opens kev: Opens key: HKCU\software\microsoft\internet explorer\international\scripts\26

```
HKLM\software\microsoft\windows
    Opens key:
nt\currentversion\languagepack\surrogatefallback\simsun
    Opens key:
                                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
    Opens kev:
                                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
                                                             HKCU\software\classes\mime\database\content type\image/png
    Opens key:
                                                             HKCR\mime\database\content type\image/png
    Opens key:
                                                             \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \application/javascript \end{tabular}
    Opens key:
    Opens key:
                                                             HKCR\mime\database\content type\application/javascript
    Opens kev:
                                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
    Opens key:
                                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
    Opens key:
                                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
                                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
    Opens key:
                                                             HKCU \setminus software \setminus classes \setminus clsid \setminus \{30c3b080 - 30fb - 11d0 - b724 - b
    Opens key:
00aa006c1a01}\treatas
    Opens key:
                                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
    Opens key:
                                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\progid
                                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid
    Opens key:
                                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
    Opens kev:
00aa006c1a01}\inprocserver32
    Opens key:
                                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
                                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
    Opens key:
00aa006c1a01}\inprochandler32
                                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
    Opens key:
                                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
    Opens kev:
00aa006c1a01}\inprochandler
    Opens key:
                                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler
                                                             HKCU \setminus software \setminus classes \setminus clsid \setminus \{6a01fda0-30df-11d0-b724-00aa006c1a01\}
    Opens key:
    Opens key:
                                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
    Opens key:
                                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
    Opens key:
                                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
    Opens key:
                                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\progid
    Opens key:
                                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\progid
    Opens key:
                                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
    Opens key:
                                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
    Opens key:
                                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
    Opens key:
                                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
    Opens key:
                                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler
    Opens key:
                                                             HKCR \clsid \end{6a01fda0-30df-11d0-b724-00aa006c1a01} \label{eq:hkcr} in prochandler
                                                             HKCU\software\classes\mime\database\content type
    Opens kev:
    Opens key:
                                                             HKCR\mime\database\content type
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/bmp\bits
    Opens key:
                                                             HKCR\mime\database\content type\image/bmp\bits
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/gif\bits
    Opens key:
                                                             HKCR\mime\database\content type\image/gif\bits
    Opens kev:
                                                             \label{local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-loc
    Opens key:
                                                             HKCR\mime\database\content type\image/jpeg\bits
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/pjpeg\bits
    Opens key:
                                                             HKCR\mime\database\content type\image/pjpeg\bits
                                                             \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \mime \database \content type \mime \mi
    Opens key:
    Opens key:
                                                             HKCR\mime\database\content type\image/png\bits
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/tiff\bits
    Opens key:
                                                             HKCR\mime\database\content type\image/tiff\bits
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/x-icon\bits
    Opens key:
                                                             HKCR\mime\database\content type\image/x-icon\bits
                                                             \label{local-content} HKCU \ software \ \ lasses \ \ ime \ \ database \ \ type \ \ image/x-jg \ bits
    Opens key:
    Opens key:
                                                             HKCR\mime\database\content type\image/x-jg\bits
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/x-png\bits
    Opens key:
                                                             HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt image} \mbox{\tt x-png} \mbox{\tt bits}
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/x-wmf\bits
    Opens key:
                                                             HKCR\mime\database\content type\image/x-wmf\bits
    Opens key:
                                                             HKCU\software\classes\mime\database\content type\image/x-png
    Opens key:
                                                             HKCR\mime\database\content type\image/x-png
    Opens key:
                                                             HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
                                                             HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
    Opens key:
```

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\progid

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid Opens key: Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprocserver32

Opens key: $HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\$

```
HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
  Opens key:
00a0c913f750}\inprochandler32
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
  Opens key:
                                     HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
  Opens key:
00a0c913f750}\inprochandler
  Opens key:
                                     HKCR \verb|\clsid|{a3ccedf7-2de2-11d0-86f4-00a0c913f750} \verb|\inprochandler| \\
                                     HKCU\software\classes\mime\database\content type\image/gif
  Opens key:
                                     HKCR\mime\database\content type\image/gif
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
                                     HKLM\software\microsoft\internet
  Opens kev:
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\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
  Opens kev:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
  Opens key:
                                     HKCU\software\microsoft\internet explorer\new windows
  Opens key:
                                     HKLM\software\microsoft\internet explorer\new windows
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
                                     HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_xmlhttp
  Opens key:
                                     HKCU\software\classes\shockwaveflash.shockwaveflash
                                     HKCR\shockwaveflash.shockwaveflash
  Opens key:
  Opens key:
                                     HKCU\software\classes\shockwaveflash.shockwaveflash\clsid
  Opens key:
                                     HKCR\shockwaveflash.shockwaveflash\clsid
                                     HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:
  Opens key:
                                     HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:
                                     HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\treatas
  Opens key:
                                     HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000}\treatas
  Opens key:
                                     HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\progid
  Opens key:
                                     HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid
  Opens key:
                                     HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
                                     HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32
  Opens kev:
  Opens key:
                                     HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
  Opens key:
                                     HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler32
                                     HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
  Opens kev:
444553540000}\inprochandler
                                     HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\\\label{eq:hkcr} \label{eq:hkcr} In prochamble for the control of the control
  Opens key:
                                     HKLM\hardware\description\system\centralprocessor\0
  Opens key:
                                     HKCU \setminus software \setminus classes \setminus typelib \setminus \{d27cdb6b-ae6d-11cf-96b8-444553540000\}
  Opens key:
  Opens key:
                                     HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
  Opens kev:
                                     HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000\}\1.0
                                     HKCR \ typelib \ \{d27cdb6b-ae6d-11cf-96b8-444553540000\} \ \ 1.0
  Opens key:
                                     HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
  Opens key:
444553540000}\1.0\409
                                     HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\409
  Opens key:
  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
                                     HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0
  Opens key:
  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}
  Opens key:
                                     HKCR\typelib\{00020430-0000-0000-c000-00000000046}
                                     HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\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 kev:
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\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0

HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0 Opens kev: Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c200c04fb6bfc4}\1.0\0

Opens kev:

HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0 Opens key: Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-

00c04fb6bfc4}\1.0\0\win32

HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_domstorage

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_domstorage

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key:

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\treatas

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler32

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32 Opens kev:

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler Opens key: Opens key: HKCU\software\microsoft\internet explorer\feed discovery Opens key: HKLM\software\microsoft\internet explorer\feed discovery

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

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

compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000} HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_addon_management HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_addon_management HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_alloweddomainlist Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_alloweddomainlist

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

compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}

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

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

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

units\{d27cdb6e-ae6d-11cf-96b8-444553540000} HKCU\software\classes\clsid Opens key:

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

444553540000}\availableversion

Opens kev: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion

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

444553540000}\installedversion

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\installedversion $HKCU\software\classes\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\appid$ Opens key:

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

444553540000}\languagecheckperiod

HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\languagecheckperiod Opens key:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915

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

444553540000}\miscstatus

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

444553540000}\miscstatus\1

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1

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

Opens key: HKCU\software\classes\mime\database\content type\application/x-

shockwave-flash

Opens key: HKCR\mime\database\content type\application/x-shockwave-flash Opens key: HKCU\software\classes\protocols\filter\application/x-shockwave-flash

Opens key: HKCR\protocols\filter\application/x-shockwave-flash

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60} Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\treatas

