# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 7, Task ID: 24

Task ID: 24

Risk Level:

Date Processed: 2016-04-08 09:39:51 (UTC)

Processing Time: 61.25 seconds Virtual Environment: IntelliVM

**Execution Arguments:** 

"c:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe"

Sample ID: basic Type: Owner: admin

Label: 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb

Date Added: 2016-04-08 09:39:50 (UTC)

File Type: PE32:win32:gui 955904 bytes File Size:

4c838f1570b3a7ff6f491e6ec1ef6895 MD5:

SHA256: 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb

Description:

### Pattern Matching Results

2 ECMA Script

3 HTTP connection - response code 200 (success)

5 Possible injector

2 HTML file 5 JavaScript: Writes a string of text to a document stream

3 Connects to local host

1 YARA score 1

4 JavaScript: Eval method

3 Long sleep detected

4 Checks whether debugger is present

#### Static Events

YARA rule hit: SWF YARA rule hit: Nonexecutable

## Process/Thread Events

Creates process:

C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe ["C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe" ]

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

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0 Creates mutex:

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

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

\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex Creates mutex:

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

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

\Sessions\1\BaseNamedObjects\WininetStartupMutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex

Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile

Creates mutex: \Sessions\1\BaseNamedObjects\IESQMMUTEX\_0\_208 Creates mutex: \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex

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

\Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x00000A30) Creates mutex: \Sessions\1\BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069} Creates mutex:

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

Creates mutex:

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

\Sessions\1\BaseNamedObjects\InternetExplorerDOMStoreQuota Creates mutex:

Creates mutex:

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

Creates mutex: \Sessions\1\BaseNamedObjects\\_!SHMSFTHISTORY!\_

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!mshistO12016040820160409!

\Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex

\KernelObjects\MaximumCommitCondition Creates event:

Creates event:  $\verb|\Sessions| 1 \\ BaseNamedObjects \\ MSCTF.CtfActivated.Default1 \\$ 

Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX

Creates event: \BaseNamedObjects\BFE\_Notify\_Event\_{23b668c8-ef04-42b1-a05bCreates 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
                        C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Creates:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Creates:
 Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
 Creates:
Creates:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\index[1].php
 Creates:
                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files \verb|\Content.IE5| KQ5TVCON \verb|\bd_logo1[1].png| \\
                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Creates:
Files \verb|\Content.IE5| X3IPB3Z1 \verb|\jquery-1.10.2.min_f2fb5194[1].js|
                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\BX3UL1G0\baidu_jgylogo3[1].gif
                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\KO5TVCON\zbios 62c636fe[1].png
                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\X3IPB3Z1\icons_0e814c16[1].png
                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\X3IPB3Z1\nuomi_510f7472[1].png
                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\BX3UL1G0\all_async_search_d0d1b2ec[1].js
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\BX3UL1G0\every_cookie_aa168cb4[1].js
                        C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\6K541L89\www.baidu[1].xml
 Creates:
Creates:
Creates:
                        \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet|\\
Files\Content.IE5\KQ5TVCON\nu_instant_search_ebeb5baa[1].js
 Creates:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\KO5TVCON\env beb83b45[11.swf
                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\KQ5TVCON\bdsug_async_1cb857eb[1].js
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\WG2VLW5Y\baiduia_b45d552b[1].js
                        C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
 Creates:
                        C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Creates:
Explorer\UserData\index.dat
 Creates:
                        C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\VZW4XVOK
 Creates:
                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\BZUZR9CZ
                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Creates:
Explorer\UserData\LLYISAMK
 Creates:
                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\1AQVVH0E
 Creates:
                       {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
 Creates:
                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Creates:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
 Creates:
                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com
                       C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Creates:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Creates:
Explorer\UserData\VZW4XVOK\userDataBIDUPSID[1].xml
 Creates:
                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\JSocket_9a52fc3e[1].swf
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
 Creates:
 Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409
 Creates:
C:\Users\Admin\Favorites
 Creates:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\BX3UL1G0\his[1]
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\WG2VLW5Y\bdbri_icons_2e35e84b[1].png
 Creates:
                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\X3IPB3Z1\favicon[1].ico
 Creates:
                       {\tt C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico}\\
 Creates:
                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\BX3UL1G0\union[1].gif
                       C:\Windows\Prefetch\62DDFBF757BE511F30B6D330963C1-E2075B81.pf
 Opens:
 Opens:
                        C:\Windows\Svstem32
 Opens:
                       C:\Windows\System32\sechost.dll
 Opens:
```

 $\textbf{C:} \\ \text{windows} \\ \text{temp} \\ \text{62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe.Local} \\ \text{C:} \\ \text{windows} \\ \text{Temp} \\ \text{C:} \\ \text{A} \\ \text{C:} \\$ 

```
Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2 \setminus comctl32.dl1
                         C:\windows\temp\MSIMG32.dll
 Opens:
                         C:\Windows\System32\msimg32.dll
 Opens:
 Opens:
                         C:\windows\temp\VERSION.dll
                         C:\Windows\System32\version.dll
 Opens:
 Opens:
                         C:\Windows\System32\imm32.dll
                         C:\Windows\WindowsShell.Manifest
 Opens
 Opens:
                         C:\program files\qqd1eae\log.dat
 Opens:
                         C:\Windows\System32\ntdll.dll
 Opens:
                         C:\windows\temp\msdialg100_D.dll
                         C:\Windows\system32\msdialg100_D.dll
 Opens:
                         C:\Windows\system\msdialg100_D.dll
 Opens:
 Opens:
                         C:\Windows\msdialg100_D.dll
                         C:\Windows\System32\Wbem\msdialg100_D.dll
 Opens:
 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 PowerShell\\ | v1.0\\ | MFC90ENut.dll
 Opens:
 Opens:
                         C:\windows\temp\Afx100net.dll
 Opens:
                         C:\Windows\system32\Afx100net.dll
 Opens:
                         C:\Windows\system\Afx100net.dll
 Opens:
                         C:\Windows\Afx100net.dll
                         C:\Windows\System32\Wbem\Afx100net.dll
 Opens:
                         C:\Windows\System32\WindowsPowerShell\v1.0\Afx100net.dll
 Opens:
                         C:\program files\qqd1eae\Log.dat
 Opens:
                         C:\Program Files\QQd1eae\slowt64.dll
 Opens:
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 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.dll
 Opens:
                         C:\Windows\Fonts\StaticCache.dat
 Opens:
                         C:\Windows\Fonts\tahoma.ttf
                         C:\Windows\Fonts\meiryo.ttc
 Opens:
                         C:\Windows\Fonts\msgothic.ttc
 Opens:
 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:
                         {\tt C:\Windows\Fonts\gulim.ttc}\\
                         C:\Windows\System32\en-US\user32.dll.mui
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
 Opens:
                         C:\Windows\system32\uxtheme.dll.Config
 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\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                         C:\windows\temp\ntmarta.dll
 Opens:
                         C:\Windows\System32\ntmarta.dll
 Opens:
                         C:\Windows\System32\en-US\urlmon.dll.mui
 Opens:
 Opens:
                         C:\Windows\System32\shell32.dll
 Opens:
                         C:\windows\temp\apphelp.dll
 Opens:
                         C:\Windows\System32\apphelp.dll
 Opens:
                         C:\WINDOWS\Temp\MJPGC.TMP
 Opens:
                         C:\Windows\System32\en-US\ieframe.dll.mui
 Opens:
                         C:\windows\temp\SspiCli.dll
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
                         C:\Windows\System32\wininet.dll
 Opens:
                         C:\windows\temp\profapi.dll
 Opens:
                         C:\Windows\System32\profapi.dll
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         \hbox{\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet\ Files}
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\desktop.ini
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
 Opens:
                         {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat}
 Opens:
\verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\Index.dat| \\
 Opens:
                         C:\windows\temp\dnsapi.DLL
                         C:\Windows\System32\dnsapi.dll
 Opens:
```

```
Opens:
                         C:\windows\temp\iphlpapi.DLL
 Opens:
                         C:\Windows\System32\IPHLPAPI.DLL
                         C:\windows\temp\WINNSI.DLL
 Opens:
                         C:\Windows\System32\winnsi.dll
 Opens:
                         C:\windows\temp\RASAPI32.dll
 Opens:
                         C:\Windows\System32\rasapi32.dll
 Opens:
 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
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
                         C:\windows\temp\sensapi.dll
 Opens:
                         C:\Windows\System32\SensApi.dll
 Opens:
 Opens:
                         C:\Windows\System32\nlaapi.dll
                         C:\windows\temp\rasadhlp.dll
 Opens:
 Opens:
                         C:\Windows\System32\rasadhlp.dll
 Opens:
                         C:\Windows\System32\NapiNSP.dll
 Opens:
                         C:\Windows\System32\pnrpnsp.dll
 Opens:
                         C:\Windows\System32\mswsock.dll
 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
                         C:\windows\temp\dhcpcsvc.DLL
 Opens:
                         C:\Windows\System32\dhcpcsvc.dll
 Opens:
                         C:\Windows\System32\drivers\etc\hosts
 Opens:
                         C:\Windows\System32\FWPUCLNT.DLL
 Opens:
                         C:\Windows\System32\netprofm.dll
 Opens:
                         C:\windows\temp\MLANG.dll
 Opens:
 Opens:
                         C:\Windows\System32\mlang.dll
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\windows\temp\RpcRtRemote.dll
                         C:\Windows\System32\RpcRtRemote.dll
 Opens:
 Opens:
                         C:\Windows\System32\npmproxy.dll
                         C:\Program Files\Common Files\microsoft shared\ink\tiptsf.dll
 Opens:
 Opens:
Opens:
Opens:
                         C:\Windows\System32\C_20127.NLS
 Opens:
                         C:\Windows\System32\mshtml.dll
 Opens:
                         C:\Windows\System32\msls31.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Content.IE5\BX3UL1G0\index[1].php|
                         {\tt C:\Windows\System32\msimtf.dll}
 Opens:
                         C:\Windows\System32\jscript.dll
 Opens:
                         C:\Windows\System32\iepeers.dll
 Opens:
 Opens:
                         C:\Windows\System32\winspool.drv
 Opens:
                         C:\Windows\System32\dxtrans.dll
 Opens:
                         C:\Windows\System32\atl.dll
 Opens:
                         C:\Windows\System32\ddrawex.dll
 Opens:
                         C:\Windows\System32\ddraw.dll
 Opens:
                         C:\Windows\System32\dciman32.dll
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Windows\win.ini
                         C:\Windows\System32\en-US\ddraw.dll.mui
 Opens:
 Opens:
                         C:\Windows\System32\dxtmsft.dll
 Opens:
                         C:\windows\temp\ImgUtil.dll
 Opens:
                         C:\Windows\System32\imgutil.dll
 Opens:
                         C:\windows\temp\SXS.DLL
 Opens:
                         C:\Windows\System32\sxs.dll
 Opens:
                         C:\Windows\Fonts\arial.ttf
                         C:\Windows\System32\pngfilt.dll
 Opens:
 Opens:
                         C:\Windows\System32\en-US\mlang.dll.mui
 Opens:
                         C:\Windows\System32\C_1250.NLS
                         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
 Opens:
                        C:\Windows\System32\C_1256.NLS
C:\Windows\System32\C_1257.NLS
 Opens:
 Opens:
 Opens:
                         C:\Windows\System32\C_1258.NLS
 Opens:
                         C:\Windows\System32\C_874.NLS
 Opens:
                         C:\Windows\System32\C_932.NLS
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\X3IPB3Z1\jquery-1.10.2.min_f2fb5194[1].js
 Opens:
                         C:\Windows\System32\C_936.NLS
                         C:\Windows\System32\C_949.NLS
 Opens:
                         C:\Windows\System32\C_950.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_1361.NLS
 Opens:
                         C:\Windows\Fonts\arialbd.ttf
 Opens:
                         C:\Windows\Fonts\ariali.ttf
 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
```

C:\Windows\winsxs\x86\_microsoft.windows.gdiplus\_6595b64144ccf1df\_1.1.7601.17514\_none\_72d18a4386696c80 Opens:

```
C:\windows\temp\D3DIM700.DLL
   Opens:
   Opens:
                                                 C: \verb|\windows\System32\d3dim700.dl1| \\
   Opens:
                                                 C:\Windows\System32\en-US\mshtml.dll.mui
   Opens:
                                                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\all asvnc search d0d1b2ec[1].is
                                                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5\BX3UL1GO\every_cookie_aa168cb4[1].js
                                                 C:\Windows\System32\Macromed\Flash\Flash10h.ocx
   Opens:
                                                 C:\Windows\system32\Macromed\Flash\WINMM.dll
   Opens
   Opens:
                                                 C:\Windows\System32\winmm.dll
   Opens:
                                                 C:\Windows\system32\Macromed\Flash\DSOUND.dll
                                                 C:\Windows\System32\dsound.dll
   Opens:
   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
                                                 C:\Windows\system32\Macromed\Flash\USERENV.dll
   Opens:
                                                 C:\Windows\System32\userenv.dll
   Opens:
   Opens:
                                                 C:\
   Opens:
                                                 C:\Windows\system32\Macromed\Flash\ss.sgn
   Opens:
                                                 C:\Windows\System32\Macromed\Flash
   Opens:
                                                 C:\Windows\system32\Macromed\Flash\ss.cfg
   Opens:
                                                 {\tt 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
                                                 C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
   Opens:
                                                 C:\Users\Admin\AppData\Local\Microsoft\Internet
   Opens:
Explorer\DOMStore\index.dat
   Opens:
                                                 C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\6K541L89\www.baidu[11.xml
                                                 C:\windows\temp\XmlLite.dll
   Opens:
                                                 C:\Windows\System32\xmllite.dll
   Opens:
   Opens:
                                                 C:\Windows\System32\mshtml.tlb
   Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
   Opens:
Opens:
                                                 C:\Windows\System32\urlmon.dll
   Opens:
                                                 C:\Windows
                                                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5\KQ5TVCON\nu_instant_search_ebeb5baa[1].js
                                                 {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\KQ5TVCON\bdsug_async_1cb857eb[1].js
                                                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5\WG2VLW5Y\baiduia_b45d552b[1].js
                                                 C:\windows\temp\Secur32.dll
   Opens:
                                                 C:\Windows\System32\secur32.dll
   Opens:
   Opens:
                                                 C:\windows\temp\credssp.dll
   Opens:
                                                 C:\Windows\Svstem32\credssp.dll
                                                 C:\Windows\Svstem32\schannel.dll
   Opens:
   Opens:
                                                 C:\Program Files\Internet Explorer\ieproxv.dll
                                                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
   Opens:
                                                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
   Opens:
                                                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
   Opens:
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:\Windows\System32\msxml3.dll
   Opens:
                                                 C:\Windows\System32\msxml3r.dll
   Opens:
   Opens:
                                                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\env_beb83b45[1].swf
                                                 C:\windows\temp\MMDevAPI.DLL
   Opens:
   Opens:
                                                 C:\Windows\System32\MMDevAPI.dll
   Opens:
                                                 {\tt C:\windows\temp\PROPSYS.dll}
   Opens:
                                                 C:\Windows\System32\propsys.dll
                                                 C:\Windows\System32\en-US\msxml3r.dll.mui
   Opens:
                                                 {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Internet\ Explorer\UserData\AppData\Roaming\Microsoft\Ninternet\ Explorer\UserData\AppData\Roaming\Microsoft\Ninternet\ Explorer\UserData\AppData\Roaming\Microsoft\Ninternet\ Explorer\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninternet\Roaming\Ninter
   Opens:
   Opens:
                                                 C: \verb|VarsAdminAppDataRoamingMicrosoftInternet Explorer \verb|VarsBata| | C: 
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Opens
Explorer\UserData\index.dat
   Opens:
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\VZW4XVOK
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Opens:
Explorer\UserData\BZUZR9CZ
   Opens:
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\LLYISAMK
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Opens:
Explorer\UserData\1AQVVH0E
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Opens:
Explorer\UserData\*.*1AQVVH0E\desktop.ini
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\BZUZR9CZ\desktop.ini
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Opens:
Explorer\UserData\LLYISAMK\desktop.ini
   Opens:
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\VZW4XVOK\desktop.ini
                                                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
   Opens:
{\tt Player\+Shared0bjects\+HA2GV3VL\+s1.bdstatic.com\+shared0bjectBIDUPSID.sol}
```

```
Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\
 Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
 Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\s1.bdstatic.com\
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Opens:
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
                         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
 Opens:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
 Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer
 Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
 Opens:
                         {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com
 Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL
                         {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
 Opens:
{\tt Player\+Shared0bjects\+HA2GV3VL\s1.bdstatic.com\+shared0bjectBIDUPSID.sxx}
                         C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Opens:
Explorer\UserData\VZW4XVOK\userDataBIDUPSID[1].xml
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\X3IPB3Z1\JSocket_9a52fc3e[1].swf
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
 Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000006.db
 Opens:
                         C:\Users\desktop.ini
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin\AppData
                         C:\Users\Admin\AppData\Local\Microsoft
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\
{\tt C:\Wisers\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409}
 Opens:
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
                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
 Opens:
                         {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Opens:
Files\Content.IE5\X3IPB3Z1\favicon[1].ico
                         {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Opens:
Files\Content.IE5\BX3UL1G0\union[1].gif
 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
 Writes to:
                         \label{lem:c:standard} $$C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet $$
Files \verb|\| Content.IE5 \verb|\| BX3UL1G0 \verb|\| index[1].php
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bd_logo1[1].png
                         {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Writes to:
Files \verb|\| Content.IE5 \verb|\| X3IPB3Z1 \verb|\| jquery-1.10.2.min_f2fb5194[1].js \\
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\BX3UL1G0\baidu_jgylogo3[1].gif
 Writes to:
                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet|\\
Files\Content.IE5\KQ5TVCON\zbios_62c636fe[1].png
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Writes to:
Files\Content.IE5\X3IPB3Z1\icons_0e814c16[1].png
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Writes to:
Files\Content.IE5\X3IPB3Z1\nuomi_510f7472[1].png
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
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[1].txt
 Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\nu_instant_search_ebeb5baa[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\KQ5TVCON\bdsug_async_1cb857eb[1].js
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\baiduia_b45d552b[1].js
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\env_beb83b45[1].swf
```

