Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 718, Task ID: 450007

Task ID: 450007

Risk Level: 7

Date Processed: 2016-04-08 16:37:33 (UTC)

Processing Time: 62.27 seconds
Virtual Environment: IntelliVM

Execution Arguments:

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

Sample ID: 718 Type: basic Owner: admin

Label: 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb

 Date Added:
 2016-04-08 16:37:32 (UTC)

 File Type:
 PE32:win32:gui

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

MD5: 4c838f1570b3a7ff6f491e6ec1ef6895

SHA256: 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb

Description: None

Pattern Matching Results

3 Long sleep detected

5 Possible injector

7 Creates malicious events: FakelE [PUA , Downware]

1 YARA score 1

3 Connects to local host

Checks whether debugger is present

3 HTTP connection - response code 200 (success)

Static Events

YARA rule hit: Nonexecutable
YARA rule hit: SWF

Process/Thread Events

Creates process:

C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
\[\text{C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe} \]

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

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

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

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

Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects_!MSFTHISTORY!_

Creates mutex:

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

Creates mutex:

Creates mutex:

 $\verb|\Sessions|| 1 \\| BaseNamedObjects|| c: !users! admin! appdata! roaming! microsoft! windows! cookies! \\| Cookie$

Creates mutex:

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

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

Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile Creates mutex: \Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208

 $\label{lem:continuous} Creates \ mutex: $$ \Sessions\1\BaseNamedObjects\!PrivacIE\!SharedMemory\!Mutex $$$

Creates mutex: \Sessions\1\BaseNamedObjects_DDrawExclMode_
Creates mutex: \Sessions\1\BaseNamedObjects_DDrawCheckExclMode_
Creates mutex: \Sessions\1\BaseNamedObjects\DDrawWindowListMutex
Creates mutex: \Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex

 $\label{lem:creates} $$ \operatorname{Sessions}\BaseNamedObjects\DirectSound\ DIMain\ mutex\ (0x00000948)$$ $$ \operatorname{Sessions}\BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069}$$$

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

Creates mutex:

 $\verb|\Sessions|1| BaseNamedObjects| c: !users! admin! appdata! local! microsoft! internet explorer! domstore! for the property of the property$

Creates mutex: \Sessions\1\BaseNamedObjects\InternetExplorerDOMStoreQuota

Creates mutex:

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

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

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history.ie5!mshist012016040820160409!

Creates mutex: \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex

Creates event: \KernelObjects\MaximumCommitCondition

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

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

Creates event: \BaseNamedObjects\BFE_Notify_Event_{56eb04b7-1706-4bab-ae1a-

bf60096e9395}

Creates event: \Sessions\1\BaseNamedObjects\DINPUTWINMM

File System Events

```
Creates
                                             C:\Users\Admin
                                             C:\Users\Admin\AppData\Local
   Creates:
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
   Creates:
                                             C:\Users\Admin\AppData\Roaming
   Creates:
   Creates:
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\History
   Creates:
   Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
  Creates:
\label{lem:cosoftwindows} Cookies \ admin@baidu[2].txt
   Creates:
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\index[1].php
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\KQ5TVCON\bd_logo1[1].png
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\X3IPB3Z1\baidu_jgylogo3[1].gif
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\BX3UL1G0\jquery-1.10.2.min_f2fb5194[1].js
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\KQ5TVCON\nuomi_510f7472[1].png
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\X3IPB3Z1\zbios_62c636fe[1].png
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\BX3UL1G0\icons_0e814c16[1].png
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\KQ5TVCON\all_async_search_d0d1b2ec[1].js
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\every_cookie_aa168cb4[1].js
  Creates
                                             C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\6K541L89\www.baidu[1].xml
   Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
   Creates:
Creates:
                                             {\tt C:\Windows\Temporary\ Internet}
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\X3IPB3Z1\bdsug_async_1cb857eb[1].js
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
  Creates:
  Creates:
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\index.dat
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\CYCCFJ6M
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Creates:
Explorer\UserData\28I7G5HR
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Creates:
Explorer\UserData\5IVMI5HF
   Creates:
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\FSLFFMJ7
   Creates:
                                             C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
                                             C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Creates:
{\tt Player\macromedia.com\support\flashplayer\sys\macromedia.com\support\flashplayer\sys\macromedia.com\support\flashplayer\sys\macromedia.com\support\flashplayer\sys\macromedia.com\support\flashplayer\sys\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\macromedia.com\support\support\macromedia.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
                                             C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Creates:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                                             C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Creates:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com
                                             C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Creates:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Creates:
                                             C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\CYCCFJ6M\userDataBIDUPSID[1].xml
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
   Creates:
   Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409
   Creates:
{\tt C: Users Admin App Data Local Microsoft Windows History . IE5 \MSH is to 12016040820160409 \setminus index. data and the state of the stat
                                             C:\Users\Admin\Favorites
   Creates:
   Creates:
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\error[1].htm
   Creates:
                                             {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\KQ5TVCON\favicon[1].ico
                                             \verb|C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico| \\
  Creates:
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\WG2VLW5Y\JSocket_9a52fc3e[1].swf
                                             {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
   Creates:
Files\Content.IE5\WG2VLW5Y\union[1].gif
                                             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\X3IPB3Z1\bdbri_icons_2e35e84b[1].png
Opens: C:\Windows\Prefetch\62DDFBF757BE511F30B6D330963C1-E2075B81.pf
                                             C:\Windows\System32
   Opens:
   Opens:
                                             C:\Windows\System32\sechost.dll
   Opens:
{\tt C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe.Local\temp\columnwidth} \\
                                             C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
   Opens:
                                             C:\Windows\winsxs\x86_microsoft.windows.common-
```

```
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                                         C:\windows\temp\MSIMG32.dll
  Opens:
  Opens:
                                         C:\Windows\System32\msimg32.dll
  Opens:
                                         C:\windows\temp\VERSION.dll
                                         C:\Windows\System32\version.dll
  Opens:
  Opens:
                                         {\tt C:\Windows\System32\imm32.dll}
  Opens:
                                         C:\Windows\WindowsShell.Manifest
  Opens:
                                         C:\program files\qqd1eae\log.dat
                                         C:\Windows\System32\ntdll.dll
  Opens:
                                         C:\windows\temp\msdialg100_D.dll
  Opens:
  Opens:
                                         C:\Windows\system32\msdialg100_D.dll
  Opens:
                                         C:\Windows\system\msdialg100_D.dll
  Opens:
                                         C:\Windows\msdialg100_D.dll
                                         C:\Windows\System32\Wbem\msdialg100_D.dll
  Opens:
                                         C:\Windows\System32\WindowsPowerShell\v1.0\msdialg100_D.dll
  Opens:
  Opens:
                                         C:\windows\temp\MFC90ENut.dll
                                         C:\Windows\system32\MFC90ENut.dll
  Opens:
  Opens:
                                         C:\Windows\system\MFC90ENut.dll
                                         C:\Windows\MFC90ENut.dll
  Opens:
  Opens:
                                         C:\Windows\System32\Wbem\MFC90ENut.dll
  Opens:
                                         C: \verb|\windows| System 32 \le Power Shell \le 1.0 \le MFC 90 EN ut. dll = 1.0 \le Power Shell \le 1.0 \le Power Shell
  Opens:
                                         C:\windows\temp\Afx100net.dll
  Opens:
                                         C:\Windows\system32\Afx100net.dll
  Opens:
                                         C:\Windows\system\Afx100net.dll
  Opens:
                                         C:\Windows\Afx100net.dll
  Opens:
                                         C:\Windows\System32\Wbem\Afx100net.dll
                                         C: \verb|\windows| System 32 \verb|\windows| Power Shell \verb|\v1.0| Afx 100 net.dll| \\
  Opens:
  Opens:
                                         C:\program files\qqd1eae\Log.dat
                                         C:\Program Files\QQd1eae\slowt64.dll
  Opens:
                                         C:\Windows\System32\rpcss.dll
  Opens:
                                         C:\windows\temp\CRYPTBASE.dll
  Opens:
  Opens:
                                         C:\Windows\System32\cryptbase.dll
                                         C:\Windows\System32\uxtheme.dll
  Opens:
                                         C:\Users\Admin\AppData\Local\Temp\restart.dat
  Opens:
  Opens:
                                         C:\windows\temp\dwmapi.dll
  Opens:
                                         C:\Windows\System32\dwmapi.dll
  Opens:
                                         C:\Windows\Fonts\StaticCache.dat
  Opens:
                                         C:\Windows\Fonts\tahoma.ttf
  Opens:
                                         C:\Windows\Fonts\meiryo.ttc
  Opens:
                                         C:\Windows\Fonts\msgothic.ttc
  Opens:
                                         C:\Windows\Fonts\msjh.ttf
                                         C:\Windows\Fonts\msyh.ttf
  Opens:
  Opens:
                                         C:\Windows\Fonts\malgun.ttf
  Opens:
                                         C:\Windows\Fonts\mingliu.ttc
  Opens:
                                         C:\Windows\Fonts\simsun.ttc
  Opens:
                                         {\tt C:\Windows\Fonts\gulim.ttc}\\
  Opens:
                                         C:\Windows\System32\en-US\user32.dll.mui
  Opens:
                                         C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:
                                         {\tt C:\Windows\system32\uxtheme.dll.Config}
  Opens:
                                         C:\Windows\System32\ieframe.dll
  Opens:
                                         C:\Windows\System32\oleacc.dll
  Opens:
                                         C:\windows\temp\OLEACCRC.DLL
  Opens:
                                         C:\Windows\System32\oleaccrc.dll
  Opens:
C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                         C:\windows\temp\ntmarta.dll
  Opens:
                                         C:\Windows\System32\ntmarta.dll
  Opens:
  Opens:
                                         C:\Windows\System32\en-US\urlmon.dll.mui
  Opens:
                                         C:\Windows\System32\shell32.dll
  Opens:
                                         C:\windows\temp\apphelp.dll
  Opens:
                                         C:\Windows\System32\apphelp.dll
  Opens:
                                         C:\WINDOWS\Temp\MJPGC.TMP
  Opens:
                                         C:\Windows\System32\en-US\ieframe.dll.mui
  Opens:
                                         C:\windows\temp\SspiCli.dll
                                         C:\Windows\System32\sspicli.dll
  Opens:
  Opens:
                                         C:\Windows\System32\wininet.dll
  Opens:
                                         C:\windows\temp\profapi.dll
  Opens:
                                         C:\Windows\System32\profapi.dll
  Opens:
                                         C:\Users\Admin
  Opens:
                                         C:\Users\Admin\AppData\Local
                                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet\ Files}
  Opens:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\desktop.ini
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\desktop.ini
                                         C:\Users\Admin\AppData\Roaming
  Opens:
                                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:
  Opens:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Opens:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
                                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
  Opens:
                                         C:\windows\temp\dnsapi.DLL
  Opens:
                                         C:\Windows\System32\dnsapi.dll
  Opens:
                                         C:\windows\temp\iphlpapi.DLL
  Opens:
                                         C:\Windows\System32\IPHLPAPI.DLL
                                         C:\windows\temp\WINNSI.DLL
  Opens:
```

```
Opens:
                         C:\Windows\System32\winnsi.dll
 Opens:
                         C:\windows\temp\RASAPI32.dll
 Opens:
                         C:\Windows\System32\rasapi32.dll
 Opens:
                         C:\windows\temp\rasman.dll
 Opens:
                         C:\Windows\System32\rasman.dll
 Opens:
                         C:\windows\temp\rtutils.dll
 Opens:
                         C:\Windows\Svstem32\rtutils.dll
                         C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens:
 Opens:
                         C:\Windows\Svstem32\ras
                         C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
 Opens:
 Opens:
                         C:\windows\temp\sensapi.dll
 Opens:
                         C:\Windows\System32\SensApi.dll
 Opens:
                         C:\Windows\System32\nlaapi.dll
 Opens:
                         C:\windows\temp\rasadhlp.dll
                         C:\Windows\System32\rasadhlp.dll
 Opens:
 Opens:
                         C:\Windows\System32\NapiNSP.dll
                         C:\Windows\System32\pnrpnsp.dll
 Opens:
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\winrnr.dll
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\Windows\System32\wship6.dll
 Opens:
                         C:\windows\temp\dhcpcsvc6.DLL
 Opens:
                         C:\Windows\System32\dhcpcsvc6.dll
 Opens:
                         C:\windows\temp\dhcpcsvc.DLL
 Opens:
                         C:\Windows\System32\dhcpcsvc.dll
 Opens:
                         C:\windows\temp\MLANG.dll
 Opens:
                         C:\Windows\System32\mlang.dll
                         C:\Windows\System32\drivers\etc\hosts
 Opens:
                         C:\Windows\System32\FWPUCLNT.DLL
 Opens:
 Opens:
                         C:\Program Files\Common Files\microsoft shared\ink\tiptsf.dll
                         C:\Windows\System32\netprofm.dll
 Opens:
 Opens:
                         C:\windows\temp\CRYPTSP.dll
                         C:\Windows\System32\cryptsp.dll
 Opens:
 Opens:
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\windows\temp\RpcRtRemote.dll
 Opens:
                         C:\Windows\System32\RpcRtRemote.dll
 Opens:
                         C:\Windows\System32\npmproxy.dll
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
C:\Windows\System32\C_20127.NLS
 Opens:
 Opens:
                         C:\Windows\System32\mshtml.dll
 Opens:
                         C:\Windows\System32\msls31.dll
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files \verb|\Content.IE5\BX3UL1G0\index[1].php|
 Opens:
                         C:\Windows\System32\msimtf.dll
 Opens:
                         C:\Windows\System32\jscript.dll
 Opens:
                         C:\Windows\System32\iepeers.dll
 Opens:
                         C:\Windows\System32\winspool.drv
                         C:\Windows\System32\dxtrans.dll
 Opens:
 Opens:
                         C:\Windows\System32\atl.dll
 Opens:
                         C:\Windows\System32\ddrawex.dll
 Opens:
                         C:\Windows\Svstem32\ddraw.dll
 Opens:
                         C:\Windows\System32\dciman32.dll
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Windows\win.ini
 Opens:
                         C:\Windows\System32\en-US\ddraw.dll.mui
 Opens:
                         C:\Windows\System32\dxtmsft.dll
 Opens:
                         C:\windows\temp\ImgUtil.dll
 Opens:
                         C:\Windows\System32\imgutil.dll
 Opens:
                         C:\Windows\System32\pngfilt.dll
 Opens:
                         C:\windows\temp\SXS.DLL
 Opens:
                         C:\Windows\System32\sxs.dll
 Opens:
                         C:\Windows\Fonts\arial.ttf
 Opens:
                         C:\Windows\System32\en-US\mlang.dll.mui
 Opens:
                         C:\Windows\System32\C_1250.NLS
 Opens:
                         C:\Windows\System32\C_1251.NLS
 Opens:
                         C:\Windows\System32\C_1253.NLS
 Opens:
                         C:\Windows\System32\C_1254.NLS
                         C:\Windows\System32\C_1255.NLS
C:\Windows\System32\C_1256.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_1257.NLS
 Opens:
                         C:\Windows\System32\C_1258.NLS
 Opens:
                         C:\Windows\System32\C_874.NLS
 Opens:
                         C:\Windows\System32\C_932.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_936.NLS
                         C:\Windows\System32\C_949.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_950.NLS
                         C:\Windows\System32\C_1361.NLS
 Opens:
 Opens:
                         C:\Windows\Fonts\arialbd.ttf
 Opens:
                         C:\Windows\Fonts\ariali.ttf
 Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
 Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
                         C:\windows\temp\D3DIM700.DLL
 Opens:
                         C:\Windows\System32\d3dim700.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\jquery-1.10.2.min_f2fb5194[1].js
 Opens:
                         C:\Windows\System32\tzres.dll
 Opens:
                         C:\Windows\System32\en-US\tzres.dll.mui
 Opens:
                         C:\Windows\System32\en-US\jscript.dll.mui
 Opens:
                         C:\Windows\System32\en-US\KernelBase.dll.mui
```

```
Opens:
                          C:\Windows\System32\en-US\mshtml.dll.mui
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\| Content.IE5 \verb|\| KQ5TVCON \verb|\| all_async_search_d0d1b2ec[1].js \\
 Opens:
                          {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\KQ5TVCON\every_cookie_aa168cb4[1].js
                          C:\Windows\System32\Macromed\Flash\Flash10h.ocx
 Opens:
 Opens:
                          C:\Windows\system32\Macromed\Flash\WINMM.dll
 Opens:
                          C:\Windows\System32\winmm.dll
                          C:\Windows\system32\Macromed\Flash\DSOUND.dll
 Opens:
                          C:\Windows\System32\dsound.dll
 Opens:
 Opens:
                          C:\Windows\system32\Macromed\Flash\POWRPROF.dll
 Opens:
                          C:\Windows\System32\powrprof.dll
                          C:\Windows\system32\Macromed\Flash\mscms.dll
 Opens:
 Opens:
                          C:\Windows\System32\mscms.dll
                          C:\Windows\system32\Macromed\Flash\USERENV.dll
 Opens:
 Opens:
                          C:\Windows\System32\userenv.dll
 Opens:
                          C:\
                          C:\Windows\system32\Macromed\Flash\ss.sgn
 Opens:
                          C:\Windows\System32\Macromed\Flash
 Opens:
 Opens:
                          C:\Windows\system32\Macromed\Flash\ss.cfg
 Opens:
                          C:\Windows\System32\Macromed\Flash\mms.cfg
 Opens:
                          C:\Windows\system32\Macromed\Flash\oem.cfg
 Opens:
                          C:\Windows\system32\oem.cfg
 Opens:
                          {\tt C:\Users\Admin\AppData\Roaming\Adobe\Flash\ Player\AssetCache}
 Opens:
                          {\tt C:\Users\Admin\AppData\Roaming\Adobe\Flash\ Player}
 Opens:
                          C:\Windows\System32\stdole2.tlb
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\index.dat
                          C:\Users\Admin\AppData\Local\Microsoft\Internet
 Opens:
Explorer\DOMStore\6K541L89\www.baidu[1].xml
 Opens:
                          C:\windows\temp\XmlLite.dll
 Opens:
                          C:\Windows\Svstem32\xmllite.dll
 Opens:
                          C:\Windows\Svstem32\mshtml.tlb
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
 Opens:
                          C:\Windows\System32\urlmon.dll
 Opens:
                          C:\Windows
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\bdsug_async_1cb857eb[1].js
                          C:\Windows\System32\msxml3.dll
 Opens:
                          C:\Windows\System32\msxml3r.dll
 Opens:
                          {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
 Opens
                          C:\Program Files\Internet Explorer\ieproxy.dll
 Opens:
                          C:\windows\temp\MMDevAPI.DLL
                          C:\Windows\System32\MMDevAPI.dll
 Opens:
 Opens:
                          C:\windows\temp\PROPSYS.dll
 Opens:
                          C:\Windows\System32\propsys.dll
                          C:\Windows\System32\en-US\msxml3r.dll.mui
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData\
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Opens:
Explorer\UserData\index.dat
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Opens:
Explorer\UserData\CYCCFJ6M
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\28I7G5HR
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\5IVMI5HF
 Opens:
                          {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Internet}
Explorer\UserData\FSLFFMJ7
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Opens:
Explorer\UserData\*.*28I7G5HR\desktop.ini
 Opens:
                          {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Internet}
Explorer\UserData\5IVMI5HF\desktop.ini
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\CYCCFJ6M\desktop.ini
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\FSLFFMJ7\desktop.ini
                          C:\windows\temp\Secur32.dll
 Opens:
                          C:\Windows\System32\secur32.dll
 Opens:
                          C:\windows\temp\credssp.dll
 Opens:
                          C:\Windows\System32\credssp.dll
 Opens:
                          C:\Windows\System32\schannel.dll
 Opens:
 Opens:
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
 Opens:
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Opens:
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\settings.sol
 Opens:
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\
 Opens:
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash
{\tt Player} \verb| macromedia.com \verb| support \verb| flashplayer \verb| sys \verb| settings.sol| \\
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Opens:
{\tt Player\+Shared0bjects\+HA2GV3VL\s1.bdstatic.com\+shared0bjectBIDUPSID.sol}
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
                          C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\s1.bdstatic.com\
 Opens:
```

```
Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\*Shared\*Objects\*HA2GV3VL\*macromedia.com\*support\*flashplayer\*sys\*s1.bdstatic.com\*settings.sol
  Opens:
                                   {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
Opens:
                                   C: \verb|\Users\Admin\AppData\Roaming\Macromedia\Flash|
Player\macromedia.com\support\flashplayer\svs\#s1.bdstatic.com\settings.sol
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\#SharedObjects\HA2GV3VL
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
{\tt Player\+Shared0bjects\+HA2GV3VL\s1.bdstatic.com\+shared0bjectBIDUPSID.sxx}
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
{\tt Explorer} \verb|\USerData| CYCCFJ6M \verb|\USerDataBIDUPSID[1].xml|
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
  Opens
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000006.db
                                   C:\Users\desktop.ini
  Opens:
  Opens:
                                   C:\Users
  Opens:
                                   C:\Users\Admin\AppData
                                   C:\Users\Admin\AppData\Local\Microsoft
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History.IE5\MSHist012016040820160409
  Opens:
\label{local-wicrosoft-windows-history-listory-listory-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listony-listo
  Opens:
                                   C:\Windows\System32\en-US\shell32.dll.mui
  Opens:
                                   C:\Users\Admin\Favorites
  Opens:
                                   C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
  Opens:
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Internet\ Explorer\MSIMGSIZ.DAT}
  Opens:
                                   C:\windows\temp\netmsg.dll
  Opens:
                                   C:\Windows\System32\netmsg.dll
                                   C:\Windows\System32\en-US\netmsg.dll.mui
  Opens:
                                   {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Opens:
Files\Content.IE5\KO5TVCON\favicon[1].ico
                                   \verb|C:\USers\Admin\AppData\Local\Microsoft\Windows\Temporary Internet|\\
  Opens:
Files\Content.IE5\WG2VLW5Y\union[1].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporarv Internet
  Opens:
Files\Content.IE5\WG2VLW5Y\JSocket_9a52fc3e[1].swf
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
  Writes to:
                                   \label{lem:c:standard} $$C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet $$
Files \verb|\Content.IE5\BX3UL1G0\index[1].php|
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bd_logo1[1].png
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\X3IPB3Z1\baidu_jgylogo3[1].gif
                                   \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet|\\
  Writes to:
Files\Content.IE5\BX3UL1G0\jquery-1.10.2.min_f2fb5194[1].js
  Writes to:
                                   \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet|\\
Files\Content.IE5\KQ5TVCON\nuomi_510f7472[1].png
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Writes to:
Files\Content.IE5\X3IPB3Z1\zbios_62c636fe[1].png
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Writes to:
Files\Content.IE5\BX3UL1G0\icons_0e814c16[1].png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\KQ5TVCON\all_async_search_d0d1b2ec[1].js
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\KQ5TVCON\every_cookie_aa168cb4[1].js
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
  Writes to:
Explorer\DOMStore\6K541L89\www.baidu[1].xml
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
                                   \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet|\\
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\X3IPB3Z1\bdsug_async_1cb857eb[1].js
  Writes to:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
  Writes to:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
```