```
Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\treatas
Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\progid
Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32
```

Opens key: $HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32$

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\inprochandler32

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler32

Opens key:

HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\inprochandler

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler
Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap

Opens key: HKLM\software\microsoft\msxml30

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

settings\5.0\cache\extensible cache\userdata

Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 001
Opens key: HKLM\system\currentcontrol\set\control\lsaextensionconfig\sspicli

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

Opens key: HKLM\system\currentcontrol\sa\sspicache\credssp.dll
Opens key: HKLM\system\currentcontrol\securityproviders\saslprofiles
Opens key: HKCU\software\microsoft\internet explorer\domstorage\baidu.com
Opens key: HKCU\software\microsoft\internet explorer\domstorage\total
Opens key: HKLM\software\microsoft\windows\currentversion\policies\system
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39} Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\treatas

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\progid

Opens key: HKCR\shockwaveflash.shockwaveflash.7

 $Opens\ key: \\ HKCU \ software \ classes \ shockwave flash. shockwave flash. 7 \ clsid$

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

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprocserver32

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprochandler32

 $Opens~key: \\ HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\ \ inprochandler 32 \\$

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprochandler

Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-

0080c7f4ee85}\proxystubclsid32

000000000046}\treatas

 Opens key:
 HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid

 Opens key:
 HKCU\software\classes\clsid\{00020424-0000-0000-c000

00000000046}\inprocserver32

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\inprochandler32

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandler32

000000000046}\inprochandler

0080c7f4ee85}\forward

Opens key: $\begin{tabular}{ll} HKCR \end{tabular} HKCR \end{tabular} HKCQ \end{tabular} HCQ \end{tabular} HKCQ \end{tabular} HCQ \end{tabular$

0080c7f4ee85}\typelib

 $\label{lem:continuous} Opens key: $$ HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib$$ Opens key: $$ HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}$$$

Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}

Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1

Opens key: $\begin{tabular}{ll} HKCR \typelib & eab22ac0-30c1-11cf-a7eb-0000c05bae0b & 1.1 \\ Opens key: & HKCU \software \classes \typelib & eab22ac0-30c1-11cf-a7eb- \end{tabular}$

```
0000c05bae0b}\1.1\0
```

HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0 Opens key: Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-

0000c05bae0b}\1.1\0\win32

Opens kev: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32 Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}

HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-Opens key:

00000000046}\proxystubclsid32

HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046}

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

000000000046}\treatas

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

000000000046}\progid

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

000000000046}\inprocserver32

 $\label{local-cond} \mbox{HKCR\clsid\{00020420-0000-0000-c000-000000000046\}\inprocserver32}} \\ \mbox{ } \mbox{$ Opens key:

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

00000000046}\inprochandler32

HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler32 Opens key:

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

0000000000046}\inprochandler

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

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

00aa006009fa}\proxystubclsid32

HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32 Opens key: Opens key: $\label{local-hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \a4a1a128-768f-41e0-bf75-e4fddd \clsid \clsid \a4a1a128-768f-41e0-bf75-e4fddd \clsid \clsid$

HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba} Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-41e$ Opens key:

e4fddd701cba}\treatas

HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75e4fddd701cba}\progid

HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-Opens key:

e4fddd701cba}\inprocserver32

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32

HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-Opens key:

e4fddd701cba}\inprochandler32

 $HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba\}\inprochandler32$ Opens key:

HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-Opens key:

e4fddd701cba}\inprochandler

HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler Opens kev: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5078f35 - c551 - 11d3 - 89b9 - 0000f81fe221\}$ Opens key:

Opens key: HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221} Opens key: HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-

0000f81fe221}\treatas

HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-

0000f81fe221}\progid

HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid Opens key: Opens key: HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-

0000f81fe221}\inprocserver32

Opens key: Opens key: HKCU\software\classes\interface\{00020404-0000-0000-0000-000000000046}

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

00000000046}\proxystubclsid32

HKCR\interface\{00020404-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: Opens key: HKCU\software\classes\clsid\{00020421-0000-0000-c000-00000000046}

Opens key: HKCR\clsid\{00020421-0000-0000-c000-00000000046} HKCU\software\classes\clsid\{00020421-0000-0000-c000-Opens key:

000000000046}\treatas

HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-Opens kev:

0000f81fe221}\inprochandler32

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

000000000046}\progid

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

00000000046}\inprocserver32

Opens key: Opens key: HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5078f35 - c551 - 11d3 - 89b9 - f648f35 - c551 - 6566 - 6$ Opens key:

0000f81fe221}\inprochandler

HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{00020421-0000-0000-c000-c000-c000-c000-c0000-c00-c00-c000-c000-c00-c00-c000-c00-$