```
Writes to:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\index.dat
  Writes to:
                                     {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
Writes to:
                                     C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                                     C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Writes to:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Writes to:
Explorer\UserData\VZW4XVOK\userDataBIDUPSID[1].xml
  Writes to:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\JSocket_9a52fc3e[1].swf
  Writes to:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\his[1]
  Writes to:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\bdbri_icons_2e35e84b[1].png
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\favicon[1].ico
                                     C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Writes to:
  Reads from
                                     C:\Windows\Fonts\StaticCache.dat
  Reads from:
C: \verb|\windows| Temp| 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe | C: \verb|\windows| Temp| 62ddfbf757be511f30b6d330963c134b0c7afbb.exe | C: \verb|\windows| Temp| 62ddfbf757be75b0c7afbb.exe | C: \verb|\windows| Temp| 62ddfbf757b0c7afbb.exe | C: \verb|\windows| Temp| 62ddfbf757b0c7afbb.e
  Reads from:
                                     C:\Windows\System32\drivers\etc\hosts
  Reads from:
                                     C:\Windows\win.ini
  Reads from:
                                     C:\Windows\System32\dxtmsft.dll
  Reads from:
                                     C:\Windows\System32\dxtrans.dll
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Reads from:
Files\Content.IE5\X3IPB3Z1\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:
  Reads from:
                                     C:\Windows\System32\Macromed\Flash\Flash10h.ocx
  Reads from:
                                     C:\Windows\System32\stdole2.tlb
  Reads from:
                                     C:\Windows\System32\iepeers.dll
  Reads from
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\all_async_search_d0d1b2ec[1].js
                                     C:\Windows\System32\mshtml.tlb
                                     {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Reads from:
Files\Content.IE5\KQ5TVCON\nu_instant_search_ebeb5baa[1].js
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bdsug_async_1cb857eb[1].js
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\baiduia_b45d552b[1].js
  Reads from:
                                     C:\Windows\System32\ieframe.dll
  Reads from:
                                     C: \verb|\Users\Admin\AppData\Roaming\Macromedia\Flash|
{\tt Player\macromedia.com\support\flashplayer\sys\settings.sol}
  Reads from:
                                     {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\KQ5TVCON\env_beb83b45[1].swf
                                     {\tt 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\X3IPB3Z1\JSocket_9a52fc3e[1].swf
                                     C:\Users\desktop.ini
  Reads from:
  Reads from:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Reads from:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\favicon[1].ico
  Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
                                     C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Deletes:
Deletes:
                                     {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
Player\macromedia.com\support\flashplayer\sys\settings.sol
  Deletes:
                                     {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
{\tt Player\macromedia.com\support\flashplayer\sys\settings.sxx}
                                     {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
```

#### **Network Events**

DNS query:	wpad
DNS query:	www.baidu.com
DNS query:	s1.bdstatic.com
DNS query:	sclick.baidu.com
DNS response:	www.a.shifen.com ⇒ 14.215.177.37
DNS response:	www.a.shifen.com ⇒ 14.215.177.38
DNS response:	wwwbaidu.jomodns.com ⇒ 119.146.74.40
DNS response:	s.a.shifen.com ⇒ 14.215.177.42
Connects to:	224.0.0.252:5355
Connects to:	8.8.8.8:53
Connects to:	14.215.177.37:80
Connects to:	127.0.0.1:58396
Connects to:	119.146.74.40:80
Connects to:	14.215.177.42:80
Sends data to:	224.0.0.252:5355
Sends data to:	8.8.8.8:53
Sends data to:	127.0.0.1:58396
Sends data to:	www.a.shifen.com:80 (14.215.177.37)
Sends data to:	wwwbaidu.jomodns.com:80 (119.146.74.40)

Sends data to: s.a.shifen.com:80 (14.215.177.42)

Receives data from: 8.8.8.8:53 Receives data from: 127.0.0.1:58396

www.a.shifen.com:80 (14.215.177.37) Receives data from: Receives data from: wwwbaidu.jomodns.com:80 (119.146.74.40) Receives data from: s.a.shifen.com:80 (14.215.177.42)

## Windows Registry Events

HKLM\software\microsoft\internet Creates key: explorer\main\featurecontrol\feature\_scripturl\_mitigation Creates key: HKCU\software\explore Creates key: HKCU\software\microsoft\windows\currentversion\internet settings Creates key: HKLM\software\microsoft\tracing Creates key: HKLM\software\microsoft\tracing\rasapi32 Creates key: HKLM\software\microsoft\tracing\rasmancs Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\connections Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location awareness Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters HKCU\software\microsoft\windows\currentversion\explorer\runmru Creates key: Creates kev: HKCU\software\microsoft\internet explorer\typedurls HKCU\software\microsoft\windows\currentversion\explorer\typedpaths Creates kev: Creates kev: HKCU\software\microsoft\windows\currentversion\internet

settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}\d6-48-41-0b-3a-5a Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\d6-48-41-0b-3a-5a

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

settings\p3p\history

Creates key: HKLM\software\microsoft\directdraw\mostrecentapplication HKCU\software\microsoft\windows script\settings Creates key: Creates key: HKLM\software\microsoft\direct3d\mostrecentapplication Creates key: HKCU\software\microsoft\internet explorer\domstorage\total Creates key: HKCU\software\microsoft\internet explorer\domstorage\baidu.com Creates key: 

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

 ${\tt settings \ 1.0 \ cache \ extensible \ cache \ userdata}$ 

HKCU\software\macromedia\flashplayer Creates key:

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

settings\5.0\cache\extensible cache\mshist012016040820160409

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

Creates key: HKLM\software\microsoft\downloadmanager

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

settings\zonemap[proxybypass]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[intranetname]

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

Deletes value:

HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]

Deletes value:

HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]

Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: Opens key:  ${\tt HKLM \ } system \verb|\ current control set \verb|\ control \ } srp \verb|\ gp \verb|\ dll \\$ 

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key HKCU\software\policies\microsoft\windows\safer\codeidentifiers

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 kev:

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

Opens key:

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: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ diagnostics$ 

Opens key: HKLM\software\microsoft\ole

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

Opens key:  $HKLM \setminus system \setminus current control set \setminus services \setminus crypt 32$ 

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

settings

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

Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol HKLM\software\microsoft\windows\windows error reporting\wmr Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\customiocale

```
Opens key:
                                                      HKLM\system\currentcontrolset\control\nls\extendedlocale
   Opens key:
                                                      HKLM\system\currentcontrolset\control\nls\locale
   Opens key:
                                                      Opens key:
                                                      {\tt HKLM \ } system \verb|\ current control \ | \ language \ groups
                                                      HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
   Opens kev:
                                                      HKLM\software\microsoft\windows
   Opens kev:
nt\currentversion\languagepack\datastore_v1.0
                                                      HKLM\software\microsoft\windows
   Opens kev:
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:
                                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
   Opens key:
HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 62 ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
   Opens key:
                                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
                                                      HKCU\software\explore
   Opens kev:
   Opens key:
                                                      HKCU\software\classes\
   Opens key:
                                                      HKLM\software\microsoft\com3
   Opens key:
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
   Opens key:
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
   Opens key:
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
   Opens key:
                                                      \label{locality} $$ HKCR \clsid_{8856f961-340a-11d0-a96b-00c04fd705a2} \le as $$ (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5) + (2.5)
   Opens key
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\progid
                                                      \label{locality} $$HKCR\clsid{8856f961-340a-11d0-a96b-00c04fd705a2} \rightarrow \cline{1.00} $$HKCR\clsid{88566f961-340a-11d0-a96b-00c04fd705a2} \rightarrow \cline{1.00} $$HKCR\clsid{88566660-340a-11d0-a96b-00c04fd705a2} \rightarrow \cline{1.00} $$HKCR\clsid{88566660-340a-11d0-a96b-00c04fd705a2} \rightarrow \cline{1.00} $$HKCR\clsid{8856660-340a-11d0-a96b-00c04fd705
   Opens key:
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens key:
00c04fd705a2}\inprocserver32
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
   Opens key:
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens key:
00c04fd705a2}\inprochandler32
   Opens kev:
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens kev:
00c04fd705a2}\inprochandler
   Opens key:
                                                      Opens key:
                                                      HKLM\software\microsoft\rpc
   Opens key
                                                      HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:
                                                      HKLM\system\setup
                                                      \begin{tabular}{ll} \hline HKLM\software\policies\microsoft\windows nt\pc \end{tabular}
   Opens key:
                                                      HKLM\software\policies\microsoft\sqmclient\windows
   Opens key:
   Opens key:
                                                      HKLM\software\microsoft\sqmclient\windows
   Opens key:
                                                      HKCU\software\classes\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
   Opens key:
                                                      HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
   Opens key:
                                                      HKCU\software\policies\microsoft\windows\app management
   Opens key:
                                                      HKLM\software\policies\microsoft\windows\app management
   Opens key:
                                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{004b0726 - a010 - 4abf - 8556 - fcdb7f1fca1e\}
                                                      HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
   Opens key:
                                                      HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be18 - b
   Opens key:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                      HKLM\software\microsoft\ctf\
   Opens key:
   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
                                                      HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
   Opens key:
                                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
   Opens key:
                                                      HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
   Opens key:
                                                      HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
   Opens key:
                                                      HKCU\software\microsoft\internet explorer\main\featurecontrol
                                                      HKCU\software\microsoft\internet
   Opens key
explorer \verb|\main| featurecontrol| feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562
   Opens key:
                                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
   Opens key:
                                                      HKCU\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature_use_ietldlist\_for\_domain\_determination| \\
   Opens key:
                                                      {\tt HKLM \backslash software \backslash microsoft \backslash internet}
explorer \verb|\main| featurecontrol| feature\_use\_ietldlist\_for\_domain\_determination
   Opens kev:
                                                      HKLM\system\currentcontrolset\control\lsa\accessproviders
   Opens key:
                                                      HKLM\system\currentcontrolset\services\ldap
                                                      HKCU\software\microsoft\internet explorer\ietld
   Opens key:
                                                      HKLM\software\microsoft\internet explorer\main
   Opens key:
   Opens key:
                                                      HKLM\software\policies\microsoft\internet explorer\main
   Opens key:
                                                      HKCU\software\policies\microsoft\internet explorer\main
                                                      HKLM\software\microsoft\windows\currentversion\policies\explorer
   Opens key:
   Opens key:
                                                      HKCU\software\microsoft\windows\currentversion\policies\explorer
   Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current \lor ersion \setminus shell compatibility \setminus applications \setminus 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                                      HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
   Opens key:
08002b30309d}\shellfolder
                                                      HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder
   Opens kev:
                                                      HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
   Opens key:
42a0-1069-a2ea-08002b30309d}\shellfolder
   Opens key:
                                                      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:
                                                      \label{lem:hklm} \verb+Kklm/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:
                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt 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
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
   Opens key:
                                              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
   Opens kev:
08002b30309d}\progid
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
   Opens key:
                                             HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
   Opens key
08002b30309d}\inprochandler32
                                             HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
   Opens key
   Opens key
                                              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler
   Opens key:
                                             Opens key:
a2ea-08002b30309d}
   Opens key:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
                                             HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_iedde_register_protocol
   Opens key:
                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} soft \end{tabular} in the thick that the local hammon is a substitution of the local hammon is a sub
   Opens key:
                                              \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \ internet explorer \browsere mulation
   Opens key:
                                             HKLM\software\microsoft\internet explorer\mediatypeclass
  Opens key:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
                                             HKLM\software\microsoft\windows\currentversion\policies\ratings
   Opens key:
                                             HKCU\software\microsoft\internet
   Opens key
explorer\main\featurecontrol\feature show failed connect content kb942615
                                             HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
   Opens kev:
                                             HKLM\software\policies
                                             HKCU\software\policies
   Opens kev:
   Opens key:
                                             HKCU\software
   Opens key:
                                              HKLM\software
   Opens key:
                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
   Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\domains\
  Opens key:
                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
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\
                                             HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                             HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                             HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\
                                             HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                              HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
   Opens key:
                                              HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\zonemap
   Opens key:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                              HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\protocoldefaults\
  Opens key:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                             HKLM\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\domains\
                                             HKLM\software\policies\microsoft\internet explorer
   Opens key:
   Opens key:
                                              HKLM\software\policies\microsoft\internet explorer\security
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet settings\zones\
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
   Opens key:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
   Opens key:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
   Opens key:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
   Opens key:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
   Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\1
   Opens key:
                                              \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\so
settings\zones\1
   Opens key:
                                              HKLM\software\microsoft\windows\currentversion\internet
```

```
settings\zonemap\
   Opens key:
                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
   Opens key:
                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\3
                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\3
                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\4
   Opens key:
                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                                            HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
    Opens key
                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
   Opens key:
                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                            HKCU\software\microsoft\windows\currentversion\internet
   Opens key
settings\lockdown_zones\
   Opens key:
                                                            HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                            \label{lem:hklm} \verb+Kklm \+ olicies + microsoft + windows + current version + internet
   Opens key
settings\lockdown_zones\0
   Opens key
                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
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
                                                            \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation}} \mbox{\tt local_equation} \mbox{\tt local_
   Opens key:
settings\lockdown_zones\2
   Opens key:
                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
    Opens key:
                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                            \label{lem:hkcu} \begin{tabular}{ll} HKCU \end{tabular} windows \current version \end{tabular} internet
    Opens key:
settings\lockdown_zones\3
                                                            \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
    Opens key
settings\lockdown_zones\3
   Opens key:
                                                            \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\3
   Opens key
                                                            HKCU\software\microsoft\windows\currentversion\internet
{\tt settings \lockdown\_zones \label{lockdown} 4}
   Opens key:
                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
   Opens kev:
                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                                            HKLM\software\microsoft\windows\currentversion\internet
   Opens kev
settings\5.0\cache
                                                            HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache
                                                            HKCU\software\microsoft\windows\currentversion\internet
   Opens key
settings\5.0\cache\content
                                                            \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
   Opens key:
settings\5.0\cache\content
    Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
    Opens key:
ba85-6007caedcf9d}
    Opens key:
ba85-6007caedcf9d}\propertybag
   Opens key:
                                                            HKCU\software\microsoft\windows\currentversion\explorer
    Opens key:
                                                            HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
   Opens kev:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders
   Opens key:
                                                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
    Opens key:
                                                            HKLM\software\policies\microsoft\windows\explorer
                                                            HKCU\software\policies\microsoft\windows\explorer
    Opens key:
    Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}
   Opens key:
HKLM \label{lem:hklm} Which is the latest and the
9d55-7b8e7f157091}\propertybag
    Opens kev:
9afe-ea3317b67173}
    Opens key:
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ 'explorer' \ 'folder descriptions \ 'to be a finite of the content of the 
9afe-ea3317b67173}\propertybag
    Opens key:
                                                            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
    Opens key:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in cosoft \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} known folders ettings
    Opens key:
                                                            HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache\cookies
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
 Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
 Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}\propertybag
 Opens key
a03a-e3ef65729f3d}
 Opens key:
a03a-e3ef65729f3d}\propertybag
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
 Opens kev:
                        HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
 Opens key:
a781-5a1130a75963}
 Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}\propertybag
 Opens key
                        \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache
 Opens key
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key
settings\5.0\cache\extensible cache\feedplat
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\iecompat
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\ietld
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\privacie:
 Opens key:
                        HKCU\software\microsoft\internet
\verb|explorer| \verb|main| feature control| \verb|retry_header only post_on connection reset| \\
 Opens key:
                        HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\retry_header on ly post\_on connection reset| \\
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                        HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954
 Opens key:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                        HKCU\software\microsoft\internet
 Opens kev:
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
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                        HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature_disable_notify_unverified\_spn_kb2385266
                         HKLM\software\microsoft\internet
 Opens key
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
                        HKLM\software\microsoft\internet
 Opens key:
\verb|explorer| main feature control feature compat_use connection_based_negotiate_auth_kb2151543| \\
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens kev:
                        HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_allow_long_international_file names| \\
 Opens key
                        HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature_permit_cache\_for\_authenticated\_ftp\_kb910274
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature permit cache for authenticated ftp kb910274
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens kev:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature exclude invalid client cert kb929477
 Opens key:
                        HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                                    HKCU\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_use\_utf8\_for\_basic\_auth\_kb967545
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens kev:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on unload kb975619
  Opens kev:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature release keys on unload kb975619
                                    HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                                    HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
  Opens key:
                                    HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\381e2851
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
  Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004
  Opens key:
Opens kev:
HKLM \label{lem:hklm} Which is the minimum of the
  Opens key:
Opens kev:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000010
  Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014
  Opens key:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000015
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000016
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000017
  Opens key:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameter \ sprotocol\_catalog 9 \ catalog\_entries \ 0000000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\0000000c
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
  Opens key:
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
  Opens key:
                                    HKLM\software\microsoft\tracing\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\rasmancs
  Opens key:
                                     HKCU\software\classes\autoproxytypes
  Opens key:
                                     HKCR\autoproxytypes
  Opens key:
                                     HKCU\software\classes\autoproxytypes\application/x-internet-signup
  Opens key:
                                     HKCR\autoproxytypes\application/x-internet-signup
  Opens key:
                                     \label{lem:hkcu} \verb+KKCU \software \classes \autoproxy types \application / x-ns-proxy-autoconfiged and the lemma of the
```