Explorer\UserData\index.dat

```
Writes to:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
 Writes to:
                         {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
{\tt Player\macromedia.com\support\flashplayer\sys\settings.sxx}
                         {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
 Writes to:
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                         C:\Users\Admin\AppData\Roaming\Microsoft\Internet
 Writes to:
Explorer\UserData\CYCCFJ6M\userDataBIDUPSID[1].xml
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
 Writes to:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\index.dat Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\BX3UL1G0\error[1].htm
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
 Writes to:
                         C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\JSocket_9a52fc3e[1].swf
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\bdbri_icons_2e35e84b[1].png
 Reads from:
                         C:\Windows\Fonts\StaticCache.dat
 Reads from:
C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
 Reads from:
                         C:\Windows\System32\drivers\etc\hosts
 Reads from:
                         C:\Windows\win.ini
                         C:\Windows\System32\dxtmsft.dll
 Reads from:
                         C:\Windows\System32\dxtrans.dll
 Reads from:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Reads from:
Files\Content.IE5\BX3UL1GO\jquery-1.10.2.min_f2fb5194[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Reads from:
Files\Content.IE5\KQ5TVCON\every_cookie_aa168cb4[1].js
                         C:\Windows\System32\Macromed\Flash\mms.cfg
 Reads from:
 Reads from:
                         C:\Windows\System32\Macromed\Flash\Flash10h.ocx
 Reads from:
                         C:\Windows\System32\stdole2.tlb
 Reads from:
                         C:\Windows\System32\iepeers.dll
 Reads from
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\all_async_search_d0d1b2ec[1].js
                         C:\Windows\Svstem32\mshtml.tlb
                          {\tt C:\Windows\Temporary\ Internet}
 Reads from:
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\bdsug_async_1cb857eb[1].js
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1G0\env_beb83b45[1].swf
                          C:\Windows\System32\ieframe.dll
 Reads from:
 Reads from:
                         C: \verb|\Users\Admin\AppData\Roaming\Macromedia\Flash|
{\tt Player\macromedia.com\support\flashplayer\sys\settings.sol}
 Reads from:
                         {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
{\tt Player\+Shared0bjects\+HA2GV3VL\+s1.bdstatic.com\+shared0bjectBIDUPSID.sxx}
                         C:\Users\desktop.ini
 Reads from:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Reads from:
 Reads from:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Reads from:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Reads from:
Files\Content.IE5\KQ5TVCON\favicon[1].ico
 Reads from
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\JSocket_9a52fc3e[1].swf
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
 Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
                          {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
 Deletes:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
 Deletes:
                          {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
{\tt Player\macromedia.com\support\flashplayer\sys\settings.sol}
 Deletes:
                          {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Deletes:
{\tt Player\ + Shared 0bjects\ + HA2GV3VL\ + s1.bdstatic.com\ + shared 0bjectBIDUPSID.sxx}
```

Network Events

DNS query:	wpad
DNS query:	www.baidu.com
DNS query:	s1.bdstatic.com
DNS query:	sclick.baidu.com
DNS query:	formi.baidu.com
DNS response:	www.a.shifen.com ⇒ 103.235.46.39
DNS response:	wwwbaidu.jomodns.com ⇒ 119.146.74.40
DNS response:	s.a.shifen.com ⇒ 14.215.177.42
DNS response:	formi.baidu.com ⇒ 61.135.169.120
DNS response:	formi.baidu.com ⇒ 180.149.131.55
Connects to:	127.0.0.1:53021
Connects to:	103.235.46.39:80
Connects to:	119.146.74.40:80
Connects to:	14.215.177.42:80
Connects to:	61.135.169.120:843
Connects to:	61.135.169.120:8843
Sends data to:	0.0.0:5355

 Sends data to:
 224.0.0.252:5355

 Sends data to:
 8.8.8.8:53

 Sends data to:
 127.0.0.1:53021

 Sends data to:
 www.a.shifen.com:80 (103.235.46.39)

 Sends data to:
 wwwbaidu.jomodns.com:80 (119.146.74.40)

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

Receives data from: 8.8.8.8:53
Receives data from: 127.0.0.1:53021

Receives data from: www.a.shifen.com:80 (103.235.46.39)
Receives data from: wwwbaidu.jomodns.com:80 (119.146.74.40)
Receives data from: s.a.shifen.com:80 (14.215.177.42)

Windows Registry Events

Creates key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation

Creates key: HKCU\software\explore

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

Creates key: HKLM\software\microsoft\tracing

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

settings\connections

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

awareness

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\runmru

Creates key: HKCU\software\microsoft\internet explorer\typedurls

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\typedpaths

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

settings\wpad\{8700a497-6961-4e6d-86e2-18954850414c}

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{8700a497-6961-4e6d-86e2-18954850414c}\ea-f1-1d-61-e0-3e Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\wpad\ea-f1-1d-61-e0-3e

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

settings\p3p\history

Creates key: HKLM\software\microsoft\directdraw\mostrecentapplication
Creates key: HKLM\software\microsoft\direct3d\mostrecentapplication
Creates key: HKCU\software\microsoft\windows script\settings

Creates key: HKCU\software\microsoft\internet explorer\domstorage\total
Creates key: HKCU\software\microsoft\internet explorer\domstorage\baidu.com

 $\label{lem:creates} \begin{tabular}{lll} Creates key: & HKCU \software \microsoft \windows \current version \internet \end{tabular} .$

settings\5.0\cache\extensible cache\userdata

Creates key: HKLM\system\currentcontrolset\control\securityproviders\schannel

Creates key: HKCU\software\macromedia\flashplayer

 $\label{lem:condition} {\it Creates key:} \qquad \qquad {\it HKCU\software\microsoft\windows\currentversion\internet}$

settings\5.0\cache\extensible cache\mshist012016040820160409

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

Creates key: HKLM\software\microsoft\downloadmanager

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

settings\zonemap[proxybypass]

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

settings\zonemap[proxybypass]
Deletes value: HKCU\software\microsoft\windows\currentyersion\internet

settings\zonemap[intranetname]

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

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\

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

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

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

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
                                           HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:
  Opens key:
                                           \label{lem:hklm} \mbox{HKLM\software\mbox{$\backslash$ microsoft\windows\windows error reporting\wmr}} \mbox{$\backslash$ windows\windows error reporting\wmr} \mbox{$\backslash$ windows\windows\windows\windows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindows\whindow
  Opens kev:
                                           HKLM\svstem\currentcontrolset\control\nls\customlocale
  Opens key:
                                           HKLM\svstem\currentcontrolset\control\nls\extendedlocale
  Opens key:
                                           HKLM\svstem\currentcontrolset\control\nls\locale
  Opens kev:
                                           HKLM\svstem\currentcontrolset\control\nls\locale\alternate sorts
                                           HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:
                                           HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens kev:
  Opens key:
                                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:
                                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:
                                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:
                                           HKLM\system\currentcontrolset\control\cmf\config
                                           HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key
  Opens key:
HKLM\software\microsoft\windows
  Opens key:
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
  Opens key:
                                           HKCU\software\explore
  Opens key:
                                           HKCU\software\classes\
  Opens key:
                                           HKLM\software\microsoft\com3
                                           \label{local-eq:hkcu} \mbox{HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2\}}}
  Opens key:
                                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:
                                           HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
  Opens key:
00c04fd705a2}\treatas
                                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
  Opens key:
                                           HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
  Opens key:
00c04fd705a2}\progid
  Opens key:
                                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
  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}\inprochandler32
  Opens kev:
                                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
                                           HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens key:
00c04fd705a2}\inprochandler
  Opens key:
                                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler
                                           HKLM\software\microsoft\rpc
  Opens key:
  Opens key:
                                           \label{lem:hklm} {\tt HKLM \ } system \verb|\ current control \ \\ control \verb|\ computername \ \\ active computername \ \\
  Opens key:
                                           HKLM\system\setup
  Opens key:
                                           HKLM\software\policies\microsoft\windows nt\rpc
                                           HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:
  Opens key:
                                           HKLM\software\microsoft\sqmclient\windows
                                           HKCU\software\classes\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key
                                           HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key:
                                           HKCU\software\policies\microsoft\windows\app management
  Opens kev:
  Opens key:
                                           HKLM\software\policies\microsoft\windows\app management
                                           HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  Opens key:
                                           HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  Opens kev:
                                           HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
  Opens kev:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                           HKLM\software\microsoft\ctf\
  Opens key:
                                           HKLM\software\microsoft\ctf\knownclasses
  Opens key:
  Opens key:
                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key
                                           HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                           HKLM\software\microsoft\internet
  Opens key
\verb|explorer'| \verb|main| featurecontrol| feature_http_username_password_disable| \\
  Opens key:
                                           HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                           HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                           HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                           {\tt HKCU \ } software \verb|\ microsoft \> \ internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:
                                           HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562
                                           HKCU\software\microsoft\internet
  Opens key:
Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:
                                           \label{lem:hklmsystem} \begin{tabular}{ll} HKLM \end{tabular} Access providers
  Opens key:
                                           HKLM\system\currentcontrolset\services\ldap
  Opens key:
                                           HKCU\software\microsoft\internet explorer\ietld
  Opens key:
                                           HKLM\software\microsoft\internet explorer\main
  Opens key:
                                           HKLM\software\policies\microsoft\internet explorer\main
  Opens key:
                                           HKCU\software\policies\microsoft\internet explorer\main
  Opens key:
                                           HKLM\software\microsoft\windows\currentversion\policies\explorer
                                           HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key
  Opens key:
HKLM \software \microsoft \windows \current version \shell compatibility \applications \end{constraints} 130b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                           HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea
  Opens key:
08002b30309d}\shellfolder
   Opens key:
                                           HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder
   Opens key:
                                           42a0-1069-a2ea-08002b30309d}\shellfolder
  Opens key:
                                           \label{thm:local_hammon} \parbox{$HKCU\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkcu$} \parbox{$
  Opens key:
                                           HKLM\software\microsoft\windows\currentversion\policies\nonenum
                                           HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
  Opens key:
```

```
08002b30309d}\inprocserver32
  Opens key:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
 Opens key
                         HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
 Opens kev:
                         HKLM\system\currentcontrolset\control\session manager\appcompatibility
                          HKLM\software\policies\microsoft\windows\appcompat
 Opens kev:
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\shell extensions\cached
 Opens kev:
                          HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea
08002b30309d}\treatas
 Opens key:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
                          HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
 Opens key
08002b30309d}\progid
 Opens key:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
 Opens key:
                          HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea
08002b30309d}\inprochandler32
                         HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
 Opens kev:
                         HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
 Opens key
08002b30309d}\inprochandler
                         HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler
 Opens key:
 Opens key:
a2ea-08002b30309d}
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
                          HKLM\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
                          HKCU\software\policies\microsoft\internet explorer\browseremulation
 Opens key
                          HKLM\software\microsoft\internet explorer\mediatypeclass
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\accepted documents
                         HKLM\software\microsoft\windows\currentversion\policies\ratings
 Opens kev:
                         HKCU\software\microsoft\internet
 Opens kev:
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 kev:
                         HKLM\software\policies
 Opens key:
                          HKCU\software\policies
 Opens key:
                          HKCU\software
  Opens key:
                          HKLM\software
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
                         HKCU\software\microsoft\internet
 Opens key
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key:
                         \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap\domains\
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\ranges\
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\ranges\
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\zonemap\protocoldefaults\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                         HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
                         HKLM\software\policies\microsoft\internet explorer
 Opens key:
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\security
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens kev:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                          HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus 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
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
   Opens key:
                                                           HKI M\software\microsoft\windows\currentversion\internet
settings\zonemap\
                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\2
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
   Opens key:
                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
   Opens key:
                                                           HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\zones\4
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
    Opens key:
                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
                                                           HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
    Opens key:
                                                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \notation{Internet}{ll} \end{tabular}
settings\lockdown_zones\
   Opens key:
                                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
\verb|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 kev:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\0
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\1
                                                           HKLM \verb|\software\policies\microsoft\windows\currentversion\ | internet
   Opens key:
settings\lockdown_zones\1
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens key:
                                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\2
   Opens key:
                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                           \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \normalisatio
   Opens key:
settings\lockdown_zones\2
   Opens key
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens key
                                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} on the constraint of the
settings\lockdown_zones\3
   Opens key
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                          HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown zones\4
                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\4
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
   Opens key
                                                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
   Opens key:
                                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache
    Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
    Opens key:
                                                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
    Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions
    Opens key:
ba85-6007caedcf9d}
   Opens kev:
HKLM \ software \ microsoft \ windows \ current version \ (352481e8-33be-4251-614erdescriptions) \ (352481e8-33be-425
ba85-6007caedcf9d}\propertybag
    Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer
    Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
    Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
   Opens key:
                                                           HKLM\software\policies\microsoft\windows\explorer
                                                           HKCU\software\policies\microsoft\windows\explorer
    Opens key:
    Opens key:
9d55-7b8e7f157091}
    Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}\propertybag
    Opens key:
9afe-ea3317b67173}
    Opens key:
9afe-ea3317b67173}\propertybag
```