```
00000000046}\inprochandler32
                          HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprochandler32
 Opens kev:
                           HKCU\software\classes\clsid\{00020421-0000-0000-c000-
 Opens kev:
00000000046}\inprochandler
 Opens key:
                          HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprochandler
 Opens key:
                           HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
                          HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
 Opens key:
                           HKCU \setminus software \setminus classes \setminus interface \setminus \{332c4425-26cb-11d0-b483-00c04fd90119\}
 Opens key:
 Opens key:
                           HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
                          HKCU\software\classes\interface\{332c4425-26cb-11d0-b483-
```

Opens key: HKCU\
00c04fd90119}\proxystubclsid32

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\interface $$ (332c4425-26cb-11d0-b483-00c04fd90119) proxystubclsid32 \\ Opens key: \\ HKCU\software $$ (lasses\clsid\e569bde7-a8dc-47f3-893f-fd2b31b3eefd) $$ (asset) $$$

Opens key: $\label{eq:hkclsid} \mbox{HKCR\clsid\e569bde7-a8dc-47f3-893f-fd2b31b3eefd} \\ \mbox{Opens key:} \mbox{HKCU\software\classes\clsid\e569bde7-a8dc-47f3-893f-}$

fd2b31b3eefd}\treatas

fd2b31b3eefd}\progid

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

fd2b31b3eefd}\inprocserver32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32

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

fd2b31b3eefd}\inprochandler32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32

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

fd2b31b3eefd}\inprochandler

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler Opens key: HKLM\software\policies\microsoft\internet explorer\services

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

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

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

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites

Opens key: HKCU\software\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

 $Opens~key: \\ HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\\\ shellfolder$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

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

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

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

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \end{tabular} \label{lem:hkcu}$

Opens key:

11e3-b3bc-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

b8dc300d9f9d}\treatas

Opens key: $\begin{tabular}{ll} HKCR\clsid\f1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\treatas \\ Opens key: \\ HKCU\software\classes\clsid\f1f486a52-3cb1-48fd-8f50-\\ \end{tabular}$

b8dc300d9f9d}\progid

 $\label{lem:continuous} Opens~key: $$ HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid $$ Opens~key: $$ HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}\progid $$ HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}\progid $$ Opens~key: $$ HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}\progid $$ Opens~key: $$ HKCU\software\classes\clsid\clsi\$

b8dc300d9f9d}\inprocserver32

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

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

b8dc300d9f9d}\inprochandler32

 $Opens \ key: \\ HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler 32$

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

b8dc300d9f9d}\inprochandler

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler Opens key: HKCU\software\microsoft\windows\currentversion\explorer\

Opens key:

 $HKLM \ software \ microsoft \ windows \ shell \ registered applications \ urlassociations \ directory \ open with progids$

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \microsoft \windows \shell \associations \urlassociations \directory \end{tabular}$

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver Opens key: HKCR\directory\curver Opens key: HKCR\directory\ HKCU\software\classes\directory\shellex\iconhandler Opens key: Opens kev: 11e3-b3bc-806e6f6e6963}\ HKCR\directory\shellex\iconhandler Opens key: Opens key: HKCU\software\classes\folder Opens key: HKCR\folder Opens key: HKCU\software\classes\folder\shellex\iconhandler Opens key: HKCR\folder\shellex\iconhandler Opens key: HKCU\software\classes\allfilesystemobjects Opens key: HKCR\allfilesystemobjects Opens key: HKCU\software\classes\allfilesystemobjects\shellex\iconhandler HKCR\allfilesystemobjects\shellex\iconhandler Opens key: HKCU\software\classes\directory\docobject Opens kev: Opens key: HKCR\directory\docobject Opens key: HKCU\software\classes\folder\docobject Opens key: HKCR\folder\docobject Opens key: HKCU\software\classes\allfilesystemobjects\docobject Opens key: HKCR\allfilesystemobjects\docobject HKCU\software\classes\directory\browseinplace Opens kev: Opens key: HKCR\directory\browseinplace Opens key: HKCU\software\classes\folder\browseinplace Opens key: HKCR\folder\browseinplace Opens key: HKCU\software\classes\allfilesystemobjects\browseinplace Opens key: HKCR\allfilesystemobjects\browseinplace Opens key: HKCU\software\classes\directory\clsid Opens key: HKCR\directory\clsid Opens key: HKCU\software\classes\folder\clsid Opens key: HKCR\folder\clsid Opens key: HKCU\software\classes\allfilesystemobjects\clsid Opens key: HKCR\allfilesystemobjects\clsid $HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\}$ Opens key: Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000} Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32 $HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\tinprocserver32$ Opens key: Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellfolder Opens key: $HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\$ HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens kev: 444553540000}\treatas HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens kev: 444553540000}\inprochandler32 HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32 Opens kev: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens key: 444553540000}\inprochandler $\label{local-eq:hkcr} $$ HKCR\clsid{ff393560-c2a7-11cf-bff4-444553540000} \in \clsid{ff393560-c2a7-11cf-bff4-444553540000} = \cline{hkcr} $$ The content of the content of$ Opens key: Opens kev: bff4-444553540000} Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042220160423 HKCU\software\microsoft\windows\currentversion\app Opens key: paths\1af5338669efabe0a9841478396871b1.exe HKLM\software\microsoft\windows\currentversion\app Opens key: paths\1af5338669efabe0a9841478396871b1.exe $HKCU \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus (20d04feo-block) + (20d04feo-block) +$ Opens kev: 3aea-1069-a2d8-08002b30309d} Opens kev: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session \inf o 1 \setminus desktop \setminus names pace \setminus name customizations$ $HKCU \setminus software \setminus classes \setminus clsid \setminus \{20d04fe0-3aea-1069-a2d8-08002b30309d\}$ Opens key: Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d} Opens key: HKCU\software\microsoft\internet explorer\main\windowssearch Opens key: HKLM\software\policies\microsoft\internet explorer\feeds HKCU\software\microsoft\internet explorer\feeds Opens key: Opens key: HKLM\software\microsoft\internet explorer\feeds Opens key:

87bd-30b759fa33dd} Opens key: 87bd-30b759fa33dd}\propertybag

Opens key: HKLM\software\microsoft\windows search

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f391-98b5-11cf-bb82-00aa00bdce0b\}$

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b} Opens kev: Opens key: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb8200aa00bdce0b}\treatas

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens kev: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\progid

Opens key: HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\progid Opens key: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\inprochandler32

Opens kev: HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32

Opens key: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprochandler Opens key: Opens key: HKCU\software\classes\mime\database\content type\image/x-icon

Opens key: HKCR\mime\database\content type\image/x-icon Opens key: HKCU\software\classes\protocols\filter\image/x-icon Opens key: HKCR\protocols\filter\image/x-icon

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative Opens kev: HKLM\software\microsoft\internet explorer\activex

compatibility\{adc6cb82-424c-11d2-952a-00c04fa34f05}

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}

HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05} Opens key: Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\treatas

HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\progid

Opens key: Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\inprocserver32

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\inprochandler32

 $HKCR\clsid\\ \{adc6cb82-424c-11d2-952a-00c04fa34f05\}\\ \cline{Constraints}$ Opens key:

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\inprochandler

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprochandler Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}

Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d} HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-Opens key:

00c04fd9189d}\treatas

HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-Opens key:

00c04fd9189d}\progid

HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\progid Opens kev: Opens key:

00c04fd9189d}\inprocserver32

HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-

00c04fd9189d}\inprochandler32

Opens kev: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32

HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-Opens key:

00c04fd9189d}\inprochandler

HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler Opens key:

Oueries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

HKCU\control panel\desktop[preferreduilanguages] Queries value:

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Oueries value:

 $HKLM \verb|\software\microsoft\windows \verb|\currentversion\side| preferex ternal manifest| \\$ Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\microsoft\windows Queries value:

nt\currentversion\compatibility32[1af5338669efabe0a9841478396871b1]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] HKLM\software\microsoft\windows\currentversion\internet Oueries value:

settings[disableimprovedzonecheck]

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

settings[security_hklm_only]

Oueries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]

```
Oueries value:
                                                HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Oueries value:
                                                HKLM\system\currentcontrolset\control\nls\locale[000004091
   Oueries value:
                                                HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
   Queries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
   Oueries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
   Oueries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
   Queries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                                               HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
   Queries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
                                                HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                                                HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:
   Oueries value:
                                                \label{lem:hklmsoftware} \verb+ MKLM \software \microsoft \windows nt \current version \fontsubstitutes [segoe to the lemma 
ui]
   Oueries value:
                                                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
                                                HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Oueries value:
   Queries value:
                                                HKLM\software\microsoft\com3[com+enabled]
   Queries value:
                                                \label{locality} $$HKCR\clsid_{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]$
   Queries value:
                                                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
                                                HKCR\clsid\{8856f961-340a-11d0-a96b-
   Oueries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                                                \label{locality} \begin{tabular}{ll} HKCR\clsid & 8856f961-340a-11d0-a96b-00c04fd705a2} \in \cline{2.00cm} \end{tabular} \label{locality} All the content of the content of
   Oueries value:
                                                HKCR\clsid\{8856f961-340a-11d0-a96b-
   Oueries value:
00c04fd705a2}\inprocserver32[threadingmodel]
   Queries value:
                                                HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
                                                HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Oueries value:
                                                HKLM\system\setup[oobeinprogress]
   Oueries value:
                                                HKLM\system\setup[systemsetupinprogress]
                                                HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:
   Queries value:
                                                Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
   Queries value:
                                                HKLM\software\microsoft\ctf[enableanchorcontext]
   Oueries value:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Oueries value:
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                                HKLM\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[createuricachesize]
   Oueries value:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
   Queries value:
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablepunycode]
   Queries value:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[1af5338669efabe0a9841478396871b1.exe]
   Queries value:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
   Oueries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus access providers [martaextension]
```

```
HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Oueries value:
  Oueries value:
                                     HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
                                     HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Queries value:
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
                                     HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Oueries value:
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\main[frametabwindow]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\main[framemerging]
                                     HKLM\software\microsoft\internet explorer\main[framemerging]
  Oueries value:
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\main[sessionmerging]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:
                                     HKLM\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:
                                     HKLM\software\microsoft\internet explorer\main[navigationdelay]
  Queries value:
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
  Queries value:
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsfordisplay]
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[usedrophandler]
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
  Oueries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforoverlay]
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Queries value:
08002b30309d}\shellfolder[queryforinfotip]
  Oueries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideinwebview]
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
  Queries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsuniversaldelegate]
  Oueries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[nofilefolderjunction]
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
  Queries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hasnavigationenum]
                                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
  Oueries value:
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}1
                                     \label{local-eq:hkcr} $$HKCR\clsid_{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]$
  Queries value:
  Queries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                                     HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0xffff1
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
                                    \label{thm:local_hammon} \begin{tabular}{l} HKLM \end{tabular} software \end{tabular} in constraints 
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[urlencoding]
  Queries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[1af5338669efabe0a9841478396871b1.exe]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
  Oueries value:
                                    HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\1[flags]
```