```
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 kev:
    Opens kev:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
    Opens kev:
                                                       HKLM\software\policies\microsoft\system\dnsclient
    Opens key:
                                                       HKLM\system\currentcontrolset\services\winsock\parameters
    Opens key:
                                                       HKLM\svstem\currentcontrolset\services\tcpip6\parameters\winsock
    Opens key:
                                                       HKLM\system\currentcontrolset\services\psched\parameters\winsock
    Opens key:
                                                       HKLM\system\currentcontrolset\services\winsock\setup migration\providers
                                                       HKLM\system\currentcontrolset\services\winsock\setup
    Opens key:
migration\providers\psched
    Opens key:
                                                       \label{lem:hklm} \verb+Kklm \system \current control set \services \slice 
    Opens key:
                                                       HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
    Opens key:
                                                       HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
    Opens key
                                                       Opens key:
c19ce8a73253}
    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
                                                       HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
    Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
    Opens kev:
                                                       HKCU\software\classes\protocols\name-space handler\
    Opens kev:
                                                       HKCR\protocols\name-space handler
    Opens key:
                                                       HKCU\software\classes\protocols\name-space handler\http\
    Opens key:
                                                       HKCR\protocols\name-space handler\http
    Opens key:
                                                       HKCU\software\classes\protocols\name-space handler\*\
    Opens kev:
                                                       HKCR\protocols\name-space handler\*
    Opens key:
HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \
806e6f6e6963}
    Opens key:
806e6f6e6963}
    Opens key:
1709a0196aed}
   Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d343
    Opens kev:
                                                       HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens kev:
                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature enable compat logging
                                                       HKLM\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_enable_compat_logging
   Opens key
                                                       HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
   Opens key
                                                       HKLM\software\microsoft\windows\currentversion\internet settings\user
agent
   Opens key:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
    Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
    Opens key:
                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\user agent
    Opens key:
                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\user agent
   Opens key:
                                                       \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} which is a constant, which is 
agent\ua tokens
    Opens key
                                                       HKLM\software\microsoft\windows\currentversion\internet settings\user
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
                                                       HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_maxconnectionsperserver
    Opens key:
                                                       HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_max connection sper1\_0 server
    Opens key
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
```

```
Opens key:
                                               HKCU\software\microsoft\windows\currentversion\urlmon settings
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
   Opens key:
                                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                               HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
   Opens kev:
                                               HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
   Opens key:
                                               HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
   Opens key:
199fdba5723b}\treatas
                                               HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
   Opens key:
   Opens key
                                               HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\progid
   Opens key:
                                               HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid
   Opens key:
                                               HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
   Opens key:
                                               HKCR\clsid\\\{dcb00c01-570f-4a9b-8d69-199fdba5723b\\\}\inprocserver32
                                               HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
   Opens key:
199fdba5723b}\inprochandler32
                                               HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprochandler32
   Opens key:
   Opens key:
                                               HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69
199fdba5723b}\inprochandler
   Opens key:
                                               HKCR \ clsid \ \{dcb00c01-570f-4a9b-8d69-199fdba5723b\} \ \ in prochandler
   Opens key:
                                               HKLM\software\microsoft\rpc\extensions
   Opens key:
                                               HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
   Opens key:
                                               HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
   Opens key
                                               HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\treatas
                                               HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
   Opens key:
   Opens key:
                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{a47979d2-c419-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d9-a5b4-11d
001185ad2b89}\progid
                                               HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
   Opens key:
                                               HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
   Opens key:
001185ad2b89}\inprocserver32
   Opens kev:
                                               HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32
                                               HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
   Opens key
001185ad2b89}\inprochandler32
   Opens key:
                                               HKCR \ clsid \ \{a47979d2-c419-11d9-a5b4-001185ad2b89\} \ \ in prochandler 32
   Opens key
                                               HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
                                               HKCR \ clsid \ \{a47979d2-c419-11d9-a5b4-001185ad2b89\} \ \ in prochandler
   Opens key:
                                               HKCU\software\microsoft\internet explorer\international
   Opens key
                                               HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disable_legacy_compression
                                               HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disable_legacy_compression
   Opens key:
                                               \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \protocols \name-space handler \end{tabular}
   Opens key
                                               Opens key:
                                               HKLM\software\microsoft\windows\currentversion\explorer\travellog
   Opens key
HKCU \setminus software \setminus classes \setminus appid \setminus 62 ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exee, appid \setminus 62 ddfbf757be511f30b6d330963c134b0c7afbb.exee, appid \setminus 62 ddfbf757be511f30b6d330963c13b0c7afbb.exee, appid \setminus 62 ddfbf757b0c7afbb.exee, appid \setminus 62 ddfbf75b0c7afbb.exee, appid \setminus 6
   Opens key
HKCR\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
   Opens key:
                                               HKLM\software\microsoft\ole\appcompat
   Opens kev:
                                               HKLM\svstem\currentcontrolset\control\lsa
                                               {\tt HKLM \coftware \cosoft \cryptography \defaults \provider \microsoft \ strong}
   Opens key:
cryptographic provider
   Opens key:
                                               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
   Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
   Opens key:
                                               HKLM\software\policies\microsoft\cryptography
                                               HKLM\software\microsoft\cryptography
   Opens key:
   Opens key:
                                               HKLM\software\microsoft\cryptography\offload
   Opens key:
                                               HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
                                               HKCR\interface\{00000134-0000-0000-c000-00000000046}
   Opens key
                                               HKCU\software\classes\interface\{00000134-0000-0000-c000-
   Opens key
00000000046}\proxystubclsid32
   Opens key:
                                               Opens key
                                               HKLM\svstem\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:
199fdba5723b}\proxystubclsid32
                                               HKCR \verb|\| terface \verb|\| d0074ffd-570f-4a9b-8d69-199fdba5723b \verb|\| \| proxystubclsid32
   Opens key:
                                               HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
   Opens key:
                                               HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
   Opens key:
   Opens key:
                                               HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\treatas
                                               HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
   Opens key:
                                               HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
   Opens key
2299f0398e27}\progid
   Opens key:
                                               HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
   Opens key:
                                               HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32
                                               Opens kev:
                                               HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f
   Opens key:
2299f0398e27}\inprochandler32
                                               HKCR \ clsid \ \{1299cf18-c4f5-4b6a-bb0f-2299f0398e27\} \ \ in prochandler 32
   Opens key:
   Opens key:
                                               HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler
```

Opens key:

 $HKCR \verb|\clsid| \{1299cf18-c4f5-4b6a-bb0f-2299f0398e27\} \verb|\inprochandler| \} where the prochamble of the context of the context$ Opens key:  $HKCU \setminus software \setminus classes \setminus interface \setminus \{26656eaa-54eb-4e6f-8f85-4f0ef901a406\}$ Opens key: HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}

Opens key: HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-

4f0ef901a406}\proxystubclsid32

```
Opens key:
                         HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32
 Opens key:
                         HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
 Opens key:
                         HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
 Opens key:
                         HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-
6d613e2ceaec}\proxystubclsid32
                         HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32
 Opens kev:
                         HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
 Opens kev:
                         HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
 Opens kev:
                         HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-
 Opens key:
00aa004bb851}\proxystubclsid32
 Opens key:
                         HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32
                         HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
 Opens key:
 Opens key:
                         HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
 Opens key:
                         HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\treatas
 Opens key:
                         \label{local-bab4-101a-b69c-00aa00341d07} \verb|\treatas| \\
                         HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
 Opens key:
00aa00341d07}\progid
                         HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c
00aa00341d07}\inprocserver32
 Opens key:
                         HKCR \ clsid \ \{b196b286-bab4-101a-b69c-00aa00341d07\} \ \ inprocserver 32
 Opens key:
                         HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler32
 Opens key:
                         HKCR \verb|\clsid|{b196b286-bab4-101a-b69c-00aa00341d07} \verb|\inprochandler32|
 Opens key
                         HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
                         HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
 Opens key:
 Opens key:
HKCU\software\policies\microsoft\windows\currentversion\explorer\autocomplete
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
 Opens key:
{\tt HKLM} \verb|\software\policies\microsoft\windows\currentversion\explorer\autocomplete}
 Opens kev:
                         HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
                         HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
 Opens kev:
 Opens key:
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
 Opens key:
                         HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\treatas
 Opens kev:
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
                         HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
  Opens key
00c04fd7d062}\progid
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid
 Opens key:
 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:
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32
 Opens key
                         HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler
 Opens key:
                         HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
 Opens key:
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
 Opens key:
                         HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
 Opens kev:
9fe3c77a297a}\treatas
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
 Opens key
9fe3c77a297a}\progid
 Opens key:
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid
 Opens key:
                         HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
 Opens key:
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\tinprocserver32
                         HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
  Opens key
9fe3c77a297a}\inprochandler32
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\nprochandler32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9
9fe3c77a297a}\inprochandler
 Opens key:
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\nprochandler
 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
                         Opens key:
                         HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
 Opens key:
                         HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
 Opens key:
                         HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-
 Opens key
63278fcb8037}\proxystubclsid32
                         HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key
settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}
 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
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\treatas
 Opens key:
  Opens key:
                         HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\progid
 Opens key:
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062\}\progid
 Opens key:
                         HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:
                         Opens key
                         HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler32
 Opens key:
```

```
Opens key:
                                   HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler
  Opens key:
                                   HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
  Opens key:
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
                                   HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
  Opens kev:
00c04fd7d062}\treatas
  Opens kev:
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
                                   HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
  Opens key:
00c04fd7d062}\progid
  Opens key:
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
  Opens key:
                                   HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:
                                   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
                                   HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535
  Opens key
00c04fd7d062}\inprochandler
  Opens key:
                                   Opens key
                                   HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
  Opens key:
                                   HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
  Opens key:
Opens key:
                                   HKCU \setminus software \setminus classes \setminus clsid \setminus \{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}\treatas
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas
  Opens key:
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
  Opens key:
b61bb7cdd997}\progid
  Opens kev:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
  Opens key
b61bb7cdd997}\inprocserver32
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\nprocserver32
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
  Opens kev:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprochandler32
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
  Opens key
b61bb7cdd997}\inprochandler
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprochandler
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key
                                   HKLM\system\currentcontrolset\services\netbt\linkage
  Opens key
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\baidu.com
  Opens key:
                                   HKCU\software\classes\mime\database\content type\text/html; charset=utf-
  Opens key:
                                   \label{localization} \mbox{HKCR} $$ HKCR \rightarrow \mbox{Lext/html; charset=utf-8} $$
  Opens key:
                                   HKCU\software\classes\mime\database\content type\text/html
  Opens kev:
                                   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
                                   HKCU\software\classes\protocols\filter\text/html
  Opens kev:
                                   HKCR\protocols\filter\text/html
  Opens kev:
                                   HKCU\software\microsoft\internet
  Opens key:
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
                                   HKCU\software\microsoft\internet
  Opens key
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}
  Opens key:
                                   HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:
                                   HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
                                   HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
  Opens kev:
  Opens key:
                                   HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
                                   HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
  Opens key:
                                   HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key
00aa00686f13}\inprocserver32
                                   HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
  Opens key:
                                   HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key
00aa00686f13}\inprochandler32
  Opens key:
                                   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 kev:
                                   HKCU\software\microsoft\internet
  Opens key:
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
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:
                                   HKLM\software\microsoft\internet
\verb|explorer| main feature external_style_sheet_fix_for_smartnavigation_kb926131| explorer fix_for_smartnavigation_kb926131| explorer fix_for_smartnavigation_fix_for_smartnavigation_kb926131| explorer fix_for_smartnavigation_kb926131| explo
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
```

```
Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
                                    HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature private font setting
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens key:
                                    HKLM\software\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 key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:
                                    HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_body\_size\_in\_editable\_if rame\_kb943245
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_databinding_support
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens kev:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                    HKLM\software\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
\verb|explorer|| \verb|main|| feature control | feature enable om screen origin_display_pixels||
                                    HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature restrict crash recovery save kb978454
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens key:
                                    HKLM\software\microsoft\internet explorer\application compatibility
  Opens key:
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                    HKCU\software\microsoft\internet explorer\domstorage
  Opens key:
                                    HKLM\software\microsoft\internet explorer\domstorage
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKLM\software\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\microsoft\internet
\dot{\text{explorer}}. \\ \dot{\text{main}} \\ \text{featurecontrol}. \\ \text{feature\_manage\_script\_circular\_refs}
                                    HKLM\software\microsoft\internet
  Opens kev:
\verb|explorer\main\featurecontrol\feature\_manage\_script\_circular\_refs| \\
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature restrict filedownload
  Opens kev:
                                    HKLM\software\microsoft\internet
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
  Opens key:
                                    HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:
                                    HKCU\software\classes\protocols\name-space handler\about\
                                    HKCR\protocols\name-space handler\about
  Opens kev:
                                    HKCU\software\classes\protocols\handler\about
  Opens key:
  Opens key:
                                    HKCR\protocols\handler\about
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
  Opens key:
                                    HKCR \verb|\clsid|{3050f406-98b5-11cf-bb82-00aa00bdce0b} \verb|\treatas|
  Opens key:
                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f406-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11c
00aa00bdce0b}\progid
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:
```

```
Opens key:
                                              HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
   Opens key:
                                              HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
   Opens key:
                                              HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
                                              HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
   Opens kev:
                                              HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
   Opens key
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
   Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
                                              HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
   Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                                              HKLM\software\policies\microsoft\internet explorer\zoom
   Opens kev:
   Opens key:
                                              HKCU\software\policies\microsoft\internet explorer\zoom
   Opens key:
                                               HKCU\software\microsoft\internet explorer\zoom
   Opens key:
                                              HKLM\software\microsoft\internet explorer\zoom
   Opens key:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
   Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
   Opens key:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\url history
Opens key:
settings\url history
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet settings\url
history
   Opens key:
                                               HKLM\software\microsoft\windows\currentversion\internet settings\url
history
   Opens key:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
   Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
   Opens kev:
                                               HKCU\software\policies\microsoft\internet explorer
                                               HKLM\software\policies\microsoft\internet explorer\international\scripts
   Opens key:
   Opens key:
                                               \label{thm:hkcu} \mbox{HKCU\software\mbox{$\stackrel{\cdot}{m}$ icrosoft\internet explorer\space{$\stackrel{\cdot}{m}$ international\scripts}}} \\
   Opens key:
                                               HKLM\software\microsoft\internet explorer\international\scripts
   Opens key:
                                               HKLM\software\policies\microsoft\internet explorer\settings
   Opens key:
                                               HKCU\software\microsoft\internet explorer\settings
   Opens key:
                                               HKLM\software\microsoft\internet explorer\settings
   Opens key:
                                               HKCU\software\microsoft\internet explorer\styles
   Opens key:
                                               \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ policies \verb+ active desktop+ active active desktop+ active ac
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\policies
   Opens key:
                                               HKCU\software\microsoft\internet explorer\pagesetup
   Opens key:
                                               HKCU\software\microsoft\internet explorer\menuext
   Opens key:
                                               \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc menuext\sc w}s} \\
                                              HKLM\system\currentcontrolset\control\nls\codepage
   Opens kev:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\international\scripts\3
   Opens kev:
                                              HKLM\software\microsoft\internet explorer\version vector
   Opens kev:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
                                              HKLM\software\microsoft\internet
   Opens key:
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
                                              HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
                                              HKLM\software\microsoft\internet
   Opens key:
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
\verb| explorer\main\featurecontrol\feature\_subdownload\_lockdown| \\
                                              HKI M\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_subdownload_lockdown
   Opens key:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
                                              HKLM\software\microsoft\internet
   Opens kev:
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:
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
   Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
                                               HKLM\software\policies\microsoft\internet explorer\restrictions
   Opens key:
   Opens key:
                                               \label{local-observation} \mbox{HKCU\software\policies\mbox{\sc 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 \setminus software \setminus classes \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d
f4ceaaf59cfc}\progid
```

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}\innrochandler32
                         HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
 Opens kev:
                         HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
 Opens key
f4ceaaf59cfc}\inprochandler
                         HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler
 Opens key:
                          HKCU\software\policies\microsoft\internet explorer\control panel
 Opens key
 Opens key
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
                          HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
 Opens key
 Opens key
                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
                          HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
 Opens key:
00aa00bbbb58}\treatas
                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\progid
 Opens key:
                          HKCR \ clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \ \ progid
 Opens key:
                         HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
 Opens key:
                          HKCR \verb|\clsid| \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \verb|\inprocserver32|
 Opens key
                         HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
                         HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32
 Opens key
                         HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
 Opens key:
00aa00bbbb58}\inprochandler
                         HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler
 Opens key:
                          HKLM\software\microsoft\windows script\features
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\recovery
 Opens kev:
 Opens key
                         HKCU\software\microsoft\internet explorer\recovery
                         HKCU\software\microsoft\internet
 Opens kev:
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
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
 Opens key
                          HKCU\software\microsoft\internet
explorer\main\featur
                        ntrol\feature_behaviors
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
 Opens key:
                          HKLM\software\microsoft\internet explorer\default behaviors
                          HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
 Opens key
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
Opens key:
00aa00bdce0b}\treatas
                          HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
                          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
 Opens kev:
00aa00bdce0b}\progid
                          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
                          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82
00aa00bdce0b}\inprochandler
                          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\ \ in prochandler
 Opens key:
 Opens key
                          HKCU\software\policies\microsoft\internet explorer\persistence
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\persistence
 Opens key:
                          HKCU \setminus software \setminus classes \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - dc030521aabd\}
 Opens key:
                         HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
 Opens key:
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\treatas
 Opens key:
                          HKCR\clsid\{81397204-f51a-4571-8d7h-dc030521aabd}\treatas
                         HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
 Opens key
dc030521aabd}\progid
                          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
                         HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
 Opens key
dc030521aabd}\inprochandler32
 Opens key:
                         HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler32
 Opens key:
                         HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler
 Opens key:
                         HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
 Opens key
                          HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
 Opens key
  Opens key:
                          HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\treatas
 Opens key:
                          HKCR\clsid\d1fe6762-fc48-11d0-883a-3c8b00c10000\treats
 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:
                                                       HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
   Opens key:
                                                       HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler32
   Opens key:
                                                       HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler
                                                       HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler
   Opens kev:
                                                       HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
   Opens key:
   Opens kev:
                                                       HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
   Opens key:
                                                       HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\treatas
   Opens key:
                                                       HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas
   Opens key:
                                                       HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\progid
   Opens key:
                                                       HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
   Opens key:
                                                       HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32
   Opens key:
                                                       HKCR \c1sid \end{4fd} 2a832-86c8-11d0-8fca-00c04fd\\ 9189d \end{4fd} inprocserver 32
                                                       HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
   Opens key
00c04fd9189d}\inprochandler32
   Opens key:
                                                       HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler 32
    Opens key:
                                                       HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
   Opens key:
                                                       HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler
   Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\setup
   Opens key:
                                                       HKLM\software\microsoft\windows\currentversion
   Opens key:
                                                       HKLM\hardware\devicemap\video
   Opens key:
                                                       HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
   Opens key:
HKLM \ system \ current controls et \ enum \ pci \ ven\_80ee \& dev\_beef \& subsys\_00000000 \& rev\_00 \ \& 267a616a \& 0&10 \ enum \
                                                       HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
   Opens key:
9dd4432fa2e9}\0000
   Opens kev:
                                                       HKLM\svstem\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000
                                                       HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
   Opens kev:
8ed0c8eb59a8}\0000
   Opens key:
                                                       HKLM\software\microsoft\directdraw\compatibility
   Opens key:
                                                       HKLM\software\microsoft\directdraw\compatibility\bug!
   Opens kev:
                                                       HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
                                                       HKLM\software\microsoft\directdraw\compatibility\diablo
   Opens key:
   Opens key:
                                                       HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat 3
                                                       HKLM\software\microsoft\directdraw\compatibility\msgolf98
   Opens key:
   Opens key:
                                                       HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
   Opens key:
                                                       HKLM \label{limits} IKLM \label{limits} HKLM \label{limits} IKLM \label{limits} IKLM
   Opens key:
                                                       HKLM\software\microsoft\directdraw\compatibility\rogue squadron
   Opens key:
                                                       HKLM\software\microsoft\directdraw\compatibility\savage
   Opens key:
                                                       {\tt HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus scorched planet}
   Opens key:
                                                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ directdraw\+ compatibility\+ silentthunder
   Opens key:
                                                       HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus starcraft 100
   Opens key:
                                                       HKLM \ software \ microsoft \ direct draw \ compatibility \ starcraft 115
                                                       HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\starcraft demo
   Opens key:
   Opens key:
                                                       HKLM\software\microsoft\directdraw\compatibility\terracide
   Opens kev:
                                                       HKLM\software\microsoft\directdraw\compatibility\thirddimension
   Opens kev:
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
   Opens key:
                                                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ msasn1
   Opens key:
                                                       HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
                                                       HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
    Opens key:
                                                       HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key
f941e9b7e1fe}\treatas
   Opens key:
                                                       HKCR\clsid\arrowantered{HKCR\clsid}\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid}\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\arrowantered{HKCR\clsid\clsid\arrowantered{HKCR\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\cls
   Opens key:
                                                       HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\progid
   Opens key:
                                                       HKCR \ clsid \ \{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\} \ \ progid
   Opens key:
                                                       HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32
                                                       HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\) in procserver 32
   Opens kev:
                                                       Opens key:
f941e9b7e1fe}\inprochandler32
                                                       HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\
   Opens key:
                                                       HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key
f941e9b7e1fe}\inprochandler
                                                       HKCR\clsid\a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\\\inprochandler
   Opens key:
   Opens key:
                                                       HKCU\software\classes\dximagetransform.microsoft.shadow
   Opens key:
                                                       HKCR\dximagetransform.microsoft.shadow
   Opens key:
                                                       HKCU\software\classes\dximagetransform.microsoft.shadow\clsid
   Opens key:
                                                       HKCR\dximagetransform.microsoft.shadow\clsid
                                                       HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
   Opens key:
                                                       HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
   Opens key
                                                       HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
   Opens key:
00c04fa34f05}\treatas
                                                       HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\progid
   Opens key:
                                                       HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\ \ progid
   Opens key
                                                       00c04fa34f05}\inprocserver32
```

