# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 7, Task ID: 23

Task ID: 23

Risk Level:

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

Processing Time: 61.66 seconds IntelliVM Virtual Environment:

**Execution Arguments:** 

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

Sample ID: Type: basic Owner:

62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb Label:

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

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

MD5: 4c838f1570b3a7ff6f491e6ec1ef6895

SHA256: 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb

Description:

## Pattern Matching Results

2 HTML file

3 HTTP connection - response code 200 (success)

4 Checks whether debugger is present

2 ECMA Script

3 Connects to local host

1 YARA score 1

3 Long sleep detected

5 Possible injector

#### Static Events

YARA rule hit: SME YARA rule hit: Nonexecutable

### Process/Thread Events

Creates process:

["c:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe"] RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service:

## Named Object Events

\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-Creates mutex

1957994488-1003

Creates mutex: 

1957994488-1003 Creates mutex:

1957994488-1003 \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-

\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-

Creates mutex:

\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003 Creates mutex:

1957994488-1003

\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-Creates mutex: 507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

\BaseNamedObjects\c:!documents and settings!admin!local Creates mutex: settings!temporary internet files!content.ie5!

Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!cookies! \BaseNamedObjects\c:!documents and settings!admin!local Creates mutex:

settings!history!history.ie5!

\BaseNamedObjects\WininetConnectionMutex Creates mutex: Creates mutex: \BaseNamedObjects\ZonesCounterMutex

Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex \BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EJH Creates mutex: Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex Creates mutex: \BaseNamedObjects\DDrawWindowListMutex Creates mutex: \BaseNamedObjects\DDrawDriverObjectListMutex

Creates mutex: \BaseNamedObjects\\_\_DDrawExclMode Creates mutex: \BaseNamedObjects\\_\_DDrawCheckExclMode Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.IEB

\BaseNamedObjects\c:!documents and settings!admin!ietldcache! Creates mutex:

\BaseNamedObjects\MSIMGSIZECacheMutex Creates mutex: Creates mutex:

\BaseNamedObjects\DirectSound DllMain mutex (0x0000058C) Creates mutex: \BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069}

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

\BaseNamedObjects\c:!documents and settings!admin!local Creates mutex

settings!application data!microsoft!internet explorer!domstore! Creates mutex:  $\verb|\BaseNamedObjects|| ! SHMSFTHISTORY!|_$ 

Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local

settings!history!history.ie5!mshist012016040820160409!

Creates mutex: **\BaseNamedObjects\InternetExplorerDOMStoreQuota** 

Creates mutex:  $\verb|\BaseNamedObjects\c:| documents and settings! admin! application| \\$ 

data!microsoft!internet explorer!userdata!

Creates event: \BaseNamedObjects\userenv: User Profile setup event Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.IEB.IC \BaseNamedObjects\MSCTF.SendReceiveConection.Event.IEB.IC Creates event:

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore:  $\verb|\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}| \\$ 

#### File System Events

Creates: C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt C:\Documents and Settings\Admin\Cookies\admin@baidu[2].txt Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\index[1].php Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\jquery-1.10.2.min\_f2fb5194[1].js Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\baidu\_jgylogo3[1].gif Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\nuomi\_510f7472[1].png C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\CXCXW1MR\zbios\_62c636fe[1].png C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\icons\_0e814c16[1].png C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\UH4D6D6X\s[1].txt C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\CXCXW1MR\bd\_logo1[1].png C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\ONWV4FIP\u=3925724364,2158606337&fm=58&s=7F84AA0AB5A46F111452CD6403007033[1].jpg Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet  $Files \verb|\| Content.IE5 \verb|\| ONWV4FIP \verb|\| u = 3070482661, 4157819617\&fm = 96[1].jpg \\$ Creates:  ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}$ Files\Content.IE5\ONWV4FIP\u=4247961311,3377350606&fm=58[1].jpg C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:  $Files \verb|\| Content.IE5 \verb|\| ONWV4FIP \verb|\| 1c5d7b26-f3f0-4dd7-a025-8c79809 fecac[1].js \\$ Creates:  ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}$ Files\Content.IE5\UH4D6D6X\u=3227862542,4058823482&fm=58&s=80327E97D8B101801D3083750300C066[1].jpg Creates C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\u=3520324766,1135887067&fm=96&s=19843C7AF9FF569A5DF5E0D7030090E2[1].jpg C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:  $Files \\ \verb|Content.IE5| \\ UH4D6D6X \\ \verb|u=3776762194,2342817517\&fm=96\&s=1B0AA64416B6966D4A9714070300E0CB[1].jpg \\ | Ignormal | Ignor$ C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\CXCXW1MR\u=2683104694,4195795178fm=96&s=F580F1115AF81F86383184D60300E0B2[1].jpg C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\CXCXW1MR\u=3734835402,589306938&fm=96&s=29A8279E5583C6E012D5B5F40300E078[1].jpg C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\CXCXW1MR\u=3610240597,3088990761&fm=58[1].jpg
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\u=1931034822,32205454-7&fm=58[1].jpg C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\every\_cookie\_aa168cb4[1].js C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\u=1266350913,3659364910&fm=96&s=71B11CD1CCA3B84B50295D2D03007040[1].jpg C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\9a504fc2d5628535e75664d992ef76c6a6ef6397[1].jpg C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\all\_async\_search\_d0d1b2ec[1].js Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\DOMStore\3FDD734T\www.baidu[1].xml  $\label{lem:cokies-admin@www.baidu[1].txt} C:\Documents\ and\ Settings\Admin\Cookies\admin@www.baidu[1].txt$ Creates: Creates:  ${\tt C:\Documents\ and\ Settings\Admin\Cookies\admin@www.baidu[2].txt}$ Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\nu\_instant\_search\_ebeb5baa[1].js C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\CXCXW1MR\quickdelete\_9c14b01a[1].png Creates: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012016040820160409 C:\Documents and Settings\Admin\Local Creates: Settings\History\History.IE5\MSHist012016040820160409\index.dat C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\ONWV4FIP\bdsug\_async\_1cb857eb[1].js Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\env\_beb83b45[1].swf Creates:  ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}$ Files\Content.IE5\UH4D6D6X\favicon[1].ico Creates: C:\Documents and Settings\Admin\Local Settings\Temp\httpwww.baidu.comfavicon.ico Creates: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\UserData C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Creates: Explorer\UserData\index.dat C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Creates: Explorer\UserData\BORP04R6 C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Creates: Explorer\UserData\DI4SV2D0 C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Creates: Explorer\UserData\W9PUTXLL Creates: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\UserData\8N45SSPX C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\CXCXW1MR\baiduia\_b45d552b[1].js C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Creates: Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Creates: Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx

C:\Documents and Settings\Admin\Application Data\Macromedia\Flash

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

```
C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com
  Creates:
                                    {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Creates:
Explorer\UserData\BQRP04R6\userDataBIDUPSID[1].xml
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\Content.IE5| ONWV4FIP \verb|\union[1].gif| \\
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\JSocket_9a52fc3e[1].swf
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ielib_0108[1].js
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\wb[1].gif
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Creates:
Files\Content.IE5\ONWV4FIP\wb[1].gif
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\union[1].gif
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\wb[1].gif
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\o_0108[1].swf
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\wb[1].gif
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Creates:
Files\Content.IE5\CXCXW1MR\wb[2].gif
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\wb[2].gif
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\wb[2].gif
  Creates:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\DI4SV2D0\oXMLStore[1].xml
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\wb[2].gif
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\wb[3].gif
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ps_fp[1].htm
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Creates:
Files\Content.IE5\ONWV4FIP\wb[3].gif
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\wb[3].gif
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Creates:
Files\Content.IE5\CXCXW1MR\wb[4].gif
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Creates:
Files \verb|\| Content.IE5 \verb|\| QXMNQBKF \verb|\| wb[3].gif
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\wb[4].gif
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Creates:
Files\Content.IE5\UH4D6D6X\wb[4].gif
                                    C:\WINDOWS\Prefetch\62DDFBF757BE511F30B6D330963C1-075A1102.pf
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin
  Opens:
                                    C:\WINDOWS\WinSxS\x86 Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                                    C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
  Opens:
Controls 6595b64144ccf1df 6.0.2600.5512 x-ww 35d4ce83\comctl32.dll
                                    C:\WINDOWS\system32\msimg32.dll
  Opens:
                                    C:\WINDOWS\system32\ws2_32.dll
  Opens:
  Opens:
                                    C:\WINDOWS\svstem32\ws2help.dll
                                    C:\WINDOWS\svstem32\psapi.dll
  Opens:
                                    C:\WINDOWS\system32\imm32.dll
  Opens:
                                    C:\WINDOWS\system32\shell32.dll
  Opens:
                                    C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:
                                    C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:
  Opens:
                                    C:\WINDOWS\WindowsShell.Manifest
                                    C:\WINDOWS\WindowsShell.Config
  Opens:
  Opens:
                                    C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:
                                    C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:
                                    C:\program files\qqd1eae\log.dat
  Opens:
                                    C:ntdll.dll
  Opens:
                                    C:\program files\qqd1eae\Log.dat
                                    C:\WINDOWS\system32\rpcss.dll
  Opens:
  Opens:
                                    C:\WINDOWS\svstem32\MSCTF.dll
                                    C:\DOCUME~1\Admin\LOCALS~1\Temp\restart.dat
  Opens
                                    C:\WINDOWS\system32\uxtheme.dll
  Opens:
                                    C:\WINDOWS\system32\MSCTFIME.IME
  Opens:
                                    C:\WINDOWS\system32\clbcatq.dll
  Opens
                                    C:\WINDOWS\system32\comres.dll
  Opens:
                                    C:\WINDOWS\Registration\R000000000007.clb
  Opens:
  Opens:
                                    C:\WINDOWS\system32\ieframe.dll
                                    C:\Program Files\Internet Explorer\iexplore.exe
  Opens:
  Opens:
                                    C:\WINDOWS\system32\ieframe.dll.123.Manifest
  Opens:
                                    C:\WINDOWS\system32\ieframe.dll.123.Config
  Opens:
                                    C:\WINDOWS\system32\en-US\ieframe.dll.mui
  Opens:
{\tt C:\WINDOWS\backslash Temp\backslash 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exeeld of the control o
  Opens:
                                    C:\WINDOWS\system32\MSIMTF.dll
  Opens:
                                    C:\WINDOWS\Temp\MJPGC.TMP
  Opens:
                                    C:\WINDOWS\system32\WININET.dll.123.Manifest
  Opens:
                                    C:\WINDOWS\system32\WININET.dll.123.Config
                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet\ Files}
  Opens:
  Opens:
                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\History
```

Creates:

```
Opens:
                                                  C:\Documents and Settings\Admin\Local Settings\History\History.IE5
   Opens:
                                                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
   Opens:
                                                  C:\Documents and Settings\Admin\Cookies
   Opens:
                                                  {\tt C:\Documents\ and\ Settings\Admin\Cookies\index.dat}\\
                                                   C:\Documents and Settings\Admin\Local
   Opens:
Settings\History\History.IE5\index.dat
                                                  C:\WINDOWS\system32\rasapi32.dll
   Opens:
   Opens:
                                                  C:\WINDOWS\system32\rasman.dll
                                                  C:\WINDOWS\system32\netapi32.dll
   Opens:
   Opens:
                                                  C:\WINDOWS\system32\tapi32.dll
                                                  C:\WINDOWS\system32\rtutils.dll
   Opens:
                                                  C:\WINDOWS\system32\winmm.dll
   Opens:
                                                  C:\WINDOWS\system32\TAPI32.dll.124.Manifest
   Opens:
                                                  C:\WINDOWS\system32\TAPI32.dll.124.Config
   Opens:
                                                  C:\AUTOEXEC.BAT
   Opens:
   Opens:
                                                  C:\
                                                  C:\Documents and Settings\All Users\Application
   Opens:
.
Data\Microsoft\Network\Connections\Pbk
                                                  C:\WINDOWS\system32\ras
   Opens:
                                                  C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\Network\Connections\Pbk\
   Opens:
                                                  C:\WINDOWS\system32\sensapi.dll
   Opens:
                                                  C:\WINDOWS\system32\mswsock.dll
   Opens:
                                                  C:\WINDOWS\system32\mlang.dll
   Opens:
                                                  C:\WINDOWS\system32\MLANG.dll.123.Manifest
   Opens:
                                                  C:\WINDOWS\system32\MLANG.dll.123.Config
   Opens:
                                                  C:\WINDOWS\system32\hnetcfg.dll
   Opens:
                                                   C:\WINDOWS\system32\wshtcpip.dll
                                                  C:\WINDOWS\system32\browseui.dll
   Opens
                                                  C:\WINDOWS\system32\browseui.dll.123.Manifest
   Opens
   Opens:
                                                  C:\WINDOWS\system32\browseui.dll.123.Config
   Opens:
                                                  C:\WINDOWS\system32\msv1_0.dll
                                                   C:\WINDOWS\system32\iphlpapi.dll
   Opens
                                                   C:\WINDOWS\system32\rasadhlp.dll
   Opens
   Opens:
                                                  C:\WINDOWS\system32\dnsapi.dll
   Opens:
                                                  C:\WINDOWS\system32\drivers\etc\hosts
   Opens:
                                                  C:\WINDOWS\system32\rsaenh.dll
   Opens:
                                                  C:\WINDOWS\system32\crypt32.dll
   Opens:
                                                  C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt
   Opens:
                                                   C:\Documents and Settings\Admin\Cookies\admin@baidu[2].txt
   Opens:
                                                  C:\WINDOWS\Temp\cb71a213-4d82-47ce-99b7-1419ae33ffd2
   Opens:
                                                  C:\WINDOWS\system32\mshtml.dll
   Opens:
                                                  C:\WINDOWS\system32\msls31.dll
   Opens:
                                                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\Content.IE5\QXMNQBKF\| index[1].php \\
   Opens:
                                                  C:\WINDOWS\system32\iepeers.dll
                                                  C:\WINDOWS\system32\winspool.drv
   Opens:
   Opens:
                                                  C:\WINDOWS\system32\iepeers.dll.123.Manifest
                                                  C:\WINDOWS\system32\iepeers.dll.123.Config
   Opens:
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\jquery-1.10.2.min_f2fb5194[1].js
                                                  C:\WINDOWS\system32\jscript.dll
   Opens:
                                                  C:\WINDOWS\system32\winlogon.exe
   Opens:
   Opens:
                                                  C:\WINDOWS\system32\xpsp2res.dll
                                                  C:\WINDOWS\system32\en-US\jscript.dll.mui
   Opens:
                                                  C:\WINDOWS\Fonts\arialbd.ttf
   Opens:
   Opens:
                                                  C:\WINDOWS\Fonts\ariali.ttf
                                                  C:\WINDOWS\system32\dxtrans.dll
   Opens:
                                                  C:\WINDOWS\system32\atl.dll
   Opens:
   Opens:
                                                  C:\WINDOWS\system32\ddrawex.dll
   Opens:
                                                  C:\WINDOWS\system32\ddraw.dll
   Opens:
                                                  C:\WINDOWS\system32\dciman32.dll
   Opens:
                                                  C:\WINDOWS\win.ini
                                                  C:\WINDOWS\system32\dxtmsft.dll
   Opens:
   Opens:
                                                  C:\WINDOWS\system32\sxs.dll
   Opens:
                                                  C:\WINDOWS\system32\en-US\mshtml.dll.mui
   Opens:
                                                  C:\WINDOWS\system32\imgutil.dll
   Opens
                                                  C:\WINDOWS\system32\pngfilt.dll
   Opens
                                                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\s[1].txt
   Opens
                                                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\icons_0e814c16[1].png
C: \verb|WINDOWS| \verb|WinSxS| x86_Microsoft. | Windows. GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-w
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-
ww_dfb54e0c\GdiPlus.dll
   Opens:
                                                   C:\WINDOWS\system32\d3dim700.dll
   Opens:
                                                  C:\Documents and Settings\Admin\IETldCache
   Opens:
                                                  C:\Documents and Settings\Admin\IETldCache\index.dat
   Opens:
                                                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\Content.IE5\verb|\ONWV4FIP| 1c5d7b26-f3f0-4dd7-a025-8c79809 fecac[1].js | files \verb|\Content.IE5| 2d7b26-f3f0-4dd7-a025-8c79809 fecac[1].js | files \verb|\Content.IE5| 2d7b26-f3f0-4dd7-a025-8c79809
   Opens:
                                                  {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\QXMNQBKF\every_cookie_aa168cb4[1].js
   Opens:
                                                  {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
\label{lem:content.IE5} \begin{tabular}{ll} \hline Files $$ \content.IE5 \QXMNQBKF\all\_async\_search\_d0d1b2ec[1].js \\ \hline \hline \end{tabular}
                                                  C:\WINDOWS\Fonts\times.ttf
   Opens:
                                                  C:\WINDOWS\system32\Macromed\Flash\Flash10h.ocx
   Opens:
                                                  C:\WINDOWS\system32\Macromed\Flash\Flash10h.ocx.2.Manifest
   Opens:
   Opens:
                                                  C:\WINDOWS\system32\Macromed\Flash\Flash10h.ocx.2.Config
                                                  C:\WINDOWS\system32\msasn1.dll
   Opens:
```

```
Opens:
                                             C:\WINDOWS\system32\dsound.dll
   Opens:
                                             C:\WINDOWS\system32\mscms.dll
                                             C:\WINDOWS\system32\Macromed\Flash\ss.sgn
   Opens:
   Opens:
                                             C:\WINDOWS\system32\Macromed\Flash
   Opens:
                                             C:\WINDOWS\system32\Macromed\Flash\ss.cfg
   Opens:
                                             C:\WINDOWS\system32\Macromed\Flash\mms.cfg
                                             C:\WINDOWS\system32\Macromed\Flash\oem.cfg
   Opens:
   Opens:
                                             C:\WINDOWS\system32\oem.cfg
                                             {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Adobe\Flash}
   Opens:
Plaver\AssetCache
                                             C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
  Opens:
                                             {\tt C:\WINDOWS\system32\stdole2.tlb}
   Opens:
                                             {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
   Opens:
Data\Microsoft\Internet Explorer\DOMStore
                                             C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Microsoft\Internet Explorer\DOMStore\index.dat
                                             C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
                                             C:\WINDOWS\system32\xmllite.dll
   Opens:
                                             C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T\www.baidu[1].xml
                                             C:\WINDOWS\system32\mshtml.tlb
   Opens:
   Opens:
                                             C:\Documents and Settings\Admin\Cookies\admin@www.baidu[1].txt
   Opens:
                                             C:\Documents and Settings\Admin\Cookies\admin@www.baidu[2].txt
   Opens:
                                             C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\nu_instant_search_ebeb5baa[1].js
   Opens:
                                             C:\WINDOWS\system32\setupapi.dll
   Opens:
                                             C:\Documents and Settings
   Opens:
                                             C:\Documents and Settings\Admin\Local Settings
                                             C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
   Opens:
                                             C:\Documents and Settings\Admin\Local
   Opens
Settings\History\History.IE5\MSHist012014033120140407
                                             C:\Documents and Settings\Admin\Local
Settings \verb|\History\History\IE5\MSHist012014033120140407\verb|\Lindex.dat| \\
                                             C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
                                             C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                                             C:\Documents and Settings\Admin\Local
   Opens:
Settings\History\History.IE5\MSHist012016040820160409
                                             C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016040820160409\index.dat
   Opens:
                                             {\tt C:\DOCUME$^1\Admin\LOCALS$^1$ Temp\httpwww.baidu.comfavicon.ico}
   Opens:
                                             C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\bdsug_async_1cb857eb[1].js
   Opens:
                                             C:\WINDOWS
   Opens:
                                             C:\WINDOWS\svstem32
   Opens:
                                             C:\WINDOWS\system32\msxml3.dll
   Opens:
                                             C:\WINDOWS\system32\msxml3r.dll
                                             {\tt C:\WINDOWS\system32\actxprxy.dll}
   Opens:
                                             C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\UH4D6D6X\favicon[1].ico
   Opens:
                                             C:\Documents and Settings\Admin\Local Settings\Temp
                                             C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\UH4D6D6X\env_beb83b45[1].swf
                                             C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Opens:
Explorer\UserData
  Opens:
                                             C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\BORP04R6
                                             C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Opens:
Explorer\UserData\DI4SV2D0
   Opens:
                                             C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\W9PUTXLL
                                             C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Opens:
Explorer\UserData\8N45SSPX
                                            C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Opens:
Explorer\UserData\index.dat
   Opens:
                                             C:\WINDOWS\system32\schannel.dll
                                             C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Opens
Player\#SharedObjects
   Opens:
                                             C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
                                             C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Opens
Player\#SharedObjects\45PY3TTW\macromedia.com\support\flashplayer\sys\settings.sol
                                             C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Opens:
Player\#SharedObjects\45PY3TTW\macromedia.com\support\flashplayer\sys\
                                             {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
   Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sol
                                             C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Opens:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sol
   Opens:
                                             C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\
   Opens:
                                             {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
   Opens:
                                             {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\s1.bdstatic.com\
   Opens:
                                             C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\baiduia_b45d552b[1].js
   Opens:
                                             {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
{\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
  Opens:
Player\*Shared0bjects\*45PY3TTW\*macromedia.com\*support\*flashplayer\*sys\*s1.bdstatic.com\*support\*flashplayer\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*sys\*s1.bdstatic.com\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*support\*s
   Opens:
                                             {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player \verb|\macromedia.com| support \verb|\flashplayer| sys \verb|\macromedia.com| settings.sol| and the support \verb|\macromedia.com| settings| settings|
                                             {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
   Opens:
```

```
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
    Opens:
                                                       C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
{\tt Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com}
   Opens:
                                                      {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\macromedia.com\support\flashplayer\sys
    Opens:
                                                       C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer
   Opens:
                                                      {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
{\tt Player} \\ {\tt macromedia.com} \\ {\tt support} \\ {\tt flashplayer} \\ {\tt sys} \\ {\tt \#s1.bdstatic.com} \\ {\tt settings.sxx} \\ {\tt sxx} \\ {\tt macromedia.com} \\ {\tt static.com} \\ {\tt stati
                                                      {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
   Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                                                      {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
   Opens:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com
                                                      {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
   Opens:
Player\#SharedObjects\45PY3TTW
                                                      C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Opens:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                                      C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Opens:
Explorer\UserData\BQRP04R6\userDataBIDUPSID[1].xml
                                                      C:\Documents and Settings\Admin\Local
   Opens:
Settings\Temp\httpwww.baidu.comfavicon.ico
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Opens:
Files\Content.IE5\CXCXW1MR\JSocket_9a52fc3e[1].swf
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\ONWV4FIP\o_0108[1].swf
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Opens:
Files\Content.IE5\CXCXW1MR\wb[1].gif
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Opens:
Files\Content.IE5\QXMNQBKF\wb[1].gif
                                                       C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Opens:
Files\Content.IE5\ONWV4FIP\wb[1].gif
    Opens:
                                                      C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroPDF.dll
                                                      C:\Program Files\Common
    Opens:
Files\Adobe\Acrobat\ActiveX\AcroPDF.dll.2.Manifest
                                                      C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroPDF.dll.2.Config
    Opens:
    Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcp80.dll
    Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcr80.dll
   Opens:
                                                      C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
{\tt Explorer \ VarData \ DI4SV2D0 \ oXMLStore[1].xml}
    Opens:
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\wb[1].gif
    Opens:
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\wb[2].gif
   Opens:
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\wb[2].gif
   Opens:
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\wb[2].gif
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\CXCXW1MR\wb[3].gif
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\QXMNQBKF\wb[2].gif
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\ONWV4FIP\wb[31.gif
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\UH4D6D6X\wb[3].gif
    Writes to:
                                                      C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt
    Writes to:
                                                      C:\Documents and Settings\Admin\Cookies\admin@baidu[2].txt
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Writes to:
Files\Content.IE5\QXMNQBKF\index[1].php
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Writes to:
Files\Content.IE5\CXCXW1MR\jquery-1.10.2.min_f2fb5194[1].js
    Writes to:
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\baidu_jgylogo3[1].gif
    Writes to:
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\nuomi_510f7472[1].png
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Writes to:
Files\Content.IE5\CXCXW1MR\zbios_62c636fe[1].png
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Writes to:
Files\Content.IE5\QXMNQBKF\icons_0e814c16[1].png
                                                       C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Writes to:
Files\Content.IE5\UH4D6D6X\s[1].txt
                                                       C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Writes to:
Files\Content.IE5\CXCXW1MR\bd_logo1[1].png
    Writes to:
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\u=3070482661,4157819617&fm=96[1].jpg
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Writes to:
Files\Content.IE5\ONWV4FIP\u=3925724364,2158606337&fm=58&s=7F84AA0AB5A46F111452CD6403007033[1].jpg
    Writes to:
                                                       {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\ONWV4FIP\u=4247961311,3377350606&fm=58[1].jpg
                                                       C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Writes to:
Files \verb|\Content.IE5\verb|\ONWV4FIP\\| 1c5d7b26-f3f0-4dd7-a025-8c79809 fecac[1].js \\
    Writes to:
                                                      {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files \verb|\content.1E5| UH4D6D6X \verb|\u=3520324766|, 1135887067\&fm=96\&s=19843C7AF9FF569A5DF5E0D7030090E2[1].jpg | A content.1E5 
                                                      {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
    Writes to:
Files\Content.IE5\UH4D6D6X\u=3776762194,2342817517&fm=96&s=1B0AA64416B6966D4A9714070300E0CB[1].jpg
    Writes to:
                                                      {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files \\ Content. \\ IE5 \\ UH4D6D6X \\ u=3227862542 \\ ,40588234 \\ \bar{e}28 \\ fm=58 \\ \&s=80327E97D8B101801D3083750300C066 \\ [1]. \\ jpg=1.00 \\ jpg=1
                                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
    Writes to:
```

```
Files\Content.IE5\CXCXW1MR\u=2683104694,419579517&fm=96&s=F580F1115AF81F86383184D60300E0B2[1].jpg
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\u=3610240597,3088990761&fm=58[1].jpg
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|| Content.IE5| CXCXW1MR \verb|| u=3734835402, 589306938\&fm=96\&s=29A8279E5583C6E012D5B5F40300E078[1].jpg || u=3734835402, u=37348362, u=373482402, u=373482402,
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\u=1931034822,3220545467&fm=58[1].jpg
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Writes to:
Files\Content.IE5\QXMNQBKF\u=1266350913,3659364910&fm=96&s=71B11CD1CCA3B84B50295D2D03007040[1].jpg
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\9a504fc2d5628535e75664d992ef76c6a6ef6397[1].jpg
                                   {\tt C:\Documents\ and\ Settings\backslash Admin\backslash Local\ Settings\backslash Temporary\ Internet}
  Writes to:
Files\Content.IE5\QXMNQBKF\every_cookie_aa168cb4[1].js
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\all_async_search_d0d1b2ec[1].js
                                   C:\Documents and Settings\Admin\Local Settings\Application
  Writes to:
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T\www.baidu[1].xml
                                   C:\Documents and Settings\Admin\Cookies\admin@www.baidu[1].txt
  Writes to:
                                   C:\Documents and Settings\Admin\Cookies\admin@www.baidu[2].txt
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Writes to:
Files\Content.IE5\UH4D6D6X\nu_instant_search_ebeb5baa[1].js
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Writes to:
Files\Content.IE5\CXCXW1MR\quickdelete_9c14b01a[1].png
  Writes to:
                                   C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016040820160409\index.dat
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\bdsug_async_1cb857eb[1].js
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\env_beb83b45[1].swf
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\favicon[1].ico
                                   C:\Documents and Settings\Admin\Local
Settings\Temp\httpwww.baidu.comfavicon.ico
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
Explorer\UserData\index.dat
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\baiduia_b45d552b[1].js
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
  Writes to:
Writes to:
                                   C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Writes to:
                                   C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Writes to:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\BQRP04R6\userDataBIDUPSID[1].xml
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\JSocket_9a52fc3e[1].swf
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ielib_0108[1].js
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Writes to:
Files\Content.IE5\ONWV4FIP\o_0108[1].swf
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Writes to:
Explorer\UserData\DI4SV2D0\oXMLStore[1].xml
  Writes to:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ps_fp[1].htm
                                   C:\WINDOWS\Registration\R00000000007.clb
  Reads from:
  Reads from:
C:\WINDOWS\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                   C:\AUTOEXEC.BAT
  Reads from:
  Reads from:
                                   C:\WINDOWS\system32\drivers\etc\hosts
  Reads from:
                                   C:\WINDOWS\system32\rsaenh.dll
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\jquery-1.10.2.min_f2fb5194[1].js
                                   C:\WINDOWS\win.ini
  Reads from:
                                   C:\WINDOWS\system32\dxtmsft.dll
  Reads from:
  Reads from:
                                   C:\WINDOWS\system32\dxtrans.dll
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\icons_0e814c16[1].png
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\1c5d7b26-f3f0-4dd7-a025-8c79809fecac[1].js
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\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:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\all_async_search_d0d1b2ec[1].js
                                   C:\WINDOWS\system32\mshtml.tlb
  Reads from:
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\Content.IE5\UH4D6D6X\nu_instant_search_ebeb5baa[1].js
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\bdsug_async_1cb857eb[1].js
  Reads from:
                                   C:\WINDOWS\system32\ieframe.dll
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\favicon[1].ico
  Reads from:
                                   {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\UH4D6D6X\env_beb83b45[1].swf
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
  Reads from:
Player\macromedia.com\support\flashplayer\sys\settings.sol
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
  Reads from:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Reads from:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\CXCXW1MR\baiduia_b45d552b[1].js
                                                     {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
   Reads from:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
   Reads from:
                                                     C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\CONTENT.IE5| CXCXW1MR \verb|\JSocket_9a52fc3e[1].swf|
   Reads from:
                                                     C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\Content.IE5| ONWV4FIP \verb|\o_0108[1].swf| \\
   Reads from:
                                                     {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
Explorer\UserData\DI4SV2D0\oXMLStore[1].xml
                                                     C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt
   Deletes:
   Deletes:
                                                     C:\Documents and Settings\Admin\Cookies\admin@baidu[2].txt
                                                     {\tt C:\Documents\ and\ Settings\Admin\Cookies\admin@www.baidu[1].txt}
   Deletes:
                                                     {\tt C:\Documents\ and\ Settings\Admin\Cookies\admin@www.baidu[2].txt}
   Deletes:
                                                     C:\Documents and Settings\Admin\Local
   Deletes:
Settings \verb|\History\History\IE5\MSHist012014033120140407\verb|\Lindex.dat| \\
   Deletes:
                                                     C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
                                                     C:\Documents and Settings\Admin\Local
   Deletes:
Settings \verb|\History\History.IE5\MSHist012014041220140413 \verb|\Lindex.dat|| at the setting and 
                                                     C:\Documents and Settings\Admin\Local
   Deletes:
Settings\History\History.IE5\MSHist012014041220140413
                                                     C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Deletes:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
   Deletes:
                                                     C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
   Deletes:
                                                     C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
   Deletes:
                                                     C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
Network Events
   DNS query:
                                                     www.baidu.com
   DNS query:
                                                     s1.bdstatic.com
   DNS query:
                                                     t10.baidu.com
```

```
DNS query:
                         t12.baidu.com
DNS query:
                         ecmb.bdimg.com
DNS query:
                         i9.baidu.com
DNS query:
                         t11.baidu.com
                         imgsrc.baidu.com
DNS query:
DNS query:
                         i7.baidu.com
                         i8.baidu.com
DNS query:
DNS query:
                         sclick.baidu.com
DNS guery:
                         c.baidu.com
                         sestat.baidu.com
DNS guery:
DNS guery:
                         formi.baidu.com
                         eclick.baidu.com
DNS query:
                         www.a.shifen.com ⇒ 14.215.177.38
DNS response:
DNS response:
                         www.a.shifen.com ⇒ 14.215.177.37
DNS response:
                         wwwbaidu.jomodns.com ⇒ 119.146.74.40
                         t1.n.shifen.com ⇒ 180.97.33.30
bcs.jomodns.com ⇒ 180.97.66.39
DNS response:
DNS response:
DNS response:
                         hiphotos.jomodns.com ⇒ 59.38.112.48
DNS response:
                         c.e.shifen.com ⇒ 123.125.114.64
DNS response:
                         s.a.shifen.com ⇒ 123.125.115.95
DNS response:
                         sestat.a.shifen.com ⇒ 14.215.177.176
                         formi.baidu.com ⇒ 61.135.169.120
DNS response:
                         formi.baidu.com ⇒ 180.149.131.55
DNS response:
DNS response:
                         eclick.e.shifen.com ⇒ 123.125.115.164
                         127.0.0.1:1040
Connects to:
Connects to:
                          14.215.177.38:80
Connects to:
                         119.146.74.40:80
Connects to:
                         180.97.33.30:80
Connects to:
                         180.97.66.39:80
Connects to:
                         59.38.112.48:80
Connects to:
                         123.125.114.64:80
Connects to:
                         123.125.115.95:80
Connects to:
                         14.215.177.176:80
Connects to:
                         61.135.169.120:843
Connects to:
                         123.125.115.164:80
Connects to:
                         61.135.169.120:8843
Connects to:
                         180.149.131.55:843
Sends data to:
                         8.8.8.8:53
Sends data to:
                         127.0.0.1:1040
                         www.a.shifen.com:80 (14.215.177.38)
Sends data to:
Sends data to:
                         wwwbaidu.jomodns.com:80 (119.146.74.40)
Sends data to:
                         bcs.jomodns.com:80 (180.97.66.39)
                         t1.n.shifen.com:80 (180.97.33.30)
Sends data to:
Sends data to:
                         hiphotos.jomodns.com:80 (59.38.112.48)
                         c.e.shifen.com:80 (123.125.114.64)
Sends data to:
                         s.a.shifen.com:80 (123.125.115.95)
Sends data to:
Sends data to:
                         sestat.a.shifen.com:80 (14.215.177.176)
                         eclick.e.shifen.com:80 (123.125.115.164)
Sends data to:
Receives data from:
                         0.0.0.0:0
                         127.0.0.1:1040
Receives data from:
Receives data from:
                         www.a.shifen.com:80 (14.215.177.38)
Receives data from:
                         wwwbaidu.jomodns.com:80 (119.146.74.40)
Receives data from:
                         t1.n.shifen.com:80 (180.97.33.30)
                         bcs.jomodns.com:80 (180.97.66.39)
Receives data from:
Receives data from:
                         hiphotos.jomodns.com:80 (59.38.112.48)
Receives data from:
                         c.e.shifen.com:80 (123.125.114.64)
Receives data from:
                         s.a.shifen.com:80 (123.125.115.95)
Receives data from:
                         sestat.a.shifen.com:80 (14.215.177.176)
Receives data from:
                         eclick.e.shifen.com:80 (123.125.115.164)
```

# Windows Registry Events

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_scripturl\_mitigation Creates key: HKCU\software\explore Creates key:  $\label{thm:condition} \begin{tabular}{ll} HKLM \end{tabular} icrosoft \end{tabular} icros$ Creates key:  $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ shell extensions \verb+ blocked | \\$ Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached Creates key: HKCU\software\microsoft\windows\currentversion\internet settings Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders. Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Creates key: HKLM\software\microsoft\tracing Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders HKCU\software\microsoft\windows nt\currentversion\winlogon Creates key: Creates kev: HKLM\software\microsoft\windows\currentversion\explorer\shell folders Creates kev: HKCU\software\microsoft\windows\currentversion\internet settings\connections Creates kev: HKCU\software\microsoft\windows\currentversion\explorer\runmru HKCU\software\microsoft\internet explorer\typedurls Creates key: Creates key HKCU\software\microsoft\windows nt\currentversion\network\location awareness Creates key HKLM\svstem\currentcontrolset\services\tcpip\parameters Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p\history Creates key: HKCU\software\microsoft\windows script\settings Creates key: HKLM\software\microsoft\directdraw\mostrecentapplication Creates key: HKLM\software\microsoft\direct3d\mostrecentapplication Creates key:  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e3-12e4\} \\ 1 \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \\ 3 \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \\ 4 \setminus \{f90255c2-6bc4-12e4\} \\ 4$ 806d6172696f}\ Creates kev: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016040820160409 Creates key: HKCU\software\microsoft\internet explorer\main\windowssearch HKLM\software\microsoft\downloadmanager Creates key: Creates key: HKCU\software\microsoft\internet explorer\domstorage\total HKCU\software\microsoft\internet explorer\domstorage\baidu.com Creates key: Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata Creates key: HKCU\software\macromedia\flashplayer  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet$ Deletes value: settings[proxyserver] Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride] Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl] Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus side by side \setminus assembly storage roots$ Opens key: HKLM\svstem\currentcontrolset\control\safeboot\option Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll Opens kev: HKLM\svstem\currentcontrolset\control\session manager Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll . Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll Opens key:  $\label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution$ options\oleaut32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msimg32.dll Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ options\iertutil.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll

```
Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
   Opens key:
                                                         HKLM\system\currentcontrolset\control\error message instrument\
   Opens key:
                                                         \label{lem:hklm} \verb+Kklm \ system \ current control \ set \ \ control \ \ \ \ message \ instrument
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\gre_initialize
   Opens kev:
                                                         HKLM\software\microsoft\windows nt\currentversion\compatibility32
                                                         HKLM\software\microsoft\windows nt\currentversion\ime compatibility
   Opens key:
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\windows
                                                         \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ winlogon
   Opens key:
   Opens key:
                                                         HKLM\
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\diagnostics
                                                         HKLM\software\microsoft\ole
   Opens kev:
   Opens kev:
                                                         HKCR\interface
                                                         HKCR\interface\{00020400-0000-0000-c000-00000000046}
   Opens kev:
   Opens kev:
                                                         HKLM\software\microsoft\windows\currentversion\explorer\performance
   Opens key:
                                                         HKLM\system\setup
   Opens key:
                                                         HKCU\
   Opens key:
                                                         HKCU\software\policies\microsoft\control panel\desktop
   Opens key:
                                                         HKCU\control panel\desktop
   Opens key:
                                                         HKLM\software\microsoft\oleaut
   Opens key:
                                                         HKLM\software\microsoft\oleaut\userera
   Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\languagepack
   Opens key:
                                                         HKCU\software\classes\
   Opens key:
                                                         HKCU\software\classes\protocols\name-space handler\
   Opens key:
                                                         HKCR\protocols\name-space handler
                                                         HKCU\software\classes\protocols\name-space handler
   Opens kev:
   Opens key:
                                                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings
   Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\internet settings
   Opens key:
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings
   Opens key:
                                                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
   Opens key:
                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
   Opens key:
                                                         settings\
   Opens key:
                                                         \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ internet\ explorer\+ main\+ feature control
   Opens key:
                                                         HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
   Opens key:
                                                         HKLM\software\microsoft\internet explorer\main\featurecontrol
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\main\featurecontrol
   Opens key:
                                                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
   Opens key:
                                                         HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915
                                                         \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\zonemap\domains\
                                                         \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Software \begin{tabular}{ll} policies \end{tabular} in the constant \begin
   Opens key:
settings\zonemap\domains\
                                                         \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} software \begin{tabular}{ll} policies \end{tabular} in the constant \begin
   Opens key:
settings\zonemap\ranges\
                                                         HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\ranges\
   Opens kev:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                                         HKLM\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_unc_savedfilecheck
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\main
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
   Opens key:
HKL\dot{M} \setminus software \\ \setminus microsoft \\ \setminus ctf \\ \setminus compatibility \\ \setminus 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exee
   Opens key:
                                                         HKLM\software\microsoft\ctf\systemshared\
   Opens kev:
                                                         HKCU\keyboard layout\toggle
   Opens key:
                                                         HKLM\software\microsoft\ctf\
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
   Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\thememanager
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\imm
                                                         HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens key:
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
   Opens key:
                                                         HKCU\software\microsoft\ctf
   Opens key:
                                                         {\tt HKLM \backslash software \backslash microsoft \backslash ctf \backslash systems hared}
   Opens key:
                                                         \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the constr
   Opens key:
                                                         HKCU\software\explore
   Opens key:
                                                         HKLM\software\microsoft\com3
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
   Opens key:
                                                         \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\clbcatq.dll
   Opens key:
                                                         HKLM\software\microsoft\com3\debug
   Opens key:
                                                         HKLM\software\classes
   Opens key:
                                                         HKU\
                                                         HKCR\clsid
   Opens key:
                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
   Opens key:
                                                         HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
   Opens key:
   Opens key:
                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
```

00c04fd705a2}\treatas

```
Opens key:
                                               HKCR \ clsid \ \{8856f961-340a-11d0-a96b-00c04fd705a2\} \ treat as
   Opens key:
                                               HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
   Opens key:
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
   Opens key:
                                               HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b
00c04fd705a2}\inprocserverx86
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86
   Opens key:
   Opens key:
                                               HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver32
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32
   Opens kev:
                                               HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens kev:
00c04fd705a2}\inprochandler32
   Opens key:
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
                                               HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens key:
00c04fd705a2}\inprochandlerx86
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
   Opens kev:
                                               HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens kev:
00c04fd705a2}\localserver
   Opens kev:
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ieframe.dll
   Opens key:
                                               HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
   Opens key:
                                               HKLM\software\microsoft\internet explorer\setup
   Opens key:
                                               HKLM\system\currentcontrolset\control\wmi\security
   Opens key:
                                               HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-
0000c05bae0b}\typelib
   Opens key:
                                                HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
   Opens key:
                                               HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
   Opens key:
                                               HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
   Opens key:
                                               HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-
00aa00404770}\proxystubclsid32
   Opens key:
                                               HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
                                               HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-
   Opens key
00aa004ba90b}\proxystubclsid32
                                               HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32
   Opens key:
   Opens key:
                                               HKCU\software\classes\interface\{000214e6-0000-0000-c000-
00000000046}\proxystubclsid32
                                               Opens key:
   Opens key:
                                               HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-
00c04f79abd1}\proxystubclsid32
   Opens key:
                                               HKCR \verb|\interface| \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \verb|\proxystubclsid32| \} |
   Opens key:
                                               HKLM\software\microsoft\rpc\pagedbuffers
   Opens key:
                                               HKLM\software\microsoft\rpc
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe\rpcthreadpoolthrottle
   Opens key:
                                               HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                               HKLM\system\currentcontrolset\control\computername
   Opens key:
                                               Opens key:
                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{889d2feb-5411-4565-8998-1dd2c5261283\}
                                               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 kev:
                                               HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
   Opens key:
                                               HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet settings
   Opens key:
                                               HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature http username password disable
                                               HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
                                               HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
   Opens key:
                                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature allow reverse solidus in userinfo kb932562
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:
                                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
   Opens key:
                                               HKCU\software\microsoft\internet explorer\ietld
   Opens kev:
                                                HKLM\software\microsoft\internet explorer\main
   Opens key:
                                               HKLM\software\policies\microsoft\internet explorer\main
   Opens key:
                                                HKCU\software\policies\microsoft\internet explorer\main
   Opens key:
                                               \textbf{HKLM} \\ \textbf{software} \\ \dot{\textbf{microsoft}} \\ \textbf{windows} \\ \textbf{currentversion} \\ \textbf{policies} \\ \textbf{explorent policies} \\ \textbf{explorent
   Opens kev:
                                               HKCU\software\microsoft\windows\currentversion\policies\explorer
   Opens kev:
a2ea-08002b30309d}
                                               HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
   Opens key:
08002b30309d}\inprocserver32
   Opens key:
                                               \label{local-eq:hkcr} $$HKCR\clsid{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32$
   Opens key:
                                               \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\apphelp.dll
   Opens key:
                                               HKLM\system\currentcontrolset\control\session manager\appcompatibility
   Opens key:
                                               HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
   Opens key:
                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
   Opens key
                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{871c5380-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-420-a2ea-420-420-420-420-420-420-420-420-42
```

08002b30309d}\treatas

HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86

Opens kev:

HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86

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

08002b30309d}\localserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32

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}\inprochandlerx86
 Opens key:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86
 Opens key
                          HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\localserver
 Opens key:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
                          HKLM\software\microsoft\internet
 Opens key:
\dot{\text{explorer}} \\ \dot{\text{main}} \\ \text{featurecontrol} \\ \text{feature\_iedde\_register\_protocol}
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
 Opens kev:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
 Opens kev:
                          HKLM\software\policies
 Opens kev:
                          HKCU\software\policies
 Opens key:
                          HKCU\software
 Opens key:
                          HKLM\software
                          HKLM\software\policies\microsoft\internet explorer
 Opens key:
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\content
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\content
 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:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
                          \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
 Opens key:
settings\5.0\cache\extensible cache\feedplat
                          \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
 Opens key:
settings\5.0\cache\extensible cache\iecompat
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
 Opens key
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
 Opens kev:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
                          HKCU\software\microsoft\internet
 Opens kev:
\verb|explorer\main\featurecontrol\retry_header on ly post\_on connection reset|\\
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry headeronlypost onconnectionreset
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature bufferbreaking 818408
 Opens kev:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature skip post retry on internetwritefile kb895954
                          HKLM\software\microsoft\internet
 Opens key:
explorer\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
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens kev:
                          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
                          HKCU\software\microsoft\internet
 Opens key:
\verb|explorer| \verb|main| featurecontrol| feature_use\_spn\_for\_ntlm_auth\_disabled| \\
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                          HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names| \\
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                          HKCU\software\microsoft\internet
explorer \verb|\main\feature| on trol\feature\_disable\_unicode\_handle\_closing\_callback
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
```

HKCU\software\microsoft\internet

Opens key:

```
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                    HKLM\software\microsoft\internet
 Opens key:
\verb|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 kev:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
                    HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens kev:
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\00000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries
 Opens key:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000003
 Opens key:
Opens key:
Opens kev:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000000
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries
 Opens key:
Opens key:
Opens key:
Opens key:
                    HKCU\software\microsoft\windows\currentversion\internet settings\wpad
                    HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature return failed connect content kb942615
 Opens key:
                   HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_return_failed_connect_content_kb942615|
 Opens kev:
                    HKLM\software\policies\microsoft\internet explorer\browseremulation
 Opens kev:
                    HKCU\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
                    HKLM\software\microsoft\internet explorer\mediatypeclass
 Opens key:
                    HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
                    HKLM\software\microsoft\windows\currentversion\policies\ratings
 Opens key:
 Opens key:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                    HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens kev:
                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                    HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\ranges\
 Opens key:
                    \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings\zonemap\protocoldefaults\
 Opens key:
                    \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings\zonemap\domains\
 Opens key:
                    HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap\domains\msn.com
 Opens key:
                    \label{lem:hklm} \verb+ Kklm \+ software \+ microsoft \+ windows \+ current version \+ internet
settings\zonemap\domains\msn.com\related
 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
```

HKCU\software\microsoft\windows\currentversion\internet settings\zones\4

Opens key:

```
Opens key:
                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
   Opens key:
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
   Opens key:
                                                             \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\0
   Opens key:
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
   Opens key:
                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\1
   Opens key:
                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\2
                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\3
   Opens key:
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
   Opens key:
                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
   Opens kev:
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
   Opens key:
                                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
    Opens key:
                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
    Opens kev:
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                             HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\lockdown_zones\
                                                             HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\lockdown zones\0
                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\lockdown_zones\0
    Opens key:
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                             \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
    Opens key:
settings\lockdown_zones\1
    Opens key:
                                                             \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\1
    Opens key:
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                                             HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
    Opens key:
                                                             \label{lem:hklmsoftware policies microsoft windows \current version \ internet \\
{\tt settings \lockdown\_zones \label{lockdown} 2}
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
                                                             HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\3
                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\3
                                                             \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \colongorder \part 
   Opens kev:
settings\lockdown_zones\3
                                                             HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown zones\4
                                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} policies \end{tabular} irror of the local hammon \end{tabular} irror of the local hammon \end{tabular} and the local hammon \end{tabular} irror of the
   Opens kev:
settings\lockdown_zones\4
                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown zones\4
                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\netapi32.dll
   Opens key:
                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
    Opens key:
                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
    Opens key:
                                                             \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\winmm.dll
    Opens key:
                                                             HKLM\software\microsoft\windows nt\currentversion\drivers32
    Opens kev:
\label{lem:hklm} \verb+KLM\+ system \land current control \verb+ we diaproperties \verb+ private properties \verb+ joystick \verb+ winmm+ in the properties \verb+ private propertie
                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\tapi32.dll
    Opens key:
                                                             HKLM\software\microsoft\windows\currentversion\telephony
    Opens key:
                                                             \label{lem:hklmsoftware} \mbox{\tt HKLM} \mbox{\tt software} \mbox{\tt microsoft} \mbox{\tt windows nt} \mbox{\tt currentversion} \mbox{\tt image file execution}
options\rasapi32.dll
                                                             HKLM\software\microsoft\tracing\rasapi32
    Opens key:
    Opens key:
                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
    Opens key:
                                                             {\tt HKLM \ } system \verb|\  current control set \verb|\  control \ | product options
    Opens key:
                                                             \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+user\ shell
folders
    Opens key:
                                                             HKLM\software\policies\microsoft\windows\system
    Opens key:
                                                             HKLM\software\microsoft\windows nt\currentversion\profilelist
    Opens key:
                                                             HKLM\system\currentcontrolset\control\session manager\environment
    Opens key:
                                                             HKLM\software\microsoft\windows\currentversion
    Opens key:
                                                             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
    Opens key:
                                                             HKCU\environment
    Opens key:
                                                             HKCU\volatile environment
```

```
Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sensapi.dll
  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
                                             \label{lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem
  Opens key:
  Opens key:
                                             HKCR\protocols\name-space handler\http
  Opens key:
                                             HKCU\software\classes\protocols\name-space handler\*\
                                             HKCR\protocols\name-space handler\*
  Opens key:
  Opens key:
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens kev:
                                             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\microsoft\windows\currentversion\internet settings\user
agent\ua tokens
  Opens key:
                                             HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\pre platform
  Opens key:
                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ 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
                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\5.0\user agent\post platform
                                             HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\user agent\post platform
  Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
                                             HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
  Opens key:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
  Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
  Opens key:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
  Opens key:
                                             HKCU\software\microsoft\windows\currentversion\urlmon settings
  Opens kev:
                                             HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
```

filters\rpa

 $Opens\ key: \\ HKLM\software\microsoft\windows\currentversion\internet\ settings\http$ 

filters\rpa

Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209
Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mswsock.dll

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mlang.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\hnetcfg.dll

Opens key: HKLM\software\microsoft\rpc\securityservice

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_legacy\_compression Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_legacy\_compression

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

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

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

00c04fd7d062}\treatas

 $\label{lem:openskey: HKCR clsid {00bb2765-6a77-11d0-a535-00c04fd7d062} $$ Opens key: $$ 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}\inprocserverx86

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserverx86

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

00c04fd7d062}\localserver32

 $Opens~key: \\ HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver 32$ 

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}\inprochandlerx86
 Opens key:
                          HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
                          HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
 Opens key
00c04fd7d062}\localserver
 Opens key:
                          HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\browseui.dll
                          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 key
9fe3c77a297a}\treatas
                          HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas
 Opens key:
                          HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
 Opens kev:
9fe3c77a297a}\inprocserver32
                          HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32
 Opens kev:
                          HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
 Opens key
9fe3c77a297a}\inprocserverx86
                          HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserverx86
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\localserver32
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\localserver32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler32
 Opens key:
                          HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\nprochandler32
 Opens key:
                          HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9
9fe3c77a297a}\inprochandlerx86
 Opens key:
                          HKCR \verb|\clsid|{6935db93-21e8-4ccc-beb9-9fe3c77a297a} \verb|\inprochandlerx86|
                          HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
 Opens kev:
9fe3c77a297a}\localserver
                          HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\localserver
 Opens key:
                          HKCU \setminus software \setminus classes \setminus clsid \setminus \{00bb2764-6a77-11d0-a535-00c04fd7d062\}
 Opens key:
 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\} \ treat as
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
                          HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\clserver32
 Opens key:
 Opens key
                          HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserverx86
 Opens key:
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
 Opens key:
                          HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\localserver32
                          HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\localserver32
 Opens key:
 Opens key
                          HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
                          HKCR \ clsid \ \ \{00bb2764-6a77-11d0-a535-00c04fd7d062\} \ \ in prochandler 32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandlerx86
                          HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
 Opens key:
                          HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
 Opens kev:
00c04fd7d062}\localserver
                          HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\localserver
 Opens key:
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
 Opens key:
                          HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
 Opens key:
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
 Opens kev:
00c04fd7d062}\treatas
                          HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
                          HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserverx86
 Opens key:
                         HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
 Opens kev:
00c04fd7d062}\localserver32
                          HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32
 Opens key:
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
 Opens key:
00c04fd7d062}\inprochandler32
                          HKCR \ clsid \ \ \{00bb2763-6a77-11d0-a535-00c04fd7d062\} \ \ in prochandler 32
 Opens key:
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
 Opens key
00c04fd7d062}\inprochandlerx86
                          \label{lem:hkcr} $$HKCR\clsid_{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx 86$
 Opens key:
                          HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
 Opens key
00c04fd7d062}\localserver
 Opens key:
                          HKCR \ clsid \ \ \{00bb2763-6a77-11d0-a535-00c04fd7d062\} \ \ localserver
 Opens key:
                          00aa005b4383}\inprocserver32
 Opens key:
                          HKCR \ clsid \ \{03c036f1-a186-11d0-824a-00aa005b4383\} \ inprocserver 32
 Opens key:
                          HKLM \verb|\software\m| icrosoft \verb|\windows\currentversion\explorer\advanced|
 Opens key:
                          {\tt HKLM \backslash system \backslash current control \backslash security providers}
 Opens key:
                          Opens key:
                          \label{lem:hklm} \verb+Kklm \+ system \+ control \+ lsa \+ spicache \+ msaps spc.dll
 Opens key:
                          \label{lem:hklm} \verb+Kklm \+ system \+ control \+ lsa \+ spicache \+ digest. dll
 Opens key:
                          Opens key:
                          HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
 Opens key:
                          {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip \verb|\ linkage \\
 Opens key:
                          HKLM\system\currentcontrolset\services\tcpip\parameters\
                          \label{lem:hklmsystem} \verb|HKLM\system\currentcontrolset\services\netbt\parameters\neters\\|
 Opens key:
```

```
Opens key:
                          HKLM\system\currentcontrolset\services\netbt\parameters
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
 Opens key:
                         HKLM\svstem\currentcontrolset\services\dnscache\parameters
 Opens key:
                         HKLM\software\policies\microsoft\windows nt\dnsclient
                         \label{lem:hklm} {\sf HKLM} \\ \verb|\system| \\ current control set \\ \verb|\services| \\ tcpip \\ \verb|\parameters| \\
 Opens kev:
 Opens kev:
c7d49d7cecdc}
 Opens key:
                         HKLM\software\policies\microsoft\system\dnsclient
 Opens kev:
                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
 Opens kev:
                         HKLM\software\policies\microsoft\cryptography
                         HKLM\software\microsoft\cryptography
 Opens key:
 Opens key:
                         HKLM\software\microsoft\cryptography\offload
 Opens key:
                          HKCU\software\microsoft\ctf\langbaraddin\
 Opens key:
                         HKLM\software\microsoft\ctf\langbaraddin\
 Opens key:
                         HKCU\software\microsoft\internet explorer\ietld\lowmic
 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:
                         HKCR\mime\database\content type\text/html; charset=utf-8
 Opens key:
                          HKCU\software\classes\mime\database\content type\text/html
 Opens key:
                         HKCR\mime\database\content type\text/html
 Opens key:
                         HKCU\software\classes\protocols\filter\text/html; charset=utf-8
 Opens key:
                         HKCR\protocols\filter\text/html; charset=utf-8
                         HKCU\software\classes\protocols\filter\text/html
 Opens key:
 Opens key:
                         HKCR\protocols\filter\text/html
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
 Opens key
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{25336920-03f9-11cf-8fd0-00aa00686f13\}
 Opens key:
 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 key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens kev:
00aa00686f13}\inprocserver32
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key
00aa00686f13}\inprocserverx86
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
 Opens key:
 Opens kev:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver32
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandlerx86
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
 Opens key:
 Opens key:
                         \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\msls31.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mshtml.dll
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
                         HKLM\software\microsoft\internet
 Opens key
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 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
\verb|explorer|| \verb|main|| feature control|| feature legacy_dispparams||
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKLM\software\microsoft\internet
```

 $\verb|explorer\main\featurecontrol\feature_private_font_setting| \\$ 

```
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
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:
                                   HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_allow\_expanduri\_by pass|
  Opens kev:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                                   HKLM\software\microsoft\internet
  Opens kev:
\verb|explorer\main\featurecontrol\feature_body_size_in\_editable\_iframe\_kb943245| \\
                                   HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_databinding_support
  Opens kev:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens kev:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_object_caching
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  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
                                    \label{lem:hklm} \begin{tabular}{ll} HKLM\software\mbox{\sc urrentversion\app paths\outlook.exe} \\ \end{tabular}
  Opens key:
  Opens kev:
                                    {\tt HKLM \setminus software \setminus microsoft \setminus internet\ explorer \setminus application\ compatibility}
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\domstorage
                                    HKCU\software\microsoft\internet explorer\domstorage
  Opens key:
                                    HKLM\software\microsoft\internet explorer\domstorage
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\safetv\privacie
  Opens kev:
                                    HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens kev:
                                    HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature manage script circular refs
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature manage script circular refs
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:
                                   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 kev:
                                    HKCU\software\classes\protocols\name-space handler\about\
  Opens key:
                                    HKCR\protocols\name-space handler\about
  Opens key:
                                    HKCU\software\classes\protocols\handler\about
  Opens key:
                                    HKCR\protocols\handler\about
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens kev:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens kev
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\treatas
                                    HKCR \verb|\clsid|{3050f406-98b5-11cf-bb82-00aa00bdce0b} \verb|\treatas|
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\tinprocserver32
  Opens key
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
  Opens key:
                                   HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
  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}\localserver32
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
                                    HKCR \verb|\clsid|{3050f406-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprochandler32|
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandlerx86
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver
```

```
Opens key:
                         HKCR \clsid \ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \localserver
 Opens key:
                         HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_document_compatible_mode|\\
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
                         HKLM\software\policies\microsoft\internet explorer\zoom
 Opens key:
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\zoom
 Opens key:
                         HKCU\software\microsoft\internet explorer\zoom
                         HKLM\software\microsoft\internet explorer\zoom
 Opens kev:
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_weboc_document_zoom
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature weboc document zoom
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens kev:
00aa00686f13}\progid
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
 Opens kev:
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet settings\url
history
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer
                         HKLM\software\policies\microsoft\internet explorer\international\scripts
 Opens key:
 Opens key:
                         HKCU\software\microsoft\internet explorer\international\scripts
 Opens key:
                         HKLM\software\microsoft\internet explorer\international\scripts
 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
                         HKCU\software\microsoft\internet explorer\styles
 Opens key:
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\policies\activedesktop
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\policies
                         HKCU\software\microsoft\internet explorer\pagesetup
 Opens key:
                         HKCU\software\microsoft\internet explorer\menuext
 Opens kev:
                         HKCU\software\microsoft\internet explorer\menuext\%s
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\control\nls\codepage
                         HKCU\software\microsoft\internet explorer\international\scripts\3
 Opens key:
 Opens key:
                         HKLM\software\microsoft\internet explorer\version vector
 Opens key:
                         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
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\dxtrans
 Opens key:
                         HKCU\software\microsoft\internet explorer\dxtrans
 Opens kev:
                         HKLM\software\microsoft\internet explorer\dxtrans
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_behaviors
 Opens kev:
                         HKLM\software\microsoft\internet explorer\default behaviors
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
 Opens key:
00aa00bdce0b}\inprocserver32
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
 Opens key:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\tinprocserverx86
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
 Opens key:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
                         HKCR \verb|\clsid|{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprochandler32|
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandlerx86
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
 Opens key:
                         HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82
 Opens key:
00aa00bdce0b}\localserver
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winspool.drv
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iepeers.dll
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\persistence
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\persistence
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
 Opens kev:
                         HKCU\software\classes\mime\database\content type\application/iavascript
                         HKCR\mime\database\content type\application/javascript
 Opens key:
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature sslux
```

HKLM\software\microsoft\internet

Opens key:

```
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\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 kev:
                                            HKCU\software\policies\microsoft\internet explorer\restrictions
  Opens key:
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
  Opens key:
  Opens key:
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
  Opens key:
f4ceaaf59cfc}\treatas
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
  Opens kev:
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
  Opens kev:
f4ceaaf59cfc}\inprocserver32
  Opens kev:
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
  Opens key:
f4ceaaf59cfc}\inprocserverx86
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86
  Opens key:
  Opens key:
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\localserver32
  Opens key:
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32
  Opens key:
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler32
  Opens key:
                                            HKCR \verb|\clsid| \{50d5107a-d278-4871-8989-f4cea af 59cfc\} \verb|\inprochandler32| 
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
  Opens key
f4ceaaf59cfc}\inprochandlerx86
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
  Opens kev:
  Opens key
                                            HKCU\software\classes\clsid\{50d5107a-d278-4871-8989
f4ceaaf59cfc}\localserver
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver
  Opens key:
                                            HKCU\software\microsoft\internet
  Opens key
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
                                            HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
  Opens key:
                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimtf.dll
  Opens key:
                                            HKLM\software\microsoft\ctf\tip
  Opens key
                                            c9633f71be64}\languageprofile
  Opens key:
                                           HKCU \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\languageprofile
  Opens key
                                           HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000
  Opens key:
                                            HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
  Opens key:
                                            HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
  Opens key:
  Opens key:
                                            HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\treatas
                                            HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
  Opens key:
  Opens key:
                                            HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32
                                            HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
  Opens key:
                                            HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
  Opens key:
431b3828ba53}\inprocserverx86
                                           HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
  Opens kev:
                                            HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
  Opens key
431b3828ba53}\localserver32
  Opens key:
                                            HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
                                            HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
  Opens key
431b3828ba53}\inprochandler32
  Opens key:
                                            HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
  Opens key:
                                            HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83
431b3828ba53}\inprochandlerx86
                                            HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86
  Opens key:
  Opens key:
                                            HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver
  Opens key:
                                            HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
                                            HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
  Opens key:
                                            HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
  Opens kev:
                                            HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
  Opens key:
869523e2d6c7}\treatas
                                            HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
   Opens key:
                                            HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
  Opens key
869523e2d6c7}\inprocserver32
  Opens key:
                                            HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\ \ \ in procserver 32
  Opens key:
                                            HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserverx86
  Opens key:
                                           HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
  Opens key:
                                            869523e2d6c7}\localserver32
  Opens key:
                                            HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
  Opens key:
                                            HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandler32
  Opens key:
                                            HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
  Opens kev:
                                            HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandlerx86
   Opens key:
                                            HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
  Opens key:
                                            HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver
```

```
Opens key:
                                                            HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
    Opens key:
                                                            HKLM\software\microsoft\ctf\tip\
    Opens key:
                                                            Opens key:
                                                            HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
   Opens key:
HKLM \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d
   Opens key
00c04fc324a1\} \\ \\ category \\ \\ \{b95f181b-ea4c-4af1-8056-7c321abbb091\} \\ \\
                                                            HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
   Opens kev:
0 f816 c09 f4 ee \} \\ category \\ \{b95 f181 b-ea4 c-4 af1-8056-7 c321 abb b091\}
   Opens key
                                                            HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
   Opens key:
                                                            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                            HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
   Opens kev:
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                            HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
   Opens key:
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                            HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
    Opens key:
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
   Opens key:
                                                            HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
    Opens key:
                                                            HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
   Opens key:
                                                            HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
    Opens key:
                                                            HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-85
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                            HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
    Opens kev:
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                             HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Opens key:
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                            HKCU\software\policies\microsoft\internet explorer\control panel
    Opens key:
    Opens key:
                                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
                                                            HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_iedde_register_urlecho
    Opens key:
                                                            HKCU \setminus software \setminus classes \setminus clsid \setminus \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\}
    Opens key:
                                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
    Opens key
                                                            HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
                                                            HKCR\clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \ treat as
    Opens key:
    Opens key:
                                                            HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
                                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
    Opens kev:
    Opens key
                                                            HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1
00aa00bbbb58}\inprocserverx86
                                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86
    Opens key:
                                                            HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
    Opens key:
00aa00bbbb58}\localserver32
                                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
    Opens key:
    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}\inprochandlerx86
                                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
    Opens kev:
                                                            HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
    Opens kev:
00aa00bbbb58}\localserver
    Opens key:
                                                            HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\localserver
    Opens key:
                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jscript.dll
    Opens key:
                                                            HKLM\software\microsoft\windows script\features
    Opens key:
                                                            HKLM\system\currentcontrolset\control\nls\locale
    Opens key:
                                                            HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
    Opens key:
                                                            HKLM\system\currentcontrolset\control\nls\language groups
Opens key:
HKCR\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                                            HKLM\system\currentcontrolset\control\lsa
    Opens key:
    Opens key:
                                                            HKLM\software\policies\microsoft\internet explorer\recovery
    Opens key:
                                                            HKCU\software\microsoft\internet explorer\recovery
    Opens key:
                                                            HKLM\software\microsoft\internet explorer\recovery
                                                            HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_scripturl_mitigation
                                                            HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_scripturl_mitigation
    Opens key:
                                                            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 \verb|\main| featurecontrol| feature\_cross\_domain\_redirect\_mitigation
    Opens key
                                                            HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_cross\_domain\_redirect\_mitigation
    Opens key:
                                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
                                                            HKLM\software\microsoft\internet
   Opens key:
\verb|explorer\main\featurecontrol\feature_block_lmz_script| \\
    Opens key:
                                                            HKCU\software\microsoft\internet
\verb|explorer'| main feature control feature active x_inactivate mode_removal_revert|
```

```
Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
 Opens key:
                          HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_use\_windowedselect control| \\
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature use windowedselectcontrol
 Opens key:
                          HKCU\software\microsoft\internet explorer\new windows
 Opens key:
                          HKLM\software\microsoft\internet explorer\new windows
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
 Opens kev:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
 Opens key:
00aa003f8646}\treatas
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
 Opens kev:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
 Opens kev:
00aa003f8646}\inprocserverx86
 Opens kev:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserverx86
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\localserver32
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler32
 Opens key:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandlerx86
 Opens key:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\tinprochandlerx86
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\localserver
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver
 Opens kev:
 Opens key:
                          HKCU\software\microsoft\internet explorer\international\scripts\24
 Opens key:
                          HKCU\software\microsoft\internet explorer\international\scripts\26
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
 Opens key:
 Opens key:
                          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
 Opens key:
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\treatas
                          HKCR \ clsid \ \{81397204-f51a-4571-8d7b-dc030521aabd\} \ treat as
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
                          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32
 Opens key:
 Opens key
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserverx86
 Opens key:
                          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserverx86
 Opens key:
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\localserver32
                          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
                          \label{local-condition} HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\ \ inprochandler 32
 Opens key:
                          HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
 Opens key:
```

dc030521aabd}\inprochandlerx86

HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandlerx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-

dc030521aabd}\localserver

HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver Opens key:

 $\label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution$ Opens key: options\atl.dll

Opens kev:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\dxtrans.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens kev:

options\xpsp2res.dll

Opens key:

HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}

Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000} Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-

3c8b00c10000}\treatas

Opens key:  $HKCR \ clsid \ \{d1fe6762-fc48-11d0-883a-3c8b00c10000\} \ treat as$ HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-Opens key

3c8b00c10000}\inprocserver32

Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32

Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a

3c8b00c10000}\inprocserverx86

Opens key:

HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-Opens key

3c8b00c10000}\localserver32

HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\localserver32 Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-Opens key

3c8b00c10000}\inprochandler32

Opens key:

Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-

3c8b00c10000}\inprochandlerx86

Opens key:  $HKCR \ clsid \ \{d1fe6762-fc48-11d0-883a-3c8b00c10000\} \ inprochandler x86$ 

Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a

3c8b00c10000}\localserver

Opens key:  $\label{localserver} $HKCR\clsid\\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\\\localserver$ Opens key:  $\label{local-bound} HKCU \setminus software \\ \\ classes \\ \\ clsid \\ \\ \{4fd2a832-86c8-11d0-8fca-00c04fd9189d\} \\ \\ \\ equivalent \\ \\ eq$ 

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

Opens kev:

HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-Opens kev: 00c04fd9189d}\inprocserver32

HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-Opens key:

```
00c04fd9189d}\inprocserverx86
  Opens key:
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserverx86
  Opens key:
                                   HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca
00c04fd9189d}\localserver32
  Opens key:
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver32
  Opens key:
                                   HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32
  Opens key:
  Opens kev:
                                   HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca
00c04fd9189d}\inprochandlerx86
  Opens key:
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandlerx86
                                   HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
  Opens key:
00c04fd9189d}\localserver
  Opens key:
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver
  Opens key:
                                   HKCU\software\classes\mime\database\content type\image/gif
  Opens kev:
                                   HKCR\mime\database\content type\image/gif
  Opens kev:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dciman32.dll
  Opens kev:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddraw.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddrawex.dll
  Opens key:
                                   HKLM\hardware\devicemap\video
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\bug!
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\mortalkombat3
  Opens key:
                                    HKLM\software\microsoft\directdraw\compatibility\msgolf98
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
                                    HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\rogue squadron
  Opens kev:
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\savage
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
                                   HKLM\software\microsoft\directdraw\compatibility\silentthunder
  Opens key:
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\terracide
  Opens key:
                                   HKLM\software\microsoft\directdraw\compatibility\thirddimension
  Opens key:
HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff davis quality benchmark for the compatibility benchmark for the
  Opens key:
HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff daviswin mark benchmark
  Opens key:
                                   HKLM\software\microsoft\directdraw\gammacalibrator
  Opens key:
                                   HKLM\software\microsoft\directdraw
  Opens key:
                                   HKLM\software\microsoft\direct3d
  Opens key:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
  Opens key:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
  Opens key:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\treatas
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\ \ treat as
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
  Opens key:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231
  Opens kev:
f941e9b7e1fe}\inprocserverx86
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserverx86
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\localserver32
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver32
  Opens key:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
  Opens key:
f941e9b7e1fe}\inprochandler32
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32
  Opens kev:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
  Opens kev:
f941e9b7e1fe}\inprochandlerx86
  Opens key:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\
  Opens key:
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\localserver
  Opens key:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver
  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:
  Opens key
                                   HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\treatas
                                    HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas
  Opens key:
  Opens key:
                                   HKLM\software\microsoft\internet explorer\activex compatibility
                                   HKLM\software\microsoft\internet explorer\activex
  Opens key
compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}
                                   HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
  Opens key
00c04fa34f05}\inprocserver32
  Opens key:
                                   HKCR \ clsid \ \{e71b4063-3e59-11d2-952a-00c04fa34f05\} \ \ inprocserver 32
  Opens key:
                                   HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserverx86
  Opens key:
                                   HKCR\clsid\e71b4063-3e59-11d2-952a-00c04fa34f05\\\label{e71b4063-3e59-11d2-952a-00c04fa34f05}\
  Opens key
                                   00c04fa34f05}\localserver32
                                   HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\localserver32
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler32
                                   HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler32
  Opens kev:
                                   HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
  Opens kev:
{\tt 00c04fa34f05} \verb|\inprochandlerx86| \\
```

 Opens key:
 HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandlerx86

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

```
00c04fa34f05}\localserver
 Opens key:
                         HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\localserver
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dxtmsft.dll
 Opens key:
                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{4cb26c03-ff93-11d0-817e-0000f87557db\}
 Opens key:
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
 Opens key:
                         HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\treatas
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
 Opens kev:
0000f87557db}\inprocserver32
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e
0000f87557db}\inprocserverx86
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserverx86
 Opens kev:
                         HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
 Opens kev:
0000f87557db}\localserver32
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver32
 Opens kev:
                         HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
 Opens key
0000f87557db}\inprochandler32
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\\label{eq:hkcr} \
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandlerx86
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\tinprochandlerx86
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\localserver
 Opens key:
                         HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
 Opens key:
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\treatas
 Opens key:
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key:
f4fc1e6ca1bd}\inprocserver32
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6
f4fc1e6ca1bd}\inprocserverx86
                         Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\localserver32
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver 32
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler32
 Opens key:
                         HKCR \clsid \ \{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\} \label{eq:hkcr} \\
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandlerx86
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandlerx86
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\localserver
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\sxs.dll
 Opens key:
                         HKCU\software\classes\typelib
 Opens key:
                         HKCR\typelib
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
 Opens key:
 Opens key:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key:
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key:
 Opens kev:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\409
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
 Opens kev:
 Opens key:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\9
 Opens key:
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
 Opens key:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0
 Opens key:
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0
 Opens key:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0\win32
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32
 Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
 Opens key:
 Opens key:
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
 Opens key:
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
 Opens key
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
 Opens key:
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:
                         Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\0
 Opens key:
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
 Opens key:
                         0000f87557db}\1.1\0\win32
 Opens key:
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
 Opens key:
                         HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_disable\_behaviors\_draw\_reentrancy
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_xmlhttp
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature xmlhttp
```

```
HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
    Opens key:
c9633f71be64\\ \\ category\\ \\ item\\ \\ \{a48fa74e-f767-44e4-bfbc-169e8b38ff58\}\\
    Opens key:
                                                                       HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
    Opens key
                                                                       e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                       HKLM \ software \ microsoft \ tip \ \{dcbd6fa8-032f-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d3-b5b1-11d
    Opens key:
Opens kev:
                                                                      HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
Of816cO9f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                       HKCU\software\classes\mime\database\content type\image/png
    Opens key:
    Opens key:
                                                                       {\tt HKCR\mime\database\content\ type\image/png}
    Opens key:
                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imgutil.dll
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
    Opens key:
                                                                       HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
    Opens kev:
    Opens kev:
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\treatas
                                                                       HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
    Opens key:
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
    Opens key:
00aa006c1a01}\inprocserver32
                                                                       HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
    Opens key:
    Opens key:
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserverx86
    Opens key:
                                                                      HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
    Opens key
00aa006c1a01}\localserver32
    Opens key:
                                                                       Opens key:
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandler32
                                                                       HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
    Opens key
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724
00aa006c1a01}\inprochandlerx86
                                                                       HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\ \ inprochandlerx86
     Opens key:
                                                                       HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
     Opens key
00aa006c1a01}\localserver
                                                                       HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
    Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{6a01fda0-30df-11d0-b724-00aa006c1a01\}
    Opens key:
    Opens key:
                                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
    Opens key:
                                                                       HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
                                                                       HKCR \ clsid \ \{6a01fda0-30df-11d0-b724-00aa006c1a01\} \ treat as
     Opens key:
    Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{6a01fda0-30df-11d0-b724-b72d-11d0-b724-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d
00aa006c1a01}\inprocserver32
    Opens key:
                                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
    Opens key
                                                                       HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserverx86
    Opens key:
                                                                      HKCR \verb|\clsid|{6a01fda0-30df-11d0-b724-00aa006c1a01} \verb|\inprocserverx86|
    Opens key
                                                                       HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\localserver32
                                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32
    Opens key:
                                                                       HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
    Opens kev:
00aa006c1a01}\inprochandler32
                                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
    Opens key:
    Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{6a01fda0-30df-11d0-b724-b72d-11d0-b724-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d0-b72d-11d
00aa006c1a01}\inprochandlerx86
                                                                       HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86
    Opens kev:
                                                                       HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
    Opens key:
00aa006c1a01}\localserver
                                                                      HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
    Opens kev:
    Opens kev:
                                                                       HKCU\software\classes\mime\database\content type
    Opens key:
                                                                       HKCR\mime\database\content type
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\image/bmp\bits
    Opens key:
                                                                       HKCR\mime\database\content type\image/bmp\bits
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\image/gif\bits
    Opens key:
                                                                       HKCR\mime\database\content type\image/gif\bits
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\image/jpeg\bits
    Opens key:
                                                                       HKCR\mime\database\content type\image/jpeg\bits
    Opens kev:
                                                                       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 key:
                                                                       HKCR\mime\database\content type\image/png\bits
    Opens kev:
                                                                       HKCU\software\classes\mime\database\content type\image/tiff\bits
    Opens kev:
                                                                       HKCR\mime\database\content type\image/tiff\bits
    Opens key:
                                                                       \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \simple \classes \mime \mim
    Opens key:
                                                                       HKCR\mime\database\content type\image/x-icon\bits
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\image/x-jg\bits
     Opens key:
                                                                       HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt image} \mbox{\tt /x-jg} \mbox{\tt bits}
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\image/x-png\bits
    Opens key:
                                                                       HKCR\mime\database\content type\image/x-png\bits
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\image/x-wmf\bits
    Opens key:
                                                                       HKCR\mime\database\content type\image/x-wmf\bits
    Opens key:
                                                                       HKCU\software\classes\mime\database\content type\image/x-png
    Opens key:
                                                                       {\tt HKCR\mbox{\tt mime}\database\content\ type\limage/x-png}
    Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-00a0c913f750\}
    Opens key:
                                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
    Opens key:
                                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\treatas
                                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
    Opens key:
    Opens key:
                                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
     Opens key:
                                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
    Opens key
                                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserverx86
```

```
Opens key:
                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\\\\
   Opens key:
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\localserver32
   Opens key:
                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
   Opens key
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
                                                       HKCR \verb|\clsid|{a3ccedf7-2de2-11d0-86f4-00a0c913f750} \verb|\inprochandler32| \\
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandlerx86
                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86
   Opens kev:
                                                       HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
   Opens kev:
00a0c913f750}\localserver
                                                       HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
   Opens key:
   Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\pngfilt.dll
                                                       HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_isolate_named_windows
                                                       HKLM\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature isolate named windows
   Opens key:
                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_navigation_sounds
                                                       HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disable_navigation_sounds
   Opens key:
                                                       HKCU\appevents\schemes\apps\explorer\navigating\.current
   Opens key:
                                                       HKCU\software\microsoft\multimedia\sound mapper
   Opens key:
                                                       HKCU\software\microsoft\windows\currentversion\multimedia\midimap
   Opens key:
                                                       HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
   Opens key:
                                                        HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
                                                        HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
   Opens key:
fd2b31b3eefd}\treatas
                                                       HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treat as
   Opens key
                                                       HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32
                                                       HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\ \ in procserver 32
    Opens key:
    Opens key
                                                       HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserverx86
                                                       HKCR\clsid\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\
   Opens key:
   Opens key
                                                       HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\localserver32
   Opens key:
                                                       HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver32
    Opens key:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893f - a8dc - 47f3 - a8dc - a
fd2b31b3eefd}\inprochandler32
   Opens key:
                                                       \label{lem:hkcr} $HKCR\clsid\\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\nprochandler 32 $$
   Opens key:
                                                       HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandlerx86
                                                       HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\nprochandlerx86
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\localserver
   Opens key:
                                                       HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver
   Opens key:
                                                       HKCU\software\classes\mime\database\content type\text/html;charset=utf-8
   Opens key:
                                                       HKCR\mime\database\content type\text/html;charset=utf-8
                                                       HKCU\software\microsoft\internet explorer\searchproviders\
   Opens key:
   Opens key:
                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup
   Opens key:
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature additional ie8 memory cleanup
   Opens key:
                                                       HKCU\appevents\schemes\apps\explorer\activatingdocument\.current
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\gdiplus.dll
   Opens kev:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d3dim700.dll
   Opens key:
                                                        HKCU\software\classes\mime\database\content type\image/jpeg
   Opens key:
                                                       HKCR\mime\database\content type\image/jpeg
   Opens key:
                                                        HKCU\software\classes\mime\database\content type\text/javascript;
charset=utf-8
   Opens key:
                                                       HKCR\mime\database\content type\text/javascript; charset=utf-8
   Opens key:
                                                       HKCU\software\classes\mime\database\content type\text/javascript
   Opens key:
                                                       HKCR\mime\database\content type\text/javascript
   Opens kev:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
   Opens key:
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
   Opens key:
                                                        HKCU\software\classes\shockwaveflash.shockwaveflash
   Opens key:
                                                       HKCR\shockwaveflash.shockwaveflash
                                                       HKCU\software\classes\shockwaveflash.shockwaveflash\clsid
   Opens key:
   Opens key:
                                                       {\tt HKCR \ } shock wave flash. shock wave flash \ \ clsid
                                                       HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
   Opens key:
    Opens key:
                                                       HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
   Opens key:
                                                       HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\treatas
                                                       HKCR \ clsid \ \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \ treat as
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
    Opens key:
                                                       HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\ \ linprocserver 32
   Opens key
                                                       HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserverx86
                                                       HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserverx86
   Opens key:
   Opens key:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{d27cdb6e-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6
444553540000}\localserver32
                                                       HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\localserver32
   Opens kev:
```

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

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

 $HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\) in prochandler 32$ 

Opens kev:

Opens key:

Opens key:

444553540000}\inprochandler32

```
444553540000}\inprochandlerx86
                                    HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandlerx86
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\localserver
  Opens key:
                                    HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\localserver
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens kev:
                                    HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:
                                    \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\dsound.dll
  Opens key:
                                    HKLM\software\microsoft\directx
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
Opens key:
options\mscms.dll
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\flash10h.ocx
  Opens key:
                                    HKLM\hardware\description\system\centralprocessor\0
  Opens key:
                                    HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
  Opens key:
                                    HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
  Opens key:
                                    HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
  Opens key:
                                    HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
  Opens key:
                                    HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\409
  Opens key:
                                    HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\409
  Opens key:
                                    HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\9
                                    HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9
  Opens kev:
  Opens key:
                                    HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0
                                    HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0
  Opens key:
                                    HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
  Opens key
444553540000}\1.0\0\win32
                                    HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32
  Opens key:
  Opens key:
                                    \label{locality} HKCU \setminus software \\ \\ classes \setminus typelib \setminus \{00020430-0000-0000-c000-0000000000046\} \\
  Opens key:
                                    HKCR\typelib\{00020430-0000-0000-c000-000000000046}
  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
  Opens key:
                                    HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
  Opens key:
                                    HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
                                    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 key:
                                    Opens key:
                                    HKCR \ typelib \ \{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4\} \ \ 1.0
  Opens key:
                                    HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
  Opens kev:
00c04fb6bfc4}\1.0\0
                                    HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0
  Opens key:
  Opens key:
                                    HKCU \setminus software \setminus classes \setminus typelib \setminus \{7e8bc440 - aeff-11d1 - 89c2 - aeff-11d1 - ae
00c04fb6bfc4}\1.0\0\win32
                                    HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32
  Opens key:
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature domstorage
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_domstorage
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xmllite.dll
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
  Opens key:
                                    HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
  Opens key:
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
  Opens key:
                                    HKCU\software\classes\drive\shellex\folderextensions
                                    HKCR\drive\shellex\folderextensions
  Opens key:
                                    HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
  Opens key:
4442-804e-409d6c4515e9}
                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Opens kev:
409d6c4515e9}
  Opens key:
                                    HKCU\software\microsoft\internet explorer\feed discovery
  Opens key:
                                    HKLM\software\microsoft\internet explorer\feed discovery
  Opens key:
                                    HKCU\software\microsoft\ftp
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\services
  Opens key:
                                    HKCU\software\microsoft\internet explorer\services
  Opens key:
                                    HKLM\software\microsoft\internet explorer\services
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\activities
  Opens key:
                                    HKCU\software\microsoft\internet explorer\activities
  Opens key:
                                    HKLM\software\microsoft\internet explorer\activities
  Opens key:
                                    HKLM\software\policies\microsoft\internet
explorer\infodelivery\restrictions
  Opens key:
                                    HKCU\software\policies\microsoft\internet
explorer\infodelivery\restrictions
                                    \label{lem:hklm} \mbox{HKLM\software\policies\mbox{\sc microsoft\internet explorer\suggested sites}}
  Opens key:
  Opens kev:
                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\suggested sites}} \\
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\setupapi.dll
  Opens key:
                                    HKLM\system\currentcontrolset\control\minint
```

Opens key: HKLM\system\wpa\pnp

```
Opens key:
                                                                                                         HKLM\software\microsoft\windows\currentversion\setup
      Opens key:
                                                                                                        HKLM\software\microsoft\windows\currentversion\setup\apploglevels
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}\
                                                                                                        HKCU\software\classes\directory
      Opens key:
                                                                                                        HKCR\directory
      Opens key:
                                                                                                        HKCU\software\classes\directory\curver
      Opens key:
                                                                                                        HKCR\directory\curver
      Opens key:
                                                                                                        HKCR\directory\
      Opens key:
      Opens key:
                                                                                                        HKCU\software\microsoft\windows\currentversion\explorer
      Opens kev:
                                                                                                        HKCU\software\microsoft\windows\currentversion\explorer\
                                                                                                        HKCU\software\microsoft\windows\currentversion\policies\system
      Opens kev:
                                                                                                        HKCU\software\classes\directorv\shellex\iconhandler
      Opens kev:
                                                                                                        HKCR\directory\shellex\iconhandler
      Opens kev:
                                                                                                        HKCU\software\classes\directory\clsid
      Opens kev:
      Opens kev:
                                                                                                        HKCR\directory\clsid
                                                                                                        HKCU\software\classes\folder
      Opens key:
      Opens key:
                                                                                                        HKCR\folder
      Opens key:
                                                                                                        HKCU\software\classes\folder\clsid
      Opens key:
                                                                                                        HKCR\folder\clsid
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
      Opens key:
      Opens key:
                                                                                                        HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560-c2a7-11cf-bff4-444553540000\} \setminus shell \in Classes \setminus clsid \setminus
      Opens key:
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell
      Opens key:
                                                                                                        HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c
444553540000}\shellex\iconhandler
      Opens key:
                                                                                                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus
      Opens key
      Opens key:
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
      Opens key:
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4
444553540000}\treatas
                                                                                                        \label{lem:hkcr} $$ HKCR\clsid{ff393560-c2a7-11cf-bff4-444553540000} \times $$ Teach $$
      Opens key:
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserverx86
      Opens key:
                                                                                                        Opens key:
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\localserver32
      Opens key:
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler32
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
      Opens kev:
      Opens key
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandlerx86
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandlerx86
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
      Opens key:
444553540000}\localserver
                                                                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver
      Opens kev:
      Opens kev:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-c2a7-11cf-
bff4-444553540000}
                                                                                                        HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
settings\5.0\cache\extensible cache\mshist012016040820160409
      Opens kev:
                                                                                                        HKCU\software\microsoft\internet explorer\main\windowssearch
      Opens key:
                                                                                                        HKLM\software\policies\microsoft\internet explorer\feeds
      Opens key:
                                                                                                        HKCU\software\microsoft\internet explorer\feeds
      Opens key:
                                                                                                        HKLM\software\microsoft\internet explorer\feeds
      Opens key:
                                                                                                        HKCU\software\classes\.url\persistenthandler
      Opens key:
                                                                                                        HKCR\.url\persistenthandler
      Opens key:
                                                                                                         HKLM\software\policies\microsoft\internet explorer\main\windowssearch
      Opens key:
                                                                                                        HKLM\software\microsoft\windows search
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
                                                                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
      Opens kev:
      Opens key:
                                                                                                        HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta \} + \{20d04f
3aea-1069-a2d8-08002b30309d}
      Opens key:
                                                                                                        \label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\policies\nonenum}} \\
                                                                                                        HKLM\software\microsoft\windows\currentversion\policies\nonenum
      Opens key
      Opens key:
                                                                                                        HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
                                                                                                        HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta, for example a substitution of the property of 
      Opens key:
3aea-1069-a2d8-08002b30309d}\shellfolder
      Opens key:
                                                                                                        HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
      Opens key:
                                                                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
      Opens key:
                                                                                                        \label{local-condition} $HKCR\clsid_{20d04fe0-3aea-1069-a2d8-08002b30309d} \end{tabular} $$
      Opens key:
                                                                                                        HKCU\software\microsoft\windows\shellnoroam
      Opens key:
                                                                                                        {\tt HKCU \ } software \verb|\ microsoft \verb|\ windows \verb|\ shell no roam \verb|\ muicache| \\
      Opens key:
                                                                                                        HKCU\software\microsoft\windows\shellnoroam\muicache\
      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
                                                                                                        HKLM\software\microsoft\internet
      Opens key:
```

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

explorer\main\featurecontrol\feature alloweddomainlist

```
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
    Opens key:
                                                              HKCU\software\classes\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
    Opens key:
                                                              HKCR\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
    Opens key:
                                                              \label{lem:hkcu} \verb+KCU\+software\+microsoft\+code\+ store\+ database\+ distribution\+ units
    Opens key:
                                                              \label{lem:hklm} \verb+Kklm \+ software + microsoft + code store database + distribution units
    Opens key
                                                              {\tt HKLM \setminus software \setminus microsoft \setminus code \ store \ database \setminus distribution}
units\{d27cdb6e-ae6d-11cf-96b8-444553540000}
    Opens key:
                                                              HKCU\software\classes\clsid
    Opens kev:
                                                              HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
                                                              HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
                                                              HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\installedversion
    Opens key:
                                                              HKCU \setminus software \setminus classes \setminus clsid \setminus \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \setminus appid \setminus classes \setminus clsid \setminus clsid \setminus classes \setminus clsid \setminus
    Opens key:
                                                              HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
    Opens kev:
                                                              HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens kev:
444553540000}\languagecheckperiod
    Opens kev:
                                                              ... HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\languagecheckperiod
    Opens key:
                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
                                                              HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
   Opens key:
                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection
                                                              HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_activex_repurposedetection
    Opens key:
                                                              HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus
    Opens key:
                                                              HKCR \ clsid \ \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \ misc status
                                                              HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key
444553540000}\miscstatus\1
                                                              Opens key:
                                                              \label{thm:linear} \mbox{HKCU\software\mbox{$\backslash$ internet explorer\domstorage\baidu.com}} \mbox{}
    Opens key:
                                                              \hbox{\tt HKCU\software\mbox{\tt microsoft\internet explorer\domstorage\total}}
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
    Opens key:
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
    Opens key:
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
    Opens key:
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
    Opens key:
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
    Opens key:
                                                              HKCR \c1sid \end{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} \label{fig:hcc} in procserver 32
    Opens kev:
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c
00c04fb6bfc4}\inprocserverx86
    Opens key:
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
    Opens key:
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\localserver32
    Opens key:
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
    Opens key:
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
    Opens key:
    Opens kev:
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandlerx86
    Opens key:
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
                                                              HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key:
00c04fb6bfc4}\localserver
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
    Opens key:
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
    Opens kev:
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
    Opens kev:
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
    Opens key
00a0c90a8f39}\treatas
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
    Opens key:
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
    Opens key
00a0c90a8f39}\inprocserver32
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserverx86
    Opens key:
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserverx86
    Opens key
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\localserver32
    Opens key:
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver32
    Opens key
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\ \ in prochandler 32
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandlerx86
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandlerx86
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442
00a0c90a8f39}\localserver
                                                              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver
    Opens key:
    Opens key:
                                                              HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5078f35 - c551 - 11d3 - 89b9 - 0000f81fe221\}
    Opens key:
                                                              HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
    Opens key:
                                                              HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5078f35 - c551 - 11d3 - 89b9 - f648 - f
0000f81fe221}\treatas
    Opens key:
                                                              HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\treatas
    Opens key:
                                                              HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32
                                                              HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\clserver32
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserverx86
                                                              HKCR \verb|\clsid| \{f5078f35-c551-11d3-89b9-0000f81fe221\} \verb|\inprocserverx86| \} | The state of the
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\localserver32
```

```
Opens key:
                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\localserver32
   Opens key:
                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler32
   Opens key:
                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32
   Opens key:
                                                       \label{localization} HKCU \setminus software \setminus classes \setminus interface \setminus \{85cb6900-4d95-11cf-960c-0080c7f4ee85\}
   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:
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000-00000000046}
   Opens kev:
                                                       HKCR\clsid\{00020424-0000-0000-c000-00000000046}
   Opens key:
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000-
   Opens key:
0000000000046}\treatas
                                                       HKCR\clsid\{00020424-0000-0000-c000-00000000046}\treatas
   Opens key:
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000-
   Opens kev:
00000000046}\inprocserver32
                                                       HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32
   Opens kev:
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000-
   Opens kev:
000000000046}\inprocserverx86
                                                       HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserverx86
   Opens key:
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000-
   Opens key
00000000046}\localserver32
   Opens kev:
                                                       HKCR\clsid\{00020424-0000-0000-c000-00000000046}\localserver32
                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
   Opens key:
0000f81fe221}\inprochandlerx86
                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandlerx86
   Opens key:
   Opens key
                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\localserver
   Opens key:
                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\localserver
   Opens key
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000-
00000000046}\inprochandler32
   Opens key:
                                                       HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandler32
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000-
    Opens key
000000000046 \} \verb|\inprochandlerx86|
                                                       HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandlerx86
    Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{00020424-0000-0000-c000
00000000046}\localserver
                                                       HKCR\clsid\{00020424-0000-0000-c000-000000000046}\localserver
    Opens key:
   Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msxml3.dll
   Opens key:
                                                       {\tt HKLM \backslash software \backslash microsoft \backslash msxml30}
   Opens key
                                                       HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
   Opens key:
                                                       HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
   Opens key:
                                                       HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
   Opens key:
                                                       HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
   Opens key:
                                                       \label{local-equation} $HKCU \sim \classes \typelib \end{2} aco-3oc1-11cf-a7eb-0000c05bae0b \} $$ \classes \typelib \end{2} $$ \classe
   Opens key:
                                                       HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
                                                       HKCU \setminus software \setminus classes \setminus typelib \setminus \{eab22ac0-30c1-11cf-a7eb-0000c05bae0b\} \setminus 1.11 + (ab22ac0-30c1-11cf-a7eb-0000c05bae0b) \setminus 1.11 + (ab22ac0-30c1-11cf-a7eb-0000c05
   Opens key:
                                                       HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
   Opens key:
   Opens key:
                                                       HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
                                                       HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
   Opens key:
   Opens key:
                                                       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\{00020400-0000-0000-0000-000000000046}
   Opens key:
   Opens kev:
                                                       HKCU\software\classes\interface\{00020400-0000-0000-c000-
00000000046}\proxystubclsid32
                                                       HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32
   Opens kev:
   Opens key:
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046}
   Opens key:
                                                       HKCR\clsid\{00020420-0000-0000-c000-00000000046}
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000-
   Opens key
000000000046}\treatas
                                                       HKCR\clsid\{00020420-0000-0000-c000-00000000046}\treatas
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
                                                       \label{locality} \mbox{HKCR\clsid\{00020420-0000-0000-0000-000000000046}\} \mbox{inprocserver32}
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserverx86
   Opens key:
                                                       HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserverx86
   Opens key
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000
000000000046}\localserver32
                                                       HKCR\clsid\{00020420-0000-0000-c000-00000000046}\localserver32
   Opens key:
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000-
    Opens key
00000000046}\inprochandler32
                                                       HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler32
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000
00000000046}\inprochandlerx86
                                                       HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandlerx86
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\localserver
    Opens key:
                                                       \label{localserver} \mbox{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\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\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:
                                                       \label{local-relation} HKCU \setminus software \setminus classes \setminus interface \setminus \{6d5140c1-7436-11ce-8034-00aa006009fa\}
   Opens key
                                                       HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
   Opens key:
                                                       HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-
{\tt 00aa006009fa} \verb|\proxystubclsid32| \\
                                                       HKCR \ interface \ \{6d5140c1-7436-11ce-8034-00aa006009fa\} \ proxystubclsid 32
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}
                                                       HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}
   Opens key:
   Opens key:
                                                       HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-
00a0c90dcaa9}\treatas
                                                       HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\treatas
   Opens key:
```

```
Opens key:
                                        HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-
00a0c90dcaa9}\inprocserver32
  Opens key:
                                        HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32
  Opens key:
                                        HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-
00a0c90dcaa9}\inprocserverx86
  Opens key:
                                        HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserverx86
  Opens key:
                                        HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-
00a0c90dcaa9}\localserver32
  Opens key:
                                        HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver32
                                        HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-
  Opens kev:
00a0c90dcaa9}\inprochandler32
                                        HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandler32
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c
00a0c90dcaa9}\inprochandlerx86
                                        HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandlerx86
  Opens kev:
                                        HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-
  Opens kev:
00a0c90dcaa9}\localserver
                                        HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver
  Opens kev:
  Opens kev:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\actxprxy.dll
  Opens key:
                                        HKCU\software\classes\interface\{00020404-0000-0000-c000-000000000046}
  Opens key:
                                        HKCR\interface\{00020404-0000-0000-c000-00000000046}
  Opens key:
                                        HKCU\software\classes\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:
                                        Opens key:
                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000-00000000046}
  Opens key:
                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}
  Opens key:
                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000
000000000046}\treatas
  Opens key:
                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}\treatas
                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000-
  Opens key
000000000046}\inprocserver32
                                        \label{local-equation} \mbox{HKCR\clsid\{00020421-0000-0000-c000-000000000046\}\inprocserver32}} \\ \mbox{ } \m
  Opens key:
                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000-
  Opens key
00000000046}\inprocserverx86
  Opens key:
                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserverx86
                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000-
   Opens key
000000000046}\localserver32
                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}\localserver32
   Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000-
00000000046}\inprochandler32
   Opens key:
                                        Opens key:
                                        000000000046}\inprochandlerx86
                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprochandlerx86
  Opens key:
  Opens key
                                        HKCU\software\classes\clsid\{00020421-0000-0000-c000-
000000000046}\localserver
  Opens key:
                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}\localserver
  Opens key:
shockwave-flash
  Opens key:
                                        HKCR\mime\database\content type\application/x-shockwave-flash
  Opens key:
  Opens key:
                                        HKCR\mime\database\content type\image/x-icon
  Opens key:
                                        HKCU\software\classes\protocols\filter\application/x-shockwave-flash
  Opens key:
                                        HKCR\protocols\filter\application/x-shockwave-flash
```

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \application/x-type \classes \mime \classes \mime \classes \classes \mime \mime \classes \mime \$ 

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \slimage / x-icon \end{tabular}$ 

HKCU\software\classes\protocols\filter\image/x-icon Opens key:

Opens kev: HKCR\protocols\filter\image/x-icon

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

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

Opens key:

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

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

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserverx86

Opens key:  $HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\tinprocserverx86$ 

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

00c04f983e60}\localserver32

Opens key:  $HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\localserver 32$ 

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

00c04f983e60}\inprochandler32

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

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

00c04f983e60}\inprochandlerx86

Opens key:

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

00c04f983e60}\localserver

Opens key:  $HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\localserver$ Opens key HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata

Opens key: HKCU\software\microsoft\cryptography\providers\type 001

Opens key:  $HKLM \verb|\software\m| icrosoft \verb|\cryptography\defaults\provider types \verb|\type 001| \\$ Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ 

options\schannel.dll

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

Opens key: HKCR\shockwaveflash.shockwaveflash.7

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

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

HKCU\software\classes\protocols\filter\application/javascript Opens key:

Opens key: HKCR\protocols\filter\application/javascript Opens key: HKCU\software\classes\msxml2.xmlhttp

HKCR\msxml2.xmlhttp Opens key:

```
Opens key:
                                     HKCU\software\classes\msxml2.xmlhttp\clsid
  Opens key:
                                     HKCR\msxml2.xmlhttp\clsid
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}
  Opens key:
  Opens key:
                                     HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}
  Opens key:
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\treatas
                                     HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\treatas
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32
                                     HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-
  Opens kev:
00c04f990bb4}\inprocserverx86
  Opens key:
                                     HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserverx86
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-
  Opens key:
00c04f990bb4}\localserver32
                                     HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\localserver32
  Opens kev:
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-
  Opens kev:
00c04f990bb4}\inprochandler32
                                     HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprochandler32
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprochandlerx86
                                     HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprochandlerx86
  Opens key:
  Opens kev:
                                     HKCU\software\classes\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\localserver
  Opens key:
                                     HKCR \ clsid \ \{f6d90f16-9c73-11d3-b32e-00c04f990bb4\} \ local server \ description of the context of the cont
  Opens key:
                                     HKCU\software\classes\shockwaveflash.shockwaveflash.12
  Opens key:
                                     HKCR\shockwaveflash.shockwaveflash.12
  Opens key:
                                     HKCU\software\classes\shockwaveflash.shockwaveflash.11
  Opens key:
                                     HKCR\shockwaveflash.shockwaveflash.11
  Opens key:
                                     HKCU\software\classes\shockwaveflash.shockwaveflash.10
  Opens key:
                                     HKCR\shockwaveflash.shockwaveflash.10
  Opens key:
                                     HKCU\software\classes\shockwaveflash.shockwaveflash.10\clsid
  Opens key:
                                     HKCR\shockwaveflash.shockwaveflash.10\clsid
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_object
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_object
                                     HKLM\software\microsoft\internet explorer\plugins\disableactivexcontrols
  Opens key:
  Opens key:
                                     HKCU\software\classes\.swf
  Opens key:
                                     HKCR\.swf
  Opens key:
                                     HKCU\software\classes\baidubar.tool.1
  Opens key:
                                     HKCR\baidubar.tool.1
  Opens key:
                                     HKCU\software\classes\baidubar.tool.2
  Opens key:
                                     HKCR\baidubar.tool.2
  Opens key:
                                     HKCU\software\classes\baidubar.tool.3
  Opens key:
                                     HKCR\baidubar.tool.3
  Opens key:
                                     HKCU\software\classes\baidubar.tool.4
  Opens key:
                                     HKCR\baidubar.tool.4
  Opens key:
                                     HKCU\software\classes\baidubar.tool.5
  Opens key:
                                     HKCR\baidubar.tool.5
                                     HKCU\software\classes\baidubar.tool.6
  Opens key:
  Opens kev:
                                     HKCR\baidubar.tool.6
  Opens kev:
                                     HKCU\software\classes\baidubar.tool.7
  Opens key:
                                     HKCR\baidubar.tool.7
                                     HKCU\software\classes\baidubar.tool.8
  Opens key:
  Opens key:
                                     HKCR\baidubar.tool.8
                                     HKCU\software\classes\baidubar.tool.9
  Opens key:
  Opens key:
                                     HKCR\baidubar.tool.9
  Opens kev:
                                     HKCU\software\classes\google.oneclickctrl.1
                                     HKCR\google.oneclickctrl.1
  Opens kev:
                                     HKCU\software\classes\google.oneclickctrl.2
  Opens kev:
  Opens key:
                                     HKCR\google.oneclickctrl.2
  Opens key:
                                     HKCU\software\classes\google.oneclickctrl.3
  Opens key:
                                     HKCR\google.oneclickctrl.3
  Opens key:
                                     HKCU\software\classes\google.oneclickctrl.4
  Opens key:
                                     HKCR\google.oneclickctrl.4
  Opens key:
                                     HKCU\software\classes\google.oneclickctrl.5
  Opens key:
                                     HKCR\google.oneclickctrl.5
  Opens kev:
                                     HKCU\software\classes\google.oneclickctrl.6
  Opens key:
                                     HKCR\google.oneclickctrl.6
  Opens key:
                                     HKCU\software\classes\google.oneclickctrl.7
  Opens key:
                                     HKCR\google.oneclickctrl.7
  Opens kev:
                                     HKCU\software\classes\google.oneclickctrl.8
                                     HKCR\google.oneclickctrl.8
  Opens kev:
                                     HKCU\software\classes\google.oneclickctrl.9
  Opens key:
  Opens key:
                                     HKCR\google.oneclickctrl.9
                                     HKCU\software\classes\qvodinsert.qvodctrl.1
  Opens key:
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.1
  Opens key:
                                     HKCU\software\classes\qvodinsert.qvodctrl.2
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.2
  Opens key:
                                     HKCU\software\classes\qvodinsert.qvodctrl.3
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.3
  Opens key:
                                     HKCU\software\classes\qvodinsert.qvodctrl.4
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.4
  Opens key:
                                     HKCU\software\classes\qvodinsert.qvodctrl.5
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.5
  Opens key:
                                     HKCU\software\classes\qvodinsert.qvodctr1.6
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.6
  Opens key:
                                     HKCU\software\classes\qvodinsert.qvodctrl.7
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.7
                                     HKCU\software\classes\qvodinsert.qvodctrl.8
  Opens key:
  Opens key:
                                     {\tt HKCR} \backslash qvodinsert.qvodctrl.8
  Opens key:
                                     HKCU\software\classes\qvodinsert.qvodctrl.9
  Opens key:
                                     HKCR\qvodinsert.qvodctrl.9
```

```
Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.2
   Opens key:
                                              HKCR\pdf.pdfctrl.2
   Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.3
   Opens key:
                                              HKCR\pdf.pdfctrl.3
   Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.4
   Opens key:
                                              HKCR\pdf.pdfctrl.4
   Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.5
   Opens key:
                                              HKCR\pdf.pdfctr1.5
   Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.6
   Opens kev:
                                              HKCR\pdf.pdfctrl.6
   Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.7
   Opens key:
                                              HKCR\pdf.pdfctrl.7
   Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.8
   Opens key:
                                              HKCR\pdf.pdfctrl.8
   Opens key:
                                              HKCU\software\classes\pdf.pdfctrl.9
                                              HKCR\pdf.pdfctrl.9
   Opens kev:
   Opens kev:
                                              HKCU\software\classes\pdf.pdfctrl.1
   Opens kev:
                                              HKCR\pdf.pdfctrl.1
   Opens key:
                                              HKCU\software\classes\acropdf.pdf.1
   Opens key:
                                              HKCR\acropdf.pdf.1
   Opens key:
                                              HKCU\software\classes\acropdf.pdf.1\clsid
   Opens key:
                                              HKCR\acropdf.pdf.1\clsid
   Opens key:
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-444553540000}
                                              HKCR\clsid\{ca8a9780-280d-11cf-a24d-444553540000}
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\treatas
   Opens key:
                                              HKCR\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\treatas
   Opens key:
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32
   Opens key:
                                              HKCR\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\ \ inprocserver 32
   Opens key
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserverx86
                                              Opens key:
   Opens key
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\localserver32
   Opens key:
                                              HKCR\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\localserver32
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-
   Opens key
444553540000}\inprochandler32
                                              \label{lem:hkcrclsid} $$HKCR\clsid{ca8a9780-280d-11cf-a24d-444553540000}\nprochandler 32 $$
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprochandlerx86
                                              HKCR\clsid\\ \{ca8a9780-280d-11cf-a24d-444553540000\\ \\ \inprochandlerx86
   Opens key:
   Opens key
                                              HKCU\software\classes\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\localserver
   Opens key:
                                              HKCR\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\localserver
   Opens key:
                                              \label{local-equation} HKCU \setminus software \setminus classes \setminus appid \setminus \{bbaa0e44-3862-490c-8e63-ac2d2d6ef733\}
   Opens key:
                                              HKCR\appid\{bbaa0e44-3862-490c-8e63-ac2d2d6ef733}
   Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\msvcr80.dll
   Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\msvcp80.dll
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acropdf.dll
                                              HKCU\software\adobe\acrobat reader\9.0\originals
   Opens key:
   Opens key:
                                              4fcb-11cf-aaa5-00401c6085003
   Opens key:
                                              HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
4fcb-11cf-aaa5-00401c608555}
                                              HKLM\software\microsoft\active setup\installed components\{22d6f312-
   Opens kev:
b0f6-11d0-94ab-0080c74c7e95}
                                              HKLM\software\microsoft\active setup\installed components\{283807b5-
   Opens kev:
2c60-11d0-a31d-00aa00b92c03}
                                              HKLM\software\microsoft\active setup\installed components\{3af36230-
   Opens key
a269-11d1-b5bf-0000f8051515}
                                              HKLM\software\microsoft\active setup\installed components\{44bba840-
   Opens key:
cc51-11cf-aafa-00aa00b6015c}
   Opens key:
                                              HKLM\software\microsoft\active setup\installed components\{44bba842-
cc51-11cf-aafa-00aa00b6015b}
   Opens key:
                                              HKLM\software\microsoft\active setup\installed components\{44bba848-
cc51-11cf-aafa-00aa00b6015c}
   Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ active setup\+ installed components\+ \{45ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75a0-164ea75
a269-11d1-b5bf-0000f8051515}
   Opens key:
                                              HKLM\software\microsoft\active setup\installed components\{4f216970-
c90c-11d1-b5c7-0000f8051515}
   Opens key
                                              HKLM\software\microsoft\active setup\installed components\{5a8d6ee0-
3e18-11d0-821e-444553540000}
   Opens key:
                                              0471-11d2-af11-00c04fa35d02}
                                              Opens key
ecbd-11cf-8b85-00aa005b4340}
                                              HKLM\software\microsoft\active setup\installed components\{89820200-
   Opens key
ecbd-11cf-8b85-00aa005b4383}
                                             HKLM\software\microsoft\active setup\installed components\{9381d8f2-
   Opens key
0288-11d0-9501-00aa00b911a5}
                                              \label{lem:hklmsoftware} HKLM \software \microsoft \micros
   Opens key
3bdd-11d0-821e-444553540000}
   Opens key:
                                              a4bf-11d1-9948-00c04f98bbc9}
   Oueries value:
                                              HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Queries value:
                                              {\tt HKLM \ } system \verb| current control \verb| session manager[safedll sear chmode] \\
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
```

```
Oueries value:
                                   HKLM\software\microsoft\windows
nt \verb| current version \verb| compatibility 32[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb]| and the sum of the su
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:
                                   HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Oueries value:
                                   HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Oueries value:
                                   HKCR\interface[interfacehelperdisableall]
                                   HKCR\interface[interfacehelperdisableallforole32]
  Oueries value:
                                   {\tt HKCR \setminus interface[interface helperdisable type lib]}
  Queries value:
                                   HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
000000000046}[interfacehelperdisableall1
                                   HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
00000000046} [interfacehelperdisableallforole32]
                                   .
HKLM\system\setup[systemsetupinprogress]
  Oueries value:
                                   HKCU\control panel\desktop[multiuilanguageid]
  Oueries value:
                                   HKCU\control panel\desktop[smoothscroll1
  Oueries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
                                   HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disableimprovedzonecheck]
                                   HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                   HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:
                                   HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:
                                   HKCU\keyboard layout\toggle[language hotkey]
  Oueries value:
                                   HKCU\keyboard layout\toggle[hotkey]
                                   HKCU\keyboard layout\toggle[layout hotkey]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\ctf[enableanchorcontext]
                                   HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:
  Queries value:
                                    HKCU\control panel\desktop[lamebuttontext]
                                   HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:
  Queries value:
                                   HKCU\software\microsoft\ctf[disable thread input manager]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus fontsubstitutes \ [ms
  Queries value:
shell dlg]
  Queries value:
                                   {\tt HKLM \setminus software \setminus microsoft \setminus ole[maximum allowed allocation size]}
  Queries value:
                                   HKLM\software\microsoft\com3[com+enabled]
  Queries value:
                                   {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create process]}
  Oueries value:
                                   HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
  Oueries value:
                                   HKLM\software\microsoft\com3[regdbversion]
  Oueries value:
                                   HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
  Oueries value:
                                   HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
  Oueries value:
                                   \label{lem:hklm} \verb+Kklm/software/microsoft/internet explorer/setup[iexplorelastmodifiedlow]+ \\
  Oueries value:
                                   HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
                                   HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
  Oueries value:
ab78-1084642581fb]
  Queries value:
                                   HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-00000000000000]
                                   HKLM\system\currentcontrolset\control\session
  Oueries value:
manager[safeprocesssearchmode]
  Queries value:
                                   HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
  Queries value:
                                   HKLM\software\microsoft\internet explorer\setup[installstarted]
                                   HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
  Queries value:
  Queries value:
                                   HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
  Queries value:
                                   HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
  Queries value:
                                   HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
  Oueries value:
                                   HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:
                                   HKLM\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                   HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Queries value:
  Queries value:
                                   HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Oueries value:
                                   HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Oueries value:
                                   HKLM\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:
                                   HKCU\software\microsoft\internet explorer\main[framemerging]
  Queries value:
                                   HKLM\software\microsoft\internet explorer\main[framemerging]
  Queries value:
                                   HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:
                                   HKLM\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:
                                   HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Oueries value:
                                   \label{lem:hklm} \verb+Kklm \+ software + microsoft + internet explorer + main[admintabprocs]
  Oueries value:
                                   HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
                                   HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
                                   HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:
                                   \label{local-operator} \verb|HKLM\| software \verb|\| microsoft\| internet explorer \verb|\| main[navigation delay]| \\
  Oueries value:
```

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows\current version$} \parbox{$\mbox{$policies$} \explorer[nonethood]$} \end{tabular}$ 

```
Oueries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Queries value:
\label{thm:local_explorer} HKCU \ software \ `microsoft \ `windows \ `current version \ `policies \ `explorer[no common groups] \ .
  Queries value:
                           HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
  Oueries value:
                           HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                           HKLM\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [enforces hellex tension security]
                           HKLM\software\microsoft\windows\currentversion\shell
 Oueries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x4011
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0x4011
  Queries value:
                           HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
                           HKCR\clsid\{871c5380-42a0-1069-a2ea-
 Queries value:
08002b30309d}\inprocserver32[inprocserver32]
                           HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
  Queries value:
  Queries value:
                           HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
                           HKLM\software\policies\microsoft\internet
  Queries value:
explorer\main[security_hklm_only]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[certificaterevocation]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablepassport]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[idnenabled]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[cachemode]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
settings[enablenegotiate]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebasicoverclearchannel]
  Oueries value:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[syncmode5]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[signature]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
settings\5.0\cache\content[cacheprefix]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cachelimit]
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings\5.0\cache\history[peruseritem]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[historv]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
{\tt settings \ `5.0 \ `cache \ 'history [cacheprefix]}
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
```

```
HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
   Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                                             \label{thm:cosoft} \begin{tabular}{ll} HKCU \software \mbox{$\dot{$}$ icrosoft \windows \current version \end{tabular} in termet \end{tabular}
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                             \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
   Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
   Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012014033120140407[cacheprefix]|
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                                             \label{thm:local_equation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt local_equation}
   Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
   Queries value:
                                             \label{thm:local_equation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt local_equation}
settings[disableworkerthreadhibernation]
                                             HKLM\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disableworkerthreadhibernation]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                                             \label{thm:linear} \mbox{HKCU\software\mbox{\sc windows\currentversion\sc internet}} \\
   Queries value:
settings[socketreceivebufferlength]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxhttpredirects]
                                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
   Queries value:
settings[maxconnectionsperserver]
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Oueries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
```

```
HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[serverinfotimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
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
 Oueries value:
settings[certcachenovalidate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Queries 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]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[disablecachingofsslpages]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[perusercookies]
                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
 Queries value:
settings[leashlegacycookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablelegacypreauthasserver]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablelegacypreauthasserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
settings[bypasssslnocachecheck]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                          \label{lem:hklm} \verb+Kklm\+ software\+ incrosoft\+ windows\+ current version\+ internet
 Queries value:
settings[sharecredswithwinhttp]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[mimeexclusionlistforcache]}
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
```

settings[dnscacheentries]

```
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscachetimeout]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                                  \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[warnalwaysonpost]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonhttpstohttpredirect]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [winsock\_registry\_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
Queries value:
Oueries value:
Queries value:
Queries value:
Queries value:
Queries value:
Queries value:
Queries value:
Oueries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [serial\_access\_num] \ system \ namespace\_catalog 5 [serial\_access\_num] \ namespace\_catalog 5 [serial\_access\_num] \ namespace\_catalog 5 \ namespace
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ (catalog\_entries \ 0000000000001[library path]) \ (catalog\_entries \ names \ pace\_catalog5 \ (catalog\_entries \ names \ pace\_catalog5) \ (catalog\_entries \ names \
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 10000000000001 \ [displaystring]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001faddressfamily1
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
  Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 000000000001[stores service class in fo]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 0000000000002[library path]
  Queries value:
HKLM \ system \ current controls et \ services \ win sock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 0000000000002 [displaystring]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 00000000000002 [providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
Queries value:
Queries value:
HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog5 \ \ catalog\_entries \ \ \ 0000000000002 \ [version]
  Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000002 [storesservice class in fo]]
  Queries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
  Oueries value:
Oueries value:
```

```
Oueries value:
HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog5 \ \ catalog\_entries \ \ \ 0000000000003 \ [enabled]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
  Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 00000000003 \ [storesserviceclass info]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Oueries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters[ws2 32spincount]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial1
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[urlencoding]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[badproxyexpirestime]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
                           HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[urlencoding]
  Queries value:
                           HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
  Queries value:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Oueries 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]
  Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Oueries value:
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + drivers + 32 [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]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Oueries value:
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midil
  Oueries value:
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midil]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Queries value:
HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer1]
  Queries value:
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer2]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 6]
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 7]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ telephony \ [tapi32 max numrequest retries]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
  Queries value:
                           {\tt HKLM \setminus software \setminus microsoft \setminus tracing[enable consolet racing]}
  Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
```

```
Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32[maxfilesize]
  Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:
                           \label{lem:hklmsoftware} \verb+microsoft+ windows+ current version+ explorer+ user shell
folders[common appdata]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
                           HKLM\system\currentcontrolset\control\productoptions[producttype]
  Oueries value:
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[local settings]
                           HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\winlogon[rsopdebuglevel]
                           HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Oueries value:
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
 Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
 Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion[programfilesdir]
                           HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
  Queries value:
                           HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyoverride]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
  Queries value:
settings[autoconfigurl]
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings\connections[savedlegacysettings]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
{\tt settings \backslash connections[default connection settings]}
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
  Queries value:
                           HKCU\software\microsoft\internet explorer[no3dborder]
  Queries value:
                           HKLM\software\microsoft\internet explorer[no3dborder]
  Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
  Queries 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:
                           HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Queries value:
                           \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\user agent[platform]
                           HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver[*]
                           HKCU\software\microsoft\internet explorer\international[acceptlanguage]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:
                           HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
                           HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters| winsock [mapping]
  Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [max sock addrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [helperdllname]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
```

```
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
 Queries value:
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[appid]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel1
                         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-beb9-9fe3c77a297a}[appid]
 Oueries value:
                         HKCR\clsid\{6935db93-21e8-4ccc-beb9-
 Oueries value:
9fe3c77a297a}\inprocserver32[threadingmodel]
                         HKCU\software\microsoft\windows\currentversion\explorer\runmruſmrulistl
 Oueries value:
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
 Queries value:
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
 Oueries value:
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[appid]
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                         HKCR\clsid\{00bb2763-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
                         HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[appid]
 Oueries value:
                         HKCR\clsid\{00bb2763-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                         HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
  Queries value:
Queries value:
\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \explorer \advanced [list views crollover]
 Queries value:
Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| [listview water mark] \\ \end{tabular}
 Queries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
 Oueries value:
                         HKLM\software\microsoft\rpc\securityservice[10]
 Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                         HKLM \verb|\system| current control \verb|\spicache| msapsspc.dll[name]|
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
 Oueries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
 Oueries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
                         HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                         HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
 Oueries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Queries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
  Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
 Queries value:
HKLM \setminus system \setminus current control \\ \  \mid sa \setminus spicache \setminus msnsspc.dll[tokensize]
 Queries value:
                         HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [autodial dll]]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [query adapter name]
 Queries value:
HKLM \verb|\system| current control set \verb|\services| to pip \verb|\parameters| [disable adapter domain name]|
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
```

```
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall1]
                      HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[quervipmatching]
 Oueries value:
                      HKLM\svstem\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
Queries value:
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [register wan adapters]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Queries value:
Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [registration maxaddress count]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
                      HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
 Oueries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [multicasts end level]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]
 Queries value:
Queries value:
                      HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
 Queries value:
c7d49d7cecdc}[enabledhcp]
 Oueries value:
c7d49d7cecdc}[leaseobtainedtime]
 Queries value:
c7d49d7cecdc}[leaseterminatestime]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
                      HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Oueries value:
 Oueries value:
                      {\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| parameters [domain] \\
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
```

```
c7d49d7cecdc}[queryadaptername]
  Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-a
c7d49d7cecdc}[disableadapterdomainname]
  Queries value:
c7d49d7cecdc}[registrationenabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
  Oueries value:
c7d49d7cecdc}[registrationmaxaddresscount]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
  Oueries value:
c7d49d7cecdc}[ipautoconfigurationenabled]
  Oueries value:
c7d49d7cecdc}[addresstype]
  Queries value:
c7d49d7cecdc}[nameserver]
  Queries value:
c7d49d7cecdc}[dhcpnameserver]
                                 HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsnbtlookuporder]
                                 \label{thm:local} \verb+HKLM\software\microsoft\cryptography\defaults\provider\microsoft\ strong
  Queries value:
cryptographic provider[type]
  Queries value:
                                 HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
                                 HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
  Queries value:
                                 HKCU\software\microsoft\internet
explorer\ietld\lowmic[ietlddllversionlow]
  Queries value:
                                 HKCU\software\microsoft\internet
explorer\ietld\lowmic[ietlddllversionhigh]
  Oueries value:
                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
  Queries value:
                                 HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
                                 HKCR\mime\database\content type\text/html[extension]
  Queries value:
  Oueries value:
                                 HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_mime_sniffing[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                 HKLM\software\microsoft\internet
  Oueries value:
\verb|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]|
                                 HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_feeds[*]
                                 HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_safe_bindtoobject[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                 HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
                                 HKCR\clsid\{25336920-03f9-11cf-8fd0-
  Queries value:
00aa00686f13}\inprocserver32[inprocserver32]
  Queries value:
                                 HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
                                 HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
  Oueries value:
  Queries value:
                                 HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
  Queries value:
                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
                                 HKLM\software\microsoft\internet
  Queries value:
explorer \verb|\main| feature control \verb|\feature_object_caching[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                 HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_object_caching[*]
  Queries value:
                                 HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:
                                 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]
  Queries value:
                                 HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
  Queries 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| feature| filedownload[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Oueries value:
                                 HKLM\software\microsoft\internet
```

explorer\main\featurecontrol\feature\_restrict\_filedownload[\*]

```
Queries value:
                          HKCR\protocols\handler\about[clsid]
 Oueries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
 Oueries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
 Queries value:
                          HKCR \verb|\clsid|{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[2106]
 Queries value:
                          HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
 Queries value:
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet settings\url
historv[davstokeep]
                          HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Oueries value:
                          HKCU\software\microsoft\internet explorer[smartdithering]
 Oueries value:
 Oueries value:
                          HKCU\software\microsoft\internet explorer[rtfconverterflags]
 Oueries value:
                          HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
                          HKCU\software\microsoft\internet explorer\main[usecleartype]
 Queries value:
                          HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[page_transitions]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[page_transitions]
                          HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[use_dlgbox_colors]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer\main[anchor
underline]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[anchor underline]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[css_compat]
                          HKCU\software\microsoft\internet explorer\main[expand alt text]
 Oueries value:
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer\main[display inline
images]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[display inline images]
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer\main[display inline
videos]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[display inline videos]
                          HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[play_background_sounds]
 Oueries value:
 Queries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[play_animations]
 Queries value:
                          HKLM\software\policies\microsoft\internet
explorer\main[print_background]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[print_background]
 Oueries value:
 Oueries value:
 Oueries value:
 Queries value:
```

HKCU\software\microsoft\internet explorer\main[play\_background\_sounds] HKLM\software\policies\microsoft\internet explorer\main[play\_animations]

 $\label{lem:hkcu} \verb+KKCU\software\microsoft\nternet explorer\main[use stylesheets]$ HKLM\software\policies\microsoft\internet explorer\main[smoothscroll] HKCU\software\microsoft\internet explorer\main[smoothscroll] HKLM\software\policies\microsoft\internet explorer\main[xmlhttp] HKCU\software\microsoft\internet explorer\main[xmlhttp] Queries value: Oueries value: HKLM\software\policies\microsoft\internet explorer\main[show image

nlaceholders1

Oueries value: HKCU\software\microsoft\internet explorer\main[show image placeholders] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[disable script

debugger]

Oueries value: HKCU\software\microsoft\internet explorer\main[disable script debugger] HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie] Oueries value: HKCU\software\microsoft\internet explorer\main[move system caret] Queries value:  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet explorer\+ main[force offscreen]$ Oueries value: composition1

Oueries value: autoimageresize]

HKLM\software\policies\microsoft\internet explorer\main[enable

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

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

HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest] Oueries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest] Queries value: HKLM\software\microsoft\internet explorer\main[xdomainrequest] Queries value: HKLM\software\policies\microsoft\internet explorer\main[domstorage]

 $\label{local-observable} \begin{tabular}{ll} HKCU\software\mbox{$\stackrel{\cdot}{m}$icrosoft\internet explorer\mbox{$\stackrel{\cdot}{m}$icrosoft}$} \\ \end{tabular}$ Queries value: HKLM\software\microsoft\internet explorer\main[domstorage] Oueries value:

HKCU\software\microsoft\internet Oueries value:

explorer\international[default\_codepage]

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

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

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

size]

color1

Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font

face]

Queries value: HKCU\software\microsoft\internet explorer\settings[disable visited hyperlinks] Oueries value: HKCU\software\microsoft\internet explorer\settings[use anchor hover

Oueries value: HKCU\software\microsoft\internet explorer\settings[miscflags]  $\label{lower} \verb+KCU\+ software\+ microsoft\+ windows\+ current version\+ policies\+ [allow - the content of t$ Queries value:

programmatic cut\_copy\_paste]

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

```
Oueries value:
                                                    HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsize]
   Oueries value:
                                                    HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
   Queries value:
                                                    HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
   Queries value:
                                                    HKCU\software\microsoft\internet
explorer\international\scripts\3[iefixedfontname]
   Oueries value:
                                                    HKLM\software\microsoft\internet explorer\version vector[vml]
    Oueries value:
                                                    HKLM\software\microsoft\internet explorer\version vector[ie]
   Oueries value:
                                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Oueries value:
                                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature zone elevation[*]
                                                    HKLM\software\microsoft\internet
   Oueries value:
explorer \verb|\main| feature| control \verb|\feature| feature| feature|
                                                    HKLM\software\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature xssfilter[*]
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones[securitysafe]
                                                    HKLM\software\microsoft\internet
   Queries value:
explorer \verb|\main| featurecontrol| feature\_behaviors[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
   Oueries value:
                                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[*]
   Queries value:
                                                    HKLM\software\microsoft\internet explorer\default behaviors[discovery]
                                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
   Queries value:
                                                    HKCR\clsid \ \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\} \ \ inprocserver 32[]
    Queries value:
                                                    HKCR \verb|\clsid|{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid]
                                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82
   Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
   Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
   Queries value:
                                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[cointernetcombineiuricachesize]
   Queries value:
                                                    HKLM\software\microsoft\internet
explorer \\ \verb|main| featurecontrol| feature_subdownload_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ expl
                                                    HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
   Oueries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
                                                    HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[securityidiuricachesize]
   Oueries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
   Queries value:
                                                    HKLM\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
   Queries value:
                                                    HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                                    HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
   Queries value:
                                                    HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
   Queries value:
                                                    HKCR\clsid\{50d5107a-d278-4871-8989-
   Oueries value:
f4ceaaf59cfc}\inprocserver32[threadingmodel]
                                                    HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
   Oueries value:
431b3828ba53}\inprocserver32[inprocserver32]
                                                    HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
   Queries value:
                                                    HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
   Oueries value:
                                                    HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
   Oueries value:
431b3828ba53}\inprocserver32[threadingmodel]
                                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-
   Oueries value:
869523e2d6c7}\inprocserver32[inprocserver32]
                                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
   Queries value:
   Queries value:
                                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
                                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-
   Queries value:
869523e2d6c7}\inprocserver32[threadingmodel]
   Oueries value:
                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Queries value:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
                                                    HKLM \setminus software \setminus icrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc
   Queries value:
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
   Oueries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
    Queries value:
                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
    Queries value:
                                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
   Queries value:
00aa00bbbb58}\inprocserver32[threadingmodel]
    Queries value:
                                                    HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:
                                                    HKLM\system\currentcontrolset\control\nls\language groups[1]
    Oueries value:
                                                    HKLM\software\microsoft\ole[defaultaccesspermission]
   Queries value:
                                                    HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
    Queries value:
                                                    HKCU\software\microsoft\internet explorer\recovery[autorecover]
   Queries value:
                                                    HKLM\software\microsoft\internet
explorer \\ \verb|main| featurecontrol| feature_scripturl_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\
   Queries value:
                                                    HKLM\software\microsoft\internet explorer\default behaviors[homepage]
    Oueries value:
                                                    HKLM\software\microsoft\internet
explorer \\ \verb|main| featurecontrol| feature\_use\_windowedselectcontrol[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Oueries value:
                                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
                                                    \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows script\+settings[jitdebug]
    Queries value:
   Oueries value:
                                                    HKCU\software\microsoft\internet explorer\new
windows[accuserinitonclick]
```

```
Oueries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
  Oueries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Oueries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[appid]
  Queries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[threadingmodel]
                                   HKLM \verb|\system| current controlset| control \verb|\nls|| codepage[1250]
  Queries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1253]
                                   HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1258]
                                   HKLM\system\currentcontrolset\control\nls\codepage[874]
  Queries value:
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\nls\codepage[932]
                                   HKLM\svstem\currentcontrolset\control\nls\codepage[936]
  Oueries value:
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\nls\codepage[949]
                                   HKLM\system\currentcontrolset\control\nls\codepage[1361]
  Oueries value:
                                   HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\24[iefontsize]
                                   HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\24[iefontsizeprivate]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\international\scripts\24[iepropfontname]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\international\scripts\24[iefixedfontname]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\international[codepointtofontmap]
  Oueries value:
                                   HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsize]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsizeprivate]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\international\scripts\26[iepropfontname]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\international\scripts\26[iefixedfontname]
                                   HKCR\clsid\{81397204-f51a-4571-8d7b-
  Queries value:
dc030521aabd}\inprocserver32[inprocserver32]
  Oueries value:
                                   HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]
  Queries value:
                                   \label{localization} $HKCR\clsid_{81397204-f51a-4571-8d7b-dc030521aabd}[appid]$
  Queries value:
                                   HKCR\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKCR\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
  Oueries value:
  Oueries value:
                                   HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[appid]
  Oueries 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-
  Oueries value:
00c04fd9189d}\inprocserver32[inprocserver32]
  Oueries value:
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[appid]
  Oueries value:
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
  Oueries value:
00c04fd9189d}\inprocserver32[threadingmodel]
  Queries value:
                                   HKCR\mime\database\content type\image/gif[extension]
  Oueries value:
                                   HKLM\hardware\devicemap\video[maxobiectnumber]
  Oueries value:
                                   HKLM\hardware\devicemap\video[\device\video01
                                   HKLM\hardware\devicemap\video[\device\video1]
  Oueries value:
  Queries value:
                                   HKLM\hardware\devicemap\video[\device\video2]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\bug![name]
                                   HKLM\software\microsoft\directdraw\compatibility\bug![flags]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\bug![id]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
                                   HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
  Queries value:
                                   HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus norton system in fo[flags]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\savage[name]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\savage[flags]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\savage[id]
  Queries value:
                                   HKLM \verb|\software\microsoft\directdraw\compatibility \verb|\scorchedplanet[name]|
  Oueries value:
                                   \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} which is a constant, and the local hammon ha
  Oueries value:
                                   \label{lem:hklmsoftware} \verb+microsoft\directdraw\compatibility\scorchedplanet[id]
  Oueries value:
                                   \label{lem:hklm} \verb+Kklm/software/microsoft/directdraw/compatibility/silentthunder[name]
                                   \label{lem:hklm} \verb+Kklm/software/microsoft/directdraw/compatibility/silentthunder[flags]
  Oueries value:
  Queries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ directdraw\+ compatibility\+ silentthunder[id]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\terracide[name]
                                   HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus terracide[flags]
  Oueries value:
```

```
Oueries value:
                          HKLM\software\microsoft\directdraw\compatibility\terracide[id]
 Oueries value:
                          HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]
 Oueries value:
                          Oueries value:
                          \label{lem:hammon} \verb|HKLM| software \verb|\microsoft| direct draw| compatibility \verb|\thirddimension[id]| \\
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
 Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
 Oueries value:
HKLM\software\microsoft\directdraw\compatibilitv\ziffdavisqualitvbenchmark[id]
 Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
 Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdayiswinmarkbenchmark[f]ags]
 Oueries value:
HKLM\software\microsoft\directdraw\compatibilitv\ziffdaviswinmarkbenchmark[id]
                          HKLM\software\microsoft\directdraw[modexonlv]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\directdraw[emulationonlv]
 Oueries value:
                          HKLM\software\microsoft\directdraw[showframerate]
                          HKLM\software\microsoft\directdraw[enableprintscreen]
 Queries value:
                          HKLM\software\microsoft\directdraw[forceagpsupport]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\directdraw[disableagpsupport]
 Queries value:
                          HKLM\software\microsoft\directdraw[disablemmx]
 Queries value:
                          HKLM\software\microsoft\directdraw[disableddscapsinddsd]
 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]
 Queries value:
                          HKLM\software\microsoft\directdraw[owndc]
 Oueries value:
                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[appid]
 Queries value:
                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
 Queries value:
f941e9b7e1fe}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\dximagetransform.microsoft.shadow\clsid[]
                          HKCR\clsid\{e71b4063-3e59-11d2-952a-
 Queries value:
00c04fa34f05}\inprocserver32[inprocserver32]
                          HKCR \ clsid \ \{e71b4063-3e59-11d2-952a-00c04fa34f05\} \ inprocserver 32[]
 Queries value:
 Oueries value:
                          HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[appid]
 Queries value:
                          HKCR\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\tinprocserver32[]
 Oueries value:
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[appid]
 Oueries value:
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[appid]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
 Queries value:
                          HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
 Oueries value:
                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Oueries value:
77e8f3d1aa80\} \land category \land em \land \{c6debc0a-f2b2-4f17-930e-ca9faff4cd04\} [iconindex]
 Oueries value:
                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[iconindex]
                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Oueries value:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[iconindex]
                          HKLM\software\microsoft\internet explorer\main[maxrenderline]
 Queries value:
                          HKCR\mime\database\content type\image/png[extension]
 Queries value:
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-
 Queries value:
00aa006c1a01}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
 Oueries value:
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-
 Oueries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-
 Queries value:
00aa006c1a01}\inprocserver32[inprocserver32]
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
 Oueries value:
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
 Oueries value:
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-
 Queries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                          HKCR\mime\database\content type\image/bmp\bits[0]
 Queries value:
                          HKCR\mime\database\content type\image/gif\bits[0]
 Queries value:
 Queries value:
                          HKCR\mime\database\content type\image/jpeg\bits[0]
 Queries value:
                          HKCR\mime\database\content type\image/pjpeg\bits[0]
 Queries value:
                          HKCR\mime\database\content type\image/png\bits[0]
 Oueries value:
                          HKCR\mime\database\content type\image/x-png\bits[0]
 Queries value:
                          HKCR\mime\database\content type\image/x-wmf\bits[0]
 Queries value:
                          \label{local-equation} \mbox{HKCR\mbox{$\mbox{$mime$}\alese$} \mbox{$\mbox{$\mbox{$clsid$}$}]} $$
 Queries value:
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
 Queries value:
 Oueries value:
                          HKCR \verb|\clsid|{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
 Oueries value:
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
                          HKCU\appevents\schemes\apps\explorer\navigating\.current[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
 Queries value:
```

```
Queries value:
                                               HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\{[appid]}
   Oueries value:
                                               HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
                                               HKLM\software\microsoft\direct3d[disablemmx]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\direct3d[disablex3d]
   Oueries value:
                                               HKLM\software\microsoft\direct3d[fewvertices]
   Queries value:
                                               HKLM\software\microsoft\direct3d[disablevidmemvbs]
   Oueries value:
                                               HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[local appdata]
   Oueries value:
                                               HKCR\mime\database\content type\image/jpeg[extension]
                                               HKCR\shockwaveflash.shockwaveflash\clsid[]
   Oueries value:
                                               HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Oueries value:
444553540000}\inprocserver32[inprocserver32]
   Oueries value:
                                               HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[]
                                               HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[appid]
   Oueries value:
                                               HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Oueries value:
444553540000}\inprocserver32[threadingmodel]
                                               HKLM\software\microsoft\directx[glitchinstrumentation]
   Oueries value:
                                               HKLM\hardware\description\system\centralprocessor\0[~mhz]
   Oueries value:
                                               HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
   Queries value:
                                               HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
   Queries value:
   Queries value:
                                               HKLM\software\microsoft\internet explorer\default behaviors[userdata]
   Queries value:
                                               HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
   Queries value:
                                               HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
   Queries value:
                                               HKCR\drive\shellex\folder extensions\f(beb8a05-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44442-804e-beee-44440-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-46
409d6c4515e9}[drivemask]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
                                               HKLM\software\microsoft\internet explorer\default behaviors[clientcaps]
                                               HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\3[2000]
   Queries value:
                                               HKLM\software\microsoft\internet explorer\feed discovery[sound]
                                               HKCU\software\microsoft\ftp[use web based ftp]
   Queries value:
                                               HKCU\software\microsoft\internet
   Queries value:
explorer\services[selectionactivitybuttondisable]
   Oueries value:
                                               HKCU\software\microsoft\internet explorer\suggested sites[enabled]
   Queries value:
                                               HKLM\system\wpa\pnp[seed]
   Queries value:
                                               HKLM\system\setup[osloaderpath]
   Queries value:
                                               HKLM\system\setup[systempartition]
   Oueries value:
                                               HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
   Queries value:
                                               HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
                                               HKLM\software\microsoft\windows\currentversion[devicepath]
   Queries value:
                                               HKLM\software\microsoft\windows\currentversion\setup[loglevel]
   Oueries value:
   Oueries value:
                                               HKLM\software\microsoft\windows\currentversion\setup[logpath]
   Oueries value:
11e3-9fc7-806d6172696f}[data]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[generation]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
   Queries value:
                                               HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Queries value:
\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \policies \explorer [separate process]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
\label{thm:local_hammon} \begin{tabular}{l} HKCU \software \verb|\microsoft| windows \current version \policies \explorer[nosimple startmenu] \end{tabular}
                                               \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidden \cite{tabular} \end{tabular}
   Queries value:
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidefile ext\cite{tabular} \end{tabular}
   Oueries value:
\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced[dontprettypath]}}
   Queries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} is a constant \cite{tabular} and \
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| fide icons| \\ \end{tabular}
   Queries value:
\label{thm:local_map} \begin{tabular}{ll} HKCU \software \verb|microsoft| windows \verb|currentversion| explorer \verb|advanced[mapnetdrvbtn]| \\ \end{tabular}
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                               HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Oueries value:
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
   Queries value:
```

```
HKCU \ software \ `microsoft \ 'windows \ 'current version' explorer \ 'advanced [separate process]
   Oueries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| explorer \end{tabular} and the linear law is a substitution of the law is a substitution of the linear law is a substitution of the law is a substitution of the linear law is a substitution of the law is a substitution of the linear law is a substitution of the law is a su
   Oueries value:
                                            HKCR\directory[docobject]
   Queries value:
                                            HKCR\directory[browseinplace]
   Oueries value:
                                            HKCR\directory[isshortcut]
   Queries value:
                                            HKCR\directory[alwaysshowext]
   Oueries value:
                                            HKCR\directory[nevershowext]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobject]
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[browseinplace]
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[isshortcut]
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[alwaysshowext]
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[nevershowext]
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-
   Oueries value:
444553540000}\inprocserver32[loadwithoutcom]
  Queries value:
                                            HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
  Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
  Queries value:
                                            HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x4011
   Queries value:
                                            \label{local-objective} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\shell}} \\
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
   Oueries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
   Queries value:
                                            HKCR\clsid\{ff393560-c2a7-11cf-bff4-
   Queries value:
444553540000}\inprocserver32[threadingmodel]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cachepath]
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheprefix]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cachelimit]
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
   Queries value:
                                           HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
   Queries value:
                                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell
folders[favorites]
                                            {\tt HKCR} \verb|\|.url\persistenthandler[]|
   Queries value:
                                            HKLM\software\microsoft\windows search[currentversion]
   Queries value:
                                            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[attributes]
                                            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
                                            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[flags]
                                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Queries value:
1757981266-507921405-1957994488-1003[state]
   Oueries value:
                                            1757981266-507921405-1957994488-1003[userpreference]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[centralprofile]
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[profileloadtimelow]
                                            1757981266-507921405-1957994488-1003[profileloadtimehigh]
                                            HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
   Queries value:
   Queries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\windows \ system 32 \ shell 32.dll, -9216]
                                            HKLM\software\microsoft\internet explorer\activex
   Queries value:
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[compatibility flags]
                                            HKLM\software\microsoft\internet explorer\activex
   Queries value:
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[miscstatus flags]
   Queries value:
                                            HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\mbox{\mbox{$$m$iscstatus$$\1[]$}}
   Queries value:
                                            HKLM\software\microsoft\downloadmanager[cacheok]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\domstorage\total[]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
   Queries value:
                                            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
                                            HKCR \c1sid \f3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \c1sid \f3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \c3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \c3b8a2d94-0ac9-11d1-896c-00c04fb6bf
   Oueries value:
                                            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
   Oueries value:
                                            HKCR\clsid\{9ba05972-f6a8-11cf-a442-
   Oueries value:
00a0c90a8f39}\inprocserver32[inprocserver32]
   Oueries value:
                                            HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32[]
                                            HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[appid]
   Oueries value:
```

```
Oueries value:
                                            HKCR\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32[threadingmodel]
                                           HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
   Oueries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
   Queries value:
                                           HKCR\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[inprocserver32]
                                            \label{locality} HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\ \ inprocserver32[]
   Queries value:
   Oueries value:
                                            HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
   Oueries value:
                                           HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}[appid]
   Oueries value:
                                            HKCR\clsid\{f5078f35-c551-11d3-89b9-
   Oueries value:
0000f81fe221}\inprocserver32[threadingmodel]
                                            HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]
   Oueries value:
                                            HKCR\clsid\{00020424-0000-0000-c000-00000000046}[appid]
   Oueries value:
                                            HKCR\clsid\{00020424-0000-0000-c000-
   Oueries value:
00000000046}\inprocserver32[threadingmodel]
                                            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[]
   Queries value:
                                            HKLM\software\microsoft\rpc[udtalignmentpolicy]
   Queries value:
                                            HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32[]
   Queries value:
   Oueries value:
                                            HKCR\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
   Queries value:
                                            HKCR\clsid\{00020420-0000-0000-c000-00000000046}[appid]
   Queries value:
   Queries value:
                                            HKCR\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Queries value:
                                            HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
   Oueries value:
                                            HKCR\clsid\{b8da6310-e19b-11d0-933c-
00a0c90dcaa9}\inprocserver32[inprocserver32]
   Queries value:
                                            HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32[]
                                            HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}[appid]
   Queries value:
                                            HKCR\clsid\{b8da6310-e19b-11d0-933c-
   Queries value:
00a0c90dcaa9}\inprocserver32[threadingmodel]
   Queries value:
                                            HKCR\interface\{00020404-0000-0000-c000-00000000046}\proxystubclsid32[]
                                            HKCR\clsid\{00020421-0000-0000-c000-
   Queries value:
00000000046}\inprocserver32[inprocserver32]
                                            Queries value:
   Queries value:
                                            HKCR\clsid\{00020421-0000-0000-c000-00000000046}[appid]
   Queries value:
                                            HKCR\clsid\{00020421-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Queries value:
                                            \label{lem:hkcr} \begin{tabular}{ll} HKCR\mbox{\content type\application/$x-shockwave-flash[extension]$} \end{tabular}
   Oueries value:
                                            HKCR\mime\database\content type\image/x-icon[extension]
   Oueries value:
                                            HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\nprocserver32[]
   Queries value:
                                            HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[appid]
   Queries value:
   Queries value:
                                            HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[threadingmodel]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1606]
   Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacherepair]
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\userdata[cacheprefix]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\userdata[cachelimit]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\userdata[cacheoptions]
                                            {\tt HKLM \ } software \verb|\ microsoft \ | cryptography \verb|\ defaults \ | provider types \verb|\ types \ | types 
  Queries value:
001[name]
   Queries value:
                                            HKCU\software\macromedia\flashplayer[flashplayerversion]
                                            HKCR\shockwaveflash.shockwaveflash.7\clsid[]
   Queries value:
   Queries value:
                                            HKCR\msxml2.xmlhttp\clsid[]
   Oueries value:
                                            HKCR\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserver32[]
   Queries value:
                                            HKCR\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}[appid]
   Queries value:
                                            HKCR\clsid\{f6d90f16-9c73-11d3-b32e-
   Queries value:
00c04f990bb4}\inprocserver32[threadingmodel]
   Oueries value:
                                            HKCR\shockwaveflash.shockwaveflash.10\clsid[]
   Queries value:
                                            HKCR\.swf[content type]
   Queries value:
                                            HKCR\mime\database\content type\application/x-shockwave-flash[clsid]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\3[1c00]
                                            HKCR\acropdf.pdf.1\clsid[]
   Queries value:
   Queries value:
                                            HKCR\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32[inprocserver32]
   Queries value:
                                            \label{locality} $$ HKCR\clsid{ca8a9780-280d-11cf-a24d-444553540000}\inprocserver32[] $$
   Queries value:
                                            HKCR\clsid\{ca8a9780-280d-11cf-a24d-444553540000}[appid]
   Queries value:
                                            HKCR \land appid \land \{bbaa0e44-3862-490c-8e63-ac2d2d6ef733\} [dllsurrogate]
   Queries value:
                                            HKCR \ appid \ \{bbaa0e44-3862-490c-8e63-ac2d2d6ef733\} [local service]
   Queries value:
                                            HKCR\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32[threadingmodel]
   Queries value:
                                            \label{lem:hkcu} \verb+KKCU\+ software \verb+\adobe+\acrobat+ reader+9.0 \verb+\originals[bbrowserintegration]+ \\
   Oueries value:
                                            HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
4fcb-11cf-aaa5-00401c608500}[isinstalled]
                                           HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
   Oueries value:
4fcb-11cf-aaa5-00401c608500}[version]
   Oueries value:
                                            \label{lem:hklmsoftware} HKLM \ software \ \ setup\ \ installed \ components \ \ \ \{08b0e5c0-bc1, 08b0e5c0-bc1, 
4fcb-11cf-aaa5-00401c608500}[keyfilename]
```

```
HKLM\software\microsoft\active setup\installed components\{22d6f312-
      Oueries value:
b0f6-11d0-94ab-0080c74c7e95}[isinstalled]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}[version]
                                                                                             Queries value:
b0f6-11d0-94ab-0080c74c7e95}[keyfilename]
      Queries value:
                                                                                             2c60-11d0-a31d-00aa00b92c03}[isinstalled]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{283807b5-
2c60-11d0-a31d-00aa00b92c03}[version]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{283807b5-
2c60-11d0-a31d-00aa00b92c03}[keyfilename]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}[isinstalled]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}[version]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}[kevfilename]
                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba840-
      Oueries value:
cc51-11cf-aafa-00aa00b6015c}[isinstalled]
                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba840-
      Queries value:
cc51-11cf-aafa-00aa00b6015c}[version]
                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba840-
      Oueries value:
cc51-11cf-aafa-00aa00b6015c}[keyfilename]
                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba842-
      Queries value:
cc51-11cf-aafa-00aa00b6015b}[isinstalled]
                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba842-
      Queries value:
cc51-11cf-aafa-00aa00b6015b}[version]
                                                                                             Queries value:
cc51-11cf-aafa-00aa00b6015b}[keyfilename]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba848-
cc51-11cf-aafa-00aa00b6015c}[isinstalled]
      Queries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba848-
cc51-11cf-aafa-00aa00b6015c}[version]
      Queries value:
                                                                                              HKLM\software\microsoft\active setup\installed components\{44bba848-
 cc51-11cf-aafa-00aa00b6015c}[keyfilename]
       Queries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{45ea75a0-
 a269-11d1-b5bf-0000f8051515}[isinstalled]
                                                                                             HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{45ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea756a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1
      Queries value:
a269-11d1-b5bf-0000f8051515}[version]
                                                                                             \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in stalled components \end{tabular} \begin{tabular}{ll} 45ea \end{tabular} 75a0-\end{tabular}
       Queries value:
a269-11d1-b5bf-0000f8051515}[keyfilename]
                                                                                             HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{4f216970-microsoft\} \ active \ setup \ \ active \ \ a
      Queries value:
 c90c-11d1-b5c7-0000f8051515}[isinstalled]
                                                                                             HKLM\software\microsoft\active setup\installed components\{4f216970-
      Queries value:
c90c-11d1-b5c7-0000f8051515}[version]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{4f216970-
 c90c-11d1-b5c7-0000f8051515}[keyfilename]
      Queries value:
                                                                                             3e18-11d0-821e-444553540000}[isinstalled]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{5a8d6ee0-
 3e18-11d0-821e-444553540000}[version]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{5a8d6ee0-
3e18-11d0-821e-444553540000}[keyfilename]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}[isinstalled]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}[version]
      Oueries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}[kevfilename]
                                                                                             HKLM\software\microsoft\active setup\installed components\{89820200-
      Oueries value:
ecbd-11cf-8b85-00aa005b4340}[isinstalled]
                                                                                             HKLM\software\microsoft\active setup\installed components\{89820200-
      Queries value:
 ecbd-11cf-8b85-00aa005b4340}[version]
                                                                                             HKLM\software\microsoft\active setup\installed components\{89820200-
      Queries value:
ecbd-11cf-8b85-00aa005b4340}[keyfilename]
      Queries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{89820200-
 ecbd-11cf-8b85-00aa005b4383}[isinstalled]
                                                                                             HKLM\software\microsoft\active setup\installed components\{89820200-
      Oueries value:
ecbd-11cf-8b85-00aa005b4383}[version]
      Queries value:
                                                                                             \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in stalled components \end{tabular} (89820200-1000) and the limit of the latest components \end{tabular} and the latest components \end{tabular} (89820200-1000) and the latest components \end{tabular} and the latest components \end{tabular} (89820200-1000) and the latest components \end{tabular} and the latest \end{tabular}
 ecbd-11cf-8b85-00aa005b4383}[keyfilename]
      Oueries value:
                                                                                             HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{9381d8f2-1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946
 0288-11d0-9501-00aa00b911a5}[isinstalled]
      Queries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{9381d8f2-
0288-11d0-9501-00aa00b911a5}[version]
       Queries value
                                                                                              HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{9381d8f2-1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946, 1946
0288-11d0-9501-00aa00b911a5}[keyfilename]
      Queries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{cc2a9ba0-
 3bdd-11d0-821e-444553540000}[isinstalled]
      Queries value:
                                                                                             HKLM\software\microsoft\active setup\installed components\{cc2a9ba0-
3bdd-11d0-821e-444553540000}[version]
                                                                                             HKLM\software\microsoft\active setup\installed components\{cc2a9ba0-
      Queries value:
 3bdd-11d0-821e-444553540000}[keyfilename]
                                                                                             \label{lem:hammon} \begin{tabular}{ll} HKLM \end{tabular} is software \verb|\microsoft| active setup \end{tabular} is software \verb|\microsoft| active setup \end{tabular} is software \end{tabular} is softw
      Queries value:
 a4bf-11d1-9948-00c04f98bbc9}[isinstalled]
      Queries value:
                                                                                             a4bf-11d1-9948-00c04f98bbc9}[version]
      Oueries value:
                                                                                             \label{lem:hklmsoftware} HKLM \software \microsoft \active setup \nstalled components \end{de} 100-1000 \mbox{de} 100-10000 \mbox{de} 100-1000 \mbox{de} 100-10000 \mbox{de} 10
 a4bf-11d1-9948-00c04f98bbc9}[keyfilename]
      Sets/Creates value:
                                                                                             HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature control| feature | scripturl mitigation [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| the first of th
      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\extensible cache\mshist012016040820160409[cacheprefix] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet  $settings \verb|\| 5.0 \verb|\| cache \verb|\| extensible | cache \verb|\| mshist012016040820160409 [cache limit]|$ Sets/Creates value:  $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\$ settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet  $settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012016040820160409[ cacherepair]|$ Sets/Creates value: HKCU\software\microsoft\internet explorer\domstorage\baidu.com[] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata[cachepath] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\userdata[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\userdata[cacheoptions] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata[cacherepair] HKLM\software\microsoft\cryptography\rng[seed] Value changes: HKCU\software\microsoft\internet explorer\main[disable script debugger] Value changes: Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache] Value changes:  $\label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell}} \\$ folders[cookies] HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[history] Value changes:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet$ settings\zonemap[proxybypass] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet]  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Value changes: settings\zonemap[autodetect] Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common appdata] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[appdata] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable] Value changes:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet$ settings\connections[savedlegacysettings] Value changes: HKLM\software\microsoft\directdraw\mostrecentapplication[name] Value changes: HKLM\software\microsoft\directdraw\mostrecentapplication[id] Value changes: HKLM\software\microsoft\direct3d\mostrecentapplication[name] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[local appdata] Value changes:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ \{f90255c2-6bc4-11e3-9fc7-16bc4-16$ 806d6172696f}[baseclass] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\5.0\cache\extensible cache\mshist012016040820160409[cachepath] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[favorites]

HKCU\software\microsoft\internet explorer\main\windowssearch[version] Value changes: HKCU\software\microsoft\internet explorer\domstorage\total[] Value changes: 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]