```
Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\4[flags]
 Queries value:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Oueries value:
                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe]
                      HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Queries value:
                       HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
                       HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
 Oueries value:
b924-d51178a59ce4]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[fromcachetimeout]
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certificaterevocation]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablepassport]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[idnenabled]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttp1_1]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
 Queries value:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablenegotiate]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
 Queries value:
                      HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Oueries value:
                      HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Oueries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
 Queries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                      HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[signature]
 Queries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
                      HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
ba85-6007caedcf9d}[category]
ba85-6007caedcf9d}[name]
 Queries value:
ba85-6007caedcf9d}[parentfolder]
 Oueries value:
ba85-6007caedcf9d}[description]
 Queries value:
```

ba85-6007caedcf9d}[relativepath]

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{352481e8-33be-4251-ba85-6007 \ caed \ ff \ 'garsing \ name]$

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{352481e8-33be-4251-ba85-6007 caed \ folder \ fol$

Queries value:

 $HKLM \software \mbox{$microsoft\windows\currentversion} \explorer \folder descriptions \folder \fold$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d\}[icon]}$

Queries value:

 $HKLM \ software \ `microsoft \ windows \ `current version \ `explorer \ folder descriptions \ `\{352481e8-33be-4251-ba85-6007 \ caedcf9d\} [security]$

Queries value:

 $HKLM \ software \ `microsoft \ windows \ `current version \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 \ caedcf9d\} \ [stream resource]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 \ caedcf9d\} \ [stream resource type]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '{352481e8-33be-4251-ba85-6007} caed \ 'folder descriptions' \ 'folder descr$

Queries value:

 $HKLM \ software \ `microsoft \ windows \ `current version \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ fold$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 \ caedcf9d\} \ [precreate]$

Oueries value:

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 \ caedcf9d\} \ [attributes]$

Queries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{352481e8-33be-4251-ba85-6007 caed \ folder \ 'handler'\}$

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cache]

Queries value:

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}[name]$

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}(description)$

Queries value:

 $\label{thm:hk.mass} $$HKL^M\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[relativepath]}$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}parsing name\figure{1}{2}$

Queries value

 $\label{lem:hkk} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[infotip]}$

Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{$microsoft$} windows \current version \explorer \folder descriptions \fill{lem:hklm} f1b32785-6fba-4fcf-9d55-7b8e7f157091 \fill{lem:hklm} fill{lem:hklm} fill{lem:h$

Queries value:

 $\label{thm:local-operator} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}recurity\figure{1}{2}$

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource type]$

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [local redirectonly]$

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [attributes]$

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

Queries value:

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

folders[local appdata]

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \colored \co$

Oueries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[name]}$

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Oueries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[description]}$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[relativepath]}$

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[infotip]} Infotip \[\] $$ (a) $$ (a) $$ (a) $$ (b) $$ (b) $$ (b) $$ (c) $$

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localized name]}$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[icon]}$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[security]}$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresource]}$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localredirectonly]}$

Queries value

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[roamable]}$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[precreate]}$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the label of the label o$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[foldertypeid]}$

9afe-ea3317b67173}[initfolderhandler]

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

2160590473-689474908-1361669368-1002[profileimagepath]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

 $\label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet$ Queries value:

settings\5.0\cache\cookies[peruseritem]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]

Queries value:

908e-08a611b84ff6}[parentfolder]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex$ 908e-08a611b84ff6}[relativepath]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]

Queries value:

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

Oueries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-d1474-d14744-d1474$ 908e-08a611b84ff6}[localizedname]

Oueries value:

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

Oueries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-d1474-d14744-d1474$ 908e-08a611b84ff6}[securitv]

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex$ 908e-08a611b84ff6}[streamresource]

Oueries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-d1474-d14744-d1474$ 908e-08a611b84ff6}[streamresourcetype]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-descriptions \ 'explorer'\} \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer'' \ 'exp$ 908e-08a611b84ff6}[localredirectonly]

Oueries value:

908e-08a611b84ff6}[roamable]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]

Oueries value:

908e-08a611b84ff6}[stream]

Oueries value:

908e-08a611b84ff6}[publishexpandedpath]

Oueries value:

908e-08a611b84ff6}[attributes]

Queries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-d1474-d14744-d1474$ 908e-08a611b84ff6}[foldertypeid]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-descriptions \ 'explorer'\} \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer'' \ 'exp$ 908e-08a611b84ff6}[initfolderhandler]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cookies]

Oueries value:

a03a-e3ef65729f3d}[category]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[name]

Oueries value:

a03a-e3ef65729f3d}[parentfolder]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [description]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[relative path]}$

Oueries value:

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[infotip]}$

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[icon]}$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[streamresource]$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[attributes]$

Queries value:

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[initfolderhandler]$

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[appdata]

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

settings\5.0\cache\cookies[cacheprefix]

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem]

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}\category\cite{Acceptable} and the second se$

Queries value:

 $HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}\[name]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folder descriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}\[parentfolder]$

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [relative path]$

Queries value:

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

Queries value:

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

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

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}\[icon]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [local redirectonly]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [roamable]$

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[stream]}$

Queries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [publish expanded path]$

Oueries value:

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

Queries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ (d9dc8a3b-b784-432e-a781-5a1130a75963) \ [folder type id]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [initfolder \ handler]$

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ value \\ \\$

folders[history]

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

settings\5.0\cache\history[cacheprefix]

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

settings\5.0\cache\history[cachelimit]

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

settings\5.0\cache\extensible cache\domstore[cacherepair]

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

settings\5.0\cache\extensible cache\domstore[cachepath]

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

settings\5.0\cache\extensible cache\domstore[cacheprefix]
Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\domstore[cachelimit]

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

settings\5.0\cache\extensible cache\domstore[cacheoptions]

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

settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Queries value: HKCU\software\microsoft\windows\currentversion\internet

queries value. HRCU\SUT (Walle\IIIICT USUT (\WITHUUW

settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value: HKCU\software\microsoft\windows\currentversion\internet

Queries value: HKCU\software\microsoft\windows\o
settings\5.0\cache\extensible cache\feedplat[cacheprefix]

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

settings\5.0\cache\extensible cache\feedplat[cachelimit]

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

settings\5.0\cache\extensible cache\feedplat[cacheoptions]

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

settings\5.0\cache\extensible cache\iecompat[cacherepair]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cachepath]

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

settings\5.0\cache\extensible cache\iecompat[cacheprefix]

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

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

settings\5.0\cache\extensible cache\iecompat[cacheoptions]

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

settings\5.0\cache\extensible cache\ietld[cacherepair]

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

settings\5.0\cache\extensible cache\ietld[cachepath]

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

settings\5.0\cache\extensible cache\ietld[cacheprefix]

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

settings\5.0\cache\extensible cache\ietld[cachelimit]

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enableautoproxyresultcache]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[displayscriptdownloadfailureui]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[mbcsservername]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsapiforcrack]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[utf8servernameres]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
 Queries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[httpdefaultexpirytimesecs]
 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[ftpdefaultexpirytimesecs]
 Queries value:
                           HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[perusercookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[leashlegacycookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                          \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[dialupuselansettings]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[wpadsearchalldomains]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                          \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
 Queries value:
settings[bypasshttpnocachecheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sharecredswithwinhttp]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[mimeexclusionlistforcache]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[headerexclusionlistforcache]
 Queries 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
 Queries 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]
 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[warnonbadcertrecving]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonhttpstohttpredirect]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
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]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
 Oueries 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\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000016 \ [packed catalog item] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
 Queries 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\000000000001[librarypath]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 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\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \pace_catalog 5 \catalog_entries \pace_catalog 5 \catalog 5 \catalog 5 \catalog 6 \ca$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 [provider info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000003 \ [storesserviceclassinfo] \ Queries \ value:$

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 00000000000003[provider in fo]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[librarypath]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000004 \ [displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000004 [supported name space]]
  Queries value:
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 0000000000004 [version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000004[storesserviceclassinfo]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[displaystring]
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 \ [address family]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[enabled]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ (version) \ and \ services \ (version) \ and \ (
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog \ entries \ 000000000005 \ [storesservice class in fo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000006 \ [displaystring]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 \ [address family]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000006[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\wpad[wpadoverride]
  Queries value:
                                 HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[nonetautodial]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[globaluseroffline]
  Queries value:
                                 HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Oueries value:
                                 HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
  Oueries value:
                                 HKLM\software\microsoft\tracing[enableconsoletracing]
  Oueries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[enablefiletracing]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filetracingmask]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[enableconsoletracing]
  Oueries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[consoletracingmask]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[maxfilesize]
```

```
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filedirectory]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\profilelist[programdata]
 Queries value:
                          HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a5ea4f8e]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled sessions [machine throttling]
 Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
                          HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
 Oueries value:
 Oueries value:
HKLM \ software \ microsoft \ tracing \ 1af5338669efabe0a9841478396871b1\_rasmancs \ [enable file tracing]
 Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[filetracingmask]
 Oueries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[enableconsoletracing]
 Oueries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[consoletracingmask]
 Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[maxfilesize]
 Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[filedirectory]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[proxysettingsperuser]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[migrateproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyenable]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyserver]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxvoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[autoconfigurl]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\connections[savedlegacysettings]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\connections[defaultconnectionsettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[autoconfigcustomua]
 Queries value:
                          HKCR\autoproxytypes\application/x-internet-signup[dllfile]
 Oueries value:
                          HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
                           HKCR\autoproxytypes\application/x-internet-signup[default]
 Queries value:
 Oueries value:
                           HKCR\autoproxytypes\application/x-internet-signup[flags]
                           HKCR \verb| autoproxytypes \verb| application/x-ns-proxy-autoconfig[dllfile]| \\
 Oueries value:
                           HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
 Oueries value:
                           HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
 Queries value:
 Queries value:
                           \label{local-config} \begin{tabular}{ll} HKCR \autoproxy types \application/x-ns-proxy-autoconfig[flags] \end{tabular}
 Queries value:
                           HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zonemap[autodetect]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [domain name devolution level]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [allow unqualified query]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Queries value:
                           HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
```