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

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

Opens key:

```
00c04fa34f05}\inprochandler32
   Opens key:
                                             HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler32
   Opens key
                                             HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler
                                            HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler
  Opens key:
                                            HKLM\software\microsoft\internet explorer\activex compatibility HKLM\software\microsoft\internet explorer\activex
   Opens kev:
  Opens key
compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}
                                             HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
   Opens key:
                                             HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
   Opens key:
                                             HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
   Opens key
0000f87557db}\treatas
   Opens key:
                                             HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
   Opens key:
                                             HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\progid
   Opens key:
                                             HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid
   Opens key:
                                             HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
                                             HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32
   Opens key:
   Opens key:
                                             HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e
0000f87557db}\inprochandler32
   Opens key:
                                             HKCR \ clsid \ \{4cb26c03-ff93-11d0-817e-0000f87557db\} \ \ in prochandler 32
   Opens key:
                                             HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler
   Opens key:
                                             HKCR \verb|\clsid| \{4cb26c03-ff93-11d0-817e-0000f87557db\} \verb|\inprochandler| \} where $(1) = (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (1) + (
   Opens key:
                                             HKCU\software\classes\mime\database\content type\image/png
   Opens key:
                                             HKCR\mime\database\content type\image/png
   Opens key:
                                             HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
                                             HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
   Opens key:
                                             HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
   Opens key:
f4fc1e6ca1bd}\treatas
  Opens key:
                                             HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas
   Opens kev:
                                             HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\progid
                                             HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid
   Opens kev:
   Opens key:
                                             HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32
   Opens kev:
                                             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}\ \ in prochandler 32
   Opens key:
                                             HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler
                                             HKCR \verb|\clsid|{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd} \verb|\inprochandler| | A constant for the constant of the 
   Opens key:
   Opens key:
                                             HKCU\software\classes\typelib
   Opens key:
                                             HKCR\typelib
   Opens key:
                                             HKCU \setminus software \setminus classes \setminus typelib \setminus \{5e77eb03-937c-11d1-b047-00aa003b6061\}
   Opens key:
                                             HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
   Opens key:
                                             \label{thm:local_hammon_hammon} HKCU \software \classes \typelib \{5e77eb03-937c-11d1-b047-00aa003b6061\} \label{thm:local_hammon} 1.1 \end{tikzpicture}
   Opens key:
                                             HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
                                             Opens key
00aa003b6061}\1.1\409
   Opens key:
                                             HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
                                             HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
  Opens kev:
00aa003b6061}\1.1\9
                                             HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
   Opens key:
                                             HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
   Opens key
00aa003b6061}\1.1\0
   Opens key:
                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
   Opens key:
                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
   Opens key:
00aa006c1a01}\treatas
                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
   Opens key:
                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
   Opens key
00aa006c1a01}\progid
   Opens key:
                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid
   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\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32
                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\inprocserver32
   Opens key:
                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724
   Opens key
00aa006c1a01}\inprochandler32
   Opens key:
                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
   Opens key:
00aa006c1a01}\inprochandler
                                             HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler
   Opens key:
   Opens key:
                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
   Opens key:
                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
   Opens key:
                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724
00aa006c1a01}\treatas
                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
   Opens kev:
                                             HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
   Opens key:
00aa006c1a01}\progid
                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\progid
   Opens key:
   Opens key:
                                             HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
   Opens key:
                                             HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
   Opens key:
                                             Opens key:
                                             HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
   Opens key:
                                             HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\409
                                             HKCR\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 key:
                                                        HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9
   Opens key:
                                                       HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\0
                                                        HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
   Opens kev:
                                                       HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
   Opens kev:
0000f87557db}\1.1\0\win32
                                                       HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
   Opens key:
   Opens key
                                                       HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
   Opens key:
                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
                                                       HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
   Opens key
00aa006c1a01}\inprochandler32
                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler33\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinprochandler32\tinpr
   Opens key:
   Opens key:
                                                        HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724
00aa006c1a01}\inprochandler
                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\tinprochandler
   Opens kev:
                                                        HKCU\software\classes\mime\database\content type
   Opens key
                                                        HKCR\mime\database\content type
   Opens key:
   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\microsoft\internet
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
                                                       HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
   Opens key:
                                                        HKCU\software\classes\mime\database\content type\image/gif\bits
   Opens key:
                                                        {\tt HKCR\mbox{\tt mime}\database\content\ type\limage/gif\bits}
                                                        \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \mime \jpeg \bits \end{tabular}
   Opens key:
   Opens key:
                                                        HKCR\mime\database\content type\image/jpeg\bits
                                                        HKCU\software\classes\mime\database\content type\image/pjpeg\bits
   Opens key:
                                                        HKCR\mime\database\content type\image/pjpeg\bits
   Opens key:
                                                        HKCU\software\classes\mime\database\content type\image/png\bits
   Opens kev:
   Opens kev:
                                                        HKCR\mime\database\content type\image/png\bits
                                                        HKCU\software\classes\mime\database\content type\image/tiff\bits
   Opens kev:
   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
   Opens kev:
                                                        HKCU\software\classes\mime\database\content type\image/x-jg\bits
                                                        HKCR\mime\database\content type\image/x-jg\bits
   Opens key:
   Opens key:
                                                        \label{lem:hkcu} \mbox{HKCU\software\classes\mbox{\sc mime\database\content\ type\image/x-png\bits}} \label{lem:hkcu}
                                                        HKCR\mime\database\content type\image/x-png\bits
   Opens key:
   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
                                                       \label{local-hkcrn} HKCR \mbox{\mbox{$\rm MKCR}$ imme} \mbox{\mbox{$\rm Classes}$ content type} \mbox{\mbox{$\rm MKCU}$ image/$x-png} \\ HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\} \mbox{\mbox{$\rm MKCR}$ imme} \mbox{\mbox{$\rm MKCR$}$ imme} \mbox{\mbox{$\rm MKCR$}$ imme} \mbox{\mbox{$\rm MKCR$}$ i
   Opens key:
   Opens key
   Opens key:
                                                        HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
   Opens key:
                                                        HKCU \setminus software \setminus classes \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-00aa003f8646\}
   Opens key:
                                                        HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
   Opens key
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\treatas
   Opens key:
                                                        HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
   Opens kev:
00aa003f8646}\progid
                                                        HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid
   Opens key:
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
   Opens key
00a0c913f750}\treatas
   Opens key:
                                                        HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
                                                        HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
   Opens key:
00a0c913f750}\progid
   Opens key:
                                                        HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\ \ progid
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
    Opens key:
00aa003f8646}\inprocserver32
                                                        HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
   Opens key:
   Opens key
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
   Opens key:
                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\\\\inprocserver32
   Opens key:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-4864\} + \{275c23e2-3746\} + \{275c23e2-3766\} + \{275c2566\} + \{275c2566\} + \{275c2566\} + \{275c2566\} + \{275c25666\} + \{275c25666\} + \{275c25666\} + 
00aa003f8646}\inprochandler32
   Opens key:
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32
                                                       HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
   Opens key
00aa003f8646}\inprochandler
                                                       HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler
   Opens key:
   Opens key
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\
   Opens key:
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
   Opens key
00a0c913f750}\inprochandler
   Opens key:
                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\
   Opens key:
                                                       HKCU\software\classes\mime\database\content type\application/javascript
   Opens key:
                                                       HKCR\mime\database\content type\application/javascript
   Opens key:
                                                       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
                                                        HKCU\software\microsoft\internet explorer\international\scripts\26
    Opens key:
   Opens key:
                                                       HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_cross\_domain\_redirect\_mitigation
   Opens key:
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
   Opens key:
                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
```

HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_block_lmz_script
    Opens key:
                                                               HKCU\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature_activex_inactivate_mode_removal_revert| \\
   Opens key:
                                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
   Opens kev:
                                                               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\classes\mime\database\content type\image/gif
    Opens key:
                                                                HKCR\mime\database\content type\image/gif
    Opens key:
                                                                HKCU\software\microsoft\internet explorer\new windows
                                                                HKLM\software\microsoft\internet explorer\new windows
    Opens key
    Opens key:
                                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
    Opens key:
                                                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
                                                               HKLM\software\microsoft\windows
    Opens kev:
\verb|nt\currentversion\language| pack\surrogatefallback\simsun|
    Opens key:
                                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
                                                               HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_binary_caller_service_provider
    Opens key:
                                                               HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
                                                               HKCR \verb|\interface| \{618736e0-3c3d-11cf-810c-00aa00389b71\} \verb|\proxystubclsid32| \} to the substitution of 
    Opens key:
    Opens key
                                                                HKCU \setminus software \setminus classes \setminus interface \setminus \{332c4425-26cb-11d0-b483-00c04fd90119\}
    Opens key
                                                                HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
    Opens key:
                                                                HKCU\software\classes\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32
                                                               HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32
    Opens key:
                                                                HKCU\software\classes\clsid\{00020424-0000-0000-c000-00000000046}
    Opens key:
                                                                HKCR\clsid\{00020424-0000-0000-c000-00000000046}
    Opens kev:
    Opens kev:
                                                               HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
                                                                HKCR\clsid\{00020424-0000-0000-c000-00000000046}\treatas
    Opens key:
    Opens key:
                                                                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\progid
    Opens kev:
                                                                HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid
                                                               HKCU\software\classes\clsid\{00020424-0000-0000-c000-
    Opens key
000000000046}\inprocserver32
                                                                HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32
    Opens key:
    Opens key
                                                                HKCU\software\classes\clsid\{00020424-0000-0000-c000
00000000046}\inprochandler32
    Opens key:
                                                               Opens key
                                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{00020424-0000-0000-c000-c000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c000-c000-c0000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c00-c000-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c0
000000000046}\inprochandler
    Opens key:
                                                               HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandler
    Opens key
                                                               HKCU\software\classes\shockwaveflash.shockwaveflash
    Opens key:
                                                                HKCR\shockwaveflash.shockwaveflash
                                                               HKCU\software\classes\shockwayeflash.shockwayeflash\clsid
    Opens kev:
    Opens key:
                                                                HKCR\shockwaveflash.shockwaveflash\clsid
    Opens key:
                                                               HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                                                                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
    Opens kev:
                                                               HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key
444553540000}\treatas
                                                                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\treatas
    Opens key:
                                                                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key:
444553540000}\progid
    Opens key:
                                                                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid
                                                               HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key:
444553540000}\inprocserver32
                                                                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32
    Opens key:
                                                               HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key
444553540000}\inprochandler32
    Opens key:
                                                               Opens key
                                                                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler
    Opens key:
                                                               HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler
    Opens key:
                                                                HKLM \verb|\hardware\description\system\central processor \verb|\lambda| 0
                                                               HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
    Opens key:
    Opens key:
                                                                \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \typelib \d27cdb6b-ae6d-11cf-96b8-444553540000 \label{line-eq:hkcu} \end{tabular} $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$ $$1.0$
    Opens key:
                                                                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
    Opens key:
    Opens key:
                                                                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\409
                                                                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\409
    Opens key:
                                                                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
    Opens key
444553540000}\1.0\9
    Opens key:
                                                                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9
   Opens key:
                                                                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0
    Opens key:
                                                                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0
                                                               HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
    Opens key
444553540000}\1.0\0\win32
    Opens key:
                                                                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32
    Opens key
                                                                HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}
    Opens key:
                                                                HKCR\typelib\{00020430-0000-0000-c000-00000000046}
    Opens key:
                                                                HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\2.0
    Opens key:
                                                                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
    Opens key
                                                                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
                                                                HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
    Opens key:
    Opens key:
                                                                \label{local_hammon_hammon_hammon} \begin{tabular}{ll} HKCU \software \classes \typelib \classes \cl
```

```
00000000046}\2.0\0\win32
   Opens key:
                                             HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
  Opens key
                                            HKCU \setminus software \setminus classes \setminus typelib \setminus \{7e8bc440 - aeff-11d1 - 89c2 - 00c04fb6bfc4\}
  Opens key:
                                             HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
  Opens kev:
                                            HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
                                             HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens kev:
  Opens kev:
                                             HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0
                                             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
  Opens key:
                                            HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32
                                            HKCU\software\microsoft\internet
  Opens key
explorer\main\featurecontrol\feature_domstorage
  Opens key:
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
  Opens key:
                                            HKCU \setminus software \setminus classes \setminus clsid \setminus \{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\}
                                             HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key
                                             HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens key:
00c04fb6bfc4}\treatas
  Opens key:
                                             HKCR \clsid \footnote{1} treat as
  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:
                                            HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c
  Opens key
00c04fb6bfc4}\inprochandler32
                                            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
  Opens key:
                                            HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens key:
00c04fb6bfc4}\inprochandler
  Opens kev:
                                            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
  Opens kev:
                                            HKCU\software\microsoft\internet explorer\feed discovery
                                             HKLM\software\microsoft\internet explorer\feed discovery
  Opens kev:
  Opens key:
                                            HKCU\software\microsoft\ftp
  Opens key:
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection
  Opens kev:
                                            HKLM\software\microsoft\internet
\dot{\texttt{explorer}} \\ \dot{\texttt{main}} \\ \dot{\texttt{feature}} \\ \dot{\texttt{activex}} \\ \dot{\texttt{repurposedetection}}
  Opens key
                                            HKLM\software\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
  Opens key:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
  Opens key
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_alloweddomainlist
  Opens key
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_alloweddomainlist
                                            HKLM\software\microsoft\internet explorer\extension
  Opens key
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 kev:
                                            HKCU\software\microsoft\code store database\distribution units
  Opens kev:
                                            HKLM\software\microsoft\code store database\distribution units
  Opens key:
                                            HKLM\software\microsoft\code store database\distribution
  Opens key
units\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                                            HKCU\software\classes\clsid
  Opens key
  Opens key
                                             HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
  Opens key:
                                            HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
                                            HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\ \ \ installed version
  Opens key:
  Opens key:
                                            HKCU \setminus software \setminus classes \setminus clsid \setminus \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \setminus appid \setminus ap
  Opens key
                                            HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
  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 \verb|\main| feature control \verb|\feature| consult_mime_kill bit_kb905915
                                            HKLM\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_consult\_mime\_killbit\_kb905915
  Opens key:
                                            HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus
                                            HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus
  Opens key:
                                            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 kev:
                                             \label{lem:hkcrmime} \begin{tabular}{ll} HKCR\mbox{$m$ime$\database$\content type$\application/$x-shockwave-flash.} \end{tabular}
                                             HKCU\software\microsoft\internet explorer\domstorage\baidu.com
  Opens key
  Opens key:
                                             HKCU\software\microsoft\internet explorer\domstorage\total
  Opens key:
                                             HKCU\software\classes\shockwaveflash.shockwaveflash.7
  Opens key:
                                             HKCR\shockwaveflash.shockwaveflash.7
  Opens key:
                                             HKCU\software\classes\shockwaveflash.shockwaveflash.7\clsid
  Opens key:
                                             {\tt HKCR \ } shock wave flash. shock wave flash. 7 \\ \verb|\ clsid|
  Opens key:
                                             HKLM\software\microsoft\windows\currentversion\policies\system
  Opens key:
                                             HKCU \setminus software \setminus classes \setminus clsid \setminus \{9ba05972 - f6a8 - 11cf - a442 - 00a0c90a8f39\}
  Opens key:
                                             HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
                                             HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
  Opens key:
```