```
Opens key:
2160590473-689474908-1361669368-1002
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
                                           HKLM\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache\cookies
  Opens key:
HKLM\software\microsoft\windows\currentyersion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
  Opens key:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-b04864, and \ box \ and \ and \ box \ and \ and \ box \ and \ and \ box \ and \ and \ box \ and \ and \ box \ and \ and
908e-08a611b84ff6}\propertybag
   Opens key:
a03a-e3ef65729f3d}
   Opens kev:
a03a-e3ef65729f3d}\propertybag
                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\5.0\cache\history
  Opens key:
                                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
   Opens key:
a781-5a1130a75963}
  Opens key:
a781-5a1130a75963}\propertybag
                                           HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache
  Opens kev:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
                                           HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\feedplat
                                           HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\iecompat
   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\privacie:
   Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                                           HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key
                                           HKCU\software\microsoft\internet
explorer \verb|\main\featurecontrol\feature\_bufferbreaking\_818408|
  Opens key
                                           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
  Opens key:
                                           HKLM\software\microsoft\internet
\verb|explorer|| \verb|main|| featurecontrol|| feature_skip_post_retry_on_internetwritefile_kb895954|| featurecontrol|| featurecont
                                           HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache
  Opens key
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                                            HKCU\software\microsoft\internet
  Opens key:
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 key:
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                                           HKLM\software\microsoft\internet
   Opens key:
explorer \verb|\main| feature control \verb|\feature| use \verb|\colore| cname for \verb|\spn| kb911149
                                           HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
   Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
   Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature compat use connection based negotiate auth kb2151543
  Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
   Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature allow long international filenames
  Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature allow long international filenames
                                           HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                                           HKCU\software\microsoft\internet
   Opens key:
explorer \verb|\main| featurecontrol| feature_disable_unicode_handle_closing_callback| \\
   Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                                            HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                                           HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens key:
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key
                                           HKLM\software\microsoft\internet
```

explorer\main\featurecontrol\feature_digest_no_extras_in_uri

```
Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature exclude invalid client cert kb929477
                           HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature use utf8 for basic auth kb967545
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature release keys on unload kb975619
                           HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  Opens key:
                           HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
                           HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\381e2851
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ 00000019
 Opens key:
Opens key:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000003
 Opens kev:
Opens key:
Opens kev:
Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011
 Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 10000000000012
 Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ (catalog\_entries \ 00000000000013) \ descriptions \ descri
 Opens key
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 10000000000014
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000015
 Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ (catalog\_entries \ 00000000000016)
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
 Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000004
  Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:
  Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                           HKLM\software\microsoft\tracing\rasapi32
  Opens key:
                           HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:
                           HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:
                           HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key:
                           HKU\
  Opens key:
                           HKLM\system\currentcontrolset\control\sqmservicelist
```

Opens key: HKLM\software\microsoft\tracing\rasmancs

```
Opens key:
                          HKCU\software\classes\autoproxytypes
 Opens key:
                          HKCR\autoproxytypes
 Opens key:
                         \label{lem:hkcu} \verb+KCU\+software\+classes\+autoproxytypes\+application\+/x-internet-signup
 Opens key:
                          {\tt HKCR} \verb|\ autoproxytypes \verb|\ application/x-internet-signup| }
 Opens kev:
                         \label{local-config} \mbox{HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig}
 Opens kev:
                          HKCR\autoproxytypes\application/x-ns-proxy-autoconfig
                          HKLM\svstem\currentcontrolset\services\dnscache\parameters
 Opens key:
 Opens kev:
                          HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key:
                         HKLM\system\currentcontrolset\services\dns
 Opens key:
                          HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
 Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
 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
                          HKLM\software\policies\microsoft\system\dnsclient
 Opens key:
 Opens key:
                          HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key:
                          HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                         HKLM\system\currentcontrolset\services\psched\parameters\winsock
 Opens key:
                         HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens key:
                         {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  winsock \verb|\  setup| \\
migration\providers\psched
 Opens key:
                         \label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip \parameters \winsock
 Opens key:
                         {\tt HKLM \ } system \ \verb| current control set \ \verb| services \ \verb| winsock \ \verb| setup \ |
migration\providers\tcpip
                         HKLM\system\currentcontrolset\services\winsock\setup
 Opens key:
migration\providers\tcpip6
                         HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
 Opens key:
                         HKCU\software\classes\protocols\name-space handler\
 Opens key:
 Opens kev:
                          HKCR\protocols\name-space handler
 Opens kev:
                         HKCU\software\classes\protocols\name-space handler\http\
                          HKCR\protocols\name-space handler\http
 Opens kev:
 Opens key:
                         HKCU\software\classes\protocols\name-space handler\*\
 Opens key:
                         HKCR\protocols\name-space handler\*
 Opens kev:
c19ce8a73253}
 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 key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
 Opens key
                          HKLM\software\microsoft\windows\currentversion\internet settings\user
agent
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
                          HKI M\software\microsoft\windows\currentversion\internet
 Opens key
settings\5.0\user agent
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\user agent
 Opens kev:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\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:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\user agent\pre platform
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\post platform
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
 Opens key:
                         HKLM\software\microsoft\internet
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
                         HKCU\software\microsoft\internet
 Opens key:
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 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\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key:
c19ce8a73253}
 Opens key:
                          HKCU\software\microsoft\internet explorer\international
 Opens key:
                         HKCU\software\microsoft\internet
```

 $\verb|explorer\main\featurecontrol\feature_disable_legacy_compression| \\$

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

explorer\main\featurecontrol\feature_disable_legacy_compression

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

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}

Opens key:

 $\label{lem:hklm} $$HKLM \simeq \operatorname{lem:hklm} \simeq \operatorname{$

Opens key:

 $\label{thm:hklmsystem} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-1709a0196aed\}$

Opens key:

a68f334c8d34}

Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key:

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

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

Opens key:

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

 $\label{thm:constraint} 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}

00c04fd7d062}\treatas

00c04fd7d062}\progid

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

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

00c04fd7d062}\inprocserver32

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062\}\inprocserver32}} \\$

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

00c04fd7d062}\inprochandler32

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler

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

HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas

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

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

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

9fe3c77a297a}\treatas

Opens key:

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

Opens key:

9fe3c77a297a}\inprocserver32

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

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

9fe3c77a297a}\inprochandler32

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

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

9fe3c77a297a}\inprochandler

Opens key: $\label{eq:hcc} \begin{tabular}{ll} HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\nprochandler \\ Opens key: \\ HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062} \\ \end{tabular}$

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

00c04fd7d062}\treatas

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

00c04fd7d062}\progid

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

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

00c04fd7d062}\inprochandler32

Opens key: HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler32

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

00c04fd7d062}\inprochandler

Opens key: HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\

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

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

00c04fd7d062}\treatas

00c04fd7d062}\progid

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

 Opens key:
 HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-046126\clsid\{00bb2763-6a77-11d0-a5

00c04fd7d062}\inprocserver32

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprochandler32

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

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

00c04fd7d062}\inprochandler

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

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

00aa005b4383}\inprocserver32

```
Opens key:
                                   HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
  Opens key:
HKLM \verb|\software\microsoft\windows\currentversion\explorer\autocomplete\client\\|
  Opens key:
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
  Opens key:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
  Opens kev:
b61bb7cdd997}\treatas
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas
  Opens kev:
  Opens key:
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\progid
  Opens key:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid
  Opens key
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
  Opens key:
                                   HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprochandler32
                                   HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
  Opens key
b61bb7cdd997}\inprochandler
  Opens key:
                                   Opens key:
                                   HKLM\software\microsoft\rpc\extensions
  Opens key
                                   \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:
                                   HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
  Opens key:
                                   HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
  Opens key:
                                   HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\treatas
  Opens key:
                                   HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
  Opens key
                                   HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\progid
                                   HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid
  Opens key:
                                   HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
  Opens key
199fdba5723b}\inprocserver32
  Opens kev:
                                   HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32
                                   HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
  Opens key
199fdba5723b}\inprochandler32
  Opens key:
                                   HKCR\clsid\\\{dcb00c01-570f-4a9b-8d69-199fdba5723b\\\}\inprochandler32
  Opens key:
                                   HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
  Opens kev:
                                   HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\\\\
                                   \label{local-optimization} HKCU \software \classes \clsid \ \{a47979d2-c419-11d9-a5b4-001185ad2b89\}
  Opens key:
  Opens key:
                                   HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
                                   HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
  Opens key:
001185ad2b89}\treatas
                                   HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\ \ treat as
  Opens key:
  Opens key
                                   HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\progid
                                   HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
  Opens key:
  Opens key
                                   HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprocserver32
  Opens key:
                                   HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32
  Opens key
                                   HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
                                   HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32
  Opens key:
                                   HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
  Opens key
001185ad2b89}\inprochandler
                                  HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler
  Opens key:
  Opens key:
Opens key
HKCR\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
  Opens key:
                                   HKLM\software\microsoft\ole\appcompat
  Opens key:
                                   HKLM\system\currentcontrolset\control\lsa
                                   \label{thm:local_hammon} \begin{tabular}{l} HKLM \end{tabular} which is a provider \end{tabular} where \
  Opens key
cryptographic provider
                                   HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:
                                   HKLM\software\policies\microsoft\cryptography
  Opens key:
                                   HKLM\software\microsoft\cryptography
  Opens key
                                   {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash offload}
                                   HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:
                                   HKCR\interface\{00000134-0000-0000-c000-000000000046}
  Opens kev:
  Opens key:
                                   HKCU\software\classes\interface\{00000134-0000-0000-c000-
000000000046 \} \verb|\proxystubclsid32|
                                   HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32
  Opens key:
  Opens key
                                   HKLM\system\currentcontrolset\services\bfe
                                   HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
  Opens key
                                   HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
  Opens key:
                                   HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-
  Opens key:
199fdba5723b}\proxystubclsid32
  Opens key:
                                   HKCR\ interface \ \{d0074ffd-570f-4a9b-8d69-199fdba5723b\}\ proxystubclsid32
  Opens key:
                                   HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\treatas
  Opens key:
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
                                   HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
  Opens key:
2299f0398e27}\progid
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32
  Opens key:
                                   HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32
  Opens key:
                                   HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler32
```

```
Opens key:
                          HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
 Opens key:
                          HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler
                          HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\ \ \ in prochandler
 Opens key:
 Opens key:
                          HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
                          HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
 Opens kev:
                          HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-
 Opens kev:
4f0ef901a406}\proxystubclsid32
                          HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32
 Opens key:
                          HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
 Opens key:
                          HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
 Opens key:
 Opens key:
                          HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-
6d613e2ceaec}\proxystubclsid32
 Opens key:
                          HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32
                          HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
 Opens key
 Opens key
                          HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
 Opens key:
                          HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-
00aa004bb851}\proxystubclsid32
                          HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32
 Opens key:
 Opens key
                          HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
 Opens key:
                          HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
 Opens key
                          HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\treatas
 Opens key:
                          HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
 Opens key:
                          HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\progid
                          HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
 Opens key:
                          HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
 Opens key
00aa00341d07}\inprocserver32
                          HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
 Opens key
00aa00341d07}\inprochandler32
 Opens kev:
                          HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
 Opens key
                          HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
 Opens key:
                         HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
                          HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
 Opens key:
                          HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
 Opens key
 Opens key:
                          HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-
4a74e101f8c1}\proxystubclsid32
 Opens key:
                          HKCR \verb|\interface| \{bcd1de7e-2db1-418b-b047-4a74e101f8c1\} \verb|\proxystubclsid32| \} \\
                          HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
  Opens key
 Opens key
                          HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
 Opens key
                          HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-
63278fcb8037}\proxystubclsid32
 Opens key:
                          Opens key
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{8700a497-6961-4e6d-86e2-18954850414c}
 Opens key:
                          {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ net bt \verb|\ linkage \\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\baidu.com
                          HKCU\software\classes\mime\database\content type\text/html; charset=utf-
 Opens key:
                          HKCR\mime\database\content type\text/html: charset=utf-8
 Opens kev:
                          HKCU\software\classes\mime\database\content type\text/html
 Opens kev:
 Opens key:
                          HKCR\mime\database\content type\text/html
 Opens key:
                          HKCU\software\classes\protocols\filter\text/html; charset=utf-8
                          HKCR\protocols\filter\text/html; charset=utf-8
 Opens key:
                          HKCU\software\classes\protocols\filter\text/html
 Opens key:
 Opens key:
                          HKCR\protocols\filter\text/html
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_feeds
                          HKLM\software\microsoft\internet
 Opens key:
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\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key:
Opens key:
00aa00686f13}\treatas
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
 Opens key:
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key
00aa00686f13}\progid
 Opens key:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
 Opens key:
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
 Opens key:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
 Opens key
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
 Opens key:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler 32
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key
00aa00686f13}\inprochandler
 Opens key:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
 Opens key:
                          {\tt HKLM \backslash software \backslash microsoft \backslash internet}
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                          HKCU\software\microsoft\internet
 Opens key:
```

```
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:
                                    HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
                                   HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_aria_support
  Opens kev:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature legacy dispparams
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens kev:
                                   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
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key
                                   HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_body\_size\_in\_editable\_if rame\_kb943245
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature databinding support
  Opens kev:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enforce_bstr
  Opens kev:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key
                                    HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_legacy_tostring_in_compatiview| \\
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                                   HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature restrict crash recovery save kb978454
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens key:
  Opens key:
                                    {\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
  Opens key:
                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\sc domstorage} \\
  Opens key:
                                    \label{lem:hklm} \verb+Kklm \+ software + microsoft + internet explorer + domstorage
                                    Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\safetv\privacie
  Opens kev:
  Opens key:
                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{$m$icrosoft\internet explorer\safety\privacie}} \\
                                    HKLM\software\microsoft\internet explorer\safety\privacie
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature manage script circular refs
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
                                    HKCU\software\microsoft\internet
  Opens key:
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 key:
                                    HKCU\software\classes\protocols\name-space handler\about\
  Opens key:
                                    HKCR\protocols\name-space handler\about
  Opens key:
                                    HKCU\software\classes\protocols\handler\about
  Opens key:
                                    HKCR\protocols\handler\about
                                    \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \cls
  Opens key:
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
```

```
00aa00bdce0b}\treatas
 Opens key:
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
 Opens key:
```

HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-Opens key

00aa00bdce0b}\inprocserver32

Opens kev: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

Opens key: $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\ \ in prochandler 32$

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler

Opens key: $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\tinprochandler$

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

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 Opens key HKLM\software\microsoft\internet explorer\zoom

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

explorer\main\featurecontrol\feature_protocol_lockdown

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

settings\url history

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

settings\url history

Opens kev: HKCU\software\microsoft\windows\currentversion\internet settings\url

history

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

history

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425

HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425

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

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

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 Opens key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\styles}} \\$

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \active desktop \end{tabular}$ Opens kev:

HKCU\software\microsoft\windows\currentversion\policies Opens kev: Opens key: HKCU\software\microsoft\internet explorer\pagesetup Opens kev: HKCU\software\microsoft\internet explorer\menuext HKCU\software\microsoft\internet explorer\menuext\%s Opens kev: Opens key: HKLM\system\currentcontrolset\control\nls\codepage

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

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

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

explorer\main\featurecontrol\feature_xssfilter

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

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

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

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

HKCU\software\microsoft\internet Opens key:

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

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

settings\

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

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

settings\zonemap\

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

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

```
f4ceaaf59cfc}\treatas
  Opens key:
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
  Opens key:
                                     HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\progid
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\progid
  Opens key:
                                     HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
  Opens key
f4ceaaf59cfc}\inprocserver32
  Opens kev:
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
                                     HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
  Opens key
f4ceaaf59cfc}\inprochandler32
  Opens key:
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
  Opens key
                                     HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler
  Opens key:
                                     HKCU\software\policies\microsoft\internet explorer\control panel
  Opens key
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:
                                     HKCU\software\classes\clsid\{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
  Opens key:
                                     HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
  Opens key:
                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\progid
  Opens key:
                                     HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid
                                     HKCU \backslash software \backslash classes \backslash clsid \backslash \{f414c260-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac
  Opens key:
00aa00bbbb58}\inprocserver32
                                     HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
  Opens key
00aa00bbbb58}\inprochandler32
  Opens kev:
                                     HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32
                                     HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
  Opens key
00aa00bbbb58}\inprochandler
                                     HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprochandler
  Opens key:
  Opens key:
                                     HKLM\software\microsoft\windows script\features
                                     HKLM\software\policies\microsoft\internet explorer\recovery
  Opens key:
  Opens kev:
                                     HKCU\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
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature behaviors
                                     HKLM\software\microsoft\internet explorer\default behaviors
  Opens key:
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
  Opens kev:
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key
00aa00bdce0b}\treatas
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\progid
  Opens key:
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key
00aa00bdce0b}\inprochandler32
  Opens key:
                                     HKCR \verb|\clsid|{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprochandler32| \\
  Opens key
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
  Opens key:
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler
  Opens key
                                     \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \nternet explorer \persistence
  Opens key:
                                     HKLM\software\policies\microsoft\internet explorer\persistence
                                     HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens key:
                                     HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens key:
                                     HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
  Opens key:
dc030521aabd}\treatas
                                     HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
  Opens key:
                                     HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
  Opens key:
dc030521aabd}\progid
                                     HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
```

 $HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver 32$ Opens key:

Opens key: dc030521aabd}\inprochandler32

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

HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler32 Opens key:

Opens key

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

dc030521aabd}\inprochandler

Opens key: $HKCR \clsid \ \{81397204-f51a-4571-8d7b-dc030521aabd\} \ \ in prochandler$ 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

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