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]$ Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazv] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [maxnegative cachettl]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] 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] HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts] Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+dns \ cache \ \verb+parameters \ [dnsquick query time outs]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Queries value:
                        HKCU\software\microsoft\internet explorer[no3dborder]
 Oueries value:
                         HKLM\software\microsoft\internet explorer[no3dborder]
 Oueries value:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
 Queries value:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
 Queries value:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[1af5338669efabe0a9841478396871b1.exe]
                        HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_mime_handling[*]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
 Queries value:
                        HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[compatible]
 Queries value:
                        HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
                        HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[version]
                        HKCU\software\microsoft\windows\currentversion\internet settings[user
 Queries value:
agent]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
                        HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[platform]
 Queries value:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[1af5338669efabe0a9841478396871b1.exe]
                        HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_browser_emulation[*]
 Oueries value:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[1af5338669efabe0a9841478396871b1.exe]
                        HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
                        HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value:
 Queries value:
                        HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:
                        HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
 Queries value:
                        HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
                        HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Oueries value:
 Queries 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]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                         HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
c19ce8a73253}[searchlist]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
 Queries value:
                         HKCU\software\microsoft\internet explorer\international[acceptlanguage]
```

```
Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[1af5338669efabe0a9841478396871b1.exe]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
  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\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
  Queries value:
                                    HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
                                    HKCR\clsid\{00bb2765-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
  Queries value:
  Queries value:
                                   HKCR\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{6935db93-21e8-4ccc-beb9-
  Queries value:
9fe3c77a297a}\inprocserver32[threadingmodel]
                                   HKCU\software\microsoft\windows\currentversion\explorer\runmru[mrulist]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
  Queries value:
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
  Queries value:
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-
  Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
  Oueries value:
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
  Oueries value:
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete\client[]
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
  Queries value:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
  Queries value:
  Queries value:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{807c1e6c-1d00-453f-b920-
  Oueries value:
b61bb7cdd997}\inprocserver32[threadingmodel]
                                   HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                    HKCU\control panel\desktop[smoothscroll]
  Queries value:
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced [acclist view v6]) \ described by the software \ described \ described by the software \ described by the software \ described \ describe
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
c19ce8a73253}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
  Queries value:
c19ce8a73253}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
  Queries value:
```

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[nameserver]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \ [nameserver]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpnameserver]

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [enabled \ hcp]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [registration enabled]$

Queries value:

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [domain]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [dhcpdomain]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [names erver]$

Queries value:

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \ [queryadaptername]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \troip \parameters \troin et \square \end{2.5} I disable adapter domain name]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \true physical parameters \true faces \end{128919e8-8a5e-41d1-ac17-c19ce8a73253} \ [registration max address count]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \ [maxnumber of addresses to register]$

Queries value:

Queries value:

 $\label{lem:hklm} HKLM \system \current controls et \services \troip \parameters \ left e29 ac 6c 2-7037-11 de-816 d-806 e6f 6e 6963 \ [query adapter name]$

Queries value:

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [disable dynamic update]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [enable adapter domain name registration]$

Queries value:

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enablemulticast]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]

Queries value: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]

Queries value: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-

199fdba5723b}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-

199fdba5723b}\inprocserver32[threadingmodel]

Queries value: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]

Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]

Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]

Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]

Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

```
HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Oueries value:
  Oueries value:
                                       HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Oueries value:
                                       HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privkey cachepurge interval seconds]
  Queries value:
                                      HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                       HKLM\software\microsoft\cryptography[machineguid]
  Oueries value:
                                       HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
  Oueries value:
  Oueries value:
                                       HKLM\software\microsoft\rpc\extensions[remoterpcdll]
                                       HKCR \setminus \{d0074ffd-570f-4a9b-8d69-199fdba5723b\} \setminus \{d0074ffd-570f-4a9b-8d69-199fdba572ab] \setminus \{d0074ffd-640ffdba572ab] \setminus \{d0074ffd-640ffdba572ab] \setminus \{d0074ffdba572ab] \setminus \{d007
  Oueries value:
                                       HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
  Oueries value:
  Queries value:
                                      HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
                                      HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
  Oueries value:
  Oueries value:
                                      HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[threadingmodel]
                                      HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32[]
  Oueries value:
  Queries value:
                                      HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32[]
  Queries value:
                                       HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32[]
  Oueries value:
                                      HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
  Queries value:
                                      HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
                                      HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
  Oueries value:
  Queries value:
                                      HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[threadingmodel]
                                      HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32[]
  Queries value:
  Queries value:
                                       HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32[]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
                                      HKLM\system\currentcontrolset\services\netbt\linkage[export]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[1a10]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[privacyadvanced]
                                      HKCR\mime\database\content type\text/html[extension]
  Queries value:
                                      HKLM\software\microsoft\internet
  Queries value:
explorer \verb|\main| featurecontrol| feature\_mime\_sniffing[1af5338669efabe0a9841478396871b1.exe]|
                                      HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_mime_sniffing[*]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
                                      HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_feeds[1af5338669efabe0a9841478396871b1.exe]
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature feeds[*]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[1af5338669efabe0a9841478396871b1.exe]
                                     HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
                                      HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
  Queries value:
                                      HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
  Oueries value:
  Queries value:
                                      HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
                                      HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
  Oueries value:
  Oueries value:
                                      HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[1af5338669efabe0a9841478396871b1.exe]
                                      HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_legacy_dispparams[*]
  Queries value:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[1af5338669efabe0a9841478396871b1.exe]
                                      HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_object_caching[*]
  Queries value:
                                      HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
                                      HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-
  Oueries value:
91a2-7b624e0e7244]
                                      HKLM\software\microsoft\internet explorer\application
  Oueries value:
compatibility[1af5338669efabe0a9841478396871b1.exe]
  Queries value:
                                      HKCU\software\microsoft\internet explorer\domstorage[totallimit]
  Queries value:
                                       HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
  Oueries value:
                                      HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
                                      HKCU\software\microsoft\windows
  Oueries value:
nt\currentversion\windows[dragscrolldelay]
  Oueries value:
                                      HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
                                      HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_restrict_filedownload[1af5338669efabe0a9841478396871b1.exe]
```