```
00a0c90a8f39}\treatas
   Opens key:
                                                            HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
   Opens key
                                                           HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\progid
                                                            HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
   Opens key:
                                                           HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
   Opens key
00a0c90a8f39}\inprocserver32
   Opens kev:
                                                           HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
                                                           HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
   Opens key
00a0c90a8f39}\inprochandler32
   Opens key:
                                                           HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32
   Opens key
                                                           HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
   Opens key:
                                                           HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler
                                                            HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
   Opens key:
   Opens key
                                                            HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
   Opens key:
                                                           HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
                                                           HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
   Opens key:
   Opens key:
                                                            HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c
0080c7f4ee85}\forward
   Opens key:
                                                           Opens key:
                                                           HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
   Opens key:
                                                            Opens key:
                                                            HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
                                                            HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
   Opens key:
                                                            \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \typelib \eab 22 ac 0 - 30 c 1 - 11 c f - a 7 e b - 000 0 c 05 ba e 0 b} \end{tabular} $$1.1$ and $$1.1$ and $$1.2$ are the solution of the sol
   Opens key:
                                                            HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
   Opens key:
                                                            HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
   Opens key:
0000c05bae0b}\1.1\0
                                                            HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
   Opens key:
   Opens kev:
                                                           HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
                                                           HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
   Opens kev:
                                                           HKCU\software\classes\interface\{00020400-0000-0000-0000-00000000046}
   Opens key:
                                                           HKCR\interface\{00020400-0000-0000-c000-00000000046}
   Opens key:
   Opens key:
                                                           HKCU\software\classes\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
                                                           Opens key:
   Opens key
                                                            HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
                                                            HKCR\clsid\{00020420-0000-0000-c000-00000000046}
   Opens key
   Opens key:
                                                            HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\treatas
    Opens key:
                                                            Opens key:
                                                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{00020420-0000-0000-c000-c000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c000-c000-c0000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c00-c000-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c0
000000000046}\progid
                                                            HKCR\clsid\{00020420-0000-0000-c000-00000000046}\progid
   Opens key:
```

Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32

Opens key:

HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32

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

00000000046}\inprochandler32

HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler32 Opens kev: HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli Opens kev: HKCU\software\classes\clsid\{00020420-0000-0000-c000-Opens key

00000000046}\inprochandler

Opens key: Opens key: HKLM\system\currentcontrolset\control\securityproviders Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa} Opens key

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

00aa006009fa}\proxystubclsid32 Opens key:

 $HKCR \land face \land \{6d5140c1-7436-11ce-8034-00aa006009fa\} \land proxystubclsid 32$ Opens key  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}$ Opens key:  $HKCR \ clsid \ \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}$ 

HKCR\clsid\{a4a1a128-768f-41e0-hf75-e4fddd701cha}\treatas

Opens key: HKCU\software\classes\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:

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

e4fddd701cba}\inprocserver32

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

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

e4fddd701cba}\inprochandler32

Opens key:  $HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\) in prochandler 32$ 

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

e4fddd701cba}\inprochandler

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

Opens key

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

00000000046}\proxystubclsid32

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

Opens key: HKCR\clsid\{00020421-0000-0000-c000-00000000046} Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{00020421-0000-0000-c000-c000-c000-c000-c0000-c00-c00-c000-c000-c000-c0$ 

000000000046}\treatas

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

```
Opens key:
                                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000-
000000000046}\progid
    Opens key:
                                                       HKCR\clsid\{00020421-0000-0000-c000-00000000046}\progid
    Opens key:
                                                       HKCU\software\classes\clsid\{00020421-0000-0000-c000-
00000000046}\inprocserver32
                                                       HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserver32
    Opens kev:
                                                       HKCU\software\classes\clsid\{00020421-0000-0000-c000-
    Opens kev:
00000000046}\inprochandler32
                                                       HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprochandler32
    Opens key:
    Opens key
                                                       HKCU\software\classes\clsid\{00020421-0000-0000-c000-
00000000046}\inprochandler
    Opens key:
                                                       \label{local-eq:hkcr} $$ HKCR\clsid_{00020421-0000-0000-c000-00000000046}\inprochandler $$ $$ $$
    Opens key:
                                                        HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
                                                        HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
    Opens key:
    Opens key:
                                                        HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\treatas
    Opens key:
                                                        HKCR \ clsid \ \{f5078f35-c551-11d3-89b9-0000f81fe221\} \ treat as
                                                        HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
    Opens key:
0000f81fe221}\progid
    Opens key:
                                                        HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid
    Opens key:
                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32
    Opens key:
                                                       HKCR \ clsid \ \{f5078f35-c551-11d3-89b9-0000f81fe221\} \ \ in procserver 32
    Opens key:
                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler32
    Opens key:
                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32
    Opens key
                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler
                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler
    Opens key:
    Opens key
                                                       HKLM\software\microsoft\msxm130
    Opens key:
                                                        HKCU\software\classes\protocols\filter\application/x-shockwave-flash
                                                       HKCR\protocols\filter\application/x-shockwave-flash
    Opens key:
    Opens kev:
                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32
    Opens kev:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
                                                       HKCU\software\microsoft\windows\currentversion\multimedia\midimap
    Opens key:
                                                        HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
    Opens key:
                                                       HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
    Opens key:
    Opens key:
                                                        HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e
00c04f983e60}\treatas
    Opens key:
                                                        \label{locality} $$ HKCR\clsid{2933bf90-7b36-11d2-b20e-00c04f983e60} \times C_{1}(1) = C_{1}(1) + C_{2}(1) + C_{2
                                                        HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
    Opens key:
00c04f983e60}\progid
                                                        HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
    Opens key:
    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\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprochandler
                                                       HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler
    Opens kev:
                                                       HKCU\software\microsoft\windows\currentversion\internet
    Opens key
settings\5.0\cache\extensible cache\userdata
                                                       HKLM\software\microsoft\cryptography\defaults\provider types\type 001
    Opens key:
                                                       HKLM\software\policies\microsoft\internet explorer\services
    Opens key
    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
                                                       HKCU\software\policies\microsoft\internet
    Opens key
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
                                                       HKLM \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-delta \ explorer \ ex
   Opens key:
3aea-1069-a2d8-08002b30309d}\shellfolder
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
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:
                                                        \label{locality} $$ HKCR\clsid_{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\times C_{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} $$ Treat as 
    Opens key
                                                        HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
```

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

```
b8dc300d9f9d}\inprocserver32
                                             HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
   Opens key:
   Opens key
                                             HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
   Opens key:
                                             HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
                                             HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
   Opens key
b8dc300d9f9d}\inprochandler
   Opens kev:
                                             HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
   Opens key:
HKCU\software\microsoft\windows\currentyersion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-
11e3-b3bc-806e6f6e6963}\
                                             Opens key:
   Opens key:
HKLM \ software \ microsoft \ windows \ shell \ registered applications \ variations \ directory \ open with progids \ directory \ open \ with \ registered \ applications \ directory \ open \ with \ registered \ applications \ directory \ open \ with \ registered \ applications \ directory \ open \ with \ registered \ applications \ directory \ open \ with \ registered \ applications \ directory \ open \ with \ registered \ applications \ directory \ open \ with \ registered \ applications \ directory \ open \ with \ registered \ applications \ open \ with \ registered \ applications \ open \ op
   Opens key:
HKCU\software\microsoft\windows\shell\associations\urlassociations\directory
   Opens key:
                                             HKCU\software\classes\directory
   Opens kev:
                                             HKCR\directorv
   Opens key:
                                             HKCU\software\classes\directory\curver
   Opens key:
                                             HKCR\directory\curver
                                             HKCR\directory\
   Opens key:
   Opens key:
                                             HKCU\software\classes\directory\shellex\iconhandler
   Opens key:
                                             HKCR\directory\shellex\iconhandler
   Opens key:
                                             HKCU\software\classes\folder
   Opens key:
                                             HKCR\folder
                                             HKCU\software\classes\folder\shellex\iconhandler
   Opens key
   Opens key:
                                             HKCR\folder\shellex\iconhandler
   Opens key:
                                             HKCU\software\classes\allfilesystemobjects
   Opens key:
                                             HKCR\allfilesystemobjects
                                             HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
   Opens kev:
   Opens key:
                                             HKCR\allfilesystemobjects\shellex\iconhandler
                                             HKCU\software\classes\directory\docobject
   Opens key:
   Opens kev:
                                             HKCR\directory\docobject
   Opens key:
                                             HKCU\software\classes\folder\docobject
   Opens key:
                                             HKCR\folder\docobject
   Opens key:
                                             HKCU\software\classes\allfilesystemobjects\docobject
                                             HKCR\allfilesystemobjects\docobject
   Opens key:
   Opens key:
                                             HKCU\software\classes\directory\browseinplace
   Opens kev:
                                             HKCR\directory\browseinplace
   Opens key:
                                             HKCU\software\classes\folder\browseinplace
   Opens key:
                                             HKCR\folder\browseinplace
                                             {\tt HKCU \ } software \verb|\ classes \ \verb|\ all file systemobjects \verb|\ browsein place| \\
   Opens key:
   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
                                             {\tt HKCR\allfilesystemobjects\clsid}
   Opens key:
                                             HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
                                             HKCR\clsid\{ff393560-c2a7-11cf-hff4-444553540000}
   Opens key:
                                             HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
   Opens key
444553540000}\inprocserver32
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
   Opens kev:
                                             HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
   Opens key
444553540000}\shellfolder
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellfolder
   Opens key:
                                             HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
   Opens key:
444553540000}\treatas
   Opens key:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
                                             HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
   Opens key:
444553540000}\progid
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
   Opens key:
                                             HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
   Opens key
444553540000}\inprochandler32
   Opens key:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
   Opens key
                                             HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler
   Opens key:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler
   Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-c2a7-11cf-
hff4-4445535400003
   Opens key
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409
                                             HKCU\software\microsoft\windows\currentversion\app
   Opens key:
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                             HKLM\software\microsoft\windows\currentversion\app
   Opens key
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                             HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-d1) + (20d04f
   Opens key:
3aea-1069-a2d8-08002b30309d}
   Opens key:
Opens key:
                                             HKCU \setminus software \setminus classes \setminus clsid \setminus \{20d04fe0-3aea-1069-a2d8-08002b30309d\}
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
   Opens key:
                                             HKCU\software\microsoft\internet explorer\main\windowssearch
   Opens key:
   Opens key:
                                             HKLM\software\policies\microsoft\internet explorer\feeds
   Opens key:
                                             HKCU\software\microsoft\internet explorer\feeds
   Opens key:
                                             HKLM\software\microsoft\internet explorer\feeds
   Opens key:
87bd-30b759fa33dd}
   Opens key:
87bd-30b759fa33dd}\propertybag
```

```
Opens key:
                                              HKLM\software\microsoft\windows search
   Opens key:
                                              HKCU\software\classes\mime\database\content type\baiduapp/json;
v6.27.2.14; charset=utf-8
   Opens key:
                                              \label{localization} HKCR\mbox{\mbox{$M$ ime}\ \content type\ \baiduapp/json; v6.27.2.14; charset=utf-8}
                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mbox{$\mbox{mime} \database \content type \baiduapp/json} \end{tabular}
   Opens key:
   Opens kev:
                                              HKCR\mime\database\content type\baiduapp/ison
  Opens key:
                                              HKCU\software\classes\protocols\filter\baiduapp/json; v6.27.2.14;
charset=utf-8
                                              HKCR\protocols\filter\baiduapp/json; v6.27.2.14; charset=utf-8
   Opens key
                                              HKLM\software\microsoft\internet explorer\activex
   Opens key
compatibility\{adc6cb82-424c-11d2-952a-00c04fa34f05}
   Opens key:
                                              HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}
   Opens key:
                                              HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}
   Opens key:
                                              HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\treatas
   Opens key:
                                              HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
   Opens key:
00c04fa34f05}\progid
                                              HKCR\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
   Opens key:
                                              HKCR \verb|\clsid|{adc6cb82-424c-11d2-952a-00c04fa34f05} \verb|\inprochandler32| \\
   Opens key
                                              HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprochandler
                                              HKCR\clsid\\ \{adc6cb82-424c-11d2-952a-00c04fa34f05\\\}\cline{Continuous}
   Opens key:
                                              HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
   Opens key:
                                              HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\treatas
                                              HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas
   Opens kev:
                                              HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
   Opens key
00c04fd9189d}\progid
   Opens key:
                                              HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\progid
   Opens key:
                                              HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32
   Opens kev:
                                              HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32
                                              HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
   Opens key
00c04fd9189d}\inprochandler32
                                              HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32
   Opens key:
   Opens key
                                              HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043
00c04fd9189d}\inprochandler
   Opens key:
                                              \label{local-bound} \mbox{HKCR\clsid} $$ \end{align*} $$ HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d} \in \end{align*} $$ \end{align*} $$
   Opens key:
                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \slimage / x-icon \end{tabular}
   Opens key
                                              {\it HKCR} \verb|\mime| database| content type| image/x-icon
   Opens key:
                                              HKCU\software\classes\protocols\filter\image/x-icon
   Opens key:
                                              {\tt 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
  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]
   Queries value:
\label{lem:hklm} \verb+KLM\software\microsoft\windows\currentversion\sidebyside[preferexternal manifest]+ of the properties of the propertie
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:
                                              HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb]
   Queries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\windows[loadappinit_dlls]| \\
   Oueries value:
                                              HKLM \setminus software \setminus microsoft \setminus ole[pageallocatoruse system heap] \\
   Oueries value:
                                              {\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocator system heap is private]}
                                              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Oueries value:
                                              {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet}
   Queries value:
settings[disableimprovedzonecheck]
                                              {\it HKLM} \\ {\it software \ policies \ microsoft \ windows \ current \ version \ \ internet}
   Oueries value:
settings[security hklm only]
                                              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                                              HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
   Queries 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]
   Queries 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
    Oueries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane6]|
    Oueries value:
                                                                HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
    Oueries value:
                                                                HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane8]|
                                                                HKLM\software\microsoft\windows
    Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
                                                                HKLM\software\microsoft\windows
    Oueries value:
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]
    Oueries value:
                                                                 HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|
    Queries value:
                                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
    Oueries value:
                                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
    Oueries value:
                                                                HKLM\system\currentcontrolset\control\cmf\config[system]
    Queries value:
                                                                \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} fontsubstitutes [segoes the constraint of the co
uil
    Queries value:
                                                                 HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
 shell dlg]
                                                                 HKLM\software\microsoft\ole[maximumallowedallocationsize]
    Queries value:
    Oueries value:
                                                                 HKLM\software\microsoft\com3[com+enab]ed1
                                                                 HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
    Queries value:
                                                                 HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
    Queries value:
                                                                HKCR\clsid\{8856f961-340a-11d0-a96b-
    Oueries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                                                                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
    Queries value:
                                                                HKCR\clsid\{8856f961-340a-11d0-a96b-
    Oueries value:
00c04fd705a2}\inprocserver32[threadingmodel]
    Oueries value:
                                                                HKLM\software\microsoft\ole[maxsxshashcount]
     Oueries value
                                                                 HKLM\software\microsoft\rpc[maxrpcsize]
     Queries value:
\label{lem:hklm} \verb+KLM\+ system \verb+ current control \verb+ computer name \verb+ (active computer name) and \verb+ (active computer name) are active name and \verb+ (active computer name) and \verb+ (active
    Queries value:
                                                                 HKLM\system\setup[oobeinprogress]
     Queries value:
                                                                 HKLM\system\setup[systemsetupinprogress]
     Queries value:
                                                                 HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Queries value:
                                                                 HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - be
0 fb 58b 01c 4a 4 \} \\ language profile \\ 0 x 00000000 \\ \{0001bea 3-ed 56-48 3d-a 2e 2-a ea e 25577436\} [enable] \\ [enab
    Queries value:
                                                                 HKLM\software\microsoft\ctf[enableanchorcontext]
    Queries value:
                                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
    Oueries value:
                                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
 settings[createuricachesize]
    Oueries value:
                                                                HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                                                HKLM\software\microsoft\windows\currentversion\internet
    Oueries value:
 settings[createuricachesize]
                                                                HKLM\software\policies\microsoft\windows\currentversion\internet
    Queries value:
settings[enablepunycode]
    Queries value:
                                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[enablepunycode]
    Queries value:
                                                                 HKLM\software\microsoft\internet
 HKLM\software\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[*]
    Queries value:
Oueries value:
                                                                 HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
    Oueries value:
                                                                 HKLM \verb|\system| current controlset \verb|\services| ldap[use old host resolution order]|
    Oueries value:
                                                                 HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
    Oueries value:
                                                                 HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
    Oueries value:
                                                                 HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
    Oueries value:
                                                                 HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
    Oueries value:
                                                                 HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
    Oueries value:
                                                                 HKCU\software\microsoft\internet explorer\main[frametabwindow]
                                                                 HKLM\software\microsoft\internet explorer\main[frametabwindow]
    Oueries value:
                                                                 HKCU\software\microsoft\internet explorer\main[framemerging]
    Queries value:
    Queries value:
                                                                 HKLM\software\microsoft\internet explorer\main[framemerging]
                                                                 HKCU\software\microsoft\internet explorer\main[sessionmerging]
    Queries value:
    Queries value:
                                                                 HKLM\software\microsoft\internet explorer\main[sessionmerging]
    Queries value:
                                                                 HKCU\software\microsoft\internet explorer\main[admintabprocs]
    Queries value:
                                                                 HKLM\software\microsoft\internet explorer\main[admintabprocs]
    Oueries 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]
                                                                HKCR\clsid\{871c5380-42a0-1069-a2ea-
    Queries value:
08002b30309d}\shellfolder[callforattributes]
     Queries value:
                                                                HKCR\clsid\{871c5380-42a0-1069-a2ea-
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 \} \verb|\shellfolder[usedrophandler]|
    Oueries value:
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsforparsing]
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
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]
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
    Queries value:
08002b30309d}\shellfolder[hideinwebview]
    Queries value:
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideondesktopperuser]
    Oueries value
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsaliasednotifications]
    Queries value:
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsuniversaldelegate]
    Queries value:
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[nofilefolderjunction]
    Oueries value:
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[pintonamespacetree]
    Oueries value
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hasnavigationenum]
    Queries value:
                                                          HKCU \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'clsid \ '{871c5380-microsoft} \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer' \ 'explorer'' \ 'explo
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
    Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea
08002b30309d}1
    Oueries value:
                                                           HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
    Oueries value:
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                                                          HKCU\software\microsoft\windows\currentversion\shell
   Oueries value:
0xffff1
    Oueries value:
                                                           HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
    Queries value:
08002b30309d}\inprocserver32[inprocserver32]
    Queries value:
                                                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
                                                           HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
    Queries value:
    Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
   Queries value:
                                                          HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_unc_savedfilecheck| [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
    Oueries value:
                                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
   Queries value
                                                          HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
   Oueries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
   Oueries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
   Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\3[flags]
   Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
    Queries value:
                                                           HKCU\software\microsoft\internet
explorer \verb|\main| feature metric metric
    Queries value:
                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                                                          HKLM\software\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
    Queries value:
                                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
    Oueries value
                                                          HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b7231
   Queries value:
                                                           HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce41
    Oueries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[secureprotocols]
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[secureprotocols]
   Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
   Queries value:
                                                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[certificaterevocation]
    Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
    Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
    Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
   Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
   Oueries value:
                                                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[enablehttp1_1]
```