```
3c8b00c10000}\progid
 Opens key:
                           HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
 Opens key:
                           HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
 Opens key:
                           HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32
                           HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
 Opens key
3c8b00c10000}\inprochandler32
                           HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler32
 Opens kev:
                           HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
 Opens key
3c8b00c10000}\inprochandler
 Opens key:
                           HKCR\clsid\d1fe6762-fc48-11d0-883a-3c8b00c10000\\\label{eq:hkcr} \label{eq:hkcr} \label{eq:hkcr}
                           HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
 Opens key:
 Opens key:
                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
 Opens key:
                           HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\treatas
 Opens key:
                           \label{local-bound} $$HKCR\clsid\\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\\\treat as
                           HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
 Opens key:
00c04fd9189d}\progid
                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
 Opens key:
 Opens key:
                           HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca
00c04fd9189d}\inprocserver32
 Opens key:
                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32
 Opens key:
                           HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
 Opens key:
                           HKCR \verb|\clsid|{4fd2a832-86c8-11d0-8fca-00c04fd9189d} \verb|\inprochandler32|
 Opens key
                           HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
                           HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler
 Opens key:
 Opens key:
                           HKLM\software\microsoft\windows\currentversion\setup
                           HKLM\software\microsoft\windows\currentversion
 Opens key:
 Opens key:
                           HKLM\hardware\devicemap\video
 Opens key:
                           HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
 Opens kev:
Opens key:
                           HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000
 Opens key:
                           HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000
                           HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
 Opens key:
8ed0c8eb59a8}\0000
                           HKLM\software\microsoft\directdraw\compatibility
 Opens key:
 Opens key:
                           HKLM\software\microsoft\directdraw\compatibility\bug!
 Opens key:
                           HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
 Opens key:
                           HKLM\software\microsoft\directdraw\compatibility\diablo
 Opens key:
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat 3
 Opens key:
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus msgolf98
 Opens key:
                           HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\nhl| powerplay
                           HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\nortonsysteminfo
 Opens key:
 Opens key:
                           {\tt HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus rogue \ squadron}
                           HKLM\software\microsoft\directdraw\compatibility\savage
 Opens kev:
                           {\tt HKLM \backslash software \backslash microsoft \backslash direct draw \backslash compatibility \backslash scorched planet}
 Opens key:
 Opens key:
                           HKLM\software\microsoft\directdraw\compatibility\silentthunder
                           HKLM\software\microsoft\directdraw\compatibility\starcraft100
 Opens kev:
 Opens key:
                           HKLM\software\microsoft\directdraw\compatibility\starcraft115
 Opens key:
                           HKLM\software\microsoft\directdraw\compatibility\starcraftdemo
 Opens key:
                           HKLM\software\microsoft\directdraw\compatibility\terracide
                           HKLM\software\microsoft\directdraw\compatibility\thirddimension
 Opens key:
 Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
 Opens key:
HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff daviswin mark benchmark
                           HKLM\software\microsoft\directdraw\gammacalibrator
 Opens key:
 Opens key:
                           HKLM\software\microsoft\directdraw
 Opens key:
                           HKLM\software\microsoft\direct3d
 Opens key:
                           HKLM\software\microsoft\windows nt\currentversion\msasn1
 Opens key:
                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\}
 Opens key:
                           HKCR\clsid\{a7ee7f34-3hd1-427f-9231-f941e9h7e1fe}
 Opens key:
                           HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\treatas
                           HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
 Opens key:
                           HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key
f941e9b7e1fe}\progid
                           HKCR\clsid\arrowantered +301-427f-9231-f941e9b7e1fe}\progid
 Opens key:
                           Opens key:
f941e9b7e1fe}\inprocserver32
                           HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
 Opens key:
                           HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key
f941e9b7e1fe}\inprochandler32
                           HKCR\clsid\\a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\\inprochandler32
 Opens key:
 Opens key:
                           HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler
                           HKCR\clsid\a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\\\inprochandler
 Opens key:
                           HKCU\software\classes\dximagetransform.microsoft.shadow
 Opens key
                           HKCR\dximagetransform.microsoft.shadow
 Opens key
 Opens key:
                           {\tt HKCU \ } software \verb|\ } dximage transform.microsoft.shadow \verb|\ } clsid
 Opens key:
                           HKCR\dximagetransform.microsoft.shadow\clsid
 Opens key:
                           HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
 Opens key:
                           HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
 Opens key:
                           HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\treatas
 Opens key:
                           HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas
```

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

Opens key:

00c04fa34f05}\progid

```
Opens key:
                                  HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid
  Opens key:
                                  HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32
  Opens key:
                                  HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32
  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:
00c04fa34f05}\inprochandler
  Opens key:
                                  HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler
  Opens key
                                  HKLM\software\microsoft\internet explorer\activex compatibility
  Opens key
                                  HKLM\software\microsoft\internet explorer\activex
compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}
                                  HKCU\software\classes\mime\database\content type\image/png
  Opens key:
  Opens key:
                                  HKCR\mime\database\content type\image/png
  Opens key:
                                  HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
                                  HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
  Opens key:
                                  HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
  Opens key:
00aa006c1a01}\treatas
  Opens key:
                                  HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
  Opens key:
                                  HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\progid
  Opens key:
                                  HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid
  Opens key:
                                  HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32
                                  HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\inprocserver32
  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-
  Opens key:
00aa006c1a01}\inprochandler
                                  Opens key:
                                  HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
  Opens kev:
                                  HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
  Opens kev:
                                  HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724
  Opens kev:
00aa006c1a01}\treatas
  Opens key:
                                  HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
  Opens key:
                                  HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\progid
                                  HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid
  Opens key:
  Opens key
                                  HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
  Opens key:
                                  HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
  Opens key
                                  HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
  Opens key:
                                  HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
  Opens key:
                                  HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler
                                  HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\tinprochandler
  Opens key:
  Opens key:
                                  HKCU\software\classes\mime\database\content type
  Opens key
                                  HKCR\mime\database\content type
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
  Opens key:
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
  Opens kev:
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
  Opens kev:
0000f87557db}\treatas
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
  Opens key:
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
  Opens key
0000f87557db}\progid
  Opens key:
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid
  Opens key:
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
  Opens key:
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
  Opens key:
0000f87557db}\inprochandler32
  Opens key:
                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \simp \bits \end{tabular}
  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:
                                  Opens key:
                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \simple \mime \database \content type \simple \mime \mime
  Opens key:
                                  HKCR\mime\database\content type\image/jpeg\bits
                                  \label{local-operator} \mbox{HKCU\software\classes\mbox{\sc mime\database\content\ type\image/pjpeg\bits}} \\
  Opens kev:
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
  Opens key:
0000f87557db}\inprochandler
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler
  Opens key:
  Opens kev:
                                  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
                                  HKCU\software\classes\mime\database\content type\image/tiff\bits
  Opens key:
  Opens key:
                                  HKCR\mime\database\content type\image/tiff\bits
  Opens key:
                                  HKCU\software\classes\mime\database\content type\image/x-icon\bits
  Opens key:
                                  HKCR\mime\database\content type\image/x-icon\bits
  Opens key:
                                  HKCU\software\classes\mime\database\content type\image/x-jg\bits
  Opens kev:
                                  HKCR\mime\database\content type\image/x-jg\bits
                                  HKCU\software\classes\mime\database\content type\image/x-png\bits
  Opens key:
  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
                                  HKCR\mime\database\content type\image/x-png
  Opens key:
```

HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}

HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

Opens key: 00a0c913f750}\treatas

Opens key: Opens key:

```
Opens key:
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\progid
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
 Opens kev:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
 Opens kev:
00a0c913f750}\inprochandler32
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler
 Opens key:
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\\\\
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
 Opens key:
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6
f4fc1e6ca1bd}\treatas
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key
f4fc1e6ca1bd}\progid
 Opens key:
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid
 Opens key
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32
 Opens key:
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32
 Opens key
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler32
                         HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32
 Opens key:
                         HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key
f4fc1e6ca1bd}\inprochandler
                         Opens key:
                         HKCU\software\classes\typelib
 Opens key:
 Opens key:
                         HKCR\typelib
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
 Opens kev:
                         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:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\409
 Opens kev:
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
  Opens key:
00aa003b6061}\1.1\9
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
 Opens key:
 Opens key:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0
 Opens key:
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0
 Opens key:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0\win32
 Opens key:
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32
 Opens key
                         HKCU \setminus software \setminus classes \setminus typelib \setminus \{54314d1d-35fe-11d1-81a1-0000f87557db\}
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
 Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
 Opens kev:
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
 Opens key:
 Opens kev:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\409
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409
 Opens kev:
 Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\9
                         HKCR\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
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
 Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
 Opens key:
0000f87557db}\1.1\0\win32
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
 Opens key
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
                         HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
 Opens key:
 Opens key:
                         HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
Opens key: 00aa003f8646}\treatas
                         HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
                         HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
 Opens key
00aa003f8646}\progid
                         HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid
 Opens key:
                         HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
 Opens key:
00aa003f8646}\inprocserver32
                         HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
 Opens key:
00aa003f8646}\inprochandler32
 Opens key:
                         HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\ \ in prochandler 32
 Opens key:
                         HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler
                         HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler
 Opens key:
 Opens key:
                         Opens key:
                         HKCU\software\classes\mime\database\content type\image/gif
 Opens key:
                         HKCR\mime\database\content type\image/gif
                         HKLM\software\microsoft\windows
 Opens key:
```

Opens key: HKCU\software\microsoft\internet

nt\currentversion\languagepack\surrogatefallback\simsun

Opens key:

Opens key:

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

HKCU\software\classes\mime\database\content type\application/javascript

HKCR\mime\database\content type\application/javascript

```
Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
   Opens key:
                                           HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation| \\
  Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature cross domain redirect mitigation
                                           HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature block lmz script
  Opens key:
                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature block lmz script
  Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature activex inactivate mode removal revert
  Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
   Opens key:
                                           HKCU\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature\_use\_windowedselectcontrol| \\
  Opens key:
                                           HKLM\software\microsoft\internet
\dot{\texttt{explorer}} \\ \dot{\texttt{main}} \\ \dot{\texttt{feature}} \\ \textbf{use\_windowedselectcontrol} \\ \dot{\texttt{main}} \\ \dot{\texttt{feature}} \\ \textbf{use\_windowedselectcontrol} \\ \dot{\texttt{main}} \\ \dot{\texttt{main}
                                           HKCU\software\microsoft\internet explorer\new windows
   Opens key:
   Opens key
                                           HKLM\software\microsoft\internet explorer\new windows
   Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
   Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
   Opens key:
                                           HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_binary\_caller\_service\_provider
   Opens key:
                                           HKLM\software\microsoft\internet
explorer \verb|\main\feature| control \verb|\feature| binary_caller_service\_provider
                                           HKCU\software\classes\shockwaveflash.shockwaveflash
   Opens key:
                                           HKCR\shockwaveflash.shockwaveflash
   Opens key
   Opens key:
                                           HKCU\software\classes\shockwaveflash.shockwaveflash\clsid
                                           HKCR\shockwaveflash.shockwaveflash\clsid
   Opens key:
                                           HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
   Opens kev:
   Opens kev:
                                           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                                           HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Opens kev:
444553540000}\treatas
   Opens key:
                                           HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\treatas
   Opens key:
                                           HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\progid
                                           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid
   Opens key:
   Opens key
                                           HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
   Opens key
                                           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32
   Opens key
                                           HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
   Opens key:
                                           HKCR \verb|\clsid|{d27cdb6e-ae6d-11cf-96b8-444553540000} \verb|\inprochandler32|
   Opens key
                                           HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler
                                           HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\\\inprochandler
   Opens key:
   Opens key:
                                           HKLM\ \ hardware \ \ lescription \ \ system\ \ central processor \ \ \ 0
                                           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 kev:
                                           HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
   Opens key
444553540000}\1.0\409
                                           HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\409
   Opens key:
                                           HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
   Opens key:
444553540000}\1.0\9
                                           HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9
   Opens key:
                                           HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
   Opens key:
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
   Opens key:
                                           HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32
   Opens key:
                                           \label{local-cond} \mbox{HKCU\software\classes\typelib\{00020430-0000-0000-c000-0000000000046\}}}
   Opens key
                                           HKCR\typelib\{00020430-0000-0000-c000-00000000046}
   Opens key:
                                           Opens key:
                                           HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
   Opens key:
                                           000000000046}\2.0\0
                                           HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
   Opens key:
                                           HKCU\software\classes\typelib\{00020430-0000-0000-c000-
   Opens key
000000000046}\2.0\0\win32
                                           HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
   Opens key:
                                           HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
   Opens key:
                                           HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
   Opens key:
                                           HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
   Opens key:
   Opens key:
                                           HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens key:
                                           HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0
   Opens key:
                                           HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0
                                           HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
   Opens key:
00c04fb6bfc4}\1.0\0\win32
   Opens key:
                                           HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32
                                           HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_domstorage
                                           HKLM\software\microsoft\internet
   Opens key:
 explorer\main\featurecontrol\feature_domstorage
   Opens key:
                                           \label{local-condition} HKCU \setminus software \setminus classes \setminus clsid \setminus \{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\} \ treat as
 Opens key:
                          HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\progid
                          HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
 Opens kev:
 Opens kev:
                         HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
 Opens key:
                         HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
 Opens key
00c04fb6bfc4}\inprochandler
 Opens key:
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
 Opens key:
                          HKCU\software\microsoft\internet explorer\feed discovery
                          HKLM\software\microsoft\internet explorer\feed discovery
 Opens key:
 Opens key
                          HKCU\software\microsoft\ftp
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection
                         HKLM\software\microsoft\internet
 Opens key:
\dot{\texttt{explorer}} \\ \dot{\texttt{main}} \\ \dot{\texttt{feature}} \\ \dot{\texttt{activex}} \\ \dot{\texttt{repurposedetection}}
                          HKLM\software\microsoft\internet explorer\activex
 Opens key:
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_alloweddomainlist
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_alloweddomainlist
 Opens key
                         HKLM\software\microsoft\internet explorer\extension
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                         HKCU\software\classes\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
 Opens kev:
 Opens kev:
                         HKCR\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
                          HKCU\software\microsoft\code store database\distribution units
 Opens kev:
                         HKLM\software\microsoft\code store database\distribution units
 Opens key:
 Opens key:
                          HKLM\software\microsoft\code store database\distribution
units\{d27cdb6e-ae6d-11cf-96b8-444553540000}
 Opens kev:
                         HKCU\software\classes\clsid
                         HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
                          HKCR \verb|\clsid|{d27cdb6e-ae6d-11cf-96b8-444553540000} \verb|\availableversion| \\
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
 Opens key:
 Opens key:
                          HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
 Opens key
 Opens key:
                         HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\languagecheckperiod
```

 $HKCR \verb|\clsid|{d27cdb6e-ae6d-11cf-96b8-444553540000} \verb|\installedversion| \\$

Opens key:

. HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\languagecheckperiod HKCU\software\microsoft\internet Opens key

explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915 Opens kev: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature consult mime killbit kb905915

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

Opens key:

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

444553540000}\miscstatus\1

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

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

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} internet explorer \domstorage \baidu.com.} \end{tabular}$ Opens key: Opens key: HKCU\software\microsoft\internet explorer\domstorage\total Opens key: HKCU\software\classes\mime\database\content type\application/x-

shockwave-flash

Opens key: $\label{lem:hkcr} \mbox{HKCR} \mbox{\sc him} \mbox{\sc hkcr} \mbox{\sc him} \mbox{\sc hkcr} \mbox{\sc him} \mbox{\sc hkcr} \mbox{\sc him} \mbox{\sc hkcr} \mb$ Opens key HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}

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

0000f81fe221}\treatas

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

0000f81fe221}\progid

HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\policies\system

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

0000f81fe221}\inprocserver32

 $HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\clserver32$ Opens key: Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39} HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39} Opens key:

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

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

00a0c90a8f39}\progid

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

00a0c90a8f39}\inprocserver32

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

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

00a0c90a8f39}\inprochandler32

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32

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

00a0c90a8f39}\inprochandler

```
Opens key:
                                                                      Opens key:
                                                                      HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
    Opens key
                                                                      HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler32
    Opens key:
                                                                      HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32
                                                                      HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
    Opens key
0000f81fe221}\inprochandler
    Opens kev:
                                                                      HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
    Opens key:
                                                                      HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
    Opens key:
                                                                      HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
                                                                      HKCU\software\classes\clsid\{00020424-0000-0000-c000-00000000046}
    Opens key:
    Opens key:
                                                                      HKCR\clsid\{00020424-0000-0000-c000-00000000046}
    Opens key:
                                                                      HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
    Opens key:
                                                                      HKCU\software\classes\clsid\{00020424-0000-0000-c000-
    Opens key:
000000000046}\progid
                                                                      HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler
    Opens key:
    Opens key:
                                                                      HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid
    Opens key:
                                                                      HKLM\software\microsoft\msxml30
    Opens key
                                                                      HKCU\software\classes\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32
    Opens key:
                                                                      HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32
    Opens key:
                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \protocols \filter \application / x-shock wave-flash \end{tabular}
    Opens key
                                                                      HKCR \verb|\protocols| filter \verb|\application| / x-shockwave-flash
                                                                      \label{local-eq:hkcu-software-classes-clsid} \begin{tabular}{ll} HKCU \software \classes \clsid \closer{local-eq:hkcu-software-classes} \end{tabular}
    Opens key:
00000000046}\inprochandler32
                                                                      HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandler32
    Opens key:
                                                                      HKCU\software\classes\clsid\{00020424-0000-0000-c000-
    Opens key
00000000046}\inprochandler
                                                                      \label{local-eq:hkcr} \mbox{HKCR\clsid\closed} \mbox{$\clsid\closed} \mbox{$\clsid\closed} \mbox{$\clsid\closed} \mbox{$\clsid\closed} \mbox{$\clsid\closed} \mbox{$\clsid\clsid\closed} \mbox{$\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\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\clsid\clsid\clsid
    Opens key:
    Opens kev:
                                                                      HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
                                                                      HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
    Opens kev:
    Opens key:
                                                                      HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
                                                                      HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
    Opens kev:
    Opens kev:
                                                                      HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
    Opens key:
                                                                      HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
    Opens key:
                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \typelib \eab 22 ac 0 - 30 c 1 - 11 c f - a 7 e b - 000 0 c 05 ba e 0 b} \end{tabular} $$1.1$ and $$1.1$ and $$1.2$ are the solution of the sol
                                                                      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
     Opens key:
                                                                      \label{limit} $HKCR\times typelib = ab22ac0-30c1-11cf-a7eb-0000c05bae0b} \ 1.1\ 0
    Opens key:
                                                                      HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
    Opens key:
                                                                      HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
    Opens key
                                                                      \label{local-eq:hkcu} \mbox{HKCU\software\classes\interface} \ \{00020400-0000-0000-c000-000000000046\} \ \mbox{HKCU\software\classes\selectforce} \ \ \mbox{HKCU\software\classes\selectforce} \ \mbox{HKCU\software\classes\selectforces} \ \mbox{HKCU\software\classes\selectforces} \ \mbox{HKCU\software\classes\selectforces} \ 
    Opens key:
                                                                      HKCR\interface\{00020400-0000-0000-c000-00000000046}
                                                                      HKCU\software\classes\interface\{00020400-0000-0000-c000-
    Opens key:
000000000046}\proxystubclsid32
                                                                      HKCR\interface\{00020400-0000-0000-0000-0000000046}\proxystubclsid32
    Opens key:
                                                                      HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046}
    Opens kev:
                                                                      HKCR\clsid\{00020420-0000-0000-c000-00000000046}
    Opens kev:
                                                                      HKCU\software\classes\clsid\{00020420-0000-0000-c000-
    Opens key:
000000000046}\treatas
                                                                      HKCR\clsid\{00020420-0000-0000-c000-00000000046}\treatas
    Opens key:
```

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

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

00000000046}\inprocser ver32

HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32 Opens key:

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

000000000046}\inprochandler32

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

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

00000000046}\inprochandler

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler Opens key: $HKCU \setminus software \setminus classes \setminus interface \setminus \{6d5140c1-7436-11ce-8034-00aa006009fa\}$

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

00aa006009fa}\proxystubclsid32

Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba} Opens key

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

e4fddd701cba}\treatas

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

e4fddd701cba}\progid

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

e4fddd701cba}\inprocserver32

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

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

e4fddd701cba}\inprochandler32

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

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

e4fddd701cba}\inprochandler

Opens key: $HKCR \verb|\clsid|{a4a1a128-768f-41e0-bf75-e4fddd701cba} \verb|\inprochandler| a4a1a128-768f-41e0-bf75-e4fddd701cba}| a4a1a128-768f-41e0-bf75$ HKCU\software\classes\interface\{00020404-0000-0000-c000-000000000046} Opens key:

HKCR\interface\{00020404-0000-0000-c000-000000000046} Opens key:

```
Opens key:
                                                                         HKCU\software\classes\interface\{00020404-0000-0000-c000-
00000000046}\proxystubclsid32
     Opens key:
                                                                         \label{local-bound} \mbox{HKCU\software\classes\clsid} \mbox{\{00020421-0000-0000-c000-000000000046\}} \mbox{ } \mbox{\clsid} \m
     Opens key:
     Opens key:
                                                                         HKCR\clsid\{00020421-0000-0000-c000-000000000046}
                                                                          HKCU\software\classes\clsid\{00020421-0000-0000-c000-
     Opens kev:
000000000046}\treatas
                                                                          HKCR\clsid\{00020421-0000-0000-c000-00000000046}\treatas
     Opens kev:
                                                                         HKCU\software\classes\clsid\{00020421-0000-0000-c000-
     Opens key:
000000000046}\progid
     Opens key:
                                                                          HKCR\clsid\{00020421-0000-0000-c000-00000000046}\progid
    Opens key:
                                                                         HKCU\software\classes\clsid\{00020421-0000-0000-c000-
 000000000046}\inprocserver32
     Opens key:
                                                                         HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserver32
                                                                         HKCU\software\classes\clsid\{00020421-0000-0000-c000-
     Opens key:
 000000000046}\inprochandler32
     Opens key:
                                                                         HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprochandler32
                                                                         HKCU\software\classes\clsid\{00020421-0000-0000-c000-
     Opens key
00000000046}\inprochandler
     Opens key:
                                                                         \label{local-eq:hkcr} \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\c
     Opens key:
                                                                         HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
     Opens key:
                                                                         HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
     Opens key:
                                                                         HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\treatas
     Opens key:
                                                                          HKCR \ clsid \ \{2933bf90-7b36-11d2-b20e-00c04f983e60\} \ treat as
     Opens key:
                                                                         HKLM\software\microsoft\windows nt\currentversion\drivers32
     Opens key:
                                                                         HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\progid
                                                                          HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
     Opens key:
                                                                         HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
     Opens key:
00c04f983e60}\inprocserver32
                                                                         HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32
    Opens key:
     Opens kev:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\iovstick\winmm
                                                                         HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
    Opens kev:
 00c04f983e60}\inprochandler32
     Opens key:
                                                                         HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\tinprochandler32
     Opens key:
                                                                         HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprochandler
                                                                         HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\tinprochandler
     Opens key:
     Opens key
                                                                          HKCU\software\microsoft\windows\currentversion\multimedia\midimap
                                                                         HKCU\software\microsoft\windows\currentversion\internet
     Opens key:
 settings\5.0\cache\extensible cache\userdata
                                                                         HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ types \ \ type \ 001
     Opens key:
     Opens key:
                                                                          HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
     Opens key:
                                                                          {\tt HKLM \ } system \verb|\ current control \ \\ security providers
     Opens key:
                                                                          Opens key:
                                                                          HKLM \ system \ current control \ lsa \ spic ache \ creds sp. dll
     Opens key:
                                                                          HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
     Opens key:
                                                                          HKLM\software\policies\microsoft\internet explorer\services
                                                                          HKCU\software\microsoft\internet explorer\services
     Opens kev:
     Opens key:
                                                                          HKLM\software\policies\microsoft\internet explorer\activities
     Opens key:
                                                                         HKCU\software\microsoft\internet explorer\activities
                                                                         HKLM\software\microsoft\internet explorer\activities
     Opens kev:
                                                                         HKLM\software\policies\microsoft\internet
    Opens key
explorer\infodelivery\restrictions
                                                                        HKCU\software\policies\microsoft\internet
    Opens key:
explorer\infodelivery\restrictions
     Opens key:
                                                                         HKLM\software\policies\microsoft\internet explorer\suggested sites
     Opens key:
                                                                          HKCU\software\microsoft\internet explorer\suggested sites
                                                                         HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
     Opens key:
08002b30309d}\shellfolder
                                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens key:
                                                                         HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-d1) + (20d04f
     Opens key
3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens key:
                                                                        HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-delta) + (20d04fe0-delta) +
3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens key:
\label{thm:local_explorer} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \end{time} \column{2cm} \colu
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}\
     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}
    Opens key:
                                                                          HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
                                                                          HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
     Opens key:
                                                                          HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
     Opens key:
    Opens key:
                                                                         HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
     Opens key:
                                                                          HKCR\clsid{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
                                                                         HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
     Opens key
b8dc300d9f9d}\progid
     Opens key:
                                                                          HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
                                                                         HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
     Opens key:
b8dc300d9f9d}\inprocserver32
                                                                         HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
     Opens key:
     Opens key:
11e3-b3bc-806e6f6e6963}\
    Opens key:
                                                                         HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
```

b8dc300d9f9d}\inprochandler32

```
Opens key:
                                                          HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
    Opens key
                                                         HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
    Opens key:
                                                          HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
    Opens kev:
                                                         HKCU\software\microsoft\windows\currentversion\explorer\
    Opens kev:
HKLM \label{lem:hklm} Software \verb|\microsoft| windows \verb|\shell| registered applications \verb|\urlassociations| directory \verb|\open with progids| and the shell registered applications \verb|\urlassociations| directory \verb|\open with progids| and the shell registered applications \verb|\urlassociations| directory \verb|\open with progids| and the shell registered applications \verb|\urlassociations| directory \verb|\open with progids| and the shell registered applications and the shell registered applications are shell registered applications and the shell registered applications are shell registered applications and the shell registered applications are shell registered applications and the shell registered applications are shell registered applications and the shell registered applications are shell registered applications and the shell registered applications are shell registered applications are shell
   Opens kev:
HKCU\software\microsoft\windows\shell\associations\urlassociations\directory
                                                          HKCU\software\classes\directory
    Opens key:
    Opens key:
                                                          HKCR\directory
    Opens key:
                                                          HKCU\software\classes\directory\curver
    Opens key:
                                                          HKCR\directory\curver
                                                          HKCR\directory\
    Opens key:
                                                          HKCU\software\classes\directory\shellex\iconhandler
    Opens key:
    Opens key:
                                                          HKCR\directory\shellex\iconhandler
                                                          HKCU\software\classes\folder
    Opens key:
    Opens kev:
                                                          HKCR\folder
    Opens key:
                                                          HKCU\software\classes\folder\shellex\iconhandler
    Opens key:
                                                          HKCR\folder\shellex\iconhandler
    Opens key:
                                                          HKCU\software\classes\allfilesystemobjects
    Opens key:
                                                          HKCR\allfilesystemobjects
                                                          HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
    Opens key:
    Opens key:
                                                          HKCR\allfilesystemobjects\shellex\iconhandler
    Opens key:
                                                          HKCU\software\classes\directory\docobject
    Opens key:
                                                          HKCR\directory\docobject
                                                          HKCU\software\classes\folder\docobject
    Opens key:
    Opens key:
                                                          HKCR\folder\docobject
                                                          HKCU\software\classes\allfilesystemobjects\docobject
    Opens key:
    Opens kev:
                                                          {\tt HKCR\ left} lesystem objects \ \ left to cobject
    Opens key:
                                                          HKCU\software\classes\directory\browseinplace
    Opens key:
                                                          HKCR\directory\browseinplace
                                                          HKCU\software\classes\folder\browseinplace
    Opens kev:
    Opens key:
                                                          HKCR\folder\browseinplace
    Opens key:
                                                          HKCU\software\classes\allfilesystemobjects\browseinplace
    Opens key:
                                                          HKCR\allfilesystemobjects\browseinplace
    Opens key:
                                                          HKCU\software\classes\directory\clsid
    Opens key:
                                                          HKCR\directory\clsid
    Opens kev:
                                                          HKCU\software\classes\folder\clsid
    Opens key:
                                                          HKCR\folder\clsid
    Opens key:
                                                          HKCU\software\classes\allfilesystemobjects\clsid
                                                          HKCR\allfilesystemobjects\clsid
    Opens key:
    Opens key:
                                                          HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
    Opens key:
                                                          HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
    Opens key
                                                          HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
                                                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
    Opens key:
    Opens key
                                                         HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\shellfolder
    Opens key:
                                                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellfolder
                                                         HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
    Opens key
444553540000}\treatas
    Opens key:
                                                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
                                                         HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
    Opens kev:
444553540000}\progid
                                                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
    Opens key:
                                                         HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
   Opens key
444553540000}\inprochandler32
    Opens key:
                                                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\nprochandler32
                                                          HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
    Opens key
444553540000}\inprochandler
    Opens key:
                                                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\
    Opens key:
bff4-444553540000}
    Opens key
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409
                                                         HKCU\software\microsoft\windows\currentversion\app
   Opens key
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
   Opens key
                                                         {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus app}
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                                         HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
   Opens key:
3aea-1069-a2d8-08002b30309d}
Opens~key: \\ HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\label{eq:hkcu} In the continuous conti
                                                         HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
    Opens key:
                                                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
    Opens key:
                                                          HKCU\software\microsoft\internet explorer\main\windowssearch
    Opens key:
    Opens key:
                                                          HKLM\software\policies\microsoft\internet explorer\feeds
    Opens key:
                                                          HKCU\software\microsoft\internet explorer\feeds
    Opens key:
                                                          HKLM\software\microsoft\internet explorer\feeds
    Opens key:
87bd-30b759fa33dd}
    Opens key:
HKLM \label{lem:hklm} Which is the latest and the
87bd-30b759fa33dd}\propertybag
    Opens key:
                                                         HKLM\software\microsoft\windows search
    Opens key:
                                                          HKCU\software\classes\shockwaveflash.shockwaveflash.7
    Opens key:
                                                          HKCR \verb|\shockwaveflash.shockwaveflash.7|
    Opens key:
                                                          \label{local-continuity} HKCU \ software \ classes \ shockwave flash. shockwave flash. 7 \ clsid
```

 ${\tt HKCR \ } shock wave flash. shock wave flash. 7 \ \verb|clsid|$

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}

HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}

Opens key:

Opens key:

Opens key:

```
Opens key:
                         HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\treatas
 Opens key:
                         HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\progid
                         HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\progid
 Opens kev:
                         HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
 Opens kev:
00aa00bdce0b}\inprocserver32
                         HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
 Opens key
00aa00bdce0b}\inprochandler32
 Opens key:
                         HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\nprochandler32
                         HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
 Opens key
00aa00bdce0b}\inprochandler
                         HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\ \ in prochandler
 Opens key:
 Opens key:
                         HKCU\software\classes\mime\database\content type\image/x-icon
                         HKCR\mime\database\content type\image/x-icon
 Opens key:
                         HKCU\software\classes\protocols\filter\image/x-icon
 Opens key
                         HKCR\protocols\filter\image/x-icon
 Opens key
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
 Opens key:
                         HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
 Opens key:
                         Opens key
                         HKCU \setminus software \setminus classes \setminus interface \setminus \{332c4425-26cb-11d0-b483-00c04fd90119\}
                         HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
 Opens key
                         HKCU\software\classes\interface\{332c4425-26cb-11d0-b483-
 Opens key:
00c04fd90119}\proxystubclsid32
                         HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32
 Opens key:
                         HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
 Opens key:
                         HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
 Opens kev:
 Opens kev:
                         HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\treatas
                         HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\progid
 Opens kev:
                         HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid
                         HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
 Opens key:
fd2b31b3eefd}\inprocserver32
                         HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32
 Opens key
 Opens key:
                         HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f
fd2b31b3eefd}\inprochandler32
 Opens key:
                         HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\ \ in prochandler 32
 Opens key:
                         HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler
 Opens key:
                         HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler
 Opens key
                         HKLM\software\microsoft\internet explorer\activex
compatibility\{adc6cb82-424c-11d2-952a-00c04fa34f05}
                         HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}
 Opens key:
                         HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}
 Opens key:
 Opens kev:
                         HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\treatas
                         HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\treatas
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\progid
                         HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\progid
 Opens key:
                         HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
 Opens key
00c04fa34f05}\inprocserver32
                         HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a
00c04fa34f05}\inprochandler32
                         HKCR\clsid\\{adc6cb82-424c-11d2-952a-00c04fa34f05}\\{inprochandler32}
 Opens key:
                         HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
 Opens key
00c04fa34f05}\inprochandler
 Opens key:
                         Opens key
                         HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
 Opens key:
                         HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
 Opens key:
                         HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\treatas
                         HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\progid
                         HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\progid
 Opens key:
                         HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
 Opens key
00c04fd9189d}\inprocserver32
                         HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
 Opens key
00c04fd9189d}\inprochandler32
 Opens key:
                         HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32
                         HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
 Opens key
00c04fd9189d}\inprochandler
                         HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler
 Opens key:
 Queries value:
                         HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
```

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

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

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus side by side [preferex ternal manifest]$

Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

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

```
Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Oueries value:
                                              HKLM\software\microsoft\windows
Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
                                              {\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocatoruse system heap]}
   Oueries value:
   Oueries value:
                                              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Oueries value:
                                              HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[security hklm only]
                                              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
   Queries value:
   Queries value:
                                               HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:
                                               HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                                              HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
   Queries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane1]|
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
   Queries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane3]|
   Oueries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane4]|
   Queries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane5]|
   Oueries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane6]|
                                              HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
   Oueries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane9]|
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                                              HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane12]|
   Queries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane13]|
   Oueries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
   Oueries value:
                                              HKLM\svstem\currentcontrolset\control\cmf\config[svstem]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
   Queries value:
                                               HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
   Queries value:
                                               HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:
                                               HKLM\software\microsoft\com3[com+enabled]
   Queries value:
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
   Queries value:
                                               HKCR\clsid\{8856f961-340a-11d0-a96b-
   Queries value:
00c04fd705a2}\inprocserver32[inprocserver32]
   Queries value:
                                              \label{lem:hkcrclsid} $$HKCR\clsid_{8856f961-340a-11d0-a96b-00c04fd705a2} \in \clsid_{8856f961-340a-11d0-a96b-00c04fd705a2} inprocessing the second s
   Oueries value:
                                              HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
   Queries value:
                                              HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
                                              HKLM\software\microsoft\rpc[maxrpcsize]
   Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Queries value:
                                               HKLM\system\setup[oobeinprogress]
   Oueries value:
                                               HKLM\system\setup[systemsetupinprogress]
   Oueries value:
                                               HKLM\software\microsoft\sqmclient\windows[ceipenable]
                                              Oueries value:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
   Queries value:
                                              HKLM\software\microsoft\ctf[enableanchorcontext]
   Queries value:
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Queries value:
                                              \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \cite{Linear transformation} and \cite{Linear transformation}. The lemma \cite{Linear transformation} and \cite{Linear transformation} and \cite{Linear transformation} and \cite{Linear transformation}.
settings[createuricachesize]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[createuricachesize]
   Queries value:
                                              HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
   Queries value
settings[enablepunycode]
   Queries value
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
   Queries value:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
   Oueries value:
                                              HKLM\software\microsoft\internet
explorer \\ \verb|main| feature control| feature with pure reason disable [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ \verb|main| feature control| feature with pure reason disable [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ \verb|main| feature control| feature with pure reason disable [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ \verb|main| feature with pure reason disable [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ \verb|main| feature with pure reason disable [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ expl
```

```
Oueries value:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                                               HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Oueries value:
   Oueries value:
                                               HKLM\svstem\currentcontrolset\services\ldap[useoldhostresolutionorder]
                                               HKLM\svstem\currentcontrolset\services\ldap[usehostnameasalias]
   Oueries value:
   Oueries value:
                                               HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
   Oueries value:
                                               HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
   Oueries value:
                                               HKCU\software\microsoft\internet explorer\ietld[iet]dversionlow]
   Queries value:
                                               HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
   Queries value:
                                               HKCU\software\microsoft\internet explorer\main[frametabwindow]
   Queries 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]
   Oueries value:
                                               HKLM\software\microsoft\internet explorer\main[sessionmerging]
                                               HKCU\software\microsoft\internet explorer\main[admintabprocs]
   Oueries value:
                                               HKLM\software\microsoft\internet explorer\main[admintabprocs]
   Queries value:
   Queries value:
                                               HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
   Queries value:
                                               HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
   Oueries value:
                                               HKLM\software\microsoft\internet explorer\main[navigationdelay]
   Oueries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
   Queries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[usedrophandler]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
   Oueries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsparsedisplayname]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value
08002b30309d}\shellfolder[queryforoverlay]
   Queries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[mapnetdriveverbs]
   Queries value
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideinwebview]
   Oueries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideondesktopperuser]
   Oueries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[nofilefolderiunction]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
                                              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
   Queries value:
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\, \{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2
08002b30309d}]
                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
   Queries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\inprocserver32[loadwithoutcom]
                                              HKCU\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xffff]
   Queries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
   Oueries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
   Oueries value:
                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
                                              HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
   Oueries value:
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
                                              HKLM\software\microsoft\internet
   Queries value:
explorer \verb|\main| feature f
   Queries value:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
                                              HKLM\software\policies\microsoft\internet
   Queries value:
explorer\security[disablesecuritysettingscheck]
   Oueries 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:
                                               \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\zones\3[flags]
   Queries value:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
                                               HKCU\software\microsoft\internet
   Queries value:
```

```
explorer \verb|\main| feature metric metric
                                                          HKCU\software\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
    Oueries value:
                                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
    Oueries value:
                                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown[*]
                                                          HKLM\system\currentcontrolset\control\wmi\security[OcfeO455-93ba-440d-
    Oueries value:
a3fe-553973d0b7231
                                                          HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
    Oueries value:
b924-d51178a59ce41
                                                          HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[fromcachetimeout]
   Queries value:
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
    Queries value:
                                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Software \end{tabular} in the constraint of the constr
settings[secureprotocols]
    Oueries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
    Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
   Oueries value:
                                                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[disablekeepalive]
   Queries value:
                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \end{tabular} windows \current version \end{tabular} internet
settings[disablepassport]
   Queries value:
                                                          \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+internet
settings[idnenabled]
   Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
   Oueries value
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[enablehttp1_1]
                                                          HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablehttp1 11
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[proxyhttp1.1]
   Queries value:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
    Queries value
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
    Queries value
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                                                          \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
    Queries value:
settings[disablebasicoverclearchannel]
    Queries value:
                                                          HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
    Queries value:
                                                          HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol[feature\_clientauthcertfilter]| \\
    Oueries value:
                                                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[clientauthbuiltinui]
   Oueries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
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]
                                                          \label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} internet \end{tabular}
    Queries value:
settings\5.0\cache\content[peruseritem]
    Queries value:
ba85-6007caedcf9d}[category]
ba85-6007caedcf9d}[name]
    Oueries value:
ba85-6007caedcf9d}[parentfolder]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[description]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[relativepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parsingname]
    Queries value:
ba85-6007caedcf9d}[infotip]
    Oueries value:
ba85-6007caedcf9d}[localizedname]
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[icon]
    Queries value
HKLM \label{lem:hklm} Which is the software \label{lem:hkklm} Which is the software \label{le
ba85-6007caedcf9d}[security]
    Queries value:
```

 $ba85\text{-}6007 caedcf9d} [stream resource] \\$

Oueries value:

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

Queries value:

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

Oueries value:

ba85-6007caedcf9d}[roamable]

Oueries value:

ba85-6007caedcf9d}[precreate]

Queries value:

ba85-6007caedcf9d}[stream]

Queries value:

ba85-6007caedcf9d}[publishexpandedpath]

 $HKLM \label{lem:hkk} In the latest and the latest$ ba85-6007caedcf9d}[attributes]

Oueries value:

ba85-6007caedcf9d}[foldertypeid]

Queries value:

ba85-6007caedcf9d}[initfolderhandler]

Queries value:

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

folders[cache]

Oueries value:

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

Oueries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f1b32785-6fba-4fcf-10b3278-6fba-$ 9d55-7b8e7f157091}[parentfolder]

Oueries value:

 $HKLM \label{lem:hkkkk} In the latest and the latest and the latest and the latest angle of the latest and the latest angle of the latest angle o$ 9d55-7b8e7f157091}[description]

Queries value:

9d55-7b8e7f157091}[relativepath]

Queries value:

9d55-7b8e7f157091}[parsingname]

Queries value:

9d55-7b8e7f157091}[infotip]

Oueries value:

9d55-7b8e7f157091}[localizedname1

Oueries value:

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

9d55-7b8e7f157091}[security] Queries value: $HKLM \label{lem:hklm} Which is a fixed by the sum of the sum of$

9d55-7b8e7f157091}[streamresource]

Queries value:

9d55-7b8e7f157091}[streamresourcetype] Queries value:

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

9d55-7b8e7f157091}[roamable]

Oueries value:

9d55-7b8e7f157091}[precreate]

Oueries value:

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

Queries value:

9d55-7b8e7f157091}[publishexpandedpath]

Queries value:

 $HKLM \label{lem:hkkkk} In the latest and the latest and the latest and the latest angle of the latest and the latest angle of the latest angle o$ 9d55-7b8e7f157091}[attributes]

Oueries value:

9d55-7b8e7f157091}[foldertypeid]

Queries value:

9d55-7b8e7f157091}[initfolderhandler]

Queries value: $\label{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}$

folders[local appdata]

Queries value:

9afe-ea3317b67173}[category]

Oueries value:

9afe-ea3317b67173}[name]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

9afe-ea3317b67173}[parsingname]

Queries value:

9afe-ea3317b67173}[infotip]

 $HKLM \label{lem:hkkkk} In the latest and the late$ 9afe-ea3317b67173}[localizedname]

Oueries value:

9afe-ea3317b67173}[icon]

Queries value:

9afe-ea3317b67173}[security]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

9afe-ea3317b67173}[roamable1

9afe-ea3317b67173}[precreate]

Queries value:

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

Queries value:

9afe-ea3317b67173}[publishexpandedpath]

Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-

9afe-ea3317b67173}[attributes] Oueries value:

9afe-ea3317b67173}[foldertypeid]

Oueries value:

9afe-ea3317b67173}[initfolderhandler]

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Queries value: 2160590473-689474908-1361669368-1002[profileimagepath] HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

Oueries value:

908e-08a611b84ff6}[category]

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-d0e7d-c$ 908e-08a611b84ff6}[parentfolder]

Queries value:

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

Queries value:

908e-08a611b84ff6}[relativepath]

Oueries value:

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

908e-08a611b84ff6}[infotip]

Queries value:

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

Oueries value:

908e-08a611b84ff6}[icon]

Oueries value:

908e-08a611b84ff6}[security]

Queries value:

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

Oueries value:

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

Oueries value:

908e-08a611b84ff6}[localredirectonly]

Queries value:

908e-08a611b84ff6}[roamable]

Queries value:

908e-08a611b84ff6}[precreate]

 $HKLM \label{lem:hkkkk} In the latest and the late$ 908e-08a611b84ff6}[stream]

Queries value:

908e-08a611b84ff6}[publishexpandedpath]

Queries value:

908e-08a611b84ff6}[attributes]

Queries value:

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

Queries value:

908e-08a611b84ff6}[initfolderhandler]

Oueries value:

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

folders[cookies]

Queries value:

a03a-e3ef65729f3d}[category]

 $HKLM \label{lem:hkk} In the constant of the$ a03a-e3ef65729f3d}[name]

Queries value:

a03a-e3ef65729f3d}[parentfolder]

Queries value:

a03a-e3ef65729f3d}[description]

Queries value:

a03a-e3ef65729f3d}[relativepath]

Oueries value:

a03a-e3ef65729f3d}[parsingname]

Oueries value:

a03a-e3ef65729f3d}[infotip]

Queries value:

a03a-e3ef65729f3d}[localizedname]

Queries value:

a03a-e3ef65729f3d}[icon]

Queries value:

a03a-e3ef65729f3d}[security]

Queries value:

a03a-e3ef65729f3d}[streamresource]

Oueries value:

a03a-e3ef65729f3d}[streamresourcetype]

Oueries value:

a03a-e3ef65729f3d}[localredirectonly]

Oueries value:

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

Queries value:

a03a-e3ef65729f3d}[precreate]

Queries value:

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

Oueries value:

 $HKLM \label{lem:hkk} White the latest and the lat$ a03a-e3ef65729f3d}[publishexpandedpath]

a03a-e3ef65729f3d}[attributes]

Queries value:

a03a-e3ef65729f3d}[foldertypeid]

Oueries value:

a03a-e3ef65729f3d}[initfolderhandler] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cacheprefix] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\history[peruseritem] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\history[peruseritem] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[category] Queries value: $HKLM \label{lem:hklm} Which is the software \label{lem:hkklm} Which is the software \label{le$ a781-5a1130a75963}[name] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[parentfolder] Queries value: a781-5a1130a75963}[description] Queries value: a781-5a1130a75963}[relativepath] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[parsingname] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[infotip] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[localizedname] Queries value: a781-5a1130a75963}[icon] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[security] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[streamresource] Queries value: a781-5a1130a75963}[streamresourcetype] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-d9dc8a5b-b784-432e-d9dc8a5b-b784-436e-d9dc8a5b-b784-436e-d9dc8a5b-b784-436e-d9dc8a5b-b784-436e-d9dc8a5b-b784-436e-d9dc8a5b-b78$ a781-5a1130a75963}[localredirectonly] Oueries value: a781-5a1130a75963}[roamable] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[precreate] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[stream] Queries value: $HKLM \label{lem:hklm} Which is the software \label{lem:hkklm} Which is the software \label{le$ a781-5a1130a75963}[publishexpandedpath] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[attributes] Queries value: a781-5a1130a75963}[foldertypeid] Oueries value: $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lkklm} White \label{lk$ a781-5a1130a75963}[initfolderhandler] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[history] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\history[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\domstore[cacherepair] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\domstore[cachepath] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\domstore[cacheprefix] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cachelimit] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheoptions] $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\5.0\cache\extensible cache\feedplat[cacherepair]

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

```
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries 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]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
                                    \label{lem:hkcu} \verb+KKCU \software \end{+microsoft windows \verb+currentversion \verb+internet+} \\
  Queries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
  Oueries value
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[enableautoproxyresultcache]
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[displayscriptdownloadfailureui]
  Queries value:
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
  Queries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
  Queries value
                                     \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\so
settings[utf8s
                           nameresl
                                    \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
  Queries value
                            kerthreadhibernation]
settings[disablewo
  Queries value:
                                    \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} internet \end{tabular}
settings[disableworkerthreadhibernation]
  Queries value
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[keepalivetimeout]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxhttpredirects]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsperserver]
  Queries value:
                                    \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[maxconnectionsper1_0server]
  Queries value
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[serverinfotimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendtimeout]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                                     \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[receivetimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
  Queries value:
settings[scavengecachelowerbound]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache[scavengecachefilelimit]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[ftpdefaultexpirytimesecs]
                                  HKLM\software\microsoft\internet
  Queries value:
explorer \\ \verb|main| feature control| feature_disable_unicode_handle_closing_callback [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\ explorer \\ explorer
                                  HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature disable unicode handle closing callback[*]
                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[disablecachingofsslpages]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Oueries value
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Oueries value
                                  HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value
                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[wpadsearchalldomains]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                                  HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[bvpasssslnocachecheck]
                                  HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                                  HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscacheentries]
                                  Queries value:
settings[dnscachetimeout]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:
                                  \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+internet
settings[warnonzonecros
                                sing]
  Queries value
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value
                                  HKI M\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
Queries value:
Queries value:
Queries value:
Queries value
```

Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Queries value:
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
 Oueries value:
- $HKLM\system\current control set\services\winsock 2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]\queries\value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog5 \catalog_entries \0000000000001 \cite{Lem:hklmsystem}. Oueries \value:$
- $\label{lem:lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_c$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000001 [stores service class in fo] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily] Queries value:
- $HKLM\system\current controls et\services\winsock 2\parameters\namespace_catalog 5\catalog_entries\namespace] upported namespace Queries value:$
- $\label{lem:hklmsystem} HKLM \system \controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \namespace_catalog5 \catalog5 \catalog6 \catalog6$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog \catalog_entries \000000000003 \[library path]\] Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version] Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog5 \ catalog_entries \ 0000000000003 \ [storesserviceclassinfo] \ Queries \ value:$
- $\label{lem:hklmsystem} HkLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003[providerinfo]\ Queries\value:$
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog \catalog_entries \0000000000004 [library path] \queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- $\label{lem:hklmsystem} HkLM \system \current controls et\services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \namespace_lements \namespace_catalog5 \catalog_entries \namespace_lements \namespace_lements$

```
Oueries value
Oueries value:
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
  Oueries value:
Oueries value:
HKLM \ system \ (current controls et \ services \ win sock \ parameters \ namespace\_catalog5 \ (catalog\_entries \ 0000000000005 \ [displaystring])
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000005[providerid]
  Queries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[enabled]
  Queries value:
Oueries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 000000000005 [storesserviceclass info]
  Oueries value
HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ name space\_catalog5 \ catalog\_entries \ 000000000005 \ [providerinfo]
  Queries value:
HKLM \ system \ current controls et \ services \ win sock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000006 [library path]
  Queries value
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[addressfamily]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006fsupportednamespace1
  Queries value:
HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog5 \ \ \ catalog\_entries \ \ \ 0000000000006 \ [enabled]
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 spin count]
  Queries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
  Queries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Oueries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[globaluseroffline]
                                HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[badproxyexpirestime]
  Queries value:
                                HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
                                HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:
  Queries value:
                                HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Queries value:
                                HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
                                HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Queries value:
                                HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Queries value:
                                HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
  Queries value:
                                HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [filedirectory]
  Queries value:
                                HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\profilelist[programdata]
  Oueries value:
                                HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \cite{Months} (2ac 077a7) \label{eq:microsoft}
  Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:
                                HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
                                {\tt HKLM \ } \\ \\ \text{Software \ } \\ \\ \text{microsoft \ } \\ \\ \text{tracing \ } \\ \\ \text{rasmancs \ } \\ \\ \text{enable file tracing \ } \\ \\ \\ \text{rasmancs \ } \\ \\ \text{enable file tracing \ } \\ \\ \\ \text{rasmancs \ } \\ \\ \text{enable file tracing \ } \\ \\ \text{enable file tracin
  Oueries value:
  Oueries value:
                                HKLM\software\microsoft\tracing\rasmancs[filetracingmask]
                                \label{lem:hklm} \verb+Kklm/software/microsoft/tracing/rasmancs[enableconsoletracing]
  Queries value:
                                Queries value:
                                HKLM\software\microsoft\tracing\rasmancs[maxfilesize]
  Queries value:
                                HKLM\software\microsoft\tracing\rasmancs[filedirectory]
  Queries value:
                                HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[proxysettingsperuser]
                                HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[migrateproxy]
  Queries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Oueries value:
                                HKCU\software\microsoft\windows\currentversion\internet
```

 ${\tt settings \backslash connections [savedlegacy settings]}$

```
Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigcustomua]
 Oueries value:
                         HKCR\autoproxytypes\application/x-internet-signup[dllfile]
                         \label{localization} \mbox{\tt HKCR} \verb|\ autoproxytypes \verb|\ application/x-internet-signup[file extensions]| \\
 Oueries value:
 Oueries value:
                         HKCR\autoproxytypes\application/x-internet-signup[default]
 Oueries value:
                         HKCR\autoproxytypes\application/x-internet-signup[flags]
 Oueries value:
                         HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
                         HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
 Oueries value:
 Queries value:
                         HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
                         HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
 Queries value:
                         HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zonemap[autodetect]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [used omain named evolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
 Queries value
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen badtlds]
 Oueries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen default servers]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Queries value:
Queries value:
                         HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[useedns]|
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Queries value
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [direct access query order]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Queries value:
{\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ dns cache \verb|\ parameters [registration enabled]|
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Oueries value:
Oueries value
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register reverse lookup]
 Oueries value:
Queries value
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries 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:
Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [updates ecurity level]
 Queries value:
```

```
Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Oueries value:
Oueries value:
                         HKLM \verb|\system| current control set \verb|\services| dns cache \verb|\parameters[dnstest]|
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use compartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use new registration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[resolverregistrationonlv]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]
 Queries value:
                         HKCU\software\microsoft\internet explorer[no3dborder]
  Queries value:
                         HKLM\software\microsoft\internet explorer[no3dborder]
 Queries value:
                         settings[urlencoding]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_mime_handling[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
 Oueries value:
                         HKLM\svstem\currentcontrolset\services\tcpip\parameters[hostname]
                         HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
 Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
 Queries value:
                         HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
 Queries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
                         HKLM\system\currentcontrolset\services\winsock\setup
  Queries value:
migration\providers\tcpip[winsock 2.0 provider id]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [used elayed acceptance]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
 Queries value:
                         HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
 Oueries value:
Queries value:
c19ce8a73253}[searchlist]
 Oueries value:
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\user agent[]
 Queries value:
                         \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\user agent[]
                         Queries value:
settings\5.0\user agent[compatible]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\user agent[compatible]
  Oueries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Oueries value:
                               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
                               HKCU\software\microsoft\windows\currentversion\internet settings[user
  Oueries value:
agent]
  Oueries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
                               HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[platform]
                               HKLM\software\microsoft\internet
  Queries value:
explorer \verb|\main| feature_browser_emulation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Queries value:
                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
  Queries value:
                               HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_maxconnectionsperserver[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Oueries value:
                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Queries value:
                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Oueries value:
                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
  Queries value:
                               \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \normalisatio
settings[enableutf8]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
                               \label{lem:hkcu} \verb|HKCU| software \verb|microsoft| internet explorer \verb|linternational[acceptlanguage]| \\
  Queries value:
                               HKLM\software\microsoft\internet
  Oueries value:
explorer \verb|\main| feature control \verb|\feature_disable_legacy_compression[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                               HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
  Oueries value:
c19ce8a73253}[registrationenabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
c19ce8a73253}[domain]
  Queries value:
c19ce8a73253}[dhcpdomain]
  Queries value:
c19ce8a73253}[dhcpv6domain]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
  Oueries value:
c19ce8a73253}[dhcpnameserver]
  Queries value:
806e6f6e6963}[enabledhcp]
  Queries value:
806e6f6e6963}[registrationenabled]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
  Queries value:
806e6f6e6963}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[nameserver]
  Oueries value:
806e6f6e6963}[dhcpnameserver]
                               HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[queryadaptername]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[disableadapterdomainname]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
  Queries value:
c19ce8a73253}[maxnumberofaddressestoregister]
  Queries value:
c19ce8a73253}[enablemulticast]
```

```
Oueries value:
806e6f6e6963}[queryadaptername]
  Oueries value:
806e6f6e6963}[disableadapterdomainname]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disabledynamicupdate]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
806e6f6e6963}[registrationmaxaddresscount]
  Queries value:
806e6f6e6963}[maxnumberofaddressestoregister]
806e6f6e6963}[enablemulticast]
  Queries value:
                                  HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Oueries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\autocomplete[append]| completion] \end{tabular}
  Queries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \autocomplete \cite{tabular} autocomplete \cite{tabular} autocomple
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
                                  HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
  Oueries value:
  Oueries value:
                                  HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:
  Oueries value:
                                  HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                  HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
  Oueries value:
                                  HKCR\clsid\{6935db93-21e8-4ccc-beb9-
  Queries value:
9fe3c77a297a}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\nprocserver32[]
  Queries value:
  Queries value:
                                  HKCR\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[threadingmodel]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\explorer\runmru[mrulist]
  Queries value:
                                  \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\numru[c]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
                                  HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
  Oueries value:
                                  HKCR\clsid\{00bb2764-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Oueries value:
                                  HKCR\clsid\{00bb2764-6a77-11d0-a535-
  Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel1
                                  HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
  Oueries value:
                                  HKCR\clsid\{00bb2763-6a77-11d0-a535-
  Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:
                                  HKCR\clsid\{00bb2763-6a77-11d0-a535-
  Queries value:
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:
                                  HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus autocomplete \setminus client[]
                                  HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
  Queries value:
                                  HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
  Queries value:
  Queries value:
                                  HKCR\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[]
  Oueries value:
  Oueries value:
                                  HKCR\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                                  HKCU\control panel\desktop[smoothscroll]
  Oueries value:
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
                                  HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]
  Oueries value:
                                  HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
  Oueries value:
199fdba5723b}\inprocserver32[inprocserver32]
  Queries value:
                                  HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32[]
                                  HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
  Oueries value:
199fdba5723b}\inprocserver32[threadingmodel]
  Queries value:
                                  HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
  Queries value:
                                  {\tt HKLM \ } software \verb|\ microsoft \verb|\ ole \verb|\ app compat[raise default authnlevel]
  Queries value:
                                  HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
                                  \label{lem:hklmsystem} \verb| HKLM \rangle is a [everyone includes a nonymous] | \\
  Oueries value:
                                  HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong
cryptographic provider[type]
```

```
Oueries value:
                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
 Oueries value:
                          manager[safeprocesssearchmode]
 Oueries value:
                          HKLM\svstem\currentcontrolset\control\lsa\fipsalgorithmpolicv[enabled]
 Oueries value:
                          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
 Oueries value:
                          {\tt HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography[privkey cachemaxitems]}
 Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privkey cachepurge interval seconds]
                          HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\cryptography[machineguid]
 Queries value:
                          HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
 Queries value:
                          HKLM\software\microsoft\rpc\extensions[remoterpcdll]
                          HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32[]
 Queries value:
                          HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
 Queries value:
 Queries value:
                          HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
                          HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
                          HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
  Queries value:
2299f0398e27}\inprocserver32[threadingmodel]
 Queries value:
                          Oueries value:
                          HKCR \ interface \ \{8a40a45d-055c-4b62-abd7-6d613e2ceaec\} \ proxystubclsid32[]
 Queries value:
                          Queries value:
                          HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
 Queries value:
                          HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
                          HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{b196b286-bab4-101a-b69c-
 Queries value:
00aa00341d07}\inprocserver32[threadingmodel]
                          HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32[]
 Oueries value:
                          HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32[]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\wpad[wpadlastnetwork]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxvdetecttype]
 Queries value:
                          HKLM\system\currentcontrolset\services\netbt\linkage[export]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\zones\3[1a10]
                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version \internet} \end{tabular}
 Oueries value:
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings[privacyadvanced]
                          HKCR\mime\database\content type\text/html[extension]
 Queries value:
  Queries value:
                          HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_mime_sniffing[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
 Queries value:
                          HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_feeds[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| \\
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature feeds[*1
                          HKLM\software\microsoft\internet
 Oueries 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-8fd0-00aa00686f13}\progid[]
 Queries value:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
 Queries value:
 Queries value:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\nprocserver32[]
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-
  Queries value:
00aa00686f13}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_legacy_dispparams[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_legacy_dispparams[*]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
 Queries value:
                          HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
 Queries value:
                          HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-
91a2-7b624e0e72441
                          HKLM\software\microsoft\internet explorer\application
 Oueries value:
compatibility[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                          HKCU\software\microsoft\internet explorer\domstorage[totallimit]
 Queries value:
                          HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
 Queries value:
 Queries value:
                          HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
                          HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\windows[dragscrolldelay]
                          HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\windows[dragscrollinterval]
                          HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature| feature restrict_filedownload[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
 Queries value:
                          HKCR\protocols\handler\about[clsid]
 Queries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
 Queries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
 Queries value:
```

```
Oueries value:
                                  HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_protocol\_lockdown [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| the featurecontrol feature\_protocol\_lockdown [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| the featurecontrol feature\_protocol\_lockdown [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| the featurecontrol featureco
  Oueries value:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature protocol lockdown[*]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
  Oueries value:
                                  HKLM\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
  Queries value:
                                  HKLM\software\policies\microsoft\internet explorer[smartdithering]
  Queries value:
                                  HKCU\software\microsoft\internet explorer[smartdithering]
                                  HKCU\software\microsoft\internet explorer[rtfconverterflags]
  Queries value:
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[usecleartype]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[page_transitions]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
                                  HKCU\software\microsoft\internet explorer\main[anchor underline]
  Oueries value:
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[css_compat]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[expand alt text]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[display inline images]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[display inline videos]
  Oueries value:
                                  HKLM\software\microsoft\internet explorer\main[display inline videos]
  Oueries value:
                                  \label{lem:hccu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main[play\_background\_sounds]}} \label{lem:hccu}
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[play_animations]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[print_background]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[use stylesheets]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[smoothscroll]
                                  HKCU\software\microsoft\internet explorer\main[xmlhttp]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[show image placeholders]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[disable script debugger]
  Queries value:
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
                                  HKCU\software\microsoft\internet explorer\main[move system caret]
  Oueries value:
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[force offscreen
composition]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[usethemes]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[usehr]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\main[q300829]
                                  HKCU\software\microsoft\internet explorer\main[cleanup htcs]
  Queries value:
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[xdomainrequest]
                                  HKLM\software\microsoft\internet explorer\main[xdomainrequest]
  Queries value:
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[domstorage]
  Queries value:
                                  HKCU\software\microsoft\internet
explorer\international[default_codepage]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\international[autodetect]
  Oueries value:
                                  HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\settings[anchor color]
  Oueries 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]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\settings[always use my font
size1
  Queries value:
                                  HKCU\software\microsoft\internet explorer\settings[always use mv font
face]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\settings[use anchor hover
color]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\settings[miscflags]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut copy pastel
                                  HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[disablecachingofsslpages]
  Queries value:
                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\pagesetup[print_background]
  Oueries value:
                                  HKLM \verb|\system| current controlset \verb|\codepage[950]|
  Queries value:
                                  HKCU\software\microsoft\internet
explorer\international\scripts\3\iefontsizel
                                  HKCU\software\microsoft\internet
  Oueries value:
explorer\international\scripts\3[iefontsizeprivate]
  Oueries value:
                                  HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
  Oueries value:
                                  HKCU\software\microsoft\internet
explorer\international\scripts\3[iefixedfontname]
  Queries value:
                                  HKLM\software\microsoft\internet explorer\version vector[ie]
  Queries value:
                                  HKLM\software\microsoft\internet explorer\version vector[vml]
  Queries value:
                                  HKLM\software\microsoft\internet explorer\version vector[windowsedition]
  Queries value:
                                  HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature| supplementation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Oueries value:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[*]
  Queries value:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                  HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_xssfilter[*]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones[securitysafe]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
  Queries value:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature mshtml autoload ieframe[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
```

Queries value:

HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
                                            HKLM\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[cointernetcombineiuricachesize]
  Oueries value:
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[cointernetcombineiuricachesize]
                                            HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[cointernetcombineiuricachesize]
                                            HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature subdownload lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Queries value:
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
  Queries value:
                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:
                                            HKLM\software\microsoft\internet
explorer \verb|\main| feature| solux[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| feature| featu
  Oueries value:
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux[*]
  Queries value:
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:
                                            HKLM\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:
                                            HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings[warnonintranet]
  Queries value:
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonintranet]
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
  Queries value:
  Oueries value:
                                            HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
  Oueries value:
                                            HKCR\clsid\{50d5107a-d278-4871-8989-
  Queries value:
f4ceaaf59cfc}\inprocserver32[threadingmodel]
                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid[]
  Oueries value:
  Oueries value:
                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
                                            HKCR \verb|\clsid| \{f414c260-6ac0-11cf-b6d1-
  Queries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\nprocserver32[]
  Queries value:
   Queries value:
                                            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
   Queries value:
                                            HKCU\software\microsoft\internet explorer\recovery[autorecover]
  Queries value:
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Queries value:
                                            HKLM\software\microsoft\internet
explorer \verb|\main| feature control| feature\_block_lmz\_img[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Oueries value:
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
  Oueries value:
                                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature behaviors[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                            HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_behaviors[*]
                                            HKLM\software\microsoft\internet explorer\default behaviors[homepage]
  Queries value:
                                            \label{local-bb82-00aa00bdce0b} HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]
  Queries value:
                                            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[]
  Queries value:
                                            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
  Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Queries value:
                                            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
  Queries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
                                            HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]
  Queries value:
                                            HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]
   Queries value:
  Queries value:
                                            HKCR\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[inprocserver32]
   Oueries value:
                                            \label{lem:hkcrclsid} $$ HKCR\clsid_{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[] $$
  Oueries value:
                                            HKCR \ clsid \ \ \{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[threadingmodel]
                                            HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[]
  Oueries value:
                                            HKCR\clsid\{d1fe6762-fc48-11d0-883a-
  Oueries value:
3c8b00c10000}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
  Queries value:
  Oueries value:
                                            HKCR\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[threadingmodel]
                                            HKLM\software\microsoft\internet explorer\default
  Queries value:
behaviors[dxtfilterbehavior]
                                            HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]
  Queries value:
                                            HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
  Queries value:
00c04fd9189d}\inprocserver32[inprocserver32]
                                            HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]
  Queries value:
  Oueries value:
                                            HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
  Queries value:
                                            HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:
                                            HKLM\software\microsoft\windows\currentversion[devicepath]
  Queries value:
                                            HKLM\hardware\devicemap\video[maxobjectnumber]
  Queries value:
                                            HKLM\hardware\devicemap\video[\device\video3]
                                            HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
  Queries value:
fd27e3774e32}\0000[pruningmode]
   Queries value:
                                            HKLM\hardware\devicemap\video[\device\video0]
  Queries value:
                                            HKLM \ system \ control \ video \ \{deb 0 39cc-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 3 e-b 7 0 4-4 f 5 3-b 4 5 e-b 7 0 4-4 f 5 3-b 4 6 e-b 7 0 4-4 f 5 3-b 4 6 e-b 7 0 4-4 f 5 3-b 4 6 e-b 7 0 4-4 f 5 3-b 4 6 e-b 7 0 4-4 f 5 6 e-b 7 0 4-4 f 7 0 4-4 f 7 0 4-4 f 7 0 
9dd4432fa2e9}\0000[pruningmode]
  Queries value:
                                            HKLM\hardware\devicemap\video[\device\video1]
```

```
Queries value:
                                          HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[pruningmode]
  Oueries value:
                                           HKLM\hardware\devicemap\video[\device\video2]
                                          Oueries value:
8ed0c8eb59a8}\0000[pruningmode]
                                           HKLM\software\microsoft\directdraw\compatibility\bug![name]
  Oueries value:
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\bug![flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibilitv\bug![id]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\diablo[name]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\diablo[flags]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\diablo[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
  Queries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat 3 [flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
                                           HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
   Queries value:
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
  Oueries value:
                                           HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\nortonsysteminfo[name]|
  Queries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus norton system in fo[flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
  Queries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus rogue \ squadron [flags]
                                           HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
  Oueries value:
  Oueries 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]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibilitv\scorchedplanet[name]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\silentthunder[id]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\starcraft100[name]
                                           HKLM\software\microsoft\directdraw\compatibility\starcraft100[flags]
   Queries value:
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\starcraft100[id]
                                           HKLM\software\microsoft\directdraw\compatibility\starcraft115[name]
   Queries value:
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\starcraft115[flags]
   Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\starcraft115[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[name]
  Queries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus starcraft demo[flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[id]
  Queries value:
                                           HKLM\software\microsoft\directdraw\compatibility\terracide[name]
  Oueries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus terracide [flags]
  Oueries value:
                                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus terracide [id]
                                           HKLM \verb|\software\microsoft\directdraw\compatibility \verb|\thirddimension[name]|
  Oueries value:
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]
  Oueries value:
                                           HKLM\software\microsoft\directdraw\compatibilitv\thirddimension[id]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff daviswin mark benchmark [name]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Queries value
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ KLM \end{tabular} $$ in mark benchmark [id] $$ in the local part of the 
  Queries value:
                                           HKLM\software\microsoft\directdraw[modexonly]
   Oueries value:
                                           HKLM\software\microsoft\directdraw[emulationonly]
  Oueries value:
                                           HKLM\software\microsoft\directdraw[showframerate]
  Oueries value:
                                           HKLM\software\microsoft\directdraw[enableprintscreen]
  Oueries value:
                                           HKLM\software\microsoft\directdraw[forceagpsupport]
  Oueries value:
                                           HKLM\software\microsoft\directdraw[disableagpsupport]
                                           HKLM\software\microsoft\directdraw[disablemmx]
  Oueries value:
  Oueries value:
                                           HKLM\software\microsoft\directdraw[disableddscapsinddsd]
  Oueries value:
                                           HKLM\software\microsoft\directdraw[disablewidersurfaces]
                                           HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Oueries value:
  Oueries value:
                                           HKLM\software\microsoft\directdraw[forcerefreshrate]
                                           HKLM\software\microsoft\direct3d[flipnovsync]
  Queries value:
                                           HKLM\software\microsoft\directdraw[owndc]
  Queries value:
                                           HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
  Queries value:
                                           HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
  Queries value:
  Queries value:
                                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
                                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
  Oueries value:
                                          HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
  Oueries value
f941e9b7e1fe}\inprocserver32[threadingmodel]
  Queries value:
                                          HKCR\dximagetransform.microsoft.shadow\clsid[]
                                           HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
  Queries value:
   Oueries value:
                                          HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
                                          HKCR\clsid\{e71b4063-3e59-11d2-952a-
  Queries value:
00c04fa34f05}\inprocserver32[inprocserver32]
   Queries value:
                                          \label{lem:hkcrclsid} $$ HKCR\clsid_{e71b4063-3e59-11d2-952a-00c04fa34f05} \in \clsid_{e71b4063-3e59-11d2-952a-00c04fa34f05} $$ inprocessor of the context o
  Queries value:
                                          HKCR\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[threadingmodel]
  Queries value:
                                          {\tt HKCR} \verb| mime | database | content type | image/png[extension] \\
```

```
Oueries value:
                           HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
  Oueries value:
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
  Oueries value:
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Oueries value:
                          HKCR\clsid\{30c3b080-30fb-11d0-b724-
  Oueries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
  Oueries value:
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
  Oueries value:
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-
  Oueries value:
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
                          HKCR\clsid\{6a01fda0-30df-11d0-b724-
  Queries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[]
  Queries value:
  Queries value:
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[inprocserver32]
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]
                          HKCR\clsid\{4cb26c03-ff93-11d0-817e-
  Queries value:
0000f87557db}\inprocserver32[threadingmodel]
  Queries value:
                          HKCR\mime\database\content type\image/bmp\bits[0]
  Oueries value:
                          HKCR\mime\database\content type\image/gif\bits[0]
  Oueries value:
                           HKCR\mime\database\content type\image/jpeg\bits[0]
  Oueries value:
                          HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt bits} \mbox{\tt [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{lem:hkcr} \begin{tabular}{ll} HKCR\mbox{$mime$\database$\content type$$\image/$x-png[image filter clsid]$} \end{tabular}
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid[]
HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
  Oueries value:
  Oueries value:
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
  Queries value:
00a0c913f750}\inprocserver32[inprocserver32]
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Oueries value:
  Oueries value:
                          HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]
  Queries value:
  Oueries value:
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Oueries value:
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
  Queries value:
                          HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Queries value:
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
  Queries value:
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
  Queries value:
                           HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
  Queries value:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
  Queries value:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
                          Queries value:
  Oueries value:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[threadingmodel]
                          HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Oueries value:
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1251]
                          HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Oueries value:
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1257]
                           HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Queries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[874]
                           HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[949]
                           HKLM\system\currentcontrolset\control\nls\codepage[1361]
  Queries value:
                          HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\26[iefontsize]
  Queries value:
                          HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsizeprivate]
  Oueries value:
                          HKCU\software\microsoft\internet
explorer\international\scripts\26[iepropfontname]
  Oueries value:
                          HKCU\software\microsoft\internet
explorer\international\scripts\26[iefixedfontname]
                          HKCR\mime\database\content type\image/gif[extension]
  Oueries value:
                           HKLM\software\microsoft\direct3d[disablemmx]
  Queries value:
                          HKLM\software\microsoft\direct3d[disablex3d]
  Queries value:
  Oueries value:
                           HKLM\software\microsoft\direct3d[fewvertices]
                          HKLM\software\microsoft\direct3d[disablevidmemvbs]
  Oueries value:
                          HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane1]|
                          HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane2]|
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane3]
  Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane4]
                           HKLM\software\microsoft\windows
  Queries value:
\verb| nt/currentversion/languagepack/surrogatefallback/simsun[plane5]| \\
                          HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane6]|
                          HKLM\software\microsoft\window
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane7]
  Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane8]
  Oueries value:
                          HKLM\software\microsoft\window
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane9]|
```

```
Queries value:
                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane10]
  Oueries value:
                                  HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane11]|
  Oueries value:
                                  HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback\simsun[plane12]
                                  HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane13]
  Oueries value:
                                  HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback\simsun[plane14]
  Queries value:
                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane15]
                                  HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane16]
  Queries value:
                                  HKLM\software\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_block_lmz_script[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Oueries value:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature block lmz script[*]
                                  HKLM\software\microsoft\internet
  Queries value:
HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
  Oueries value:
                                  HKCU\software\microsoft\windows script\settings[jitdebug]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\new
windows[accuserinitonclick]
  Oueries value:
                                  HKCR\shockwaveflash.shockwaveflash\clsid[]
                                  HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid[]
  Queries value:
                                  HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
  Queries value:
                                  HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
  Oueries value:
444553540000}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[]
  Queries value:
                                  HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
  Queries value:
444553540000}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKLM\svstem\currentcontrolset\control\wmi\securitv[12e1ddac-7ebb-434f-
bc58-54c27d745f8f]
                                  HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
  Queries value:
958a-dad20c90073c]
  Oueries value:
                                  HKLM\hardware\description\system\centralprocessor\0[~mhz]
  Oueries value:
                                  HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
                                  HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
  Queries value:
  Queries value:
                                  HKLM\software\microsoft\internet explorer\default behaviors[userdata]
                                  HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
  Queries value:
  Queries value:
                                  HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
  Queries value:
                                  HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
  Queries value:
                                  HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
  Oueries value:
                                  HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
                                  HKLM\software\microsoft\internet explorer\feed discovery[sound]
  Oueries value:
                                  HKCU\software\microsoft\ftp[use web based ftp]
  Oueries value:
                                  HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature activex repurposedetection[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                  HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_activex_repurposedetection[*]
                                  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:
                                  HKLM\software\microsoft\internet
\verb|explorer| main feature control feature_addon_management[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| | the feature feature for the feature featu
                                  HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_addon_management[*]
  Queries value:
                                  HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1[]
  Queries value:
                                  HKLM\software\microsoft\windows\tablet pc[istabletpc]
  Queries value:
                                  HKCU\software\microsoft\internet explorer\domstorage\total[]
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Oueries value:
                                  \label{lem:hkcrmime} \begin{tabular}{ll} HKCR\mbox{\content type} \application/x-shockwave-flash[extension] \end{tabular}
  Oueries value:
                                  HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid[]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
                                  HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}[]
  Queries value:
                                  HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
  Queries value:
                                  HKCR\clsid\{f5078f35-c551-11d3-89b9-
  Oueries value:
0000f81fe221}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
  Queries value:
                                  HKCR\clsid\{f5078f35-c551-11d3-89b9-
  Queries value:
0000f81fe221}\inprocserver32[threadingmodel]
  Queries value:
                                  HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
  Queries value:
                                  HKCR\clsid\{00020424-0000-0000-c000-00000000046}[]
  Queries value:
                                  HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]
  Oueries value:
                                  HKCR\clsid\{00020424-0000-0000-c000-
  Queries value:
00000000046}\inprocserver32[threadingmodel]
                                  HKCR \ interface \ \ \{85cb6900-4d95-11cf-960c-0080c7f4ee85\} \ \ typelib[]
  Queries value:
  Queries value:
                                  HKCR \land effect (85cb6900-4d95-11cf-960c-0080c7f4ee85) \land typelib[version]
  Queries value:
                                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
  Queries value:
                                  HKLM\software\microsoft\rpc[udtalignmentpolicy]
                                  HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32[]
  Queries value:
  Queries value:
                                  HKCR\clsid\{00020420-0000-0000-c000-00000000046}[]
                                  HKCR\clsid\{00020420-0000-0000-c000-
  Oueries value:
```

00000000046}\inprocserver32[inprocserver32]

```
Oueries value:
                                  HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32[]
  Oueries value:
                                  HKCR\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
                                  HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
  Oueries value:
                                  HKCR\clsid\{a4a1a128-768f-41e0-bf75-
  Oueries value:
e4fddd701cba}\inprocserver32[inprocserver32]
  Oueries value:
                                  HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
                                  HKCR\clsid\{a4a1a128-768f-41e0-bf75-
  Oueries value:
e4fddd701cba}\inprocserver32[threadingmodel]
  Queries value:
                                  HKCR\interface\{00020404-0000-0000-c000-00000000046}\proxystubclsid32[]
                                  HKCR\clsid\{00020421-0000-0000-c000-00000000046}[]
  Queries value:
                                  HKCR\clsid\{00020421-0000-0000-c000-
  Queries value:
00000000046}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserver32[]
  Queries value:
  Queries value:
                                  HKCR\clsid\{00020421-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Oueries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Oueries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Oueries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Oueries value:
                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 6]
  Queries value:
                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 7]
  Oueries value:
                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 8]
  Queries value:
                                  HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid[]
  Queries value:
                                  HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[]
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Oueries value:
  Oueries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midil
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midil]
  Queries value:
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Oueries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Oueries value:
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Oueries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Oueries value:
  Oueries value:
                                  HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[inprocserver32]
  Queries value:
                                  \label{local-bound} \mbox{HKCR\clsid} $$ \arrowver32[] 
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
Queries value:
                                  HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[threadingmodel]
  Oueries 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]
  Oueries 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
  Queries value:
settings\5.0\cache\extensible cache\userdata[cacheoptions]
  Queries value:
                                  HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:
                                  HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Oueries value:
                                  HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Oueries value:
HKLM\system\currentcontrol\sa\sspicache\credssp.dll[capabilities]
                                  Oueries value:
                                  HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Oueries value:
  Queries value:
                                  HKLM \ system \ current control \ set \ control \ lsa \ sspic ache \ creds sp. dll [type]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Oueries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount]
                                  HKCU\software\microsoft\internet
  Queries value:
explorer\services[selectionactivitybuttondisable]
                                  HKCU\software\macromedia\flashplayer[flashplayerversion]
  Queries value:
  Oueries value:
                                  HKCU\software\microsoft\internet explorer\suggested sites[enabled]
                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value
08002b30309d}\shellfolder[attributes]
                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:
                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
  Queries value:
                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
```

```
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
   Queries value:
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsaliasednotifications]
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value
08002b30309d}\shellfolder[wantsuniversaldelegate]
   Queries value:
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
   Oueries value:
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
   Queries value:
                                                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-44d}
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
   Oueries value:
11e3-b3bc-806e6f6e6963}[data]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}[generation]
                                                HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
   Oueries value:
409d6c4515e9}[drivemask]
   Oueries value:
                                                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
   Oueries value:
                                                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
11e3-b3bc-806e6f6e6963}[data]
   Queries value
11e3-b3bc-806e6f6e6963}[generation]
   Queries value:
                                                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
   Oueries value:
                                                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Oueries value:
                                                \label{local-observation} \verb+HKCU\+ software\+ windows\+ current version\+ explorer\+ [shell state]
   Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+ advanced [hideicons]+ \\
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced \cite{tabular} map net drvbtn] \end{tabular}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \[shows uper hidden] \end{tabular}
   Queries value
\label{thm:cursoftware} \begin{tabular}{l} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} \end{tabular} and the constraint \cite{tabular} \end{tabular} \end{tabular} \end{tabular} 
   Oueries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
   Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Oueries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
   Queries value:
                                                HKCR\directory[docobject]
   Queries value:
                                                HKCR\folder[docobject]
   Queries value:
                                                HKCR\allfilesystemobjects[docobject]
   Queries value:
                                                HKCR\directory[browseinplace]
   Queries value:
                                                HKCR\folder[browseinplace]
   Oueries value:
                                                HKCR\allfilesystemobjects[browseinplace]
   Oueries value:
                                                HKCR\directory[isshortcut]
                                                HKCR\folder[isshortcut]
   Queries value:
   Queries value:
                                                HKCR\allfilesystemobjects[isshortcut]
                                                HKCR\directory[alwaysshowext]
   Queries value:
   Queries value:
                                                HKCR\directory[nevershowext]
   Queries value:
                                                HKCR\folder[nevershowext]
   Queries value:
                                                HKCR\allfilesystemobjects[nevershowext]
   Queries value:
                                                \label{lem:hkcrclsid} $$ HKCR\clsid{ff393560-c2a7-11cf-bff4-444553540000} \in \clsid{ff393560-c2a7-11cf-bff4-444553540000} in processing the second context of the second contex
   Queries value:
                                                HKCR \ clsid \ \{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[loadwithoutcom]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\shell
```

```
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046}
0xffff1
   Queries value:
                                                    HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]
   Oueries value:
                                                    HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
                                                    HKCR\clsid\{ff393560-c2a7-11cf-bff4-
   Oueries value:
444553540000}\inprocserver32[threadingmodel]
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cachepath]
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheprefix]
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cachelimit]
   Queries value:
                                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
   Oueries value:
                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta, for example a context of the c
3aea-1069-a2d8-08002b30309d}[]
   Queries value:
                                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
                                                    HKCU\software\microsoft\internet
    Oueries value:
explorer\main\windowssearch[enabledscopes]
   Queries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} which is a constant, and the lemma support \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} Which \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} Which \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} Which \label{lem:hkklm} HKLM \label{lem:hkklm} HKLM \label{lem:hkklm} Which \label{lem:hkklm} Which \label{lem:hkklm} HKLM \label{lem:hkklm} Software \label{lem:hkklm} Which \label{lem:hkklm} Which \label{lem:hkklm} HKLM \label{lem:hkklm} Software \label{lem:hkklm} Which \label{lem:hkklm} HKLM \label{lem:hkklm} Which 
87bd-30b759fa33dd}[category]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[name]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[parentfolder]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[description]
   Oueries value:
HKLM \label{lem:hkkkk} INTO The thick the state of the 
87bd-30b759fa33dd}[relativepath]
   Oueries value:
87bd-30b759fa33dd}[parsingname]
87bd-30b759fa33dd}[infotip]
   Queries value:
87bd-30b759fa33dd}[localizedname]
   Queries value:
87bd-30b759fa33dd}[icon]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[security]
   Oueries value:
87bd-30b759fa33dd}[streamresource]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[streamresourcetype]
   Queries value:
87bd-30b759fa33dd}[localredirectonly]
   Queries value:
87bd-30b759fa33dd}[roamable]
87bd-30b759fa33dd}[precreate]
   Oueries value:
87bd-30b759fa33dd}[stream]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[publishexpandedpath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[attributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[foldertypeid]
   Queries value:
87bd-30b759fa33dd}[initfolderhandler]
   Oueries value:
                                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
   Queries value:
                                                    HKLM\software\microsoft\windows search[currentversion]
    Queries value:
                                                    HKCR\shockwaveflash.7\clsid[]
                                                    HKLM\software\microsoft\downloadmanager[cacheok]
   Queries value:
   Queries value:
                                                    HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}[]
                                                    HKCR\clsid\{3050f391-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
    Queries value:
                                                    HKCR \verb|\clsid|{3050f391-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprocserver32[]|
   Queries value:
                                                    HKCR\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
   Queries value:
                                                    \label{local_hammon_hammon} \begin{tabular}{ll} HKCR\mbox{$m$ime$\database$$\content type$$\scalebox{$image/x-icon[extension]$} \end{tabular}
```

```
Oueries value:
                          HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]
 Oueries value:
                          HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32[]
 Oueries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[]
 Oueries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
 Oueries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-
 Oueries value:
fd2b31b3eefd}\inprocserver32[threadingmodel]
 Oueries value:
                          HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\progid[]
 Oueries value:
                          HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}[]
                          HKCR\clsid\{adc6cb82-424c-11d2-952a-
 Queries value:
00c04fa34f05}\inprocserver32[inprocserver32]
                          HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32[]
 Queries value:
 Queries value:
                          HKCR\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[]
                          HKCR\clsid\{0e890f83-5f79-11d1-9043-
 Oueries value:
00c04fd9189d}\inprocserver32[inprocserver32]
                          HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]
 Queries value:
 Queries value:
                          HKCR\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32[threadingmodel]
 Sets/Creates value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
 Sets/Creates value:
                          HKLM \verb|\software\microsoft\tracing\rasapi32[enablefile tracing]|
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
 Sets/Creates value:
                          HKLM \verb|\software\microsoft\tracing\rasapi32[maxfilesize]|
                          HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [filedirectory]
 Sets/Creates value:
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasmancs[enablefiletracing]
                          {\tt HKLM \coftware \microsoft \tracing \rasmancs[enable consoletracing]}
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasmancs[filetracingmask]
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasmancs[consoletracingmask]
 Sets/Creates value:
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasmancs[maxfilesize]
 Sets/Creates value:
                          HKLM\software\microsoft\tracing\rasmancs[filedirectorv]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\wpad\{8700a497
                         .6961-4e6d-86e2-18954850414c}[wpaddecisionreason]
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{8700a497
                         -6961-4e6d-86e2-18954850414c}[wpaddecisiontime]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\wpad\{8700a497
                         6961-4e6d-86e2-18954850414c}[wpaddecision]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\wpad\{8700a497
                         -6961-4e6d-86e2-18954850414c}[wpadnetworkname]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\wpad\ea-f1
                     1d-61-e0-3e[wpaddecisionreason]
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\ea-f1
                      d-61-e0-3e[wpaddecisiontime]
 Sets/Creates value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\ea-f1-1d-61-e0-3e[wpaddecision]
 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cacherepair]
 Sets/Creates value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache
                      tensible cache\mshist012016040820160409[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Sets/Creates value:
settings\5.0\cache\e
                      tensible cache\mshist012016040820160409[cacheoptions]
 Sets/Creates value:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
 Value changes:
                          HKCU\software\microsoft\internet explorer\main[disable script debugger]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\connections[savedlegacysettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\connections[defaultconnectionsettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\wpad[wpadlastnetwork]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{8700a497-6961-4e6d-86e2-18954850414c}[wpaddecisionreason]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{8700a497-6961-4e6d-86e2-18954850414c}[wpaddecisiontime]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\wpad\{8700a497-6961-4e6d-86e2-18954850414c}[wpaddecision]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{8700a497-6961-4e6d-86e2-18954850414c}[wpadnetworkname]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\ea-f1-1d-61-e0-3e[wpaddecisionreason]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
```

settings\wpad\ea-f1-1d-61-e0-3e[wpaddecisiontime]

 $\begin{tabular}{ll} HKCU \software \mbox{$\stackrel{-}{\rm microsoft }$} \windows \current version \end{tabular} \label{table}$ Value changes:

settings\wpad\ea-f1-1d-61-e0-3e[wpaddecision]

HKLM\software\microsoft\directdraw\mostrecentapplication[name]
HKLM\software\microsoft\directdraw\mostrecentapplication[id]
HKLM\software\microsoft\direct3d\mostrecentapplication[name]
HKCU\software\microsoft\internet explorer\domstorage\total[]
HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
HKCU\software\microsoft\windows\currentversion\internet Value changes: Value changes: Value changes: Value changes: Value changes:

Value changes: HKCU\software\microsoft\window settings\5.0\cache\extensible cache\userdata[cachepath]

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

settings\5.0\cache\extensible cache\mshist012016040820160409[cachepath]

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