```
Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature restrict filedownload[*]
 Oueries value:
                          HKCR\protocols\handler\about[clsid]
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
 Queries value:
 Oueries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
 Oueries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
 Queries value:
                          HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
                          HKLM\software\microsoft\windows\currentversion\internet settings\url
 Queries value:
history[daystokeep]
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Oueries value:
                          HKCU\software\microsoft\internet explorer[smartdithering]
 Queries value:
                          HKCU\software\microsoft\internet explorer[rtfconverterflags]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[usecleartype]
                          HKCU\software\microsoft\internet explorer\main[page_transitions]
 Queries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[anchor underline]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[css_compat]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[expand alt text]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[display inline images]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[display inline videos]
 Queries value:
                          HKLM\software\microsoft\internet explorer\main[display inline videos]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[play_background_sounds]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[play_animations]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[print_background]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[use stylesheets]
                          HKCU\software\microsoft\internet explorer\main[smoothscroll]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[xmlhttp]
 Queries value:
 Oueries value:
 Queries value:
 Queries value:
                          \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main[force offscreen]}} \label{lem:hkcu}
 Queries value:
composition]
 Oueries value:
 Oueries value:
 Oueries value:
 Queries value:
```

HKCU\software\microsoft\internet explorer\main[show image placeholders] HKCU\software\microsoft\internet explorer\main[disable script debugger] HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie] HKCU\software\microsoft\internet explorer\main[move system caret]

HKCU\software\microsoft\internet explorer\main[enable autoimageresize]

HKCU\software\microsoft\internet explorer\main[usethemes] HKCU\software\microsoft\internet explorer\main[usehr] HKCU\software\microsoft\internet explorer\main[q300829] Oueries value: HKCU\software\microsoft\internet explorer\main[cleanup htcs] Queries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest] HKLM\software\microsoft\internet explorer\main[xdomainrequest] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\main[domstorage] HKCU\software\microsoft\internet Oueries value:

explorer\international[default codepage]

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

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: HKCU\software\microsoft\internet explorer\settings[anchor color hover] Queries value: Oueries value: HKCU\software\microsoft\internet explorer\settings[always use my colors] Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font size1

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

color1

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

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]
 Oueries value:
                         HKLM\software\microsoft\internet explorer\version vector[ie]
 Oueries value:
                         HKLM\software\microsoft\internet explorer\version vector[vml]
                         HKLM\software\microsoft\internet explorer\version vector[windowsedition]
 Queries value:
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_zone_elevation[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[*]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[*]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[cointernetcombineiuricachesize]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[cointernetcombineiuricachesize]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[cointernetcombineiuricachesize]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_sslux[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux[*]
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonintranet]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_subdownload_lockdown[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[securityidiuricachesize]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonintranet]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[securityidiuricachesize]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[securityidiuricachesize]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[securitvidiuricachesize]
                         HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
 Queries value:
                         HKCR\clsid\{50d5107a-d278-4871-8989-
 Oueries value:
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                         HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{50d5107a-d278-4871-8989-
 Queries value:
f4ceaaf59cfc}\inprocserver32[threadingmodel]
                         HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid[]
 Queries value:
                         HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[inprocserver32]
                         HKCR \clsid \f414c260-6ac0-11cf-b6d1-00aa00bbb58 \inprocserver 32[]
 Queries value:
 Queries value:
                         HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
                         HKCU\software\microsoft\internet explorer\recovery[autorecover]
 Queries value:
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_block_lmz_img[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[*]
                         HKLM\software\microsoft\internet explorer\default behaviors[homepage]
 Oueries value:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]
 Oueries value:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[]
 Queries value:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
 Queries value:
00aa00bdce0b}\inprocserver32\inprocserver32\
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
                         HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]
 Oueries value:
 Queries value:
                         HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]
 Oueries value:
                         HKCR\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[inprocserver32]
```

Oueries value: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]

HKCR\clsid\{81397204-f51a-4571-8d7b-Oueries value:

dc030521aabd}\inprocserver32[threadingmodel]

HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[] Queries value:

HKCR\clsid\{d1fe6762-fc48-11d0-883a-Oueries value:

3c8b00c10000}\inprocserver32[inprocserver32]

 $HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\tinprocserver32[]$ Oueries value:

HKCR\clsid\{d1fe6762-fc48-11d0-883a-Oueries value:

3c8b00c10000}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\internet explorer\default

behaviors[dxtfilterbehavior]

Queries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]

Queries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]

Oueries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprocserver32[threadingmodel]

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

Oueries value: HKLM\hardware\devicemap\video[maxobjectnumber] Queries value: HKLM\hardware\devicemap\video[\device\video3]

Queries value: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-

fd27e3774e32}\0000[pruningmode]

Queries value: HKLM\hardware\devicemap\video[\device\video0]

Queries value: $HKLM \ system \ current control \ video \ \{deb 0 3 9 cc-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 5 e-b 7 0 4-4 f 5 3-b 4 5 e-b 7 0 4-4 f 5 3-b 4 5 e-b 7 0 4-4 f 5 3-b 4 5 e-b 7 0 4-4 f 5 3-b 4 5 e-b 7 0 4-4 f 5 3-b 4 6 e-b 7 0 4-4 f 5 6-b 7 0 4-4 f$

9dd4432fa2e9}\0000[pruningmode]

HKLM\hardware\devicemap\video[\device\video1] Queries value:

Queries value: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-

0d8e74595f78}\0000[pruningmode]

HKLM\hardware\devicemap\video[\device\video2] Queries value:

Queries value: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-

8ed0c8eb59a8}\0000[pruningmode]

HKLM\software\microsoft\directdraw\compatibility\bug![name] Queries value: Queries value: HKLM\software\microsoft\directdraw\compatibility\bug![flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\bug![id]

Queries value: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name] Queries value: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id] HKLM\software\microsoft\directdraw\compatibility\diablo[name] Queries value: Queries value: HKLM\software\microsoft\directdraw\compatibility\diablo[flags]

Oueries value: HKLM\software\microsoft\directdraw\compatibility\diablo[id] HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name] Queries value: Oueries value: HKLM\software\microsoft\directdraw\compatibilitv\mortalkombat3[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id] HKLM\software\microsoft\directdraw\compatibility\msgolf98[name] Oueries value: Queries value: HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\msgolf98[id] Queries value:

HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name] $HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus nhl powerplay [flags]$ Oueries value: Oueries value: HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id] HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name] Oueries value: HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags] Oueries value: Oueries value: HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id] HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name] Queries value: Oueries value: HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags] Queries value: HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id] Oueries value: HKLM\software\microsoft\directdraw\compatibility\savage[name]

HKLM\software\microsoft\directdraw\compatibility\savage[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\savage[id] HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name] Queries value: Queries value: HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]

HKLM\software\microsoft\directdraw\compatibility\silentthunder[name] Queries value: Queries value: HKLM\software\microsoft\directdraw\compatibilitv\silentthunder[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\silentthunder[id] HKLM\software\microsoft\directdraw\compatibility\starcraft100[name] Oueries value: Queries value: HKLM\software\microsoft\directdraw\compatibility\starcraft100[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\starcraft100[id] Queries value: HKLM\software\microsoft\directdraw\compatibility\starcraft115[name] Oueries value: HKLM\software\microsoft\directdraw\compatibility\starcraft115[flags] Queries value: HKLM\software\microsoft\directdraw\compatibility\starcraft115[id] HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[name] Oueries value:

Oueries value: HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[id] Queries value: HKLM\software\microsoft\directdraw\compatibility\terracide[name] $HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus terracide [flags]$ Oueries value: Queries value: HKLM\software\microsoft\directdraw\compatibility\terracide[id] Oueries value: HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]

Oueries value: HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags] Oueries value: HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]

Queries value:

Oueries value:

 $HKLM \verb|\software\m| it ros of t\direct draw \verb|\compatibility\ariff davis quality benchmark[name]|$

```
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[modexonly]
                                    HKLM\software\microsoft\directdraw[emulationonlv]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\directdraw[showframerate]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[enableprintscreen]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[forceagpsupport]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[disableagpsupport]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[disablemmx]
                                    HKLM\software\microsoft\directdraw[disableddscapsinddsd]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[forcerefreshrate]
  Queries value:
                                    HKLM\software\microsoft\direct3d[flipnovsync]
  Queries value:
                                    HKLM\software\microsoft\directdraw[owndc]
                                    HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
  Queries value:
                                    HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
                                    HKCR\clsid{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
  Queries value:
  Queries value:
                                    HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[threadingmodel]
                                    HKCR\dximagetransform.microsoft.shadow\clsid[]
  Queries value:
  Queries value:
                                    HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
                                    HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
  Oueries value:
                                    HKCR\clsid\{e71b4063-3e59-11d2-952a-
  Queries value:
00c04fa34f05}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{e71b4063-3e59-11d2-952a-
  Queries value:
00c04fa34f05}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[]
  Oueries value:
                                    HKCR\clsid\{4cb26c03-ff93-11d0-817e-
  Queries value:
0000f87557db}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{4cb26c03-ff93-11d0-817e-
  Queries value:
0000f87557db}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]
  Queries value:
                                    HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]
  Oueries value:
                                    HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Queries value:
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\tinprocserver32[]
                                    HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Oueries value:
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
                                    HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
  Oueries value:
                                    HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Queries value:
00aa003f8646}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[threadingmodel]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1254]
                                    HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Queries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1257]
                                    HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[874]
  Oueries value:
                                    HKLM \setminus system \setminus current control \setminus nls \setminus codepage \cite{Managements} 
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[1361]
                                    HKCU\software\microsoft\internet
  Oueries value:
explorer\international\scripts\26[iefontsize]
  Queries value:
                                    HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsizeprivate]
  Oueries value:
                                    HKCU\software\microsoft\internet
explorer\international\scripts\26[iepropfontname]
  Oueries value:
                                    HKCU\software\microsoft\internet
explorer\international\scripts\26[iefixedfontname]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane1]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane2]
```

```
Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane3]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane4]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane5]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane6]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane7]
  Oueries value:
                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback\simsun[plane8]|
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane9]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane10]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane11]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane12]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane13]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane14]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane15]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane16]
                                    HKCU\software\microsoft\windows script\settings[jitdebug]
  Oueries value:
  Queries value:
                                    HKCR\mime\database\content type\image/png[extension]
  Queries value:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
  Oueries value:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-
  Queries value:
00aa006c1a01}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-
  Queries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{6a01fda0-30df-11d0-b724-
  Oueries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                                    HKCR\mime\database\content type\image/bmp\bits[0]
  Oueries value:
  Queries value:
                                    HKCR\mime\database\content type\image/gif\bits[0]
                                    HKCR \verb|\mime| database \verb|\content| type \verb|\image/jpeg| bits[0]|
  Oueries value:
  Queries value:
                                    HKCR\mime\database\content type\image/pjpeg\bits[0]
                                    HKCR\mime\database\content type\image/png\bits[0]
  Oueries value:
                                    HKCR\mbox{\tt Mime\database\content\ type\image/x-png\bits[0]}
  Oueries value:
                                    HKCR\mime\database\content type\image/x-wmf\bits[0]
  Oueries value:
                                    HKCR\mime\database\content type\image/x-png[image filter clsid]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid[]
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
  Queries value:
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
  Oueries value:
00a0c913f750}\inprocserver32[inprocserver32]
                                    HKCR \c1sid \a3ccedf7-2de2-11d0-86f4-00a0c913f750 \hdots a3ccedf7-2de2-11d0-86f4-00a0c913f750 \hdots a3ccedf
  Queries value:
                                    HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
  Oueries value:
00a0c913f750}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\direct3d[disablemmx]
  Queries value:
  Queries value:
                                    HKLM\software\microsoft\direct3d[disablex3d]
  Oueries value:
                                    HKLM\software\microsoft\direct3d[fewvertices]
                                    HKLM\software\microsoft\direct3d[disablevidmemvbs]
  Queries value:
                                    HKCR\mime\database\content type\image/gif[extension]
  Queries value:
                                    HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_block_lmz_script[1af5338669efabe0a9841478396871b1.exe]
  Queries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[*]
  Queries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[1af5338669efabe0a9841478396871b1.exe]
  Queries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\new
windows[accuserinitonclick]
  Queries value:
                                    HKCR\shockwaveflash.shockwaveflash\clsid[]
                                    HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid[]
  Oueries value:
                                    HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
  Queries value:
                                    HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
  Oueries value:
444553540000}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32[threadingmodel1
  Queries value:
                                    HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
```

```
bc58-54c27d745f8f]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
958a-dad20c90073c]
                                   HKLM\hardware\description\system\centralprocessor\0[~mhz]
  Queries value:
  Oueries value:
                                   HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
  Queries value:
                                   HKLM\software\microsoft\internet explorer\default behaviors[userdata]
  Oueries value:
                                   HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
  Oueries value:
  Oueries value:
                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
  Oueries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[2000]
                                   HKLM\software\microsoft\internet explorer\feed discovery[sound]
  Queries value:
  Queries value:
                                   HKCU\software\microsoft\ftp[use web based ftp]
  Queries value:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection[1af5338669efabe0a9841478396871b1.exe]
  Queries value:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection[*]
  Oueries value:
                                   HKLM\software\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[compatibility flags]
                                   HKLM\software\microsoft\internet explorer\activex
  Queries value:
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[miscstatus flags]
                                   HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_addon_management[1af5338669efabe0a9841478396871b1.exe]
                                   HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_addon_management[*]
  Queries value:
                                   HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1[]
  Queries value:
                                   HKLM\software\microsoft\windows\tablet pc[istabletpc]
  Queries value:
                                   \label{lem:hkcrmime} \begin{tabular}{ll} HKCR\mbox{\content type} \application/x-shockwave-flash[extension] \end{tabular}
  Queries value:
                                   HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid[]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Oueries value:
  Queries value:
                                   HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[]
  Queries value:
                                   HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[inprocserver32]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Oueries value:
                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 9]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midill
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Oueries value:
                                   HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32[]
  Oueries value:
  Oueries value:
                                   HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi41]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
                                   HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash drivers 32 [midi6]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
  Queries value:
\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
  Queries value:
settings\zones\3[1606]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\userdata[cacherepair]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\userdata[cachepath]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheprefix]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachelimit]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\userdata[cacheoptions]
  Queries value:
                                   {\tt HKLM \ } software \verb|\ microsoft \ | cryptography \verb|\ defaults \ | provider types \verb|\ types \ | types 
001[name]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
  Oueries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
```

```
Oueries value:
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
  Queries value:
                                    HKLM\svstem\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Oueries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount]
  Oueries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\domstorage\total[]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
  Queries value:
                                    HKCU\software\macromedia\flashplayer[flashplayerversion]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Queries value:
                                    HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
  Queries value:
                                    HKCR\shockwaveflash.shockwaveflash.7\clsid[]
                                    HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}[]
  Queries value:
                                    HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
  Queries value:
                                    HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
                                    HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\rpc[udtalignmentpolicy]
  Queries value:
                                    HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32[]
                                    HKCR\clsid\{00020420-0000-0000-c000-00000000046}[]
  Queries value:
                                    HKCR\clsid\{00020420-0000-0000-c000-
  Queries value:
00000000046}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{00020420-0000-0000-c000-
  Queries value:
00000000046}\inprocserver32[threadingmodel]
                                    HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
  Queries value:
                                    HKCR\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
                                    HKCR\clsid\{a4a1a128-768f-41e0-bf75-
  Oueries value:
e4fddd701cba}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid[]
  Oueries value:
                                    HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}[]
  Queries value:
                                    HKCR\interface\{00020404-0000-0000-c000-00000000046}\proxystubclsid32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[inprocserver32]
                                    HKCR \verb|\clsid| \{f5078f35-c551-11d3-89b9-0000f81fe221\} \verb|\inprocserver32[]|
  Queries value:
                                    HKCR\clsid\{f5078f35-c551-11d3-89b9-
  Oueries value:
0000f81fe221}\inprocserver32[threadingmodel1
                                    HKCR\clsid\{00020421-0000-0000-c000-00000000046}[]
  Queries value:
                                    HKCR\clsid\{00020421-0000-0000-c000-
  Queries value:
00000000046}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{00020421-0000-0000-c000-
  Oueries value:
00000000046}\inprocserver32[threadingmodel]
                                    \label{local-bound} \begin{tabular}{ll} HKCR \arraycolor=0.000389b71 \arrayc
  Oueries value:
  Queries value:
                                    HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32[]
  Queries value:
                                    HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[]
  Oueries value:
                                    HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
  Oueries value:
  Oueries value:
                                    HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
                                    HKCU\software\microsoft\internet
  Queries value:
explorer\services[selectionactivitybuttondisable]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\suggested sites[enabled]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[attributes]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[restrictedattributes]
  Oueries value:
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
  Oueries value:
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
```

08002b30309d}\shellfolder[wantsforparsing]

```
HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
  Oueries value:
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
  Queries value:
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
  Queries value:
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
  Queries value:
11e3-b3bc-806e6f6e6963}[data]
  Oueries value:
11e3-b3bc-806e6f6e6963}[generation]
                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Queries value:
409d6c4515e9}[drivemask]
  Queries value:
                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
  Oueries value:
                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
  Oueries value:
  Oueries value:
                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
                                    HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
  Oueries value:
                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidden \cite{tabular} \end{tabular}
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Queries value:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ adva
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
  Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show type overlay]
11e3-b3bc-806e6f6e6963}[data]
11e3-b3bc-806e6f6e6963}[generation]
  Queries value:
                                    HKCR\directory[docobject]
  Oueries value:
                                    HKCR\folder[docobiect]
  Queries value:
                                    HKCR\allfilesystemobjects[docobject]
  Oueries value:
                                    HKCR\directory[browseinplace]
  Oueries value:
                                    HKCR\folder[browseinplace]
  Oueries value:
                                    HKCR\allfilesystemobjects[browseinplace]
  Queries value:
                                    HKCR\directory[isshortcut]
  Oueries value:
                                    HKCR\folder[isshortcut]
  Queries value:
                                    HKCR\allfilesystemobjects[isshortcut]
```

Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKCR\folder[nevershowext]

Queries value: HKCR\allfilesystemobjects[nevershowext]

Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]

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

444553540000}\inprocserver32[loadwithoutcom]

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

0xffff]

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

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

444553540000}\inprocserver32[inprocserver32]

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

444553540000}\inprocserver32[threadingmodel]

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

settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair]
 Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix] Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit]

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

settings\5.0\cache\extensible cache\mshist012016042220160423[cacheoptions]

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

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

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]

Queries value: HKCU\software\microsoft\internet

explorer\main\windowssearch[enabledscopes]

Oueries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Larrent version \explorer \folder descriptions \explorer \folder descriptions \folder \f$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd\[name]

Oueries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [parent folder]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the constant of the constant of$

Oueries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\ [parsing name]$

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\[localized\name]$

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [security]$

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [stream resource]$

Oueries value:

 $\label{local-equation} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\[streamresourcetype]$

Queries value:

 $HKLM\software\mbox{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localredirectonly] \\$

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\[roamable]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \eqref{1777f761-68ad-4d8a-87bd-30b759fa33dd} [precreate]$

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\[stream]$

Queries value:

 $\label{thm:local-prop} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\[publishexpandedpath]$

Queries value:

```
87bd-30b759fa33dd}[attributes]
  Oueries value:
87bd-30b759fa33dd}[foldertypeid]
  Oueries value:
87bd-30b759fa33dd}[initfolderhandler]
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[favorites]
  Queries value:
                                    HKLM\software\microsoft\windows search[currentversion]
                                    HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\downloadmanager[cacheok]
  Oueries value:
  Queries value:
                                    HKCR\mime\database\content type\image/x-icon[extension]
  Queries value:
                                    HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\progid[]
                                    HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{adc6cb82-424c-11d2-952a-
  Queries value:
00c04fa34f05}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[]
  Queries value:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-
  Queries value:
00c04fd9189d}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-
  Queries value:
00c04fd9189d}\inprocserver32[threadingmodel]
  Sets/Creates value:
HKLM \ software \ microsoft \ tracing \ 1af5338669efabe0a9841478396871b1\_rasapi32[enable file tracing] \ microsoft \ microso
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[enableconsoletracing]
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filetracingmask]
  Sets/Creates value:
HKLM \ software \ microsoft \ tracing \ 1af5338669e fabe 0a9841478396871b1\_rasapi32 [consoletracing mask]
  Sets/Creates value:
HKLM \setminus software \setminus microsoft \setminus tracing \setminus 1af5338669e fabe 0a9841478396871b1\_rasapi32[maxfilesize]
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filedirectory]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[enablefiletracing]
  Sets/Creates value:
HKLM \ software \ microsoft \ tracing \ 1 af 5338669 ef abe 0 a 9841478396871b1\_ras mancs \ [enable consolet racing]
HKLM \setminus software \setminus microsoft \setminus tracing \setminus 1af5338669 efabe0a9841478396871b1\_rasmancs[filetracing mask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\laf5338669efabe0a9841478396871b1_rasmancs[consoletracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[maxfilesize]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[filedirectory]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecisionreason]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecisiontime]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecision]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpadnetworkname]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings\wpad\0a-23-64-39-4c-b7[wpaddecisionreason]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7[wpaddecisiontime]
  Sets/Creates value:
                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\sc internet}} \\
settings\wpad\0a-23-64-39-4c-b7[wpaddecision]
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cachepath]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheprefix]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachelimit]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheoptions]
  Sets/Creates value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacherepair]
  Sets/Creates value:
                                    HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Sets/Creates value:
                                    \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$

Sets/Creates value:

settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacheoptions]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair]

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

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

 $\label{thm:condition} \mbox{Value changes:} \qquad \mbox{HKCU\software\mbox{\sm microsoft\windows\currentversion\sm internet}}$

settings\wpad[wpadlastnetwork]

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

 $settings \verb|\wpad|{f33bffd9-5d26-428d-b279-f049ab6a7a40}| [wpaddecisionreason]|$

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

settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecisiontime]

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

settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecision]

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

 $settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40\}[wpadnetworkname]}$

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

settings\wpad\0a-23-64-39-4c-b7[wpaddecisionreason]

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

settings\wpad\0a-23-64-39-4c-b7[wpaddecisiontime]

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

settings\wpad\0a-23-64-39-4c-b7[wpaddecision]

Value changes: HKLM\software\microsoft\directdraw\mostrecentapplication[name]
Value changes: HKLM\software\microsoft\directdraw\mostrecentapplication[id]
Value changes: HKLM\software\microsoft\direct3d\mostrecentapplication[name]
Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\userdata[cachepath]

Value changes: HKCU\software\microsoft\internet explorer\domstorage\total[]
Value changes: HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]

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

settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]