```
Oueries value:
                                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Oueries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Oueries value:
                                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                                     HKCU\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[proxyhttp1.1]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                                     HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enablenegotiate]
                                                     \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt definition} \
   Queries value:
settings[disablebasicoverclearchannel]
   Queries value:
                                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
   Queries value:
                                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
   Queries value:
                                                     HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Queries value:
settings[syncmode5]
   Queries value:
                                                     \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
{\tt settings \ 1.0 \ cache[sessions tart time default deltasecs]}
                                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Queries value:
settings\5.0\cache[signature]
   Queries value:
                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
   Queries value:
                                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[category]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[name]
   Oueries value:
ba85-6007caedcf9d}[parentfolder]
HKLM \label{lem:hklm} Which is the latest and the
ba85-6007caedcf9d}[description]
   Queries value:
HKLM \label{lem:hklm} Which is the latest and the
ba85-6007caedcf9d}[relativepath]
   Queries value:
ba85-6007caedcf9d}[parsingname]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[infotip]
   Oueries value:
ba85-6007caedcf9d}[localizedname]
   Oueries value:
ba85-6007caedcf9d}[icon]
   Queries value:
ba85-6007caedcf9d}[security]
   Queries value:
ba85-6007caedcf9d}[streamresource]
ba85-6007caedcf9d}[streamresourcetype]
   Oueries value:
ba85-6007caedcf9d}[localredirectonly]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[roamable]
   Queries value:
ba85-6007caedcf9d}[precreate]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[stream]
   Queries value:
ba85-6007caedcf9d}[publishexpandedpath]
   Queries value:
ba85-6007caedcf9d}[attributes]
   Queries value:
ba85-6007caedcf9d}[foldertypeid]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[initfolderhandler]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
   Oueries value:
```

9d55-7b8e7f157091}[category]

Oueries value:

9d55-7b8e7f157091}[name]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]

Queries value:

9d55-7b8e7f157091}[relativepath]

Oueries value:

 $HKLM \label{lem:hklm} Which is a constant of the second constant o$ 9d55-7b8e7f157091}[parsingname]

Oueries value:

9d55-7b8e7f157091}[infotip]

Queries value:

9d55-7b8e7f157091}[localizedname]

Queries value:

9d55-7b8e7f157091}[icon]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]

Oueries value:

 $HKLM \label{lem:hkkkk} In the latest and the late$ 9d55-7b8e7f157091}[localredirectonly]

Oueries value:

9d55-7b8e7f157091}[roamable]

Queries value:

9d55-7b8e7f157091}[precreate]

Queries value:

 $HKLM \label{lem:hklm} Which is a constant of the second constant o$ 9d55-7b8e7f157091}[stream]

Queries value:

9d55-7b8e7f157091}[publishexpandedpath] Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid] Queries value: 

9d55-7b8e7f157091}[initfolderhandler]

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

Queries value:

folders[local appdata]

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White$ 9afe-ea3317b67173}[category]

9afe-ea3317b67173}[name]

Oueries value:

9afe-ea3317b67173}[parentfolder]

Queries value:

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

Queries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ 'explorer' \ 'explore$ 9afe-ea3317b67173}[infotip]

Queries value:

9afe-ea3317b67173}[localizedname]

9afe-ea3317b67173}[icon]

Oueries value:

9afe-ea3317b67173}[security]

Queries value:

9afe-ea3317b67173}[streamresource]

Queries value:

9afe-ea3317b67173}[streamresourcetype]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e46661-16e4e461-16e4e461-16e4e4601-16e4e4661-16e4e461-16e4e461-16e$ 9afe-ea3317b67173}[localredirectonly]

Oueries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]

Queries value:

9afe-ea3317b67173}[stream]

Queries value:

 $HKLM \label{lem:hklm} Which is the latest and the$ 9afe-ea3317b67173}[publishexpandedpath]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]

Queries value:

9afe-ea3317b67173}[foldertypeid]

Queries value:

9afe-ea3317b67173}[initfolderhandler]

Queries value: 2160590473-689474908-1361669368-1002[profileimagepath]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-b04864, \ and \ box \ b$ 908e-08a611b84ff6}[category]

 $HKLM \label{lem:hklm} Which is the latest and the$ 908e-08a611b84ff6}[name]

Queries value:

 $HKLM \label{lem:hklm} Which is the latest and the$ 908e-08a611b84ff6}[parentfolder]

Queries value:

908e-08a611b84ff6}[description]

Oueries value:

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

Oueries value:

908e-08a611b84ff6}[parsingname] Oueries value:

908e-08a611b84ff6}[infotip] Queries value:

908e-08a611b84ff6}[localizedname] Queries value:

908e-08a611b84ff6}[icon]

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-b0464, and box \ and box$ 908e-08a611b84ff6}[security]

908e-08a611b84ff6}[streamresource]

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

908e-08a611b84ff6}[stream]

Queries value:

908e-08a611b84ff6}[publishexpandedpath]

Oueries value:

908e-08a611b84ff6}[attributes]

Queries value:

908e-08a611b84ff6}[foldertypeid]

Queries value:

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

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

folders[cookies]

Oueries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[name1

Queries value:

a03a-e3ef65729f3d}[parentfolder]

Oueries value:

a03a-e3ef65729f3d}[description]

Oueries value:

a03a-e3ef65729f3d}[relativepath]

Queries value:

a03a-e3ef65729f3d}[parsingname]

Oueries value:

a03a-e3ef65729f3d}[infotip]

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

 $HKLM \label{lem:hkkkk} In the latest and the late$ a03a-e3ef65729f3d}[streamresource]

Oueries value:

a03a-e3ef65729f3d}[streamresourcetype]

a03a-e3ef65729f3d}[localredirectonly]

Queries value:

a03a-e3ef65729f3d}[roamable]

Queries value:

a03a-e3ef65729f3d}[precreate]

Oueries value:

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

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[publishexpandedpath] Oueries value: 

a03a-e3ef65729f3d}[attributes]

Queries value: 

a03a-e3ef65729f3d}[foldertypeid]

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

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

folders[appdata]

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\cookies[cachelimit]

Oueries 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]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[category]

Queries value:

a781-5a1130a75963}[name]

Queries value:

 $HKLM \label{lem:hkkkk} In the latest and the late$ a781-5a1130a75963}[parentfolder]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[description]

Queries value:

a781-5a1130a75963}[relativepath]

Queries value:

a781-5a1130a75963}[parsingname]

Oueries value:

```
a781-5a1130a75963}[infotip]
   Oueries value:
a781-5a1130a75963}[localizedname]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[icon]
  Oueries value:
a781-5a1130a75963}[security]
  Queries value:
a781-5a1130a75963}[streamresource]
   Oueries value:
HKLM \label{lem:hklm} Which is the latest and the
a781-5a1130a75963}[streamresourcetype]
  Oueries value:
a781-5a1130a75963}[localredirectonly]
a781-5a1130a75963}[roamable]
   Queries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lkklm} White \label{lk
a781-5a1130a75963}[precreate]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[stream]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[attributes]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[foldertypeid]
   Oueries value:
a781-5a1130a75963}[initfolderhandler]
   Queries value:
                                           \label{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}
folders[history]
   Queries value
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\history[cachelimit]
  Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\5.0| cache \verb|\extensible| cache \verb|\domstore[cacherepair]|
  Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
  Oueries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                                          HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                                          HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                                           Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
   Queries value:
                                           \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ 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]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
```

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

 $settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|privacie:[cachelimit]|$ 

```
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Oueries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
 Oueries value
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
 Oueries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
 Oueries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
                            HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[utf8servernameres]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
 Queries value:
                            {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet}
settings[disableworkerthreadhibernation]
                            \label{thm:local_equation} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
 Queries value:
settings[disablereadrange]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[socketreceivebufferlength]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                            \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \sinternet \end{tabular}
  Queries value:
settings[maxhttpredirects]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[maxconnectionsperserver]}
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperproxy]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[serverinfotimeout]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:
                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[connecttimeout]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Oueries value
                            HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value
                            HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
  Queries value
                            \label{lem:hkcu} \verb+KCU\+software\+policies\+microsoft\+windows\+currentversion\+internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                            \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
  Queries value
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[httpdefaultexpirytimesecs]
  Oueries value
                            HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
 Queries value:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Oueries value:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*1
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
                            \label{thm:cut-software} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \sin ternet \end{tabular}
 Queries value:
settings[dialupuselansettings]
  Queries value
                            HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value
                            HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
```

 ${\tt settings[bypasshttpnocachecheck]}$ 

```
\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[bypasssslnocachecheck]
 Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Oueries value
                             HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                             HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[mimeexclusionlistforcache]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[dnscacheentries]
                             \label{lem:hkcu} \verb+KKCU\+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
 Queries value:
settings[warnonzonecrossing]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonpostredirect]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[alwaysdrainonredirect]
  Oueries value:
                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[warnonhttpstohttpredirect]
  Queries value:
                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[tcpautotuning]
  Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [namespace\_callout]
  Queries value
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [serial\_access\_num] \ access\_num] \ but the protocol\_catalog of the protocol\_ca
  Oueries value
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ [next\_catalog\_entry\_id]
  Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
 Oueries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004[packedcatalogitem]
  Queries value:
Queries value:
Queries value:
Queries value
Queries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value
Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000014[packedcatalogitem]
 Queries value:
Queries value:
Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 [num\_catalog\_entries]
  Oueries value
```

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[addressfamily] Oueries 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\000000000001[enabled]
  Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace\_catalog5 \catalog\_entries \names \name$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000001 [stores service class in fo] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[displaystring] Queries value:
- $\label{lem:hklmsystem} HKLM \system \controlset \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catalog 5 \cat$
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \00000000000002 \[address family]\] Queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[supportednamespace] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_provider \normalises \namespace\_catalog 5 \catalog\_entries \n$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[librarypath] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
  Queries value:
- $\label{lem:hklmsystem} HKLM \system \controlset \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \namespace\_catalog5 \namespace\_catalog5 \catalog\_entries \namespace\_catalog5 \namespace\_catalog6 \namespace\_catalog6 \namespace\_catalog6 \namespace\_catalog6 \namespace\_catalog6 \namespace\_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
   Oueries value:
- $\label{lem:hklmsystem} HkLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \namespace\_lements \namespace\_catalog5 \catalog\_entries \namespace\_lements \namespace\_lements$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storesserviceclassinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo] Oueries value:
- $\label{librarypath} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000000004[librarypath]\ Queries\value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
  Queries value:
  HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
- Queries value:

  HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace]
- Queries value:

  HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000004[enabled]
- $Queries \ value: \\ HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 000000000004 \ [version]$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 00000000000004 [stores service class in fo] \ Queries \ value:$
- $\label{lem:hklmsystem} HkLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \names \names pace\_catalog 5 \catalog\_entries \names \names$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[librarypath]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring] Oueries value:
- $\label{local-prop} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000005[providerid]\\ Oueries\ value: \begin{tabular}{ll} Color of the properties of the$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
   Queries value:
  HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace Queries value:
- $\label{thklm} HKL\ Mksystem \ current controls et \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 0000000000005 \ [enabled] \ Queries \ value:$
- $HKLM\system\current control set\services\winsock 2\parameters\names pace\_catalog 5\catalog\_entries\000000000005[storesserviceclassinfo]\queries\value:$
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \0000000000006 [library path] \queries \value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 0000000000006 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]

```
Oueries value:
Oueries value:
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[enabled]
  Oueries value:
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\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]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nonetautodial]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Queries value:
                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[badproxyexpirestime]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
                                  HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:
  Oueries value:
                                  HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
                                  HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Queries value:
  Queries value:
                                  HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Oueries value:
                                  HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Oueries value:
                                  HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                                  HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Oueries value:
                                  HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\profilelist[programdata]
  Oueries value:
                                  HKLM\software\microsoft\sqmclient\windows\disabledprocesses[2ac077a7]
  Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled sessions [global session]
  Queries value:
                                  HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
                                  HKLM\software\microsoft\tracing\rasmancs[enablefiletracing]
  Queries value:
                                  HKLM\software\microsoft\tracing\rasmancs[filetracingmask]
  Queries value:
                                  HKLM\software\microsoft\tracing\rasmancs[enableconsoletracing]
  Oueries value:
                                  HKLM\software\microsoft\tracing\rasmancs[consoletracingmask]
  Queries value:
                                  HKLM\software\microsoft\tracing\rasmancs[maxfilesize]
  Oueries value:
                                  HKLM\software\microsoft\tracing\rasmancs[filedirectory]
  Oueries value:
                                  \label{lem:hklm} \verb+Kklm/software\policies\microsoft/windows\currentversion/internet and the lemma of the le
settings[proxysettingsperuser]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxvenable]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyserver]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[autoconfigurl]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\connections[defaultconnectionsettings]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigcustomua]
  Oueries value:
                                  HKCR\autoproxytypes\application/x-internet-signup[dllfile]
  Oueries value:
                                  \label{local-continuity} \verb|HKCR\| autoproxytypes \| application/x-internet-signup[file extensions]| \\
  Oueries value:
                                  HKCR \verb| autoproxytypes \verb| application/x-internet-signup[default]| \\
  Oueries value:
                                  {\tt HKCR} \verb| autoproxytypes \verb| application/x-internet-signup[flags]|
                                  HKCR \verb| autoproxytypes \verb| application/x-ns-proxy-autoconfig[dllfile]|
  Oueries value:
  Queries value:
                                  HKCR \verb|\| autoproxytypes \verb|\| application/x-ns-proxy-autoconfig[file extensions]|
  Queries value:
                                  {\tt HKCR} \verb| autoproxytypes \verb| application/x-ns-proxy-autoconfig[default]|
  Oueries value:
                                  {\tt HKCR} \verb| autoproxytypes \verb| application/x-ns-proxy-autoconfig[flags]|
                                  HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zonemap[autodetect]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
Queries value
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]
  Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
```

```
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value
HKLM\svstem\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefau]tservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [wait for name error on all]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
  Queries value:
Oueries value:
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [queryipm atching]
  Queries value:
                                      HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use hosts file]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registerprimarvname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Queries value:
Queries value:
HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[register wan adapters]|
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]
  Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Oueries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [updates ecurity level]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration overwrite]
  Queries value:
                                      HKLM \verb|\system| current controlset \verb|\services| dnscache \verb|\parameters[maxcachesize]|
  Oueries value:
                                      HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [maxcachettl]
  Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} & System \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} & System \end{tabular} & System \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} & System \end{tabular} & System \end{tabular} & System \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} & System \end{tabular} & S
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
                                      HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [use new registration]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquervtimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Queries value:
                    HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value:
                     HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:
                     HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
 Oueries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
                    HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
                    HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Queries value:
 Queries value:
                    HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                    HKLM\system\currentcontrolset\services\winsock\setup
 Queries value:
migration\providers\tcpip6[winsock 2.0 provider id]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \{ parameters \setminus winsock [maxsock addrlength] \}
 Oueries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
 Queries value:
c19ce8a73253}[searchlist]
 Queries value:
                    HKCU\software\microsoft\internet explorer[no3dborder]
 Queries value:
                    HKLM\software\microsoft\internet explorer[no3dborder]
 Oueries value:
                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
                    HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[urlencoding]
                    HKLM\software\microsoft\internet
 Oueries value:
explorer \\ \text{main} \\ \text{feature} \\ \text{mime\_handling} \\ \text{[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]}
                    HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_mime_handling[*]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
 Queries value:
c19ce8a73253}[registrationenabled]
 Queries value:
c19ce8a73253}[registeradaptername]
 Queries value:
c19ce8a73253}[domain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
 Oueries value:
c19ce8a73253}[dhcpv6domain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
 Queries value:
c19ce8a73253}[nameserver]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
 Oueries value:
806e6f6e6963}[registrationenabled]
 Queries value:
806e6f6e6963}[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
```

```
806e6f6e6963}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpdomain]
  Oueries value:
806e6f6e6963}[nameserver]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
   Queries value:
                                          HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
c19ce8a73253}[queryadaptername]
   Queries value:
c19ce8a73253}[disableadapterdomainname]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
   Queries value:
c19ce8a73253}[maxnumberofaddressestoregister]
   Oueries value:
c19ce8a73253}[enablemulticast]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[queryadaptername]
   Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-1048, and \ extractions \ extrac
806e6f6e6963}[disableadapterdomainname]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disabledynamicupdate]
  Queries value:
806e6f6e6963}[enableadapterdomainnameregistration]
   Oueries value:
806e6f6e6963}[registrationmaxaddresscount]
   Queries value:
806e6f6e6963}[maxnumberofaddressestoregister]
   Queries value:
806e6f6e6963}[enablemulticast]
   Queries value:
                                          HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Oueries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                                          HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[]
                                          .
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[compatible]
                                          HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[compatible]
                                          HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[version]
                                          HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[version]
  Queries value:
                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings[user the lem: the lem of the lem
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]
                                          HKLM\software\microsoft\internet
   Queries value:
explorer \verb|\main| feature on trol \verb|\feature browser_emulation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
   Queries value:
                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
   Oueries value:
                                          HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature max connections perserver [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
   Queries value:
                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature maxconnectionsperserver[*]
   Oueries value:
                                          HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_maxconnectionsper1_0server[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                          HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature maxconnectionsper1 Oserver[*]
                                          HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[enableutf8]
   Queries value:
                                          HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]
   Queries value:
                                          HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[inprocserver32]
                                          HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32[]
   Oueries value:
                                          HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
   Queries value:
199fdba5723b}\inprocserver32[threadingmodel]
                                          \label{lem:hklm} \verb+ HKLM \software \microsoft \rpc \extensions [ndrole extdll]
   Queries value:
   Queries value:
                                          HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
   Queries value:
                                          HKCU\software\microsoft\internet explorer\international[acceptlanguage]
   Queries value:
                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Queries value:
                                          HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_disable\_legacy\_compression[*]
```

 ${\tt HKLM \setminus software \setminus microsoft \setminus ole \setminus appcompat[raised efault authnlevel]}$ 

Queries value:

```
Oueries value:
                                   HKLM\software\microsoft\ole[defaultaccesspermission]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Oueries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ strong
cryptographic provider[type]
  Oueries value:
                                   HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
manager[safeprocesssearchmode]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicyl
                                   HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:
                                   HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                   HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
  Queries value:
                                   HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
  Queries value:
                                   HKLM\software\microsoft\rpc\extensions[remoterpcdll]
                                   HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32[]
  Oueries value:
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
  Queries value:
  Queries value:
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
  Oueries value:
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
  Oueries value:
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[threadingmodel]
  Queries value:
                                   HKCR \verb|\interface| \{ 26656eaa-54eb-4e6f-8f85-4f0ef901a406 \} \verb|\proxystubclsid32[]| \\
  Queries value:
                                   \label{local-bound} \begin{tabular}{ll} HKCR\interface \ \{8a40a45d-055c-4b62-abd7-6d613e2ceaec\}\proxystubclsid32[] \end{tabular}
  Queries value:
                                   HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32[]
                                   HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
  Queries value:
                                   HKCR\clsid\{b196b286-bab4-101a-b69c-
  Oueries value:
00aa00341d07}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{b196b286-bab4-101a-b69c-
  Queries value:
00aa00341d07}\inprocserver32[threadingmodel]
  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]
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
                                   HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
  Queries value:
  Queries value:
                                   HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:
  Oueries value:
                                   HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
                                   HKCR\clsid\{6935db93-21e8-4ccc-beb9-
  Oueries value:
9fe3c77a297a}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32[]
  Oueries value:
                                   HKCR\clsid\{6935db93-21e8-4ccc-beb9-
  Oueries value:
9fe3c77a297a}\inprocserver32[threadingmodel]
                                   HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32[]
  Queries value:
                                   HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32[]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\wpad[wpadlastnetwork]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[autoproxydetecttype]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\numru[mrulist]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
  Queries 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\}[]
  Oueries value:
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Oueries value:
                                   HKCR\clsid\{00bb2764-6a77-11d0-a535-
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:
  Oueries value:
                                   HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
  Queries value:
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete\client[]
  Queries value:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
  Queries value:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
  Oueries value:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[]
  Queries value:
  Queries value:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
  Queries value:
                                   HKCU\control panel\desktop[smoothscroll]
  Queries value:
\label{thm:linear} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]$} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]$} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]$} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\advanced\explorer\explorer\advanced\explorer\advanced\explorer\explorer\advanced\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\e
  Queries value:
HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ advanced [list viewal phase lect]
  Oueries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
```

```
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
   Oueries value:
                                           HKLM\system\currentcontrolset\services\netbt\linkage[export]
                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\3[1a10]
  Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
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[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
   Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
  Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
                                           HKLM\software\microsoft\internet
   Queries value:
explorer \verb|\main| featurecontrol| feature\_feeds[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| featurecontrol| featu
                                           HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_feeds[*]
   Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
                                           HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
   Queries value:
                                           HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
   Queries value:
                                           HKCR\clsid\{25336920-03f9-11cf-8fd0-
   Oueries value:
00aa00686f13}\inprocserver32[inprocserver32]
                                           HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
   Queries value:
                                           HKCR\clsid\{25336920-03f9-11cf-8fd0-
   Queries value:
00aa00686f13}\inprocserver32[threadingmodel]
                                           HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_legacy_dispparams[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                           HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_legacy_dispparams[*]
   Oueries value:
                                           HKLM\software\microsoft\internet
explorer \\ \verb|main| feature \\ control \\ \verb|feature_object_caching| \\ [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ \verb|main| feature \\ control \\ \verb|feature_object_caching| \\ [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ \verb|main| feature \\ control \\ \verb|feature_object_caching| \\ [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ \verb|feature_object_caching| \\ explorer \\ \verb|feature_object_caching| \\ explorer \\ explor
   Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
                                           \label{thm:current} \begin{tabular}{ll} HKCU \software \mbox{$m$icrosoft \windows nt\currentversion \windows [dragdelay] } \end{tabular}
   Queries value:
   Queries value:
                                           HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-
91a2-7b624e0e7244]
   Queries value:
                                           \label{lem:hklm} \verb+ HKLM \software \microsoft \ internet explorer \ \ application
compatibility[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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]
  Oueries value:
                                           HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
  Oueries value:
                                           HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
  Oueries value:
                                           HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature| restrict_filedownload[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
   Queries value:
                                           HKCR\protocols\handler\about[clsid]
   Queries value:
                                           HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
                                           HKCR\clsid\{3050f406-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                                           HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
   Queries value:
                                           HKCR\clsid\{3050f406-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
   Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Oueries value:
                                           HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_protocol_lockdown[*]|
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
                                           HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
   Oueries value:
   Queries value:
                                           HKLM\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
                                            HKLM\software\policies\microsoft\internet explorer[smartdithering]
   Queries value:
   Oueries value:
                                            HKCU\software\microsoft\internet explorer[smartdithering]
                                            HKCU\software\microsoft\internet explorer[rtfconverterflags]
   Queries value:
   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]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[anchor underline]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[css_compat]
   Oueries value:
                                            HKCU\software\microsoft\internet explorer\main[expand alt text]
                                            HKCU\software\microsoft\internet explorer\main[display inline images]
   Oueries value:
                                            HKCU\software\microsoft\internet explorer\main[display inline videos]
   Queries value:
   Queries value:
                                            HKLM\software\microsoft\internet explorer\main[display inline videos]
                                            HKCU\software\microsoft\internet explorer\main[play_background_sounds]
   Queries value:
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[play_animations]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[print_background]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[use stylesheets]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[smoothscroll]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[xmlhttp]
   Oueries value:
                                            HKCU\software\microsoft\internet explorer\main[show image placeholders]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\main[disable script debugger]
```

```
Oueries value:
                                                         HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
    Oueries value:
                                                         HKCU\software\microsoft\internet explorer\main[move system caret]
    Oueries value:
                                                        \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ internet explorer \verb+ main[force offscreen] \\
composition]
                                                         HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
    Oueries value:
    Oueries value:
                                                         HKCU\software\microsoft\internet explorer\main[usethemes]
                                                         HKCU\software\microsoft\internet explorer\main[usehr]
    Oueries value:
    Oueries value:
                                                         HKCU\software\microsoft\internet explorer\main[q300829]
    Oueries value:
                                                        HKCU\software\microsoft\internet explorer\main[cleanup htcs]
    Oueries value:
                                                         HKCU\software\microsoft\internet explorer\main[xdomainrequest]
    Queries value:
                                                         HKLM\software\microsoft\internet explorer\main[xdomainrequest]
                                                         HKCU\software\microsoft\internet explorer\main[domstorage]
    Queries value:
                                                        HKCU\software\microsoft\internet
    Queries value:
explorer\international[default_codepage]
    Queries value:
                                                         HKCU\software\microsoft\internet explorer\international[autodetect]
    Queries value:
                                                         HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
    Oueries value:
                                                         HKCU\software\microsoft\internet explorer\settings[anchor color]
                                                         HKCU\software\microsoft\internet explorer\settings[anchor color visited]
    Queries value:
    Queries value:
                                                         HKCU\software\microsoft\internet explorer\settings[anchor color hover]
    Queries value:
                                                         HKCU\software\microsoft\internet explorer\settings[always use my colors]
    Oueries value:
                                                        HKCU\software\microsoft\internet explorer\settings[always use my font
size]
   Queries value:
                                                         HKCU\software\microsoft\internet explorer\settings[always use my font
face]
   Queries value:
                                                         HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
   Queries value:
                                                         HKCU\software\microsoft\internet explorer\settings[use anchor hover
color1
                                                         HKCU\software\microsoft\internet explorer\settings[miscflags]
    Oueries value:
                                                        \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+policies[allow]
    Queries value:
programmatic cut_copy_paste]
   Oueries 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]
    Oueries value:
                                                         HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsize]
    Queries value:
                                                        HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
    Queries value:
                                                        HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
                                                        HKCU\software\microsoft\internet
    Queries value:
explorer\international\scripts\3[iefixedfontname]
    Queries value:
                                                        HKLM\software\microsoft\internet explorer\version vector[ie]
    Queries value:
                                                         HKLM\software\microsoft\internet explorer\version vector[vml]
    Oueries value:
                                                        \label{lem:hklm} \verb+Kklm/software/microsoft/internet explorer/version vector[windowsedition]
    Oueries value:
                                                        HKLM\software\microsoft\internet
explorer \\ \texttt{main} \\ \texttt{feature\_control} \\ \texttt{feature\_zone\_elevation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]} \\ \texttt{explorer} \\ \texttt{main} \\ \texttt{feature\_control} \\ \texttt{feature\_zone\_elevation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]} \\ \texttt{explorer} \\ \texttt{main} \\ \texttt{feature\_control} \\ \texttt{feature\_contr
    Oueries value:
                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature zone elevation[*]
                                                        HKLM\software\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_xssfilter[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                                        HKLM\software\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature xssfilter[*]
   Queries value:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
                                                        HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
    Queries value:
    Queries value:
                                                        HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_mshtml_autoload_ieframe[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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:
                                                        \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[cointernetcombineiuricachesize]
    Oueries value:
                                                        HKLM\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
   Queries value:
                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature subdownload lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
    Oueries value:
                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature subdownload lockdown[*]
   Queries value:
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[securityidiuricachesize]
   Queries value:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
                                                        \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
   Queries value:
settings[securityidiuricachesize]
    Queries value:
                                                        HKLM\software\microsoft\internet
explorer \verb|\main| feature control| feature \verb|\scale= sslux| [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| feature \verb|\scale= sslux| feature for the feature for the
                                                         HKLM\software\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_sslux[*]
    Queries value:
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
                                                        \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \normalisatio
   Queries value:
settings[warnonintranet]
   Oueries value:
                                                        \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[warnonintranet]
```

```
Queries value:
                                           HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
  Queries value:
                                           HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                           \label{local-eq:hkcr} $$ HKCR \clsid \ 50d5107a-d278-4871-8989-f4cea af 59cfc \ inprocserver 32[] $$
  Oueries value:
  Oueries value:
                                           HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
                                           HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid[]
  Oueries value:
                                           HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
  Oueries value:
                                           HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
  Oueries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
  Queries value:
                                           HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
  Queries value:
                                           HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
  Queries value:
                                           HKCU\software\microsoft\internet explorer\recovery[autorecover]
  Queries value:
                                           HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature| scripturl_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Oueries value:
                                           HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_block_lmz_img[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
                                           HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_behaviors[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Queries value:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[*]
  Queries value:
                                           \label{lem:hamilton} \begin{tabular}{ll} HKLM \label{lem:hamilton} HKLM \label{lem:hamilton} Software \mbox{$\mathbb{N}$ internet explorer $\default behaviors [homepage] $\default behaviors 
  Queries value:
                                           HKCR \clsid \ \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\} \progid[]
                                           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[]
  Oueries value:
                                           HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
  Queries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
                                           HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]
  Oueries value:
                                           HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]
  Oueries value:
                                           HKCR\clsid\{81397204-f51a-4571-8d7b-
  Oueries value:
dc030521aabd}\inprocserver32[inprocserver32]
  Oueries value:
                                           \label{lem:hkcrclsid} $$ HKCR\clsid_{81397204-f51a-4571-8d7b-dc030521aabd} \in \clsid_{81397204-f51a-4571-8d7b-dc030521aabd} $$ \clsid_{81397204-f51a-4571-8d7b-dc030521aabd} = \clid_{81397204-f51a-4571-8d7b-dc030521aabd} $$ \clid_{81397204-f51a-4571-8d7b-dc030521aabd} = \clid_{81397204-f51a-4571-8d7b-dc030521aabd} $$ \clid_{81397204-f51a-4571-8d7b-dc030521aabd} = \clid_{81397204-f51a-4571-8d7b-dc03
                                           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-
  Queries value:
3c8b00c10000}\inprocserver32[inprocserver32]
  Queries value:
                                           HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
   Queries value:
                                           HKCR\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[threadingmodel]
  Queries value:
                                           HKLM\software\microsoft\internet explorer\default
behaviors[dxtfilterbehavior]
                                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]
  Queries value:
  Oueries value:
                                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[inprocserver32]
                                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]
  Oueries value:
  Oueries value:
                                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
                                           HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Oueries 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-
  Queries value:
fd27e3774e32}\0000[pruningmode]
                                           HKLM\hardware\devicemap\video[\device\video0]
  Queries value:
  Queries value:
                                           9dd4432fa2e9}\0000[pruningmode]
                                           HKLM\hardware\devicemap\video[\device\video1]
  Queries value:
                                           HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
  Queries value:
0d8e74595f78}\0000[pruningmode]
                                           HKLM\hardware\devicemap\video[\device\video2]
  Queries value:
   Oueries value:
                                           HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[pruningmode]
  Queries value:
                                           HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\bug![name]|
  Oueries value:
                                           HKLM \verb|\software\microsoft\directdraw\compatibility\bug![flags]|
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\bug![id]
  Oueries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [name]
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [flags]
  Queries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [id]
  Queries value:
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\diablo[name]
                                           HKLM\software\microsoft\directdraw\compatibility\diablo[flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\diablo[id]
  Queries value:
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
                                           HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
  Queries value:
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
                                           HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
  Queries value:
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
  Queries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus norton system in fo[id]
   Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
  Queries 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]

Queries value:

```
HKLM\software\microsoft\directdraw\compatibility\savage[id]
 Oueries value:
                            HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
 Oueries value:
                            HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus scorched planet [flags]
 Oueries value:
                            {\tt HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus scorched planet[id]}
                            HKLM \verb|\software\microsoft\directdraw\compatibility \verb|\silentthunder[name]|
 Oueries value:
                            HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\silentthunder[flags]|
 Oueries value:
 Oueries value:
                            HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus silent thunder [id]
                            HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus starcraft 100 [name]
 Oueries value:
 Oueries value:
                            HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus starcraft 100 [flags]
 Oueries value:
                            HKLM\software\microsoft\directdraw\compatibility\starcraft100[id]
 Queries value:
                            HKLM\software\microsoft\directdraw\compatibility\starcraft115[name]
 Queries value:
                            HKLM\software\microsoft\directdraw\compatibility\starcraft115[flags]
 Queries value:
                            HKLM\software\microsoft\directdraw\compatibility\starcraft115[id]
 Queries value:
                            HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[name]
 Queries value:
                            HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus starcraft demo[flags]
 Queries value:
                            HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[id]
 Oueries value:
                            HKLM\software\microsoft\directdraw\compatibility\terracide[name]
                            HKLM\software\microsoft\directdraw\compatibility\terracide[flags]
 Oueries value:
                            HKLM\software\microsoft\directdraw\compatibility\terracide[id]
  Queries value:
 Queries value:
                            HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]
  Queries value:
                            HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]
 Oueries value:
                            HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff davis quality benchmark [name]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff davis quality benchmark [flags]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
 Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
 Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdayiswinmarkbenchmark[id]
                            HKLM\software\microsoft\directdraw[modexonly]
 Queries value:
 Queries value:
                            HKLM\software\microsoft\directdraw[emulationonly]
 Oueries value:
                            HKLM\software\microsoft\directdraw[showframerate]
 Oueries value:
                            HKLM\software\microsoft\directdraw[enableprintscreen]
 Oueries value:
                            HKLM\software\microsoft\directdraw[forceagpsupport]
                            HKLM\software\microsoft\directdraw[disableagpsupport]
 Queries value:
                            HKLM\software\microsoft\directdraw[disablemmx]
 Queries value:
                            HKLM\software\microsoft\directdraw[disableddscapsinddsd]
  Queries value:
 Queries value:
                            HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Queries value:
                            HKLM\software\microsoft\directdraw[usenonlocalvidmem]
 Queries value:
                            HKLM\software\microsoft\directdraw[forcerefreshrate]
 Queries value:
                            HKLM\software\microsoft\direct3d[flipnovsync]
 Oueries value:
                            HKLM\software\microsoft\directdraw[owndc]
 Queries value:
                            HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
 Oueries value:
                            HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
 Oueries value:
                            HKCR\clsid\a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
                            HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
 Oueries value:
 Oueries value:
                            HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[threadingmodel]
                            HKCR\dximagetransform.microsoft.shadow\clsid[]
 Oueries value:
                            HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
 Queries value:
                            HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
 Queries value:
                            HKCR\clsid\{e71b4063-3e59-11d2-952a-
 Queries value:
00c04fa34f05}\inprocserver32[inprocserver32]
 Queries value:
                            HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32[]
                            HKCR\clsid\{e71b4063-3e59-11d2-952a-
 Queries value:
00c04fa34f05}\inprocserver32[threadingmodel]
                            HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[]
 Queries value:
                            HKCR\clsid\{4cb26c03-ff93-11d0-817e-
 Queries value:
0000f87557db}\inprocserver32[inprocserver32]
  Queries value:
                            HKCR \c1sid \end{4cb26c03-ff93-11d0-817e-0000f87557db} \clinprocserver 32[]
  Oueries value:
                            HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[threadingmodel]
 Oueries value:
                            HKCR\mime\database\content type\image/png[extension]
 Oueries value:
                            HKCR \clsid \ \{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\} \progid[]
                            HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]
 Oueries value:
 Oueries value:
                            HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
 Queries value:
                            HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
 Oueries value:
                            HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
 Queries value:
                            HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
 Queries value:
                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
 Queries value:
 Queries value:
                            HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
 Queries value:
 Oueries value:
                            HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
                            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
 Queries value:
  Queries value:
                            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
                            HKCR\clsid\{6a01fda0-30df-11d0-b724-
 Queries value:
00aa006c1a01}\inprocserver32[inprocserver32]
                            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
  Queries value:
                            HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
 Queries value:
                            HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
 Oueries value:
                            HKCR\mime\database\content type\image/bmp\bits[0]
 Queries value:
                            HKCR\mime\database\content type\image/gif\bits[0]
```

Oueries value:

```
Oueries value:
                           HKCR\mime\database\content type\image/jpeg\bits[0]
  Oueries value:
                           HKCR\mime\database\content type\image/pjpeg\bits[0]
  Oueries value:
                           HKCR\mbox{\tt Mime\database\content\ type\image/png\bits[0]}
  Oueries value:
                           HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt lmage} \mbox{\tt /x-png} \mbox{\tt bits} \mbox{\tt [0]}
  Oueries value:
                           HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt image} \mbox{\tt /x-wmf} \mbox{\tt bits} \mbox{\tt [0]}
                           HKCR\mime\database\content type\image/x-png[image filter clsid]
  Oueries value:
                           HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
  Oueries value:
                           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid[]
  Oueries value:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[inprocserver32]
  Queries value:
                           HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Queries value:
                           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
  Queries value:
00a0c913f750}\inprocserver32[inprocserver32]
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Queries value:
  Queries value:
                           HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[threadingmodel]
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
  Oueries value
00a0c913f750}\inprocserver32[threadingmodel]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Oueries value:
                           Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Oueries value:
                           Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[874]
                           HKLM\system\currentcontrolset\control\nls\codepage[932]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[936]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1361]
  Queries value:
  Oueries value:
                           HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsize]
                          HKCU\software\microsoft\internet
  Oueries value:
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]
  Queries value:
                          HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_block_lmz_script[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
  Oueries value:
                           HKCU\software\microsoft\windows script\settings[jitdebug]
  Oueries value:
                          HKCR\mime\database\content type\image/gif[extension]
  Oueries value:
                          HKCU\software\microsoft\internet explorer\new
windows[accuserinitonclick]
  Oueries value:
                           HKLM\software\microsoft\direct3d[disablemmx]
                           HKLM\software\microsoft\direct3d[disablex3d]
  Oueries value:
  Queries value:
                          HKLM\software\microsoft\direct3d[fewvertices]
                           HKLM\software\microsoft\direct3d[disablevidmemvbs]
  Queries value:
                          HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane1]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane2]
  Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane3]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane4]
                          HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane5]|
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane6]
  Queries value:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane7]|
  Oueries value:
                          HKLM\software\microsoft\window
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane8]|
  Queries value:
                          HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback\simsun[plane9]
  Oueries value:
                           HKLM\software\microsoft\window
\verb|nt\currentversion\language| pack\surrogatefallback\simsun[plane10]|
                          HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\language| pack\surrogatefall back\simsun[plane11]|
                          HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback\simsun[plane12]|
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane13]
  Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane14]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane15]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane16]
  Queries value:
                           HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]
  Queries value:
                           HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32[]
  Queries value:
                           HKCR\clsid\{00020424-0000-0000-c000-00000000046}[]
  Queries value:
                          HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                          HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]
  Queries value:
```

```
Oueries value:
                                          HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Oueries value:
                                          HKCR\shockwaveflash.shockwaveflash\clsid[]
   Oueries value:
                                          HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid[]
                                          HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
   Oueries value:
                                          HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Oueries value:
444553540000}\inprocserver32[inprocserver32]
                                          HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[]
   Oueries value:
                                          HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Oueries value:
444553540000}\inprocserver32[threadingmodel1
  Queries value:
                                          HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
bc58-54c27d745f8f]
                                          HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
  Queries value:
958a-dad20c90073c]
   Queries value:
                                          HKLM\hardware\description\system\centralprocessor\0[~mhz]
   Queries value:
                                          HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
                                          HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
   Oueries value:
                                          HKLM\software\microsoft\internet explorer\default behaviors[userdata]
   Oueries value:
                                          HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
   Queries value:
   Queries value:
                                          HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
   Oueries value:
                                          HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
   Queries value:
                                          HKCR \c1sid \f3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \c1sid \f3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \c3b4b6bfc4 \c3
   Oueries value:
                                          HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
   Oueries value:
                                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\zones\3[2000]
                                          HKLM\software\microsoft\internet explorer\feed discovery[sound]
   Queries value:
   Oueries value:
                                          HKCU\software\microsoft\ftp[use web based ftp]
                                          HKLM\software\microsoft\internet
   Oueries value:
explorer \verb|\main| feature control \verb|\feature| activex\_repurpose detection[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                          HKLM\software\microsoft\internet
  Queries value:
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]\\
   Oueries value:
                                         HKLM\software\microsoft\internet
\verb|explorer| main | feature control | feature don_management[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| feature control | featu
                                         HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_addon_management[*]
                                          HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1[]
   Queries value:
   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:
                                          HKCU\software\microsoft\internet explorer\domstorage\total[]
   Queries value:
                                          HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
   Queries value:
                                          HKCR\shockwaveflash.shockwaveflash.7\clsid[]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus system[enable lua]
   Oueries value:
                                          HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
                                          HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
   Oueries value:
                                          HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
   Oueries value:
                                          HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
   Oueries value:
                                          HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
   Oueries value:
                                          HKLM\software\microsoft\rpc[udtalignmentpolicy]
   Oueries value:
                                          HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32[]
   Queries value:
                                          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[]
   Queries value:
   Queries value:
                                          HKCR\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
   Queries value:
                                          HKLM \verb|\system| current control \verb|\spicache| credssp.dll[name]|
   Oueries value:
                                          Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
                                          Queries value:
                                          Queries value:
                                          Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount]
   Queries value:
                                          HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
   Oueries value:
                                          HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
                                          HKCR\clsid\{a4a1a128-768f-41e0-bf75-
   Oueries value:
e4fddd701cba}\inprocserver32[inprocserver32]
   Queries value:
                                          HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
                                          HKCR\clsid\{a4a1a128-768f-41e0-bf75-
   Queries value:
e4fddd701cba}\inprocserver32[threadingmodel]
   Queries value:
                                          HKCR\interface\{00020404-0000-0000-c000-00000000046}\proxystubclsid32[]
   Queries value:
                                          HKCR\clsid\{00020421-0000-0000-c000-00000000046}[]
   Queries value:
                                          HKCR\clsid\{00020421-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                          HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserver32[]
   Oueries value:
                                          HKCR\clsid\{00020421-0000-0000-c000-
   Queries value:
```

```
00000000046}\inprocserver32[threadingmodel]
   Queries value:
                                             HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid[]
   Oueries value:
                                             HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}[]
   Oueries value:
                                             HKCR\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[inprocserver32]
                                             HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
   Oueries value:
                                             HKCR\clsid\{f5078f35-c551-11d3-89b9-
   Oueries value:
0000f81fe221}\inprocserver32[threadingmodel1
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Oueries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 6]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 7]
   Oueries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
   Oueries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
   Oueries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
   Oueries value:
                                              HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi5]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi6]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi7]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi8]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
   Oueries value:
HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid[]
   Queries value:
                                              HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[]
   Queries value:
                                             HKCR\clsid\{2933bf90-7b36-11d2-b20e-
   Oueries value:
00c04f983e60}\inprocserver32[inprocserver32]
                                             HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32[]
   Queries value:
                                             HKCR\clsid\{2933bf90-7b36-11d2-b20e-
   Oueries value:
00c04f983e60}\inprocserver32[threadingmodel]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1606]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacherepair]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\userdata[cachepath]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\userdata[cacheprefix]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachelimit]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheoptions]
   Queries value:
                                             \label{lem:hklm} \verb+Kklm/software/microsoft/cryptography/defaults/provider types/types and the state of the 
001[name1
   Oueries value:
                                             HKCU\software\macromedia\flashplayer[flashplayerversion]
   Oueries value:
                                             HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
                                             HKCU\software\microsoft\internet explorer\suggested sites[enabled]
   Oueries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[attributes]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[callforattributes]
   Queries value:
                                              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Queries value
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
   Oueries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value
08002b30309d}\shellfolder[queryforoverlay]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideinwebview]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
   Queries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4060-a2d8-4069-a2d8-4060-a2d8-4069-a2d8-4069-a2d8-4060-a2d8-4060-a2d8-4060-a2d8
08002b30309d}1
```

```
Oueries value:
11e3-b3bc-806e6f6e6963}[data]
      Oueries value:
HKCU \setminus software \setminus microsoft 
11e3-b3bc-806e6f6e6963}[generation]
                                                                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
     Oueries value:
409d6c4515e9}[drivemask]
                                                                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
      Oueries value:
      Oueries value:
                                                                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
      Queries value:
                                                                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
                                                                                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
      Queries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
      Queries value:
11e3-b3bc-806e6f6e6963}[data]
11e3-b3bc-806e6f6e6963}[generation]
      Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
      Oueries value:
                                                                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{linear} hidden \cite{linear} \end{tabular}
      Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
      Queries value:
\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+ advanced [hidefileext]+ of the latest of the latest and the latest of the latest and the latest of the lates
      Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
      Oueries value:
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]
     Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
      Oueries value:
                                                                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced [filter] \end{tabular}
      Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{lem:hkcu} separate process \cite{lem:hkcu} advanced \cite{lem:hkcu} separate \c
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
      Queries value
\label{thm:local_continuous} \begin{tabular}{l} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{label{local_continuous}} \end{tabular} \begin{tabular}{l} HKCU \software \microsoft \windows \cite{label{label_continuous}} \end{tabular} \begin{tabular}{l} HKCU \software \microsoft \windows \cite{label_continuous}} \begin{tabular}{l} HKCU \software \windows \windows \cite{label_continuous}} \begin{tabular}{l} HKCU \software \windows \windo
      Queries value
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{liconsonly} \end{tabular}
      Queries value:
\label{thm:local_explorer_law} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{local_explorer_law} \end{tabular} \label{thm:local_explorer_law} \end{tabular}
      Oueries value:
                                                                                    HKCR\directory[docobject]
      Oueries value:
                                                                                    HKCR\folder[docobject]
      Oueries value:
                                                                                    HKCR\allfilesystemobjects[docobject]
      Oueries value:
                                                                                    HKCR\directory[browseinplace]
                                                                                    HKCR\folder[browseinplace]
      Oueries value:
                                                                                    HKCR\allfilesystemobjects[browseinplace]
      Oueries value:
                                                                                    HKCR\directory[isshortcut]
      Queries value:
                                                                                    HKCR\folder[isshortcut]
      Queries value:
                                                                                     HKCR\allfilesystemobjects[isshortcut]
      Queries value:
      Queries value:
                                                                                    HKCR\directory[alwaysshowext]
      Queries value:
                                                                                     HKCR\directory[nevershowext]
      Queries value:
                                                                                     HKCR\folder[nevershowext]
      Queries value:
                                                                                     HKCR\allfilesystemobjects[nevershowext]
                                                                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
      Queries value:
                                                                                    HKCR\clsid\{ff393560-c2a7-11cf-bff4-
      Queries value:
444553540000}\inprocserver32[loadwithoutcom]
      Queries value:
                                                                                   HKCU\software\microsoft\windows\currentversion\shell
 extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046}
0xffff]
      Oueries value:
                                                                                    HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]
      Oueries value:
                                                                                   HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
                                                                                   HKCR\clsid\{ff393560-c2a7-11cf-bff4-
      Oueries value:
444553540000}\inprocserver32[threadingmodel]
                                                                                   HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
                                                                                    HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cachepath]
                                                                                   HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheprefix]
                                                                                    HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cachelimit]
                                                                                   HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
                                                                                    Oueries value:
3aea-1069-a2d8-08002b30309d}[]
      Queries value:
                                                                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
                                                                                    HKCU\software\microsoft\internet
      Queries value:
explorer\main\windowssearch[enabledscopes]
      Queries value:
87bd-30b759fa33dd}[category]
      Queries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \l
```

87bd-30b759fa33dd}[name]

```
Oueries value:
87bd-30b759fa33dd}[parentfolder]
   Oueries value:
HKLM\software\microsoft\windows\currentyersion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[description]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[relativepath]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[parsingname]
  Queries value:
87bd-30b759fa33dd}[infotip]
  Queries value:
87bd-30b759fa33dd}[localizedname]
HKLM \label{lem:hkkkk} INTO The properties of the second content of the second content
87bd-30b759fa33dd}[icon]
   Oueries value:
87bd-30b759fa33dd}[security]
   Queries value:
87bd-30b759fa33dd}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[localredirectonly]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[roamable]
   Oueries value:
87bd-30b759fa33dd}[precreate]
HKLM \label{lem:hklm} Which is the software \label{lem:hkklm} Which is the software \label{le
87bd-30b759fa33dd}[stream]
   Queries value:
87bd-30b759fa33dd}[publishexpandedpath]
   Queries value:
87bd-30b759fa33dd}[attributes]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
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]
   Queries value:
                                           HKLM\software\microsoft\downloadmanager[cacheok]
   Queries value:
                                           HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\progid[]
   Queries value:
                                           HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}[]
   Queries value:
                                           HKCR\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprocserver32[inprocserver32]
                                           HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32[]
   Queries value:
                                           HKCR\clsid\{adc6cb82-424c-11d2-952a-
   Queries value:
00c04fa34f05}\inprocserver32[threadingmodel]
   Queries value:
                                           HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[]
   Oueries value:
                                           HKCR\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32[inprocserver32]
   Queries value:
                                           HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]
   Oueries value:
                                           HKCR\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32[threadingmodel]
                                           \label{lem:hkcrmime} \begin{tabular}{ll} HKCR\mime\database\content type\image/x-icon[extension] \end{tabular}
   Oueries value:
   Sets/Creates value:
                                           HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature| scripturl_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| \\
                                           HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [enable file tracing]
   Sets/Creates value:
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
                                           HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32[filetracing mask]
   Sets/Creates value:
                                           \label{local-observation} {\sf HKLM} \\ {\sf software} \\ {\sf microsoft} \\ {\sf tracing} \\ {\sf rasapi32} \\ [{\sf consoletracingmask}] \\
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
   Sets/Creates value:
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasapi32[filedirectory]
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasmancs[enablefiletracing]
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasmancs[enableconsoletracing]
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasmancs[filetracingmask]
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasmancs[consoletracingmask]
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasmancs[maxfilesize]
   Sets/Creates value:
                                           HKLM\software\microsoft\tracing\rasmancs[filedirectory]
                                           HKCU\software\microsoft\windows\currentversion\internet
   Sets/Creates value:
settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}[wpaddecisionreason]
                                           HKCU\software\microsoft\windows\currentversion\internet
   Sets/Creates value:
```

settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}[wpaddecision] HKCU\software\microsoft\windows\currentversion\internet  $settings \verb|\wpad|{580a43fb-2e35-4b6b-8b33-caffb3960fdd}[wpadnetworkname]$ 

Sets/Creates value:

Sets/Creates value:

settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}[wpaddecisiontime]

HKCU\software\microsoft\windows\currentversion\internet

```
Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\d6-48-41-0b-3a-5a[wpaddecisionreason]
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\wpad| d6-48-41-0b-3a-5a[wpaddecisiontime]|
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\d6-48-41-0b-3a-5a[wpaddecision]
                          HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
 Sets/Creates value:
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\ex
                      tensible cache\userdata[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cacheoptions]
 Sets/Creates value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}}
settings\5.0\cache\ex
                         nsible cache\userdata[cacherepair]
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cachepath]
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\e
                         nsible cache\mshist012016040820160409[cacheprefix]
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cachelimit]
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
 Value changes:
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$m$icrosoft$ internet explorer $m$ain[disable script debugger]$} \end{tabular}
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\zonemap[autodetect]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxvenable]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\connections[savedlegacysettings]
 Value changes:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\connections[defaultconnectionsettings]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
 Value changes:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
\tt settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}\{[wpaddecisionreason]}
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}[wpaddecisiontime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings \verb|\wpad|{580a43fb-2e35-4b6b-8b33-caffb3960fdd}[wpaddecision]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{580a43fb-2e35-4b6b-8b33-caffb3960fdd}[wpadnetworkname]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\d6-48-41-0b-3a-5a[wpaddecisionreason]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\d6-48-41-0b-3a-5a[wpaddecisiontime]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\wpad\d6-48-41-0b-3a-5a[wpaddecision]
                          HKLM\software\microsoft\directdraw\mostrecentapplication[name]
 Value changes:
                           HKLM\software\microsoft\directdraw\mostrecentapplication[id]
 Value changes:
                           HKLM\software\microsoft\direct3d\mostrecentapplication[name]
 Value changes:
 Value changes:
                           HKCU\software\microsoft\internet explorer\domstorage\total[]
                           HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
 Value changes:
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
```

nsible cache\mshist012016040820160409[cachepath]

HKCU\software\microsoft\internet explorer\main\windowssearch[version]

settings\5.0\cache\exte

Value changes: