Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 7, Task ID: 25

Task ID: 25 Risk Level:

Date Processed 2016-04-08 09:39:52 (UTC)

Processing Time: 61.38 seconds Virtual Environment: IntelliVM

Execution Arguments:

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

Sample ID: Type: basic Owner: admin

62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb Label:

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

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

4c838f1570b3a7ff6f491e6ec1ef6895

SHA256: 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb

Description:

Pattern Matching Results

3 HTTP connection - response code 200 (success)

Possible injector 2 HTML file

JavaScript: Writes a string of text to a document stream

HTTP connection - response code 404 (file not found)

3 Connects to local host

1 YARA score 1

4 JavaScript: Eval method

3 Long sleep detected

4 Checks whether debugger is present

Static Events

YARA rule hit: YARA rule hit: Nonexecutable

Process/Thread Events

Creates process

C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe

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

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

Named Object Events

Creates mutex \Sessions\1\BaseNamedObjects\DBWinMutex

 $\verb|\Sessions|1\BaseNamedObjects| CicLoadWinStaWinSta0|$ Creates mutex:

\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1 Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex Creates mutex:

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCounterMutex

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

\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex Creates mutex: 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

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

Creates mutex:

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

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

Creates mutex: $\verb|\Sessions|1\BaseNamedObjects| RasPbFile| \\$ \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex Creates mutex:

\Sessions\1\BaseNamedObjects__DDrawExclMode__ \Sessions\1\BaseNamedObjects__DDrawCheckExclMode Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\DDrawWindowListMutex \Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex Creates mutex: Creates mutex:

\Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x0000089C) Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069}

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

Creates mutex:

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

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

\Sessions\1\BaseNamedObjects\InternetExplorerDOMStoreQuota Creates mutex:

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

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

Creates mutex:

 $\verb|\Sessions|1\BaseNamedObjects| : ! users! admin! appdata! roaming! microsoft! windows! ietldcache! | the state of the s$ \KernelObjects\MaximumCommitCondition Creates event:

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

Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED Creates event:

\BaseNamedObjects\SvcctrlStartEvent_A3752DX \BaseNamedObjects\BFE_Notify_Event_{22ad8c5a-3fa3-4bc7-8399-Creates event:

a35fa8fee727}

\Sessions\1\BaseNamedObjects\DINPUTWINMM

File System Events

Creates: C:\Users\Admin

```
Creates:
                                                       C:\Users\Admin\AppData\Local
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
    Creates:
    Creates:
                                                       C:\Users\Admin\AppData\Roaming
                                                        C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
    Creates
    Creates:
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\History
   Creates:
Creates:
C: \verb|VBers\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt|
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\TZILKL9J\index[1].php
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\266VNL5S\bd_logo1[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
   Creates:
                                                       C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet|
Files\Content.IE5\TZILKL9J\baidu_jgylogo3[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\nuomi_510f7472[1].png
                                                       {\tt C:\backslash Users\backslash Admin\backslash AppData\backslash Local\backslash Microsoft\backslash Windows\backslash Temporary\ Internet}
   Creates:
Files\Content.IE5\WM60WM90\zbios_62c636fe[1].png
                                                        \label{local-Microsoft-Windows-Temporary Internet} C: \space{-0.05\textwindows-Temporary Internet} In the content of the content
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\VB8EH8F1\all_async_search_d0d1b2ec[1].js
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
   Creates:
C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt|
                                                        {\tt C:\backslash Users\backslash Admin\backslash AppData\backslash Local\backslash Microsoft\backslash Windows\backslash Temporary\ Internet}
Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
                                                       C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
   Creates:
                                                        C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
    Creates:
                                                        {\tt C:\Wsers\Admin\AppData\Roaming\Adobe\Flash\ Player\AssetCache\QW4AL2EV}
    Creates
\label{local_windows} Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet Files\Content.IE5\266VNL5S\quickdelete\_9c14b01a[1].png
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Creates:
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
   Creates
                                                       C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\VU73CBGV\www.baidu[1].xml
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\| Content.IE5 \verb|\| TZILKL9J \verb|\| bdsug_async_1cb857eb[1].js
   Creates:
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\env_beb83b45[1].swf
                                                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
                                                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
    Creates:
Explorer\UserData\index.dat
    .
Creates:
                                                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEQSE8W1
   Creates:
                                                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP
                                                        C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\MW2QSIZ4
   Creates:
                                                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UIMZBC64
    Creates:
                                                       C:\Users\Admin\AppData\Roaming\Macromedia
    Creates:
                                                       C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
   Creates:
                                                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
    Creates:
Player\#SharedObjects\HHYYWDWK
   Creates:
                                                       C: \verb|\USers\Admin\AppData\Roaming\Macromedia\Flash\ Player\macromedia.com| \\
                                                       C:\Users\Admin\AppData\Roaming\Macromedia\Flash
    Creates:
Player\macromedia.com\support
    Creates:
                                                       C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
                                                       C:\Users\Admin\AppData\Roaming\Macromedia\Flash
   Creates:
\label{linear_player} Player\mbox{\sc Name} normalia.com\mbox{\sc Support\sc Player\sc Name} s.sxx $$ Creates: $C:\sc Name\n\sc Name\n\s\n\sc Name\n\sc Name\n\s\n\s
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
   Creates:
                                                       C:\Users\Admin\AppData\Roaming\Macromedia\Flash
\label{linear_policy} Player\mbox{\com\support\flashplayer\sys.} \#s1.bds \mbox{\com\support\flashplayer\sys.} xxx $$ Creates: $C:\Users\Admin\AppData\Roaming\Macromedia\Flash} $$
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com
   Creates:
                                                       C: \verb|\Users\Admin\AppData\Roaming\Macromedia\Flash|
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
    Creates:
Explorer\UserData\JEQSE8W1\userDataBIDUPSID[1].xml
   Creates:
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
    Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Historv\Historv.IE5\MSHist012016040820160409
    Creates:
C: \verb|Visers| Admin AppData \\ Local \\ Microsoft \\ Windows \\ History \\ . IE5 \\ MSH is to 12016040820160409 \\ \\ index. data \\ Admin \\ A
                                                       C:\Users\Admin\Favorites
   Creates:
    Creates:
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\favicon[1].ico
                                                       C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
   Creates:
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Creates:
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
   Creates:
                                                       {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\VB8EH8F1\pc[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Content.IE5|| 266VNL5S \verb|\ps_default[1].gif|
                                                       Creates:
Files\Content.IE5\WM60WM90\ps_default[1].gif
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Content.IE5| VB8EH8F1 \verb|\ps_default[1].gif|
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\TZILKL9J\ps_default[1].gif
                                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\266VNL5S\ps_default[2].gif
```

```
Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\JSocket 9a52fc3e[1].swf
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
               ent.IE5\VB8EH8F1\s[1].txt
Files\Cont
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\VB8EH8F1\union[1].gif
   Creates
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\TZILKL9J\ps_default[2].gif
                                   {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Creates:
Files\Content.IE5\266VNL5S\pc[1].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\content.IE5| \verb|\w| M60WM90| \verb|\u=658147196|, 2876094505\&fm=96\&s=418421F0022805031201C81C030050DB[1].jpg | Section (Content.IE5) | Section (
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\TZILKL9J\u=2752145054,3166876123&fm=58[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=2521629668,33371966&fm=96&s=66927722A5E7DF07E68DE8D70100C0A3[1].jpg
  Creates
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=4267309876,3923431364&fm=96&s=EA90E90821C392A6BCAFF10D0300E0E1[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=2731110358,2228192387&fm=58[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\VB8EH8F1\u=2719784904,580575759&fm=58[1].jpg
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2627075135,3105681134&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2269530877,797123279&fm=96&s=FB1A4A81CFB4358A302555930300B092[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\266VNL5S\u=2413434242,1825510918&fm=96&s=4E9241887E120FDE0C4DF0800300E081[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files \verb|\Content.IE5| \verb|\WM60WM90| \verb|\u=918841094|, 1711827117\&fm=58[1].jpg| \\
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\266VNL5S\u=2584046138,590027024&fm=96&s=4E9274884A700F8ACA30D956030050E0[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates
Files\Content.IE5\WM60WM90\his[1]
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=1010662780,933723174&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=3841058258,2231097427&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2916809114,3153528632&fm=96&s=1EF66984415003CA44803596030080C2[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=4121919617,900972282&fm=58[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\WM60WM90\union[1].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2781679007,565939595&fm=58[1].jpg
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\wb[1].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\ielib_0108[1].js
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\WM60WM90\u=532204567,887570784&fm=58[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\VB8EH8F1\wb[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2177447570,2292449148&fm=82&s=21904D3064EAEF090584C9C6010070A3&w=121&h=81&img[1].jpg
\label{local-Microsoft-Windows-Temporary Internet} Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\266VNL5S\u=1489011112,1613214565\&fm=58[1].jpg
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\VB8EH8F1\u=1779799337,1886987922&fm=58[1].jpg
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZTLKL9J\wb[1].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\266VNL5S\wb[2].gif
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\o 0108[1].swf
  Creates:
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\VB8EH8F1\wb[2].gif
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[2].gif
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Creates
Files\Content.IE5\266VNL5S\wb[3].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\WM60WM90\wb[1].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[3].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\TZILKL9J\wb[3].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\wb[4].gif
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[2].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates
Files\Content.IE5\VB8EH8F1\wb[4].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\TZILKL9J\wb[4].gif
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\wb[5].gif
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\WM60WM90\wb[3].gif
  Creates:
                                   C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Internet|
Explorer\UserData\2T2VAGUP\oXMLStore[1].xml
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\VB8EH8F1\wb[5].gif
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Content.IE5\TZILKL9J\ps_fp[1].htm|\\
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Creates:
Files\Content.IE5\266VNL5S\wb[6].gif
  Creates:
                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[4].gif
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\VB8EH8F1\wb[6].gif
```

```
Opens
                                                      C:\Windows\Prefetch\62DDFBF757BE511F30B6D330963C1-E2075B81.pf
                                                      C:\Windows
   Opens:
   Opens:
                                                       C:\Windows\System32\wow64.dll
                                                       C:\Windows\System32\wow64win.dll
   Opens:
   Opens:
                                                       {\tt C:\Windows\System32\wow64cpu.dll}
                                                      C:\Windows\system32\wow64log.dll
   Opens:
                                                       C:\Windows\SysWOW64
    Opens:
   Opens:
                                                       C:\Windows\SysWOW64\sechost.dll
   Opens:
{\tt C: windows \texttt{\colored} hosp \texttt{\colo
                                                       C:\Windows\winsxs\x86_microsoft.windows.common-
   Opens
C:\windows\temp\MSIMG32.dll
   Opens:
   Opens:
                                                      C:\Windows\SysWOW64\msimg32.dll
                                                      C:\windows\temp\VERSION.dll
   Opens
                                                       C:\Windows\SysWOW64\version.dll
    Opens:
                                                       C:\Windows\SysWOW64\imm32.dll
   Opens
   Opens
                                                      C:\Windows\WindowsShell.Manifest
                                                       C:\program files\qqd1eae\log.dat
   Opens:
                                                       C:\Windows\SysWOW64\ntdll.dll
    Opens:
   Opens:
                                                       C:\windows\temp\msdialg100_D.dll
                                                       C:\Windows\SysWOW64\msdialg100 D.dll
   Opens:
                                                       C:\Windows\system\msdialg100_D.dll
   Opens:
    Opens:
                                                       C:\Windows\msdialg100_D.dll
   Opens:
                                                       C: \verb|\windows\SysWOW64\Wbem\msdialg100_D.dl1| \\
                                                      C:\Windows\SysWOW64\WindowsPowerShell\v1.0\msdialg100_D.dll
   Opens:
   Opens:
                                                       C:\windows\temp\MFC90ENut.dll
    Opens:
                                                       C:\Windows\SysWOW64\MFC90ENut.dll
   Opens:
                                                      C:\Windows\system\MFC90ENut.dll
                                                      C:\Windows\MFC90ENut.dll
   Opens:
                                                       C:\Windows\SysWOW64\Wbem\MFC90ENut.dll
   Opens:
                                                       C: \verb|\windows| SysWOW64\windows| PowerShell \verb|\v1.0| MFC90ENut.dll| \\
   Opens:
                                                      C:\windows\temp\Afx100net.dll
C:\Windows\SysWOW64\Afx100net.dll
   Opens:
   Opens:
                                                       C:\Windows\system\Afx100net.dll
   Opens:
   Opens:
                                                       C:\Windows\Afx100net.dll
                                                      C:\Windows\SysWOW64\Wbem\Afx100net.dll
   Opens:
                                                       C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Afx100net.dll
   Opens:
                                                       C:\program files\qqd1eae\Log.dat
    Opens:
   Opens
                                                       C:\Program Files\QQd1eae\slowt64.dll
   Opens:
                                                       C:\Windows\SysWOW64\rpcss.dll
                                                       C:\Windows\SysWOW64\uxtheme.dll
   Opens:
   Opens:
                                                       C:\Users\Admin\AppData\Local\Temp\restart.dat
   Opens:
                                                      C:\windows\temp\dwmapi.dll
C:\Windows\SysWOW64\dwmapi.dll
   Opens:
    Opens:
                                                       C:\Windows\Fonts\StaticCache.dat
                                                       C:\Windows\Fonts\tahoma.ttf
   Opens:
   Opens:
                                                      C:\Windows\Fonts\meiryo.ttc
                                                       C:\Windows\Fonts\msgothic.ttc
   Opens:
                                                       C:\Windows\Fonts\msjh.ttf
    Opens:
   Opens:
                                                      C:\Windows\Fonts\msyh.ttf
   Opens:
                                                      C:\Windows\Fonts\malgun.ttf
                                                       C:\Windows\Fonts\mingliu.ttc
   Opens
                                                       C:\Windows\Fonts\simsun.ttc
    Opens:
   Opens:
                                                      {\tt C:\Windows\Fonts\gulim.ttc}\\
                                                      C:\Windows\SvsWOW64\en-US\user32.dll.mui
   Opens:
                                                       C:\Windows\Globalization\Sorting\SortDefault.nls
   Opens
                                                       C:\Windows\SysWOW64\uxtheme.dll.Config
    Opens:
   Opens:
                                                       C:\Windows\SysWOW64\ieframe.dll
                                                      C:\Windows\SysWOW64\oleacc.dll
   Opens:
                                                       C:\windows\temp\OLEACCRC.DLL
   Opens:
    Opens
                                                       C:\Windows\SysWOW64\oleaccrc.dll
   Opens
C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
   Opens:
                                                      C:\Windows\SysWOW64\ole32.dll
                                                       C:\windows\temp\ntmarta.dll
                                                      C:\Windows\SysWOW64\ntmarta.dll
   Opens:
                                                      C:\Windows\SysWOW64\en-US\urlmon.dll.mui
   Opens:
                                                       C:\Windows\SysWOW64\shell32.dll
   Opens:
                                                      C:\windows\temp\apphelp.dll
C:\Windows\SysWOW64\apphelp.dll
   Opens:
   Opens:
                                                       C:\WINDOWS\Temp\MJPGC.TMP
   Opens:
                                                       C:\Windows\SysWOW64\en-US\ieframe.dll.mui
    Opens:
   Opens:
                                                       C:\Windows\SysWOW64\wininet.dll
                                                      C:\windows\temp\profapi.dll
   Opens:
                                                       C:\Windows\SysWOW64\profapi.dll
    Opens:
                                                       C:\Users\Admin
    Opens:
   Opens:
                                                      {\tt C:\Users\Admin\AppData\Local}
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
   Opens:
    Opens
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
   Opens:
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
   Opens
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
                                                      C:\Users\Admin\AppData\Roaming
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
   Opens:
   Opens
    Opens:
                                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\History
   Opens:
                                                       {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini}
                                                      C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\History\History.IE5| \\
   Opens:
    Opens:
C: \verb|\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini| \\
   Opens:
                                                      {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\index.dat
                                                      C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat|
   Opens:
\verb|C:\Users\land Admin\land AppData\land Local\land Microsoft\land Windows\land History\land IE5\land index.data and the property of the prop
                                                      C:\windows\temp\dnsapi.DLL
   Opens:
    Opens:
                                                       C:\Windows\SysWOW64\dnsapi.dll
                                                       C:\windows\temp\iphlpapi.DLL
   Opens
```

```
Opens:
                         C:\windows\temp\WINNSI.DLL
 Opens:
                          C:\Windows\SysWOW64\winnsi.dll
                          C:\windows\temp\RASAPI32.dll
 Opens:
                          {\tt C:\Windows\SysWOW64\rasapi32.dl1}
 Opens:
                         C:\windows\temp\rasman.dll
 Opens:
                          C:\Windows\SysWOW64\rasman.dll
 Opens:
                         C:\windows\temp\rtutils.dll
C:\Windows\SysWOW64\rtutils.dll
 Opens:
 Opens:
                          C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens:
                          C:\Windows\SysWOW64\ras
  Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
                          C:\windows\temp\sensapi.dll
 Opens:
                          C:\Windows\SysWOW64\SensApi.dll
 Opens:
                          C:\Windows\SysWOW64\nlaapi.dll
 Opens:
                         C:\windows\temp\rasadhlp.dll
C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\mswsock.dll
  Opens:
                          C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
 Opens:
                         C:\windows\temp\MLANG.dll
                         C:\Windows\SysWOW64\mlang.dll
 Opens:
                          C:\Windows\SysWOW64\wship6.dll
  Opens:
 Opens:
                          C:\windows\temp\dhcpcsvc6.DLL
                          C:\Windows\SysWOW64\dhcpcsvc6.dll
 Opens:
                         C:\Program Files (x86)\Common Files\microsoft shared\ink\tiptsf.dll
 Opens
  Opens:
                          C:\windows\temp\dhcpcsvc.DLL
                         C:\Windows\SysWOW64\dhcpcsvc.dll
C:\Windows\System32\drivers\etc\hosts
 Opens:
 Opens:
 Opens:
                          C:\Windows\SysWOW64\FWPUCLNT.DLL
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
 Opens:
\label{lem:c:users} $$C: \dot Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt $$
                          C:\Windows\System32\C_20127.NLS
 Opens:
 Opens:
                          C:\Windows\SysWOW64\mshtml.dll
                         C:\Windows\SysWOW64\msls31.dll
 Opens:
  Opens
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\index[1].php
                         C:\Windows\SysWOW64\msimtf.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\jscript.dll
                          C:\windows\temp\CRYPTSP.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
                         C:\Windows\SysWOW64\rsaenh.dll
C:\windows\temp\RpcRtRemote.dll
 Opens:
 Opens:
 Opens:
                          C:\Windows\SysWOW64\RpcRtRemote.dll
 Opens:
                          C:\Windows\SysWOW64\iepeers.dll
                         C:\Windows\SysWOW64\winspool.drv
 Opens:
  Opens:
                          C:\Windows\SysWOW64\dxtrans.dll
                          C:\Windows\SysWOW64\atl.dll
 Opens:
 Opens
                         C:\Windows\SysWOW64\ddrawex.dll
                         C:\Windows\SysWOW64\ddraw.dll
 Opens:
                          C:\Windows\SysWOW64\dciman32.dll
  Opens:
 Opens:
                         C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens:
                         C:\Windows\win.ini
                         C:\Windows\SysWOW64\en-US\ddraw.dll.mui
 Opens:
                          C:\Windows\SysWOW64\dxtmsft.dll
  Opens:
 Opens:
                         C:\windows\temp\ImgUtil.dll
                         C:\Windows\SysWOW64\imgutil.dll
 Opens:
                          C:\Windows\SysWOW64\pngfilt.dll
 Opens
                          C:\windows\temp\SXS.DLL
  Opens
 Opens:
                          C:\Windows\SysWOW64\sxs.dll
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
 Opens:
                         C:\Windows\SysWOW64\kernel32.dll
 Opens:
                          C:\Windows\Fonts\arial.ttf
                         C:\Windows\SysWOW64\en-US\mlang.dll.mui
 Opens:
 Opens:
                          C:\Windows\System32\C_1250.NLS
                         C:\Windows\System32\C_1251.NLS
C:\Windows\System32\C_1253.NLS
 Opens:
 Opens
                         C:\Windows\System32\C_1254.NLS
 Opens:
                          C:\Windows\System32\C_1255.NLS
 Opens:
 Opens
                         C:\Windows\System32\C_1256.NLS
                         C:\Windows\System32\C_1250.NLS
C:\Windows\System32\C_1257.NLS
C:\Windows\System32\C_1258.NLS
 Opens:
 Opens:
                          C:\Windows\System32\C_874.NLS
  Opens:
                         C:\Windows\System32\C_932.NLS
C:\Windows\System32\C_936.NLS
 Opens:
 Opens:
                          C:\Windows\System32\C_949.NLS
  Opens
                          C:\Windows\System32\C_950.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_1361.NLS
 Opens:
                          C:\Windows\Fonts\arialbd.ttf
                          C:\Windows\Fonts\ariali.ttf
  Opens:
                          C:\Windows\SysWOW64\tzres.dll
 Opens:
                          C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens:
                          C:\Windows\SysWOW64\en-US\jscript.dll.mui
 Opens
                          C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
  Opens:
 Opens:
C:\Windows\winsxs\x86 microsoft.windows.gdiplus 6595b64144ccf1df 1.1.7601.17514 none 72d18a4386696c80
 Opens:
Opens:
                         C:\windows\temp\D3DIM700.DLL
                         C:\Windows\SysWOW64\d3dim700.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\mshtml.dll.mui
 Opens
                          {\tt C:\Windows\Temporary\ Internet}
Files\Content.IE5\VB8EH8F1\all_async_search_d0d1b2ec[1].js
                         C:\Windows\SysWOW64\stdole2.tlb
 Opens:
  Opens:
                          C:\Windows\SysWOW64\mshtml.tlb
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

Opens

C:\Windows\SvsWOW64\IPHLPAPI.DLL

```
Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
  Opens:
                                    C:\Windows\SysWOW64\urlmon.dll
  Opens:
                                    C:\Windows\SysWOW64\Macromed\Flash\Flash10h.ocx
  Opens:
  Opens:
                                    {\tt C:\Windows\SysWOW64\Macromed\Flash\WINMM.dll}\\
                                    C:\Windows\SysWOW64\winmm.dll
  Opens:
                                       :\Windows\SysWOW64\Macromed\Flash\DSOUND.dll
  Opens:
  Opens:
                                    C:\Windows\SysWOW64\dsound.dll
                                    C:\Windows\SysWOW64\Macromed\Flash\POWRPROF.dll
  Opens:
                                    C:\Windows\SysWOW64\powrprof.dll
  Opens:
                                    C:\Windows\SysWOW64\Macromed\Flash\mscms.dll
  Opens:
  Opens
                                    C:\Windows\SysWOW64\mscms.dll
                                    C:\Windows\SysWOW64\Macromed\Flash\USERENV.dll
  Opens:
                                    C:\Windows\SysWOW64\userenv.dll
  Opens:
                                    C:\Windows\SysWOW64\Macromed\Flash\ss.sgn
  Opens:
  Opens:
                                    C:\Windows\SysWOW64\Macromed\Flash
                                    C:\Windows\SysWOW64\Macromed\Flash\ss.cfg
  Opens:
                                    C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
  Opens
                                    C:\Windows\SysWOW64\Macromed\Flash\oem.cfg
  Opens:
  Opens:
                                    C:\Windows\SysWOW64\oem.cfg
                                    C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
  Opens:
  Opens
                                    C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
                                     C:\Users\Admin\AppData\Roaming\Adobe \\ C:\Users\Admin\AppData\Roaming\Adobe\Flash\ Player\AssetCache\QW4AL2EV \\
  Opens:
  Opens
  Opens
                                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\| Content.IE5 \verb|\| WM60WM90 \verb|\| nu_instant_search_ebeb5baa[1].js \\
                                    C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
  Opens:
                                    C:\Users\Admin\AppData\Local\Microsoft\Internet
  Opens
Explorer\DOMStore\index.dat
  Onens:
                                    C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\VU73CBGV\www.baidu[1].xml
                                    C:\windows\temp\XmlLite.dll
  Opens:
                                    C:\Windows\SysWOW64\xmllite.dll
  Opens
                                    {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\TZILKL9J\bdsug_async_1cb857eb[1].js
                                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\env_beb83b45[1].swf
                                    C:\windows\temp\MMDevAPI.DLL
  Opens:
                                    C:\Windows\SysWOW64\MMDevAPI.dll
  Opens:
                                    C:\windows\temp\PROPSYS.dll
  Opens:
  Opens
                                    C:\Windows\SysWOW64\propsys.dll
                                    C:\Windows\SysWOW64\msxml3.dll
  Opens:
  Opens:
                                    C:\Windows\SysWOW64\msxml3r.dll
  Opens:
                                    C:\Windows\SysWOW64\en-US\msxml3r.dll.mui
  Opens:
                                    {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Internet\ Explorer\UserData\AppData\Roaming\Microsoft\Internet\ Explorer\UserData\AppData\Roaming\Microsoft\Normalian AppData\Roaming\Microsoft\Normalian AppData\Ro
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
  Opens:
  Opens
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\index.dat
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEQSE8W1
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\MW2QSIZ4
                                    {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Internet}
Explorer\UserData\UIMZBC64
                                    {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Internet}
  Opens:
Explorer\UserData\*.*2I2VAGUP\desktop.ini
                                    \hbox{\tt C:\Users\Admin\AppData\Roaming\Microsoft\Internet}\\
  Opens:
Explorer\UserData\JEQSE8W1\desktop.ini
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\MW2QSIZ4\desktop.ini
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UIMZBC64\desktop.ini
                                    C:\windows\temp\Secur32.dll
  Opens:
  Opens:
                                    C:\Windows\SysWOW64\secur32.dll
                                    C:\windows\temp\credssp.dll
  Opens:
  Opens:
                                    C:\Windows\SysWOW64\credssp.dll
                                    C:\Windows\SysWOW64\schannel.dll
  Opens:
                                    \hbox{\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash\ Player\\#Shared0bjects}
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia
  Opens:
  Opens:
                                    C:\Users\Admin\AppData
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens
Player\#SharedObjects\HHYYWDWK
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\macromedia.com\support\flashplayer\sys\
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sol
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\
  Opens:
                                    C: \verb|\Users\Admin\AppData\Roaming\Macromedia\Flash| \\
Plaver\macromedia.com\support\flashplayer
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support
                                    .
C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\macromedia.com\
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\macromedia.com
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sol
```

```
Opens
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\
  Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
                         C: \verb|\USers\Admin\AppData\Roaming\Macromedia\Flash\ Player\s1.bdstatic.com\\|
 Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Opens:
Opens:
                         {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
Player\#SharedObjects\HHYYWDWK\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
C:\Users\Admin\AppData\Roaming\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
 Opens:
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\svs\#s1.bdstatic.com\settings.sxx
  Opens
                         C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com
 Opens:
                         C: \verb|\USers\Admin\AppData\Roaming\Macromedia\Flash| \\
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                         C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\JEQSE8W1\userDataBIDUPSID[1].xml
                         {\tt C:\Windows\Caches\cversions.1.db}
  Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
  Opens
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
                         C:\Users\desktop.ini
  Opens:
                         C:\Program Files (x86)\Internet Explorer\ieproxy.dll
  Opens:
                         C:\Users
  Opens:
                         C:\Users\Admin\AppData\Local\Microsoft
  Opens:
  Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\
C:\Users\Admin\AppData\Local\Microsoft\Windows\Historv\Historv.IE5\MSHist012016040820160409
 Opens:
{\tt C:\WSers\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\index.data} \\
                         C:\Windows\SysWOW64\en-US\shell32.dll.mui
  Opens:
  Opens:
                         C:\Users\Admin\Favorites
                         C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
  Opens:
  Opens:
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Internet\ Explorer\MSIMGSIZ.DAT}
  Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\favicon[1].ico
  Opens
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
Opens: C:\Windows\SysWOW64\en-US\winmm.dll.mui
                         C:\Windows\Media\Windows Navigation Start.wav
  Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens
Files\Content.IE5\266VNL5S\ps_default[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\JSocket_9a52fc3e[1].swf
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\s[1].txt
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
 Opens:
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\VB8EH8F1\union[1].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\TZILKL9J\ps_default[1].gif
 Opens:
                         C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\IETldCache| \\
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
  Opens
Files\Content.IE5\WM60WM90\union[1].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Onens:
Files\Content.IE5\266VNL5S\wb[1].gif
  Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[1].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\TZILKL9J\wb[1].gif
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Opens
Files\Content.IE5\266VNL5S\wb[2].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\WM60WM90\o_0108[1].swf
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[2].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens
Files\Content.IE5\TZILKL9J\wb[2].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\wb[3].gif
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[1].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens
Files\Content.IE5\VB8EH8F1\wb[3].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\TZILKL9J\wb[3].gif
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\wb[4].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\WM60WM90\wb[2].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Opens:
Files\Content.IE5\VB8EH8F1\wb[4].gif
Onens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[4].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\266VNL5S\wb[5].gif
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\WM60WM90\wb[3].gif
 Opens:
                         C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroPDF.dll
  Opens:
```

```
C:\Windows\winsxs\x86 microsoft.vc80.crt 1fc8b3b9a1e18e3b 8.0.50727.4940 none d08cc06a442b34fc\msvcp80.dll
  Opens:
\texttt{C:Nuindows} winsxs \times 86 \\ \texttt{microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.4940\_none\_d08cc06a442b34fc} \\ \texttt{msvcr80.dl1} \\ 
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP\oXMLStore[1].xml
                                      C:\Program Files (x86)\Java\jre7\bin\deploy.dll
  Opens:
   Opens
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[5].gif
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\266VNL5S\wb[6].gif
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[4].gif
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\VB8EH8F1\wb[6].gif
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
  Writes to:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\index[1].php
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\266VNL5S\bd_logo1[1].png
  Writes to:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\baidu_jgylogo3[1].gif
  Writes to:
                                      {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Writes to: C. \Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\nuomi_510f7472[1].png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\zbios_62c636fe[1].png
  Writes to:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\VB8EH8F1\all_async_search_d0d1b2ec[1].js
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
                                      {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\266VNL5S\quickdelete_9c14b01a[1].png
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
                                      C:\Users\Admin\AppData\Local\Microsoft\Internet
{\tt Explorer\DOMStore\VU73CBGV\www.baidu[1].xml}
  Writes to:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\bdsug_async_1cb857eb[1].js
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\TZILKL9J\env beb83b45[1].swf
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Writes to:
Explorer\Use
                                      C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Writes to:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
Writes to: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
                 omedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
Player\macr
  Writes to:
                                      {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Writes to:
Explorer\UserData\JEQSE8W1\userDataBIDUPSID[1].xml
  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
Files\Content.IE5\266VNL5S\favicon[1].ico
  Writes to:
                                      \verb|C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico| \\
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\VB8EH8F1\pc[1].gif
  Writes to:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\ps_default[1].gif
  Writes to:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\ps_default[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\ps_default[1].gif
  Writes to:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_default[1].gif
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\ps_default[2].gif
  Writes to:
                                      {\tt C:\backslash Users\backslash Admin\backslash AppData\backslash Local\backslash Microsoft\backslash Windows\backslash Temporary\ Internet}
Files\Content.IE5\WM60WM90\JSocket_9a52fc3e[1].swf
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\s[1].txt
                                      {\tt C:\SolvantalMicrosoft\Windows\Temporary\ Internet}
  Writes to:
Files\Content.IE5\TZILKL9J\ps_default[2].gif
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\pc[1].gif
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\WM60WM90\u=658147196,2876094505&fm=96&s=418421F0022805031201C81C030050DB[1].jpg
                                      \hbox{\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}}
Files\Content.IE5\TZILKL9J\u=2752145054,3166876123&fm=58[1].jpg
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\266VNL5S\u=2521629668,33371966&fm=96&s=66927722A5E7DF07E68DE8D70100C0A3[1].jpg
                                      {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\WM60WM90\u=4267309876.3923431364&fm=96&s=EA90E90821C392A6BCAFF10D0300E0E1[1].ipg
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\VB8EH8F1\u=2719784904,580575759&fm=58[1].jpg
                                      {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\VB8EH8F1\u=2731110358,2228192387&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2627075135,3105681134&fm=58[1].jpg
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
```

```
Files\Content.IE5\TZILKL9J\u=2269530877,797123279&fm=96&s=FB1A4A81CFB4358A302555930300B092[1].jpg
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=2413434242,1825510918&fm=96&s=4E9241887E120FDE0C4DF0800300E081[1].jpg
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Writes to:
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=2584046138,590027024&fm=96&s=4E9274884A700F8ACA30D956030050E0[1].jpg
  Writes to:
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\WM60WM90\his[1]
   Writes to:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=1010662780,933723174&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=3841058258,22310974278fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\TZILKL9J\u=2916809114,3153528632&fm=96&s=1EF66984415003CA44803596030080C2[1].jpg

Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\266VNL55\u=4121919617,900972282&fm=58[1].jpg

Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2781679007,565939595&fm=58[1].jpg
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\WM60WM90\ielib_0108[1].js
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=532204567,887570784&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2177447570,2292449148&fm=82&s=21904D3064EAEF090584C9C6010070A3&w=121&h=81&img[1].jpg
                                         {\tt C:\Wsers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\266VNL5S\u=1489011112,1613214565&fm=58[1].jpg
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Writes to:
Files\Content.IE5\VB8EH8F1\u=1779799337,1886987922&fm=58[1].jpg
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\WM60WM90\o_0108[1].swf
                                        C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Writes to:
Explorer\UserData\2I2VAGUP\oXMLStore[1].xml
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Writes to:
Files\Content.IE5\TZILKL9J\ps_fp[1].htm
Reads from: C:\Windows\Fonts\StaticCache.dat
C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                        C:\Windows\System32\drivers\etc\hosts
  Reads from:
   Reads from:
                                        C:\Windows\win.ini
                                         C:\Windows\SysWOW64\dxtmsft.dll
   Reads from:
   Reads from:
                                         C:\Windows\SysWOW64\dxtrans.dll
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Reads from:
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\all_async_search_dddfb2ec[1].js
Reads from: C:\Windows\SysWOW64\iepeers.dl1
   Reads from:
                                         C:\Windows\SysWOW64\stdole2.tlb
   Reads from:
                                        C:\Windows\SysWOW64\mshtml.tlb
   Reads from:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9\\every_cookie_aa168.cb4[1]_js
Reads from: C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
Reads from: C:\Windows\SysWOW64\Macromed\Flash\Flash\Dh.ocx
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Content.IE5\TZILKL9J\env\_beb83b45[1].swf|
Reads from: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Reads from:
Files\Content.IE5\TZILKL9J\bdsug_async_1cb857eb[1].js
Reads from: C:\Windows\Sys\WO\W64\ieframe.dll
                                         C:\Users\desktop.ini
   Reads from:
   Reads from:
                                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
                                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
   Reads from:
Files\Content.IE5\266VNL5S\favicon[1].ico
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
                                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Reads from:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                                        C:\Windows\Media\Windows Navigation Start.wav
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\JSocket_9a52fc3e[1].swf
Reads from: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEQSE8W1\userDataBIDUPSID[1].xml
   Reads from:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\o_0108[1].swf
                                        C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Reads from:
Explorer\UserData\2I2VAGUP\oXMLStore[1].xml
C: \verb|Vusers| Admin\\ App Data\\ Roaming\\ Microsoft\\ Windows\\ Cookies\\ admin\\ @baidu[1].txt
  Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
                                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Deletes:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                                        C:\Users\Admin\AppData\Roaming\Macromedia\Flash
\label{local-player-lambda} Player \arrows of the support \arrows of \arrow
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
```

Network Events

DNS query: www.baidu.com
DNS query: s1.bdstatic.com
DNS query: fpdownload2.macromedia.com
DNS query: b1.bdstatic.com

```
ecmb.bdimg.com
  DNS query:
  DNS guery:
                              i7.baidu.com
  DNS query:
                              i8.baidu.com
  DNS query:
                              i9.baidu.com
  DNS query:
                              t10.baidu.com
  DNS query:
                              t12.baidu.com
  DNS query:
                              t11.baidu.com
  DNS query:
                              sclick.baidu.com
  DNS query:
                              suggestion.baidu.com
  DNS query:
                              c.baidu.com
                              sestat.baidu.com
  DNS query:
  DNS query:
                              eclick.baidu.com
  DNS response:
                              www.a.shifen.com ⇒ 14.215.177.37
                              www.a.shifen.com ⇒ 14.215.177.38
  DNS response:
                              wwwbaidu.jomodns.com ⇒ 119.146.74.40
a1293.d.akamai.net ⇒ 58.27.86.10
a1293.d.akamai.net ⇒ 58.27.86.66
  DNS response:
  DNS response:
  DNS response:
                              bcs.jomodns.com ⇒ 180.97.66.39
  DNS response:
  DNS response:
                              t1.n.shifen.com ⇒ 180.97.33.30
  DNS response:
                              image.jomodns.com ⇒ 119.146.74.49
base64.jomodns.com ⇒ 119.146.74.49
  DNS response:
                              suggestion.a.shifen.com ⇒ 14.215.177.44
  DNS response:
                              s.a.shifen.com ⇒ 123.125.115.95
c.e.shifen.com ⇒ 123.125.114.64
  DNS response:
  DNS response:
                              sestat.a.shifen.com ⇒ 183.232.231.92
  DNS response:
  DNS response:
                              eclick.e.shifen.com ⇒ 123.125.115.164
  Connects to:
                              8.8.8.8:53
                              14.215.177.37:80
  Connects to:
 Connects to:
                              127.0.0.1:63962
  Connects to:
                              119.146.74.40:80
  Connects to:
                              58.27.86.10.80
                              180.97.66.39:80
  Connects to:
                              180.97.33.30:80
  Connects to:
  Connects to:
                              119.146.74.49:80
                              14.215.177.44.80
  Connects to:
                              123.125.115.95:80
  Connects to:
                               123.125.114.64:80
  Connects to:
  Connects to:
                              183.232.231.92:80
                              123.125.115.164:80
  Connects to:
  Sends data to:
                              8.8.8.8:53
                              127.0.0.1:63962
  Sends data to
  Sends data to:
                              www.a.shifen.com:80 (14.215.177.37)
  Sends data to:
                              wwwbaidu.jomodns.com:80 (119.146.74.40)
                              a1293.d.akamai.net:80 (58.27.86.10)
  Sends data to:
  Sends data to:
                              bcs.jomodns.com:80 (180.97.66.39)
  Sends data to:
                              base64.jomodns.com:80 (119.146.74.49)
t1.n.shifen.com:80 (180.97.33.30)
  Sends data to:
  Sends data to
                              suggestion.a.shifen.com:80 (14.215.177.44)
                              saggeston.ashifen.com:80 (123.125.115.95)
c.e.shifen.com:80 (123.125.114.64)
sestat.a.shifen.com:80 (183.232.231.92)
eclick.e.shifen.com:80 (123.125.115.164)
  Sends data to:
  Sends data to:
  Sends data to:
  Sends data to
  Receives data from:
                              8.8.8.8:53
                              127.0.0.1:63962
  Receives data from:
                              www.a.shifen.com:80 (14.215.177.37)
  Receives data from:
  Receives data from:
                              wwwbaidu.jomodns.com:80 (119.146.74.40)
  Receives data from:
                              a1293.d.akamai.net:80 (58.27.86.10)
                              bcs.jomodns.com:80 (180.97.66.39)
t1.n.shifen.com:80 (180.97.33.30)
  Receives data from:
  Receives data from:
  Receives data from:
                              base64.jomodns.com:80 (119.146.74.49)
  Receives data from:
                              s.a.shifen.com:80 (123.125.115.95)
                              c.e.shifen.com:80 (123.125.114.64)
  Receives data from:
                              sestat.a.shifen.com:80 (183.232.231.92)
  Receives data from:
  Receives data from:
                              eclick.e.shifen.com:80 (123.125.115.164)
Windows Registry Events
```

```
HKLM\software\wow6432node\microsoft\internet
     Creates key:
explorer\main\featurecontrol\feature_scripturl_mitigation
       Creates key:
                                                                                          HKCU\software\explore
                                                                                          HKCU\software\microsoft\windows\currentversion\internet settings
      Creates key
      Creates key:
                                                                                         HKLM\software\wow6432node\microsoft\tracing
      Creates key:
                                                                                          HKLM\software\wow6432node\microsoft\tracing\rasapi32
       Creates key:
                                                                                          HKLM \verb|\software| wow 6432 node \verb|\microsoft| tracing \verb|\rasmancs| rasmancs| and the state of 
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
     Creates kev:
settings\connections
     Creates key:
                                                                                          HKCU\software\microsoft\windows nt\currentversion\network\location
 awareness
      Creates kev:
                                                                                         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 kev:
                                                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
                                                                                          HKLM \ \ software \ \ \ \ \ \ microsoft \ \ \ direct draw \ \ \ most recent application
      Creates key
      Creates key
                                                                                         {\tt HKCU \backslash software \backslash microsoft \backslash windows \ script \backslash settings}
                                                                                         HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication
      Creates kev:
      Creates key:
                                                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata
     Creates key:
Creates key:
                                                                                          {\tt HKLM} \verb|\system| current controls et \verb|\control| security providers \verb|\schannel| \\
                                                                                          HKCU\software\microsoft\internet explorer\domstorage\total
                                                                                          HKCU\software\microsoft\internet explorer\domstorage\baidu.com
       Creates key
      Creates key
                                                                                         HKCU\software\macromedia\flashplayer
     Creates key
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409
      Creates key:
                                                                                          \label{thm:linear} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc min}\sc windows search} \\
      Creates key:
                                                                                          HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus microsoft \setminus download management of the software \setminus wow 6432 node \setminus wow 
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
     Deletes value:
settings\zonemap[proxybypass]
      Deletes value:
                                                                                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
```

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

```
settings\zonemap[intranetname]
                                                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
      Deletes value:
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]
                                                                                                  HKCU\software\macromedia\flashplayer[flashplayerversion]
      Deletes value:
       Opens key:
                                                                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options
       Opens key:
                                                                                                  HKLM\svstem\currentcontrolset\control\session manager
       Opens key:
                                                                                                  HKLM\software\microsoft\wow64
                                                                                                  HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
       Opens key:
execution options
      Opens kev:
                                                                                                  HKLM\svstem\currentcontrolset\control\safeboot\option
       Opens kev
                                                                                                  HKLM\system\currentcontrolset\control\srp\gp\dll
       Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
                                                                                                  HKLM\software\policies\microsoft\windows\safer\codeidentifiers
       Opens kev:
                                                                                                  HKCU\software\policies\microsoft\windows\safer\codeidentifiers
       Opens key:
       Opens key:
                                                                                                  \label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} is $$\operatorname{Lin}_{\operatorname{custom}}(x) = \operatorname{Lin}_{\operatorname{custom}}(x) = \operatorname{Lin}_{\operatorname{custo
       Opens key:
                                                                                                  HKLM\system\currentcontrolset\control\nls\language
                                                                                                  HKLM\system\currentcontrolset\control\mui\uilanguages
       Opens key:
       Opens key:
                                                                                                  HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
       Opens key:
                                                                                                  \label{local-problem} \begin{tabular}{ll} HKLM \end{tabular} System \current control \end{tabular} wil \all anguages \end{tabular} pending delete \end{tabular}
                                                                                                  HKLM\software\wow6432node\policies\microsoft\mui\settings
       Opens key:
       Opens key:
                                                                                                  HKLM\software\policies\microsoft\mui\settings
       Opens key:
                                                                                                  HKCU\
       Opens key:
                                                                                                  {\tt HKCU \backslash control\ panel \backslash desktop \backslash muicached \backslash machine language configuration}
                                                                                                  HKLM\svstem\currentcontrolset\control\mui\settings\languageconfiguration
       Opens key:
                                                                                                  HKCU\software\policies\microsoft\control panel\desktop
       Opens key:
                                                                                                  HKCU\control panel\desktop\languageconfiguration
       Opens key:
       Opens key:
                                                                                                  {\tt HKCU \backslash control\ panel \backslash desktop}
                                                                                                 HKCU\control panel\desktop\muicached
       Opens key:
                                                                                                  Opens key:
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
                                                                                                 HKLM\system\currentcontrolset\control\nls\sorting\versions
       Opens key:
       Opens key:
                                                                                                  HKLM\
       Opens key:
                                                                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
      Opens key:
                                                                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre initialize
      Opens key:
                                                                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibilitv32
      Opens kev
                                                                                                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
       Opens key:
                                                                                                  HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
                                                                                                  HKLM\software\wow6432node\microsoft\ole
       Opens kev:
                                                                                                  HKLM\software\wow6432node\microsoft\ole\tracing
       Opens kev
       Opens key:
                                                                                                  HKLM\software\microsoft\ole\tracing
       Opens key:
                                                                                                  HKLM\software\wow6432node\microsoft\oleaut
                                                                                                  HKLM\system\currentcontrolset\services\crypt32
       Opens key:
                                                                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
       Opens key:
settings
      Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
                                                                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
      Opens key:
settings
                                                                                                 HKCU\software\microsoft\internet explorer\main
       Opens key:
                                                                                                 HKLM\software\wow6432node\microsoft\internet
       Opens key:
explorer\main\featurecontrol
       Opens key:
                                                                                                 HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
                                                                                                 HKLM\system\currentcontrolset\control\nls\extendedlocale
       Opens key:
       Opens key:
                                                                                                  HKLM\system\currentcontrolset\control\nls\locale
       Opens key:
                                                                                                  {\tt HKLM \ } system \verb|\ current control \ | \ locale \verb|\ alternate \ sorts | \ system \ | \ sys
       Opens key:
                                                                                                 \label{thm:local-problem} HKLM\system\currentcontrolset\control\nls\language\ groups \\ HKLM\software\microsoft\windows\ nt\currentversion\fontlink\system\link\currentversion\fontlink\system\link\currentversion\fontlink\system\link\currentversion\fontlink\system\link\currentversion\fontlink\system\link\currentversion\fontlink\system\link\currentversion\fontlink\system\link\currentversion\font\currentversion\font\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\curre
       Opens key:
                                                                                                 HKLM\software\microsoft\windows
       Opens key:
nt\currentversion\languagepack\datastore_v1.0
                                                                                                 HKLM\software\microsoft\windows
      Opens key:
nt\currentversion\languagepack\surrogatefallback
                                                                                                 HKLM\software\microsoft\windows
       Opens key:
nt\currentversion\languagepack\surrogatefallback\segoe ui
                                                                                                 HKLM\system\currentcontrolset\control\cmf\config
      Opens key:
       Opens kev
                                                                                                  HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
      Opens key:
                                                                                                 HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
       Opens kev:
HKL\dot{M} \setminus software \setminus wow 6432 node \setminus microsoft \setminus ctf \setminus compatibility \setminus 62 ddfbf757 be 511f30 be 6432 09363 c1345 e8 be f0774 b2 baa23 c901 e164 b0 c7 af bb. execution of the compatibility is a compatibility of the com
                                                                                                 HKLM\software\microsoft\windows
       Opens key:
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
                                                                                                 HKCU\software\explore
       Opens key:
       Opens key:
                                                                                                  HKCU\software\classes
       Opens key:
                                                                                                 HKLM\software\microsoft\com3
       Opens key
                                                                                                 HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}
       Opens key:
                                                                                                  HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
       Opens key:
                                                                                                 HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
       Opens key:
                                                                                                  HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-1440a-11d0-a96b-1440a-1440a-11d0-a96b-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-1440a-144
       Opens key:
00c04fd705a2}\progid
                                                                                                  HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
      Opens key:
       Opens key:
                                                                                                 HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
                                                                                                 HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
      Opens key:
00c04fd705a2}\inprocserver32
       Opens key:
                                                                                                 \label{locality} HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-4842 \\ node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-4844 \\ node \setminus clsid \setminus clsid \setminus \{8856f961-340a-11d0-a96b-4844 \\ node \setminus clsid \setminus c
00c04fd705a2}\inprochandler32
```

```
Opens key
                                                                                        HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
       Opens key:
                                                                                        HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-12d1\} \\ \cap (3856f961-340a-11d0-a96b-12d1) 
00c04fd705a2}\inprochandler
       Opens key:
                                                                                        HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler
       Opens key:
                                                                                        HKLM\software\wow6432node\microsoft\rpc
       Opens key:
                                                                                         {\tt HKLM \ } system \verb|\ control \ \verb|\ computername \ \verb|\ active computername \ |}
       Opens key:
                                                                                         HKLM\system\setup
                                                                                         HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
       Opens key:
                                                                                         HKLM\software\policies\microsoft\windows nt\rpc
       Opens key:
       Opens key:
                                                                                         HKLM\software\policies\microsoft\sqmclient\windows
                                                                                         HKLM\software\microsoft\samclient\windows
       Opens key:
                                                                                         HKCU\software\classes\wow6432node\clsid\{889d2feb-5411-4565-8998-
       Opens key:
  1dd2c5261283}
       Opens key:
                                                                                         HKCR\wow6432node\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
                                                                                        HKCU\software\classes\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
       Opens key:
                                                                                         HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
       Opens key:
                                                                                         HKCU\software\policies\microsoft\windows\app management
       Opens key:
       Opens key:
                                                                                         HKLM\software\policies\microsoft\windows\app management
       Opens kev:
                                                                                         HKCU\software\classes\wow6432node\clsid\{004b0726-a010-4abf-8556-
       Opens key:
 fcdb7f1fca1e}
                                                                                         HKCR\wow6432node\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
       Opens key:
                                                                                         HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
       Opens key:
       Opens key:
                                                                                         HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
\label{thm:continuous} Opens~key: $$ HKLM\software\wow6432\node\wicrosoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} $$
                                                                                        HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
       Opens key:
Ofb58b01c4a4}\languagepi
                                                                                      ofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
       Opens key:
                                                                                        HKLM\software\wow6432node\microsoft\ctf\
                                                                                         HKLM\software\wow6432node\microsoft\ctf\knownclasses
       Opens key:
       Opens key:
                                                                                         \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Software \begin{tabular}{ll} PKCU \label{thm:local_hammon} Software \begin
 settings
       Opens key:
                                                                                        HKCU\software\microsoft\windows\currentversion\internet settings
                                                                                        HKCU\software\microsoft\internet
       Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
       Opens key:
                                                                                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                                                                        HKLM\software\wow6432node\policies\microsoft\internet
       Opens key:
 explorer\main\featurecontrol
       Opens key:
                                                                                        \label{lem:hklmsoftware policies microsoft} Internet explorer \verb|\main\featurecontrol| \\
       Opens key:
                                                                                        \label{thm:local-ham} HKCU\software\policies\microsoft\internet\ explorer\main\featurecontrol HKCU\software\microsoft\internet\ explorer\main\featurecontrol
       Opens key:
       Opens key:
                                                                                         HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562
                                                                                        HKLM\software\wow6432node\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                                                                         HKCU\software\microsoft\internet
       Opens key:
\verb|explorer\main\featurecontrol\feature\_use\_ietldlist\_for\_domain\_determination| \\
                                                                                        HKLM\software\wow6432node\microsoft\internet
      Opens key:
 explorer\main\featurecon
                                                                                      ntrol\feature_use_ietldlist_for_domain_determination
                                                                                         HKLM\system\currentcontrolset\control\lsa\accessproviders
       Opens key:
       Opens key:
                                                                                        HKLM\system\currentcontrolset\services\ldap
HKCU\software\microsoft\internet explorer\ietld
       Opens key:
                                                                                         HKLM\software\wow6432node\microsoft\internet explorer\main
       Opens key:
       Opens key:
                                                                                         HKLM \label{lem:hkklm} \label{lem:hkklm} HKLM \label{lem:hkklm} Software \label{lem:hkklm} wow 6432 node \label{lem:hkklm} policies \label{lem:hkklm} in the lemma in the le
       Opens key:
                                                                                        HKLM\software\policies\microsoft\internet explorer\main
                                                                                         HKCU\software\policies\microsoft\internet explorer\main
       Opens key:
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
       Opens key:
                                                                                        HKLM\software\microsoft\windows\currentversion\policies\explorer
                                                                                         HKCU\software\microsoft\windows\currentversion\policies\explorer
       Opens key:
HKLM \software \wow 6432 node \mbox{\software} a 30963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \software \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 7afbb. exection \mbox{\software} a 1200 bef0775be511f30b6d330963 c 1345e8 bef0774b2 baa23 c 901e164b0 c 901e164b
                                                                                        HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
      Opens key:
08002b30309d}\shellfolder
                                                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder
      Opens key:
                                                                                        42a0-1069-a2ea-08002b30309d}\shellfolder
       Opens key:
                                                                                        HKCU\software\microsoft\windows\currentversion\policies\nonenum
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
       Opens key:
                                                                                        \label{lem:hklm} \verb+KKLM\software\microsoft\windows\currentversion\policies\nonenum and the lemma of the lem
       Opens key
                                                                                        HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
                                                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea
       Opens key:
08002b30309d}\inprocserver32
      Opens key:
                                                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\shell
extensions\blocked
       Opens key:
                                                                                         HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
                                                                                         {\tt HKLM \backslash system \backslash current control \backslash session \ manager \backslash app compatibility}
       Opens key:
       Opens key:
                                                                                        HKLM\software\wow6432node\policies\microsoft\windows\appcompat
HKLM\software\policies\microsoft\windows\appcompat
       Opens key:
       Opens key:
                                                                                         HKCU\software\microsoft\windows\currentversion\shell extensions\cached
       Opens key
                                                                                        HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{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-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2
08002b30309d3
       Opens key:
                                                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
                                                                                         HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\treatas
                                                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
       Opens key:
       Opens key:
                                                                                         HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 08002b30309d}\progid
       Opens key:
                                                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
                                                                                        HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
       Opens key:
                                                                                         HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
       Opens key:
                                                                                         HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea
       Opens key:
08002b30309d}\progid
                                                                                         HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
       Opens key:
                                                                                         \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \wow6432 node \clsid \end{tabular} $$432 node \clsid \end{
```

08002b30309d}\inprochandler32

```
Opens key
                                                                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler32
       Opens key:
                                                                                                      HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{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-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2e
08002b30309d}\inprochandler
                                                                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
      Opens key:
08002b30309d}\inprochandler
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-
42a0-1069-a2ea-08002b30309d}
                                                                                                      HKCU\software\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_iedde_register_protocol
      Opens key:
                                                                                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
                                                                                                      HKLM\software\wow6432node\policies\microsoft\internet
       Opens key:
explorer\browseremulation
       Opens key:
                                                                                                      HKLM\software\policies\microsoft\internet explorer\browseremulation
                                                                                                      \label{thm:local-policies} HKCU \ software \ policies \ microsoft \ internet\ explorer \ browsere mulation \ HKLM \ software \ wow 6432 node \ microsoft \ internet\ explorer \ mediaty peclass
       Opens key:
        Opens key:
                                                                                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
       Opens key:
settings\accepted documents
       Opens kev:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ratings
       Opens key:
                                                                                                      HKLM\software\microsoft\windows\currentversion\policies\ratings
       Opens key:
                                                                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
       Opens key:
                                                                                                      HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_show_failed_connect_content_kb942615|
                                                                                                      HKLM\software\wow6432node\policies
       Opens key:
                                                                                                       HKCU\software\policies
       Opens key:
        Opens key:
                                                                                                       HKCU\software
       Opens key:
                                                                                                      HKLM\software\wow6432node
       Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} M\soft\begin{tabular}{ll} wow6432 node \\ policies\begin{tabular}{ll} microsoft\begin{tabular}{ll} windows\current\begin{tabular}{ll} current\begin{tabular}{ll} wow6432 node \\ policies\begin{tabular}{ll} microsoft\begin{tabular}{ll} windows\current\begin{tabular}{ll} current\begin{tabular}{ll} microsoft\begin{tabular}{ll} microsoft\begin{tabular}{ll}
                                                                                                      HKCU\software\microsoft\internet
       Opens key:
explorer \verb|\main| featurecontrol| feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915
                                                                                                      HKLM\software\wow6432node\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
       Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                                                                                       \label{local-observation} HKLM \label{local-observation} IKLM \label{local-observation} IKL
       Opens key:
settings\zonemap\domains
                                                                                                      \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Software \begin{tabular}{ll} PKCU \label{thm:local_hammon} Software \begin
      Opens key:
settings\zonemap\domains\
      Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                                                                                      HKLM\software\policies\microsoft\windows\currentversion\internet
       Opens key:
settings\zonemap\ranges
      Opens key:
                                                                                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
       Opens key:
                                                                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                                                                                      HKLM\software\wow6432node\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                                                                                       HKCU\software\microsoft\windows\currentversion\internet
       Opens key:
settings\zonemap\
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                                                                                      HKLM\software\wow6432node\microsoft\internet
       Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
      Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\soft\begin{tabular}{ll} HKL\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\soft\begin{tabular}{ll} HKL\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\soft\begin{tabular}{ll} HKL\begin{tabular}{ll} M\soft\begin{tabular}{ll} M\sof
      Opens key:
                                                                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
      Opens key:
                                                                                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
                                                                                                      HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
settings\zonemap\ranges\
      Opens key:
                                                                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
      Opens key:
                                                                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
      Opens key:
                                                                                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
       Opens key:
                                                                                                      HKLM\software\wow6432node\policies\microsoft\internet explorer
                                                                                                       HKLM\software\policies\microsoft\internet explorer
       Opens key:
        Opens key:
                                                                                                       HKLM\software\policies\microsoft\internet explorer\security
                                                                                                       HKCU\software\microsoft\windows\currentversion\internet settings\zones\
        Opens key:
       Opens key:
                                                                                                       HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
       Opens kev:
                                                                                                       HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
                                                                                                       \label{thm:local_hammon} \parbox{$HKCU\software\microsoft\windows\currentversion\internet settings\somes\soling} \parbox{$2$} \parbox
        Opens kev
                                                                                                       \label{thm:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sc}} \mbox{\tt zones\sl} \mbox{\tt 3}
       Opens key:
       Opens key:
                                                                                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
       Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
       Opens key:
                                                                                                       \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \label{lem:hklmsoftware policies microsoft windows \current version \coloner{lem:hklmsoftware policies microsoft windows \current version \coloner{lem:hklmsoftware policies \chince microsoft \chince microso
settings\zones
      Opens key:
                                                                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
      Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
      Opens key:
                                                                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
      Opens key:
                                                                                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
       Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ vanes \ 1200 \ value \ val
      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 kev:
                                                                                                                                 HKI M\software\wow6432node\microsoft\windows\currentyersion\internet
settings\zonemap\
        Opens key:
                                                                    \verb|\www6432| node \verb|\policies| microsoft \verb|\windows| current version \verb|\internet| settings \verb|\zones|| 2
HKLM\softwa
        Opens key:
                                                                                                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
         Opens key:
                                                                                                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
        Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet \ settings \ zones \ \ 3200 \ description \ de
         Opens key:
                                                                                                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                                                                                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
        Opens kev:
settings\zones\3
        Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
        Opens kev:
                                                                                                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                                                                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
        Opens key:
settings\zones\4
                                                                                                                                HKCU\software\microsoft\internet
        Opens kev:
explorer\main\featurecontrol\feature_localmachine_lockdown
         Opens key:
                                                                                                                                HKLM\software\wow6432node\microsoft\internet
\verb|explorer'| main feature control feature_local machine_lock down |
        Opens key:
\label{thm:local_equation} \begin{tabular}{ll} HKLM \label{thm:local_equation} HKLM \label{thm:local_equation} \end{tabular} $$ HKLM \label{thm:local_equation} $$ HKLM \label{thm:local_equa
 settings\lockdown_zones\
                                                                                                                                \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} policies \end{tabular} irror of the local hammon \end{tabular} irror of the local hammon \end{tabular} and the local hammon \end{tabular} irror of the
        Opens key:
settings\lockdown_zones
        Opens key:
                                                                                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                                                                                                HKCU\software\microsoft\windows\currentversion\internet
        Opens key:
settings\lockdown_zones\
                                                                                                                                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
        Opens key:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Wow 6432 node \label{lem:hklm} experience \label{lem:hklm} \label{lem:hklm} Wow 6432 node \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lkm} \label{lkm}
 settings\lockdown_zones\0
        Opens key:
                                                                                                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
        Opens key:
                                                                                                                                \label{lem:hkcu} \verb+KKCU\+software\+policies\+microsoft\+windows\+currentversion\+internet
settings\lockdown zones\0
                                                                                                                                HKCU\software\microsoft\windows\currentversion\internet
        Opens key:
settings\lockdown_zones\1
        Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                                                                                                                \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\software\policies\microsoft\windows\currentversion\notation{\color=0.5em}{\color=0.5em} HKLM\software\policies\microsoft\windows\currentversion\notation{\color=0.5em}{\color=0.5em} HKLM\software\policies\microsoft\microsoft\notation{\color=0.5em}{\color=0.5em} HKLM\software\policies\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\mic
         Opens key:
 settings\lockdown_zones\1
        Opens key:
                                                                                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\1
        Opens key:
                                                                                                                                HKCU\software\microsoft\windows\currentversion\internet
 settings\lockdown_zones\2
        Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
        Opens key:
                                                                                                                                \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} on the local constant \end{tabular} is the local constant \end{tabular} on the local constant \end{tabular} on the local constant \end{tabular} on the local \end{tabula
settings\lockdown zones\2
                                                                                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
        Opens key:
 settings\lockdown_zones\2
        Opens key:
                                                                                                                                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown zones\3
        Opens key:
settings\lockdown_zones\3
        Opens key:
                                                                                                                                settings\landslockdown_zones\3
                                                                                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
        Opens key:
settings\lockdown_zones\3
        Opens key:
                                                                                                                                HKCU\software\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
        Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                                                                                                                \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} policies \end{tabular} irror of the local hammon \end{tabular} irror of the local hammon \end{tabular} and the local hammon \end{tabular} irror of the
settings\lockdown_zones\4
                                                                                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
        Opens key:
settings\lockdown_zones\4
        Opens key:
                                                                                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache
                                                                                                                                HKCU\software\microsoft\windows\currentversion\internet
        Opens kev:
 settings\5.0\cache
                                                                                                                                \label{thm:local_HKCU} \mbox{\tt HKCU\software\mbox{\tt Microsoft\windows\currentversion\linear} \mbox{\tt Internet} \\
        Opens key:
settings\5.0\cache\content
        Opens key:
                                                                                                                                HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet in the continuous and 
 settings\5.0\cache\content
        Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
        Opens key:
HKLM \label{eq:hklm} KLM \label{eq:hklm} HKLM \label{eq:hklm} Software \label{eq:hklm} wow 6432 node \label{eq:hklm} is restricted by the software \label{eq:hklm} wow 6432 node \label{
33be-4251-ba85-6007caedcf9d}
        Opens key:
 33be-4251-ba85-6007caedcf9d}\propertybag
         Opens key:
                                                                                                                                HKCU\software\microsoft\windows\currentversion\explorer
         Opens key:
                                                                                                                                HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
         Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \session in folders \colored the local balance of the local balance \colored \colored
        Opens key:
                                                                                                                                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
         Opens key:
                                                                                                                                 HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| explorer\\|
         Opens key:
                                                                                                                                HKLM\software\policies\microsoft\windows\explorer
```

```
Opens key:
                                                                                      HKCU\software\policies\microsoft\windows\explorer
      Opens key:
 HKL\ M\ Noftware \ Now 6432 node \ Microsoft\ New Modes \ Notation \ Notati
 6fba-4fcf-9d55-7b8e7f1570913
      Opens key:
6fba-4fcf-9d55-7b8e7f157091}\propertybag
      Opens key:
0e22-4760-9afe-ea3317b67173}
      Opens key:
0e22-4760-9afe-ea3317b67173}\propertybag
      Opens key:
                                                                                      HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
      Opens key:
                                                                                      HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 980053277-1733835069-2361817685-1001
       Opens kev:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ KLM \end{tabular} $$ in \end{t
      Opens key:
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
      Opens key:
                                                                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings\5.0\cache\cookies
      Opens key:
 HKL\ M\ Noftware \ Now 6432 node \ microsoft \ Now \ Current version \ explorer \ folderdescriptions \ \ 12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f765d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f766d-12b0f76d-12b0f766d-12b0f76d-12b0f76d-12b0f76d-12b0f76d-12b0f76d-12b0f
 c0e9-4171-908e-08a611b84ff6}
      Opens key:
c0e9-4171-908e-08a611b84ff6}\propertybag
65f9-4cf6-a03a-e3ef65729f3d}
      Opens key:
65f9-4cf6-a03a-e3ef65729f3d\} \setminus property bag
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
Opens key. Settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
      Opens key:
 b784-432e-a781-5a1130a75963}
      Opens kev:
 HKLM \label{lem:hklm} Software \label{lem:hklm} Wwo 6432 node \mbox{\current} version \explorer \folder descriptions \folder \fol
 b784-432e-a781-5a1130a75963}\propertybag
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
 settings\5.0\cache\extensible cache
      Opens key:
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\domstore
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
 settings\5.0\cache\extensible cache\feedplat
      Opens key:
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\iecompat
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
 settings\5.0\cache\extensible cache\ietld
                                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings \verb|\|5.0\> cache \verb|\| extensible | cache \verb|\| privacie:
                                                                                      HKCU\software\microsoft\internet
      Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
      Opens key:
                                                                                      HKLM\software\wow6432node\microsoft\internet
 \verb|explorer\main\featurecontrol\retry_header on ly post\_on connection reset| \\
                                                                                      HKCU\software\microsoft\internet
      Opens key:
 explorer\main\featurecontrol\feature_bufferbreaking_818408
      Opens key:
                                                                                      HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_bufferbreaking_818408|
                                                                                      HKCU\software\microsoft\internet
      Opens key:
 explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                                                                                      HKLM\software\wow6432node\microsoft\internet
      Opens key:
explorer \verb|\main| featurecontrol| feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954
      Opens key:
 HKLM \label{lem:hklm} White the latest and the la
      Opens key:
                                                                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key:
                                                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\5.0\cache
      Opens key:
                                                                                      HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                                                                                      HKLM\software\wow6432node\microsoft\internet
       Opens key:
 explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
      Opens key:
                                                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
      Opens key:
                                                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
                                                                                      HKLM\software\wow6432node\microsoft\internet
      Opens key:
 \verb|explorer| in feature control feature_disable_notify_unverified\_spn\_kb2385266| feature_disable_notify_unverified\_spn\_kb2385266| feature_disable_notify_unverified\_spn\_kb2385266| feature_disable_notify_unverified_spn_kb2385266| feature_disable_notify_unverified_spn_kb238526| feature_disable_notify_unverified_spn_kb23852| feature_disable_notify_unv
                                                                                      HKCU\software\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
      Opens key:
                                                                                       HKLM\software\wow6432node\microsoft\internet
 \verb|explorer| main feature control| feature compat use connection based negotiate auth kb2151543 | leaves the control feature feature feature for the connection of the control feature featur
                                                                                      HKCU\software\microsoft\internet
      Opens key:
 explorer\main\featurecontrol\feature_allow_long_international_filenames
                                                                                      HKLM\software\wow6432node\microsoft\internet
      Opens key:
HKCU\software\microsoft\internet
      Opens key:
 explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                                                                                      HKLM\software\wow6432node\microsoft\internet
      Opens key:
 explorer\main\featurecontrol\feature_permit_cache_for_authenticated ftp kb910274
                                                                                      HKCU\software\microsoft\internet
      Opens key:
 explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
      Opens key:
                                                                                      HKLM\software\wow6432node\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\wow6432node\microsoft\internet
  Opens key:
\verb|explorer\main\featurecontrol\feature_disallow_null\_in\_response\_headers| \\
                                      HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                                      HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature exclude invalid client cert kb929477
                                      HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature use utf8 for basic auth kb967545
   Opens kev:
                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature release kevs on unload kb975619
                                      HKLM\software\wow6432node\microsoft\internet
   Opens key:
\verb|explorer\| main \\ | feature \\ | control \\ | feature \\ | release \\ | keys \\ | con \\ | unload \\ | kb975619 \\ | con \\
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  Opens key:
                                      HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_security\_flag\_ignore\_revocation\_kb2275828
  Opens key:
                                      HKLM\system\currentcontrolset\services\winsock2\parameters
                                      HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\381e2851
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\00000005
  Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000007
   Opens kev
Opens key:
\label{thm:local_catalog} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} MKL\begin{tabular}{ll} MKL\begin{tabular
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
  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
                                      HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens kev:
                                      HKLM\software\wow6432node\microsoft\tracing\rasapi32
                                      HKLM\software\wow6432node\microsoft\tracing\rasmancs
   Opens kev
                                      HKLM\software\wow6432node\microsoft\windows
  Opens key:
nt\currentversion\profilelist
                                      HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:
   Opens key:
                                      HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key:
                                      HKII\
  Opens key:
                                      HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:
                                      HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens key:
                                      HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
  Opens key:
                                      HKLM\software\policies\microsoft\windows nt\dnsclient
                                      HKLM\system\currentcontrolset\services\dns
  Opens key:
  Opens key:
                                      HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
  Opens key:
                                      HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
                                      HKCU\software\microsoft\internet explorer
  Opens key:
   Opens key:
                                      HKLM\software\wow6432node\microsoft\internet explorer
                                      HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_mime_handling
                                      HKLM\software\wow6432node\microsoft\internet
  Opens key:
```

```
explorer\main\featurecontrol\feature_mime_handling
                                                HKCU\software\classes\protocols\name-space handler\
   Opens key:
   Opens key:
                                                HKCR\protocols\name-space handler
   Opens key:
                                                HKCU\software\classes\protocols\name-space handler\http\
   Opens key:
                                                HKCR\protocols\name-space handler\http
                                                HKCU\software\classes\protocols\name-space handler\*\
   Opens key:
   Opens key:
                                                HKCR\protocols\name-space handler\*
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
                                                HKLM\software\wow6432node\microsoft\internet
   Opens key:
                                               ntrol\feature_enable_compat_logging
explorer\main\featurecom
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
   Opens key:
                                                HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings\user agent
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
   Opens key:
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent
   Opens key:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\user agent
   Opens key:
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\user agent
   Opens key:
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\ua tokens
   Opens key:
                                                settings\user agent\pre platform
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\user agent\pre platform
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
                                                ...
HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens key:
settings\user agent\post platform
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
                                                HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\user agent\post platform
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature browser emulation
                                                HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_browser_emulation
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature maxconnectionsperserver
                                                HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_maxconnectionsperserver
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature maxconnectionsper1 Oserver
   Opens key:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver
                                                {\tt HKLM \ } system \verb| current control \verb| set \verb| services \verb| winsock \verb| parameters \verb| services \verb
   Opens key:
                                                HKLM\svstem\currentcontrolset\services\tcpip6\parameters\winsock
   Opens kev:
                                                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens kev
   Opens key:
                                                \label{thm:local_equation} \mbox{HKLM} \mbox{$\tt k$} \mb
   Opens key:
                                                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\urlmon settings
   Opens key:
                                                {\tt HKCU \ } software \verb|\ microsoft \> internet|
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                                HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
   Opens key:
                                                HKCU\software\microsoft\internet explorer\international
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
   Opens key:
                                                HKLM\software\wow6432node\microsoft\internet
\verb|explorer| feature on trol feature_disable_legacy_compression| \\
   Opens key:
                                                HKCU\software\classes\protocols\name-space handler
   Opens key:
                                                \label{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\travellog}} \\
   Opens key
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\travellog
   Opens key:
                                                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
   Opens key:
                                                HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| system\\| dnsclient
   Opens key:
                                                HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \explorer \autocomplete \end{tabular}
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
   Opens key:
HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete
                                                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Opens kev:
00c04fd7d062}
   Opens key:
                                                HKCR \setminus wow6432 node \\ clsid \setminus \{00bb2765-6a77-11d0-a535-00c04fd7d062\}
   Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\treatas
   Opens key:
                                                Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\progid
   Opens key:
                                                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid
   Opens key:
                                                HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
   Opens key:
                                                HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
                                                HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535
   Opens key:
00c04fd7d062}\progid
   Opens key:
                                                HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid
   Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
                                                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Opens key:
00c04fd7d062}\inprocserver32
                                                HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Opens key:
00c04fd7d062}\inprochandler32
   Opens key:
                                                HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
```

```
Opens key
                                           HKCU\software\classes\wow6432node\clsid\{00hb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:
                                           HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler
   Opens key:
                                           HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
  Opens key:
e1e01c1f69b5}
  Opens key:
                                            HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}
   Opens key:
                                            HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
   Opens key
                                            HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\treatas
  Opens key:
                                            HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas
                                            HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
   Opens key
9fe3c77a297a}\progid
  Opens key:
                                            HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid
                                            HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
   Opens kev
                                            HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
   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
                                           HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
  Opens kev
                                           HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler32
                                           HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
   Opens key:
9fe3c77a297a}
                        \inprochandler32
  Opens key
                                           HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler
   Opens key:
                                           HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler
  Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{00hb2764-6a77-11d0-a535-
00c04fd7d062
                                            HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
   Opens key:
   Opens key
                                            HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 6a77 - 
00c04fd7d062}\treatas
                                           Opens key:
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\progid
   Opens key:
                                            HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid
                                            HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
   Opens key:
   Opens key:
                                            HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
   Opens key
                                           HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\progid
                                            HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
   Opens key
00c04fd7d062}\inprocserver32
                                           HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
  Opens key
00c04fd7d062}
                                          er32
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
  Opens key
00c04fd7d062}\inprochandler32
                                           HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
   Opens key:
00c04fd7d062}\inprochandler32
  Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler
                                           HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
  Opens key:
00c04fd7d062}\inprochandler
  Opens key
                                           HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d0623
   Opens key:
                                           HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
                                            HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\treatas
                                           HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
   Opens key:
   Opens key:
                                            HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{00bb2763-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a535-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a77-11d0-a55-6a7
00c04fd7d062}\progid
                                            HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
   Opens key:
                                            HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
   Opens key:
                                            HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
   Opens key:
   Opens kev
                                           HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\progid
                                            HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
                                           HKCR\
                                                        w6432node\clsid\{00bb2763-6a77-11d0-a535-
  Opens key
00c04fd7d062}\inprocserver32
                                           HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens kev:
                                           HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
                                           Opens key
00c04fd7d062}\inprochandler
                                           HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
  Opens key:
00c04fd7d062}\inprochandler
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
  Opens key:
                                           HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client\
                                            HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key:
b61bb7cdd997}
   Opens key:
                                           HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
                                           HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key:
b61bb7cdd997}\treatas
                                            Opens key:
   Opens kev:
                                            HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\progid
   Opens key:
                                            HKCR \setminus wow6432 \\ node \\ clsid \\ \{807c1e6c-1d00-453f-b920-b61bb7cdd997\} \\ \setminus progid
```

HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

Opens key:

```
b61bb7cdd997}\inprocserver32
                                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key:
b61bb7cdd997}\inprocserver32
                                         HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
                                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key:
b61bb7cdd997}\inprochandler32
                                         HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key:
b61bb7cdd997}\inprochandler
                                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key:
b61bb7cdd997}\inprochandler
                                         HKLM\software\wow6432node\microsoft\rpc\extensions
   Opens key:
   Opens key:
                                         HKLM\software\microsoft\rpc\extensions
   Opens key:
                                         HKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:
                                         HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
   Opens key:
806e6f6e6963}
   Opens key:
806e6f6e69633
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
   Opens key:
                                         HKLM\system\currentcontrolset\services\tcpip\linkage
                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
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 key:
                                         HKCU\software\classes\mime\database\content type\text/html
   Opens key:
   Opens key:
                                         {\it HKCR} \verb|\mime| database| content type| text/html|
                                         HKCU\software\classes\protocols\filter\text/html: charset=utf-8
   Opens key:
   Opens key:
                                         HKCR\protocols\filter\text/html; charset=utf-8
                                         {\tt HKCU}. \dot{\tilde{}} software \verb|\classes|| protocols \verb|\filter|| text/html||}
   Opens key:
   Opens key:
                                         HKCR\protocols\filter\text/html
   Opens key:
                                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
   Opens key:
                                         HKLM\software\wow6432node\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_mime\_sniffing| \\
                                         HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_feeds
                                         HKLM\software\wow6432node\microsoft\internet
   Opens key:
\verb|explorer\main\featurecontrol\feature_feeds| \\
                                         HKCU\software\microsoft\internet
  Opens key:
                                        trol\feature_safe_bindtoobject
explorer\main\featurecom
                                         HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}
   Opens key:
                                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
                                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Opens key
00aa00686f13}\treatas
                                         Opens key:
Opens key: 00aa00686f13}\progid
                                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Opens key:
                                         HKCR \setminus wow6432 \\ node \\ clsid \\ \{25336920-03f9-11cf-8fd0-00aa00686f13\} \\ \setminus progid
                                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\innrocserver32
  Opens key:
                                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
                                         HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{25336920-03f9-11cf-8fd0-0432 node \setminus clsid \setminus cl
00aa00686f13}\inprochandler32
  Opens key:
                                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
   Opens key:
                                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler
                                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Opens key:
00aa00686f13}\inprochandler
                                         HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                                         HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
  Opens key:
                                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature external style sheet fix for smartnavigation kb926131
                                         HKLM\software\wow6432node\microsoft\internet
   Opens kev:
Opens key:
                                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
                                         HKLM\software\wow6432node\microsoft\internet
   Opens key:
\verb|explorer\main\featurecontrol\feature\_aria\_support|
                                         HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_dispparams
   Opens key:
                                         HKLM\software\wow6432node\microsoft\internet
\verb|explorer\main\featurecontrol\feature_legacy_dispparams| \\
  Opens key:
                                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
                                         HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_private_font_setting
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
                                         HKLM \ software \ wow 6432 node \ microsoft \ internet
   Opens key:
explorer\main\featurecontrol\feature_css_show_hide_events
                                         HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
   Opens key:
                                         HKLM\software\wow6432node\microsoft\internet
```

```
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                                     HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_body\_size\_in\_editable\_if rame\_kb943245
                                     HKCU\software\microsoft\internet
  Opens key:
                                    ntrol\feature_databinding_support
explorer\main\featurecom
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature enforce bstr
                                      HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature enable dynamic object caching
                                      HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                     HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_legacy_tostring_in_compatview| \\
                                     HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
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\wow6432node\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\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\outlook.exe
  Opens key:
                                      \label{lem:hklm} \begin{tabular}{ll} HKLM \label{lem:hklm} software \mbox{$microsoft \windows \current version \app paths \outlook.exe} \end{tabular}
  Opens key
                                      HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility
  Opens key:
                                      HKLM\software\wow6432node\policies\microsoft\internet
explorer\domstorage
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer\domstorage
                                      HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens kev:
                                      HKCU\software\microsoft\internet explorer\domstorage
   Opens kev
  Opens key:
                                      HKLM\software\wow6432node\microsoft\internet explorer\domstorage
  Opens key:
                                     HKLM\software\wow6432node\policies\microsoft\internet
explorer\safety\privacie
   Opens key:
                                      HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \ internet explorer \soft \privacie \\
                                      HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:
                                      HKLM\software\wow6432node\microsoft\internet explorer\safety\privacie
  Opens key:
                                      HKCU\software\microsoft\internet
  Opens key:
\verb|explorer\main\featurecontrol\feature\_manage\_script\_circular\_refs|
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
                                     HKLM\software\wow6432node\microsoft\internet
  Opens key:
\verb|explorer\main\featurecontrol\feature_restrict_filedownload|
                                     HKLM\software\wow6432node\microsoft\internet explorer\security\floppy
  Opens key:
access
  Opens key:
                                      HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:
                                     HKLM\software\wow6432node\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
                                      HKCR\protocols\handler\about
  Opens key:
   Opens kev
                                      \label{locality} \begin{tabular}{ll} HKCU \begin{tabular}{ll} & & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ 
00aa00bdce0b}
                                      HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
  Opens kev:
                                     HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                      HKCR \verb|\wow6432| node \verb|\clsid| \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \verb|\treatas| 
  Opens key:
  Opens key:
                                     HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
                                      HKCR \setminus wow6432 node \\ clsid \\ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \\ \setminus progid
   Opens key:
   Opens key:
                                     HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
  Opens key:
                                      HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82
00aa00bdce0b}\progid
  Opens key:
                                     HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
                                     HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprocserver32
                                     HKCR'
                                                 w6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                                     HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandler32
                                      HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandler32
                                     HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandler
  Opens key:
                                     HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
```

```
00aa00bdce0b}\inprochandler
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_document_compatible_mode
                                   HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature document compatible mode
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                                   HKLM\software\wow6432node\policies\microsoft\internet explorer\zoom
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\zoom
  Opens key:
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\zoom
                                   HKCU\software\microsoft\internet explorer\zoom
HKLM\software\wow6432node\microsoft\internet explorer\zoom
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet
  Opens key:
\verb|explorer\main\featurecontrol\feature\_weboc\_document\_zoom| \\
\label{local-problem} Opens~key: $$ HKLM\software\wow6432node\microexplorer\min\feature\control\feature\_weboc\_document\_zoom
                                   HKLM\software\wow6432node\microsoft\internet
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\url history
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\url history
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\url
history
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url history
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature ipersistmoniker load redirected url kb976425
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecor
                                   trol\feature_ipersistmoniker_load_redirected_url_kb976425
  Opens key:
                                   HKCU\software\policies\microsoft\internet explorer
                                   HKLM\software\policies\microsoft\internet explorer\international\scripts
  Opens key:
                                    HKCU\software\microsoft\internet explorer\international\scripts
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\international\scripts
                                   HKLM\software\policies\microsoft\internet explorer\settings
  Opens key:
                                    HKCU\software\microsoft\internet explorer\settings
  Opens key:
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet explorer\settings
  Opens key:
                                   HKCU\software\microsoft\internet explorer\styles
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\policies\activedesktop
                                    {\tt HKCU \ } \dot{o} {\tt ftware \ } \dot{o} {\tt icies}
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet explorer\pagesetup
  Opens key:
                                    HKCU\software\microsoft\internet explorer\menuext
                                    HKCU\software\microsoft\internet explorer\menuext\%s
  Opens key:
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\codepage
                                   HKCU\software\microsoft\internet explorer\international\scripts\3 HKLM\software\wow6432node\microsoft\internet explorer\version vector
  Opens key:
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet
\verb| explorer\m| ain\end{| feature control\end{| feature _ zone_elevation}}
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature zone elevation
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_xssfilter
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
                                    HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:
  Opens key:
                                    \label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ low rights
                                   HKCU\software\microsoft\internet explorer\low rights
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet explorer\low rights
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\0
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
  Opens key:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:
                                    HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings\zones\2
  Opens key:
                                    settings\zones\3
  Opens key:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload ieframe
                                    HKLM\software\wow6432node\policies\microsoft\internet explorer\dxtrans
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\dxtrans
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\internet explorer\dxtrans
                                   HKLM\software\wow6432node\microsoft\internet explorer\dxtrans
  Opens kev:
                                    HKCU\software\microsoft\internet
  Opens kev
\verb|explorer'main'| feature control's feature subdownload_lockdown| \\
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_sslux
Opens key: HKLM\software\wow explorer\main\featurecontrol\feature_sslux
                                   HKLM\software\wow6432node\microsoft\internet
  Opens key:
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\
                                   HKCU\software\microsoft\windows\currentversion\internet settings\
  Opens key:
  Opens key:
HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lem:hk
  Opens key:
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:
                                    HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| internet\\|
explorer\restrictions
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\restrictions
```

HKCU\software\policies\microsoft\internet explorer\restrictions

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

Opens key:

Opens key: f4ceaaf59cfc}

```
Opens key:
                                              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
                                             HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
   Opens key:
 f4ceaaf59cfc}\treatas
                                              HKCR \setminus wow6432 node \\ clsid \\ \{50d5107a-d278-4871-8989-f4ceaaf59cfc\} \\ \\ \\ treatas
   Opens key:
   Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\progid
                                              Opens key:
   Opens key:
                                             HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
   Opens key:
                                              HKCU\software\classes\clsid\{50d5107a-d278-4871-8989
   Opens key:
f4ceaaf59cfc}\progid
   Opens key:
                                              HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\progid
                                             HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
   Opens key:
f4ceaaf59cfc}\inprocserver32
                                             HKCR\
                                                            w6432node\clsid\{50d5107a-d278-4871-8989
f4ceaaf59cfc}\inprocserver32
                                             HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
  Opens kev:
f4ceaaf59cfc}\inprochandler32
                                             HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
  Opens key:
f4ceaaf59cfc}\inprochandler32
                                             HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
  Opens kev:
f4ceaaf59cfc}\inprochandler
  Opens key:
                                             HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler
   Opens key:
                                             HKCU\software\policies\microsoft\internet explorer\control panel
   Opens key:
                                             HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_iedde\_register\_urlecho| \\
                                             HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_iedde_register_urlecho
                                              HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb583
                                             HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
   Opens key:
   Opens key:
                                              HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
   Opens key:
                                             HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
                                             HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
   Opens key:
00aa00bbbb58}\progid
   Opens key:
                                              HKCR \setminus wow6432 node \\ clsid \setminus \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \setminus progid
                                             HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1
   Opens key:
00aa00bbbb58}\inprocserver32
   Opens key:
                                             HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
  Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
   Opens key
                                             HKCR\\
                                                             v6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
  Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler
                                             HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler
                                             HKLM\software\wow6432node\microsoft\windows script\features
   Opens kev:
   Opens kev
                                              HKLM\software\wow6432node\microsoft\com3
   Opens key:
HKCU\software\classes\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
   Opens key:
HKCR\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                             HKLM\software\wow6432node\microsoft\ole\appcompat
   Opens key:
                                              HKLM\software\microsoft\ole\appcompat
   Opens key:
                                              HKLM\system\currentcontrolset\control\lsa
   Opens key:
   Opens key
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
   Opens key:
                                              {\tt HKLM \ } system \verb|\ current control \verb|\ lsa \verb|\ fipsal gor ithm policy \\
{\tt HKLM \ } system \verb|\ current control set \verb|\ policies \verb|\ microsoft \verb|\ cryptography \verb|\ configuration \\
                                              Opens key:
   Opens key:
                                              HKLM\software\microsoft\cryptography
                                              HKLM\software\wow6432node\microsoft\cryptography\offload
   Opens key:
                                             \label{thm:hkcu} \begin{tabular}{ll} HKCU \software \classes \wow 6432 node \interface \classes \wow 6432 node \classes \classe
   Opens key:
000000000046}
   Opens key:
                                              HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
   Opens key
                                             \label{local-condition} HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{00000134-0000-0000-c000-c000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c00-c000-c000-c00-c00-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00
000000000046}\proxystubclsid32
   Opens key:
                                             HKCR\wow6432node\interface\{00000134-0000-0000-c000-
00000000046}\proxystubclsid32
   Opens key:
                                              HKLM\system\currentcontrolset\services\bfe
                                              HKLM\software\wow6432node\policies\microsoft\internet explorer\recovery
   Opens key:
   Opens key:
                                              HKLM\software\policies\microsoft\internet explorer\recovery
                                              HKCU\software\microsoft\internet explorer\recovery
   Opens key:
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature scripturl mitigation
                                              HKLM\software\wow6432node\microsoft\internet
   Opens kev:
\verb| explorer\main\featurecontrol\feature\_scripturl\_mitigation| \\
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
                                             HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_block_lmz_img
                                             HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_behaviors
   Opens key:
                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature behaviors
                                              HKLM\software\wow6432node\microsoft\internet explorer\default behaviors
   Opens key:
   Opens key:
                                              HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}
   Opens key:
                                             HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
   Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                              HKCR \setminus wow6432 node \setminus clsid \setminus \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\} \setminus treatas
   Opens key:
```

HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-

Opens key:

```
00aa00bdce0b}\inprocserver32
                                                                         HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
    Opens key:
00aa00bdce0b}\inprocserver32
                                                                         Opens key
00aa00bdce0b}\inprochandler32
                                                                         HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
    Opens key:
00aa00bdce0b}\inprochandler32
                                                                         HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
     Opens key
00aa00bdce0b}\inprochandler
                                                                         HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
    Opens key:
00aa00bdce0b}\inprochandler
     Opens key:
                                                                         \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ internet\+ explorer\+ persistence
     Opens key:
                                                                         HKLM\software\wow6432node\policies\microsoft\internet
explorer\persistence
     Opens key:
                                                                         HKLM\software\policies\microsoft\internet explorer\persistence
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd
                                                                         HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
     Opens key:
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\treatas
                                                                         HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
     Opens kev:
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\progid
     Opens key:
                                                                         HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
     Opens key:
                                                                         HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
                                                                         HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - f51a - 
     Opens key:
dc030521aabd}
                                                                   ndler32
    Opens key:
                                                                         HKCR\w
                                                                                                w6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
     Opens key:
                                                                         HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - f51a -
dc030521aabd}\inp
    Opens key:
                                                                         HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler
                                                                         \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \wow6432 node \clsid \d1fe6762-fc48-11d0-883a-4444 \end{tabular} \\ \begin{tabular}{ll} HKCU \software \classes \wow6432 node \clsid \d1fe6762-fc48-11d0-883a-4444 \end{tabular} \\ \begin{tabular}{ll} HKCU \software \clsid \
     Opens key:
3c8b00c10000}
                                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
    Opens key:
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\treatas
     Opens key:
                                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\progid
     Opens key:
                                                                          HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
     Opens key:
                                                                         HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
     Opens key:
     Opens key:
                                                                         HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a
3c8b00c10000}\progid
     Opens key:
                                                                         HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
                                                                         HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
     Opens key
3c8b00c10000}\inprocser
                                                                       er32
                                                                         HKCR\
                                                                                               w6432node\clsid\{d1fe6762-fc48-11d0-883a-
    Opens key
3c8b00c10000}\inprocserver32
                                                                         HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{d1fe6762 - fc48 - 11d0 - 883a - gc48 - 
     Opens key:
3c8b00c10000}\inprochandler32
    Opens key:
                                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
                                                                         HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
     Opens key:
3c8b00c10000}\inprochandler
    Opens key
                                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler
    Opens key:
                                                                         HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{4fd2a832-86c8-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fca-11d0-8fc
00c04fd9189d}
     Opens key:
                                                                         HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
    Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\treatas
                                                                         Opens key:
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\progid
     Opens key:
                                                                         HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
     Opens key:
                                                                         HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
                                                                         HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
     Opens key:
                                                                         HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca
     Opens key:
00c04fd9189d}\progid
     Opens key:
                                                                         HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
                                                                         HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
     Opens key:
00c04fd9189d}\inprocserver32
                                                                         HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
     Opens key
00c04fd9189d}\inprocserver32
                                                                         HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
    Opens kev:
00c04fd9189d}\inprochandler32
                                                                         HKCR\
                                                                                                  /6432node\clsid\{4fd2a832-86c8-11d0-8fca-
     Opens key
00c04fd9189d}\inprochandler32
    Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
     Opens key:
                                                                         HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
     Opens key:
                                                                         HKLM\software\wow6432node\microsoft\windows\currentversion\setup
     Opens key:
                                                                          Opens key:
                                                                         HKLM\software\wow6432node\microsoft\windows\currentversion
     Opens key:
                                                                         HKLM\hardware\devicemap\video
     Opens key:
                                                                         HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-
1e1a187c13e9}\0000
    Opens key:
HKLM\system\currentcontrolset\enum\pci\ven 80ee&dev beef&subsys 00000000&rev 00\3&267a616a&0&10
                                                                         HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
     Opens key:
9dd4432fa2e9}\0000
    Opens key:
                                                                         HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000
     Opens key:
                                                                         8ed0c8eb59a8}\0000
```

```
Opens key:
                                HKI M\software\wow6432node\microsoft\directdraw\compatibility
                                HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug!
  Opens key:
  Opens key:
                e\wow6432node\microsoft\directdraw\compatibility\demolitionderby2
HKLM\softwa
                                Opens key:
  Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ direct draw \ compatibility \ msgolf 98
  Opens key:
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo
                                HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
  Opens key:
squadron
  Opens key:
                                HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet
  Opens key:
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\starcraft100
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo
  Opens key:
                                HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension
  Opens key:
HKLM \label{limits} \begin{tabular}{ll} HKLM \label{limits} Wow 6432 node \mbox{$m$icrosoft$} \directdraw \compatibility \co
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
                                HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator
  Opens key:
                                HKLM\software\wow6432node\microsoft\directdraw
  Opens key:
  Opens key:
                                HKLM\software\wow6432node\microsoft\direct3d
                                HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
  Opens key:
                                Opens key:
f941e9b7e1fe}
                                HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
  Opens key:
  Opens key:
                                f941e9b7e1fe}\treatas
  Opens key:
                                HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
  Opens key:
                                f941e9b7e1fe}\progid
                                Opens key:
  Opens key:
                                HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32
  Opens key:
                                HKCR
                                           6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserv
                               er32
  Opens key:
                                HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler32
  Opens key:
                                HKCR\\
                                           w6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler32
  Opens key:
                                HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler
  Opens key:
                                HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler
                                HKCU\software\classes\dximagetransform.microsoft.shadow
  Opens key:
  Opens key:
                                HKCR\dximagetransform.microsoft.shadow
  Opens key:
                                {\tt HKCU \backslash software \backslash classes \backslash dximage transform.microsoft.shadow \backslash clsid}
  Opens key:
                                HKCR\dximagetransform.microsoft.shadow\clsid
                                HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
  Opens key:
00c04fa34f05}
  Opens key:
                                HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
  Onens key
                                HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\treatas
  Opens key:
                                HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 00c04fa34f05\} \setminus treatas
                                Opens key
00c04fa34f05}\progid
                                HKCR \setminus wow6432 \\ node \\ clsid \\ \{e71b4063-3e59-11d2-952a-00c04fa34f05\} \\ \setminus progid
  Opens key:
  Opens key:
                                HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32
                                HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
  Opens key:
00c04fa34f05}\inprocserver32
                                HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler32
                                HKCR\v
                                           w6432node\clsid\{e71b4063-3e59-11d2-952a-
  Opens key
00c04fa34f05}\inprochandler32
                                HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
  Opens key:
00c04fa34f05}\inprochandler
                                HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
  Opens kev:
00c04fa34f05}\inprochandler
                                HKLM\software\wow6432node\microsoft\internet explorer\activex
  Opens key
compatibility
                                Opens key:
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\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}
  Opens key:
                                HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
  Opens key:
                                HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\treatas
  Opens key:
                                Opens key:
                                HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\progid
                                HKCR \setminus wow6432 node \\ clsid \setminus \{30c3b080-30fb-11d0-b724-00aa006c1a01\} \setminus progid
  Opens key:
                                HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
  Opens key:
00aa006c1a01}\inprocserver32
                                HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
  Opens key:
00aa006c1a01}\inprocserver32
  Opens key:
                                HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
```

```
00aa006c1a01}\inprochandler32
                                                              HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
    Opens key:
 00aa006c1a01}\inprochandler32
                                                              Opens key
00aa006c1a01}\inprochandler
                                                              HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
    Opens key:
00aa006c1a01}\inprochandler
     Opens key:
                                                              HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}
                                                              HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
     Opens key:
     Opens key:
                                                               HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
                                                               HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
     Opens key:
     Opens key:
                                                               00aa006c1a01}\progid
     Opens key:
                                                               HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid
     Opens kev:
                                                              HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
                                                              HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-b724-a01fda0-30df-11d0-
     Opens key:
00aa006c1a01}\inprocserver32
                                                              HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
    Opens kev:
00aa006c1a01}\inprochandler32
    Opens key:
                                                              HKCR\
                                                                                  w6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
    Opens key:
                                                              HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler
     Opens key:
                                                              HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler
    Opens key:
                                                              0000f87557db}
                                                              HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
     Opens key:
     Opens key:
                                                              HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
 0000f87557db}\treatas
                                                               HKCR \setminus wow6432 \\ node \\ \clsid \\ \{4cb26c03-ff93-11d0-817e-0000f87557db\} \\ \treat \\ as
     Opens key:
     Opens key:
                                                              HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\progid
                                                               HKCR \setminus wow 6432 \\ node \\ clsid \\ \{4cb26c03-ff93-11d0-817e-0000f87557db\} \\ \setminus progid
     Opens key:
     Opens key:
                                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{4cb26c03-ff93-11d0-817e-0000f87557db\}
                                                              HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
     Opens key:
     Opens key:
                                                               HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e
 0000f87557db}\progid
     Opens key:
                                                               HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid
     Opens key:
                                                              HKCU\software\classes\mime\database\content type
     Opens key:
                                                               HKCR\mime\database\content type
                                                               \label{local-operator} \mbox{HKCU\software\classes\mbox{\sc mime\database\content\ type\image/bmp\bits}} \label{local-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-
     Opens key:
     Opens key:
                                                               HKCR\mime\database\content type\image/bmp\bits
     Opens key
                                                              HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
                                                              HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
     Opens key:
0000f87557db}\inprocserver32
                                                              HKCU\software\classes\mime\database\content type\image/gif\bits
     Opens kev:
                                                               HKCR\mime\database\content type\image/gif\bits
     Opens kev
                                                               HKCU\software\classes\mime\database\content type\image/jpeg\bits
     Opens key:
                                                              HKCR\mime\database\content type\image/jpeg\bits
HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
     Opens key:
     Opens key
 0000f87557db}\inprochandler32
     Opens key:
                                                              HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler32
                                                              HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
    Opens key:
0000f87557db}\inprochandler
     Opens key:
                                                              HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler
     Opens key:
                                                              HKCU\software\classes\mime\database\content type\image/pjpeg\bits
     Opens key:
                                                               HKCR\mime\database\content type\image/pjpeg\bits
     Opens key:
                                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \slight for the limit of the 
     Opens key:
                                                              HKCR\mime\database\content type\image/png\bits
     Opens key:
                                                               HKCU\software\classes\mime\database\content type\image/tiff\bits
     Opens key:
                                                               HKCR\mime\database\content type\image/tiff\bits
     Opens key:
                                                               HKCU\software\classes\mime\database\content type\image/x-icon\bits
     Opens key:
                                                               HKCR\mime\database\content type\image/x-icon\bits
                                                               HKCU\software\classes\mime\database\content type\image/x-jg\bits
     Opens key:
     Opens key:
                                                               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
                                                               HKCU\software\classes\mime\database\content type\image/x-wmf\bits
     Opens key:
     Opens key:
                                                               HKCR\mime\database\content type\image/x-wmf\bits
                                                               \label{lem:hkcu} \verb+KCU \software \classes \verb+mime \database \content type \verb+limage/x-png+ and the lemma \content type \content 
     Opens key:
     Opens key:
                                                               HKCR\mime\database\content type\image/x-png
                                                               HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
     Opens key:
00a0c913f750}
                                                              HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
     Opens kev:
                                                               HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
     Opens kev
 00a0c913f750}\treatas
     Opens key:
                                                               HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
                                                              HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
     Opens key:
 00a0c913f750}\progid
     Opens key:
                                                               HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid
                                                              HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
    Opens key:
00a0c913f750}\inprocserver32
     Opens key:
                                                              HKCR\
                                                                                  w6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
                                                              HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
    Opens key:
 00a0c913f750}\inprochandler32
                                                              HKCR\\
                                                                                   6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
                                                              HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
    Opens key:
00a0c913f750}\inprochandler
Opens key: HK
00a0c913f750}\inprochandler
                                                               HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
                                                              HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
     Opens key:
 f4fc1e6ca1bd}
    Opens key:
                                                               HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
```

```
Opens key:
                         HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\treatas
 Opens key:
                          HKCR \ wow 6432 node \ clsid \ \{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\} \ treat as
                          HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6
  Opens key:
f4fc1e6ca1bd}\progid
                         HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid
 Opens key:
  Opens key:
                         HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6
f4fc1e6ca1bd}\inprocserver32
                         HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key:
f4fc1e6ca1bd}\inprocserver32
 Opens key
                         HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler32
                         HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key:
f4fc1e6ca1bd}\inprochandler32
                         HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler
                         HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens kev:
f4fc1e6ca1bd}\inprochandler
                          \label{lem:hkcu} \mbox{HKCU\software\classes\mbox{\sc mime}\database\content type\application/javascript} \\
 Opens key:
 Opens key:
                         HKCR\mime\database\content type\application/javascript
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
 Opens key:
                          HKCU\software\classes\typelib
  Opens key:
                          HKCR\typelib
 Opens key:
                          HKCU \setminus software \setminus classes \setminus typelib \setminus \{5e77eb03-937c-11d1-b047-00aa003b6061\}
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
 Opens key:
                          HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key:
  Opens key:
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key
                         00aa003b6061}\1.1\409
 Opens key:
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
Opens key:
00aa003b6061}\1.1\9
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
 Opens key:
                          HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
 Opens key:
00aa003b6061}\1.1\0
                         HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0
 Opens key:
 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
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
 Opens key:
                          HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
 Opens key:
  Opens key:
                          Opens key:
                          HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
 Opens key:
0000f87557db}\1.1\409
                          HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409
 Opens key:
 Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\9
                          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
 Opens key:
                          HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
                          HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature disable behaviors draw reentrancy
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}
                         HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
 Opens key:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\treatas
                          \label{locality} HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\ \ treat as
 Opens key:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\progid
 Opens key:
                          HKCR \setminus wow 6432 \\ node \\ clsid \\ \{275c23e2-3747-11d0-9fea-00aa003f8646\} \\ \setminus progid
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
                         HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea
00aa003f8646}\progid
 Opens key:
                          HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid
                         HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
 Opens key:
00aa003f8646}\inprocserver32
                         HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
 Opens key:
00aa003f8646}\inprocserver32
                         HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
 Opens kev:
00aa003f8646}\inprochandler32
                         HKCR\\
                                  w6432node\clsid\{275c23e2-3747-11d0-9fea-
 Opens key:
00aa003f8646}\inprochandler32
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler
 Opens key:
                         HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler
 Opens key:
                         HKCU\software\microsoft\internet explorer\international\scripts\26
  Opens key:
                          HKCU\software\classes\mime\database\content type\image/gif
 Opens key:
                         {\tt HKCR\mime\database\content\ type\image/gif}
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
\verb|explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation| \\
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_block_lmz_script
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_block lmz script
                         HKCU\software\microsoft\internet
 Opens key:
\verb|explorer\main\featurecontrol\feature_activex_inactivate_mode_removal\_revert| \\
 Opens key:
```

HKLM\software\wow6432node\microsoft\internet

```
explorer\main\featurecontrol\feature activex inactivate mode removal revert
                                                               HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_use_windowedselectcontrol
                                                               HKLM\software\wow6432node\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature use windowedselectcontrol
                                                               HKCU\software\microsoft\internet explorer\new windows
    Opens key:
                                                               HKLM\software\wow6432node\microsoft\internet explorer\new windows
     Opens key:
    Opens key
                                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature xmlhttp
                                                               HKLM\software\wow6432node\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_xmlhttp
    Opens key:
                                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun
Opens key: HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_binary\_caller\_service\_provider
   Opens key:
                                                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
                                                               HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-
     Opens kev:
00aa00389b71}\proxystubclsid32
   Opens kev
                                                               HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
     Opens key:
                                                               HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd901193
                                                               HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
    Opens key:
    Opens key:
                                                               HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32
                                                               HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
    Opens key:
00c04fd90119}\proxystubclsid32
                                                               Opens key:
00000000046}
    Opens key:
                                                               HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
    Opens key:
                                                               HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
    Opens key:
                                                               Opens key:
0000000000046}\progid
                                                               HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
    Opens key:
                                                               \label{locality} \verb+HKCR++ wow 6432 node+ clsid+ \{00020424-0000-0000-c000-000000000046\}+ progid+ prog
     Opens key:
                                                               HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}
                                                               HKCR\clsid\{00020424-0000-0000-c000-00000000046}
    Opens key:
    Opens key:
                                                               HKCU\software\classes\clsid\{00020424-0000-0000-c000
000000000046}\progid
    Opens key:
                                                               HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid
                                                               HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
    Opens key:
000000000046}\inprocserver32
                                                               HKCR
                                                                                    v6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
   Opens key
                                                               HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
                                                               HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
                                                               HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
   Opens kev:
00000000046}\inprochandler
                                                               HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
    Opens key:
000000000046}\inprochandler
    Opens key:
                                                               HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
                                                               HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
     Opens key:
    Opens key:
                                                               \label{local-condition} HKCU \ software \ \ lib \ \{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4\} \ \ 1.0
                                                               HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
    Opens key:
                                                               HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
    Opens key:
00c04fb6bfc4}\1.0\0
                                                               HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0
    Opens key:
    Opens key:
                                                               HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0\win32
    Opens key:
                                                               HKCR \ typelib \ \{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4\} \ 1.0 \ 0 \ win 32acconstant \ 1.0 \ win 32
                                                               HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
HKCR\typelib\{00020430-0000-0000-000000000046}
     Opens kev:
    Opens key:
     Opens key:
                                                               HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\2.0
                                                               HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
     Opens key:
                                                               HKCU\software\classes\typelib\{00020430-0000-0000-c000-
    Opens key:
000000000046}\2.0\0
    Opens key:
                                                               Opens key
                                                               HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
    Opens key:
                                                               HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
                                                               HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key
00c04fb6bfc4}
                                                               HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
   Opens key:
     Opens kev
                                                               HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
                                                               HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
    Opens key:
    Opens key
                                                               HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\progid
    Opens key:
                                                               HKCR \setminus wow6432 node \\ clsid \setminus \{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\} \setminus progid
    Opens key:
                                                               \label{local-equation} HKCU \software \classes \clsid \footnote{Tb8a2d94-0ac9-11d1-896c-00c04fb6bfc4} \\ HKCR \clsid \footnote{Tb8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
    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\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserv
                                                             er32
                                                               HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key
00c04fb6bfc4}\inprocserver32
                                                               HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{7b8a2d94-0ac9-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-89
    Opens key:
00c04fb6bfc4}\inprochandler32
   Opens key:
                                                               HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
    Opens key:
                                                               HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{7b8a2d94-0ac9-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-896c-11d1-89
00c04fb6bfc4}\inprochandler
                                                               HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key:
00c04fb6bfc4}\inprochandler
    Opens key:
                                                               HKCU\software\classes\shockwaveflash.shockwaveflash
    Opens key:
                                                               HKCR\shockwaveflash.shockwaveflash
```

```
Opens key:
                                                      HKCU\software\classes\shockwayeflash.shockwayeflash\clsid
    Opens key:
                                                      HKCR\shockwaveflash.shockwaveflash\clsid
    Opens key:
                                                      HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{d27cdb6e-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6d-11cf-96b8-ae6
444553540000}
    Opens key:
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
    Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\treatas
    Opens key:
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\treatas
    Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\progid
    Opens key:
                                                      HKCR \verb|\wow6432| node \verb|\clsid| \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \verb|\progid| \} where $d_1$ is the sum of the sum o
    Opens key
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
    Opens key:
                                                                      w6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
   Opens key
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
    Opens key:
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
   Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler
    Opens key:
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler
    Opens key:
                                                      HKLM\hardware\description\system\centralprocessor\0
    Opens key:
                                                      HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
 types\type 001
    Opens key:
                                                      HKCU \setminus software \setminus classes \setminus typelib \setminus \{d27cdb6b-ae6d-11cf-96b8-444553540000\}
    Opens key:
                                                      HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
                                                      HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
    Opens key:
    Opens key:
                                                      HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
    Onens key
                                                      HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\409
   Opens key:
                                                      \label{local-eq:hkcr-typelib} $$ HKCR \times d27cdb6b-ae6d-11cf-96b8-444553540000 \times 1.0 \times 409 $$ $$
    Opens key:
                                                      HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
4445535400003\1.0\9
                                                      HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9
   Opens key:
    Opens key:
                                                      HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0
                                                      HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0
   Opens key:
    Opens key:
                                                      HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0\win32
                                                      Opens key:
    Opens key:
                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection
    Opens key:
                                                      HKLM\software\wow6432node\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_activex\_repurposed etection| \\
                                                      HKLM\software\wow6432node\microsoft\internet explorer\activex
   Opens key
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                                                      HKCU\software\microsoft\internet
    Opens key:
\verb|explorer\main\featurecontrol\feature\_addon\_management| \\
                                                      HKLM\software\wow6432node\microsoft\internet
   Opens key:
                             n\featurecontrol\feature_addon_management
explorer\mai
                                                      HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_alloweddomainlist
Opens key: HKLM\software\wow6432node\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_alloweddomainlist|
    Opens key:
                                                      \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} Software \begin{tabular}{ll} wow 6432 node \end{tabular} internet explorer \end{tabular} explorer \end{tabular} and the label \begin{tabular}{ll} wow 6432 node \end{tabular} and \begin{tabular}{ll} wow 6432 node 
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                                                      HKCU\software\classes\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-
   Opens key:
00aa00615333}
    Opens key:
                                                      HKCR\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
    Opens key:
                                                      HKCU\software\microsoft\code store database\distribution units
                                                      HKLM\software\wow6432node\microsoft\code store database\distribution
    Opens key:
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\code store database\distribution
units\{d27cdb6e-ae6d-11cf-96b8-444553540000}
    Opens key:
                                                      HKCU\software\classes\wow6432node\clsid
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Opens key:
444553540000}\availableversion
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Opens key:
444553540000}\installedversion
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key:
444553540000}\installedversion
   Opens key
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\appid
                                                      Opens key:
    Opens key
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\languagecheckperiod
    Opens kev:
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\languagecheckperiod
                                                      HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
    Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus
   Opens key:
                                                      HKCR\wow6432 node\clsid\\ \{d27cdb6e-ae6d-11cf-96b8-444553540000\}\\ \mbox{miscstatus}
                                                      HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus\1
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Opens key:
444553540000}\miscstatus\1
                                                      HKLM\software\wow6432node\microsoft\windows\tablet pc\
    Opens key:
    Opens key:
                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
    Opens key:
                                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
                                                      HKCU\software\microsoft\internet explorer\feed discovery
    Opens key:
                                                      HKLM\software\wow6432node\microsoft\internet explorer\feed discovery
    Opens key:
    Opens key:
                                                      HKCU\software\microsoft\ftp
    Opens key:
                                                      HKCU\software\classes\mime\database\content type\application/x-
```

```
shockwaye-flash
                                                                          HKCR\mime\database\content type\application/x-shockwave-flash
     Opens key:
     Opens key:
                                                                          HKCU\software\classes\protocols\filter\application/x-shockwave-flash
                                                                          HKCR\protocols\filter\application/x-shockwave-flash
     Opens key:
     Opens key:
                                                                         HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32
                                                                         HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
    Opens key:
00c04f983e60}
     Opens key:
                                                                          HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\treatas
                                                                          HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\treat as
     Opens key:
     Opens key
                                                                         HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\progid
     Opens key:
                                                                          HKCR \setminus wow6432 node \\ clsid \\ \{2933bf90-7b36-11d2-b20e-00c04f983e60\} \\ \setminus progide \\ (2933bf90-7b36-11d2-b20e-00c04f983e60) \\ \setminus progide \\ (2933bf90-7b36-11d2-b20e-00c04f98) \\ \setminus progide \\ (2933bf90-7b36-11d2-b20e-00c04f98) \\ \setminus progide \\ (2935bf90-7b36-11d2-b20e-00c04f98) \\ \setminus progide \\ (2935bf90-7b36-00c04f98) \\ \setminus progide \\ (2935bf90-7b3
                                                                         HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e
     Opens key
00c04f983e60}\inprocserver32
                                                                         HKCR\\
    Opens kev:
                                                                                                w6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32
     Opens key:
HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
    Opens kev:
00c04f983e60}\inprochandler32
    Opens key:
                                                                         HKCR\\
                                                                                                  v6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprochandler32
    Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprochandler
     Opens key:
                                                                         HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprochandler
                                                                         \label{thm:limit} \mbox{HKCU\software\mbox{$\mbox{$\mbox{$\rm HKCU\software\mbox{$\mbox{$\rm MUltimedia\mbox{$\rm midimap$}$}}$} \mbox{$\mbox{$\rm MUltimedia\mbox{$\rm midimap$}$}$} \mbox{$\mbox{$\rm MUltimedia\mbox{$\rm MUltime
     Opens key:
     Opens key:
                                                                          HKLM \ software \ wow 6432 node \ microsoft \ msxml 30
     Opens key
                                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata
                                                                         HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
     Opens key:
                                                                          HKLM\system\currentcontrolset\control\securityproviders
     Opens key:
                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache
                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
     Opens key:
                                                                          HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
     Opens key:
     Opens key:
                                                                          HKCU\software\microsoft\internet explorer\domstorage\baidu.com
     Opens key:
                                                                         HKCU\software\microsoft\internet explorer\domstorage\total
     Opens key:
Opens key:
                                                                          HKLM\software\microsoft\windows\currentversion\policies\system
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}
                                                                          HKCR \setminus wow 6432 \\ node \\ clsid \\ \{9ba05972 - f6a8 - 11cf - a442 - 00a0c90a8f39\} \\
     Opens key:
     Opens key
                                                                         HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\treatas
     Opens key:
                                                                          HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
     Opens key:
00a0c90a8f39}\progid
                                                                          HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
     Opens kev:
                                                                          HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
     Opens kev
     Opens key:
                                                                          HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: 00a0c90a8f39}\progid
                                                                         HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
                                                                          HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
     Opens key:
     Opens key:
                                                                         HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{9ba05972 - f6a8 - 11cf - a442 - 11cf - a442
00a0c90a8f39}\inprocserver32
                                                                         HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
    Opens key:
00a0c90a8f39}\inprocserver32
    Opens key
                                                                         HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
     Opens key:
                                                                         HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
     Opens key:
                                                                         HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
    Opens key:
                                                                         HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
Opens key:
0080c7f4ee85}
                                                                         HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
     Opens key:
                                                                          \label{localized} HKCR\wow6432 node\interface \ \{85cb6900-4d95-11cf-960c-0080c7f4ee85\} \\
     Opens key:
                                                                         \label{locality} HKCU \setminus software \\ \\ classes \setminus wow 6432 \\ node \setminus interface \\ \\ \{85cb6900-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d9-11cf-960c-4d9-11cf-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960
0080c7f4ee85}\proxystubclsid32
     Opens key:
                                                                         HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
    Opens key:
                                                                          HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
                                                                         HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
     Opens key:
0080c7f4ee85}\forward
Opens key: 0080c7f4ee85}\forward
                                                                         HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
                                                                          HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
     Opens key:
                                                                          \label{locality} HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{85cb6900-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-96
     Opens key:
0080c7f4ee85}\typelib
                                                                          HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
    Opens key:
0080c7f4ee85}\typelib
     Opens key:
                                                                          HKLM\software\wow6432node\policies\microsoft\internet explorer\services
     Opens key:
                                                                         HKLM\software\policies\microsoft\internet explorer\services
     Opens key:
                                                                          HKCU\software\microsoft\internet explorer\services
     Opens key:
                                                                          HKLM\software\wow6432node\policies\microsoft\internet
explorer\activities
                                                                          HKLM\software\policies\microsoft\internet explorer\activities
     Opens key:
     Opens key:
                                                                          HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
                                                                          HKCR \typelib \end{cab22} aco-30c1-11cf-a7eb-0000c05bae0b \end{cab2}
     Opens key:
                                                                         \label{eq:hkculsoftware\classes\typelib} HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1$ \\ HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1$ \\
     Opens key:
     Opens key:
     Opens key:
                                                                          HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
                                                                          HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
     Opens key:
                                                                         HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
     Opens key:
0000c05bae0b}\1.1\0\win32
     Opens key:
                                                                         HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
```

```
Opens key:
                                                                                     HKCU\software\microsoft\internet explorer\activities
                                                                                     HKLM\software\wow6432node\microsoft\internet explorer\activities
      Opens key:
                                                                                     HKLM\software\wow6432node\policies\microsoft\internet
      Opens key:
explorer\infodelivery\restrictions
      Opens key:
                                                                                     HKLM\software\policies\microsoft\internet
explorer\infodelivery\restrictions
      Opens key:
                                                                                     HKCU\software\policies\microsoft\internet
explorer\infodelivery\restrictions
                                                                                     HKLM\software\wow6432node\policies\microsoft\internet explorer\suggested
     Opens key:
sites
      Opens key
                                                                                     HKLM\software\policies\microsoft\internet explorer\suggested sites
      Opens key:
                                                                                     HKCU\software\microsoft\internet explorer\suggested sites
                                                                                     HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
      Opens key:
08002b30309d}\shellfolder
                                                                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8
08002b30309d}\shellfolder
                                                                                     HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
     Opens key
000000000046}
                                                                                     Opens key:
      Opens key:
                                                                                     HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
                                                                                     HKCR\w
                                                                                                                 v6432node\interface\{00020400-0000-0000-c000-
00000000046}\proxystubclsid32
                                                                                     HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
     Opens key:
000000000046}
      Opens key:
                                                                                     HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}
      Opens key
                                                                                     \label{local-cond} \begin{tabular}{ll} HKCU \software \classes \wow 6432 node \clsid \closed \clsid \closed \clsid \cls
0000000000046}\treatas
                                                                                     Opens key:
                                                                                     000000000046}\progid
                                                                                     HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\progid
      Opens key:
      Opens key:
                                                                                     HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
                                                                                     HKCR\clsid\{00020420-0000-0000-c000-000000000046}
      Opens key:
Opens key:
0000000000046}\progid
                                                                                     HKCU\software\classes\clsid\{00020420-0000-0000-c000-
      Opens key:
                                                                                     Opens key:
                                                                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \closer{lem:hkcu} 20d04 feo-energy \clsid \clsid
3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens key:
                                                                                     HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32
      Opens key:
                                                                                     HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
     Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus clsid \setminus \{20d04fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1069-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-1046fe0-3aea-10
a2d8-08002b30309d}\shellfolder
     Opens key:
\label{thm:hkcu} \mbox{\tt HKCU} \mbox{\tt software} \mbox{\tt microsoft} \mbox{\tt windows} \mbox{\tt currentversion} \mbox{\tt explorer} \mbox{\tt mountpoints2} \mbox{\tt cpc} \mbox{\tt volume} \mbox{\tt mountpoints2} \mbox{\tt cpc} \mbox{\tt cpc} \mbox{\tt cpc} \mbox{\tt cpc} \mbox{\tt mountpoints2} \mbox{\tt cpc} \mbox{\tt cpc}
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{8063a3d4-8213-42444, \ and \ baselines \ and \ and \ baselines \ and \ baselines \ and 
11e3-a68e-806e6f6e6963}\
                                                                                     HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
                                                                                     HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
     Opens key:
000000000046}\inprochandler32
                                                                                     HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprochandler
                                                                                     HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
     Opens key:
000000000046}\inprochandler
                                                                                     HKCU\software\classes\drive\shellex\folderextensions
      Opens key:
      Opens key:
                                                                                     HKCR\drive\shellex\folderextensions
      Opens key:
                                                                                     HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
      Opens key:
                                                                                     HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e93
     Opens key:
HKCU \setminus software \\ \mbox{$13-8213-8213-} \\
11e3-a68e-806e6f6e6963}\
                                                                                     HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-
     Opens key:
00aa006009fa}
      Opens key:
                                                                                     HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
      Opens kev
                                                                                     HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-
00aa006009fa}\proxystubclsid32
                                                                                     HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-
     Opens key:
00aa006009fa}\proxystubclsid32
     Opens key:
                                                                                     HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}
                                                                                     HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
      Opens key:
      Opens key:
                                                                                     HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\treatas
     Opens key
                                                                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
                                                                                     HKCR \setminus wow6432 node \\ clsid \\ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}
      Opens key:
      Opens key
                                                                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
      Opens key:
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
      Opens key
                                                                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\progid
      Opens key:
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
      Opens key:
                                                                                     \label{local-equation} HKCR\wow6432 node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba\}\treatas}
      Opens key
                                                                                     HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\progid
     Opens key:
                                                                                     HKCR \verb|\wow6432| node \verb|\clsid| \{a4a1a128-768f-41e0-bf75-e4fddd701cba\} \verb|\progid| in the context of the conte
                                                                                     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}\progid
```

HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

Opens key: Opens key:

b8dc300d9f9d}\progid

Opens key:

Opens key:

```
HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Opens key:
b8dc300d9f9d}\inprocserver32
                                                                 HKCR
                                                                                         6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                                                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
    Opens key:
e4fddd701cba}\inprocserver32
    Opens key:
                                                                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
                                                                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Opens key:
b8dc300d9f9d}\inprochandler32
    Opens key
                                                                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
                                                                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Opens key
b8dc300d9f9d}\inprochandler
    Opens key
                                                                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
                                                                 HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf
    Opens key:
e4fddd701cba}\inprochandler32
    Opens key:
                                                                 HKCU\software\microsoft\windows\currentversion\explorer\
                                                                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
    Opens kev:
e4fddd701cba}\inprochandler32
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
    Opens key:
                                                                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
    Opens key:
HKLM \label{lem:hklm} Which is the large state of the large state of
    Opens key:
\label{thm:culsoftware} \begin{tabular}{l} HKCU \software \microsoft \windows \shell \associations \urlassociations \directory \end{tabular} \begin{tabular}{l} HKCU \software \microsoft \windows \shell \associations \urlassociations \directory \end{tabular} \begin{tabular}{l} HKCU \software \microsoft \windows \shell \associations \urlassociations \directory \end{tabular} \begin{tabular}{l} HKCU \software \microsoft \windows \shell \associations \node \nod
    Opens key:
                                                                 HKCU\software\classes\directory
                                                                  HKCR\directory
    Opens key:
                                                                  HKCU\software\classes\directory\curver
    Opens key:
                                                                  HKCR\directory\curver
    Opens key:
    Opens key:
                                                                  HKCR\directory\
                                                                  HKCU\software\classes\directory\shellex\iconhandler
    Opens key:
                                                                  HKCR\directory\shellex\iconhandler
    Opens key:
    Opens key:
                                                                  HKCU\software\classes\folder
                                                                 HKCR\folder
    Opens key:
    Opens key:
                                                                  HKCU\software\classes\folder\shellex\iconhandler
     Opens key:
                                                                  HKCR\folder\shellex\iconhandler
    Opens key:
                                                                 HKCU\software\classes\allfilesystemobjects
    Opens key:
                                                                 000000000046}
                                                                  Opens key:
    Opens kev
                                                                 HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-
000000000046 \} \\ proxystubcl sid 32
    Opens key:
                                                                 HKCR\v
                                                                                           432node\interface\{00020404-0000-0000-c000-
00000000046}\proxystubclsid32
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}
                                                                  HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}
    Opens key:
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
0000000000046}\treatas
    Opens key:
                                                                  HKCR\allfilesystemobjects
                                                                  HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
     Opens key:
    Opens key:
                                                                 {\tt HKCR\allfilesystemobjects\shellex\iconhandler}
    Opens key:
                                                                 HKCU\software\classes\directory\docobject
                                                                  HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}\treatas
    Opens key:
                                                                  HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
     Opens key:
000000000046}\progid
    Opens key:
                                                                  HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}\progid
                                                                  HKCU\software\classes\clsid\{00020421-0000-0000-c000-000000000046}
     Opens key:
     Opens key:
                                                                  HKCR\clsid\{00020421-0000-0000-c000-000000000046}
                                                                 HKCU\software\classes\clsid\{00020421-0000-0000-c000
    Opens kev
000000000046}\progid
    Opens key:
                                                                  HKCR\clsid\{00020421-0000-0000-c000-00000000046}\progid
     Opens key:
                                                                  HKCR\directory\docobject
    Opens key:
                                                                  HKCU\software\classes\folder\docobject
    Opens key:
                                                                  HKCR\folder\docobject
    Opens key:
                                                                  HKCU\software\classes\allfilesystemobjects\docobject
    Opens key:
                                                                 HKCR\allfilesystemobjects\docobject
                                                                 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
    Opens key:
000000000046}\inprocserver32
                                                                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000
000000000046}\inprocserver32
                                                                 HKCU\software\classes\directorv\browseinplace
    Opens key:
     Opens key:
                                                                  HKCR\directory\browseinplace
                                                                  HKCU\software\classes\folder\browseinplace
    Opens key:
    Opens key:
                                                                 HKCR\folder\browseinplace
                                                                 HKCU\software\classes\allfilesvstemobjects\browseinplace
    Opens kev:
                                                                  HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
     Opens kev
000000000046}\inprochandler32
    Opens key:
                                                                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler32
                                                                  HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
00000000046}\inprochandler
    Opens key:
                                                                 HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler
    Opens key:
                                                                  {\tt HKCR\ left} lesystem objects \ \verb|\ browseinplace|
    Opens key:
                                                                 HKCU\software\classes\directory\clsid
                                                                 HKCR\directory\clsid
HKCU\software\classes\folder\clsid
    Opens key:
    Opens key:
     Opens key:
                                                                  HKCR\folder\clsid
    Opens key:
                                                                  HKCU\software\classes\allfilesystemobjects\clsid
                                                                 HKCR\allfilesystemobjects\clsid
    Opens key:
    Opens key:
                                                                  HKCU \setminus software \\ \land classes \\ \setminus wow 6432 \\ node \\ \setminus clsid \\ \setminus \{ff393560-c2a7-11cf-bff4-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c12a7-c
444553540000}
                                                                 HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
     Opens key:
444553540000}\inprocserver32
    Opens key:
```

HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-

```
444553540000}\inprocserver32
                                                                       HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
     Opens key:
 444553540000}\shellfolder
                                                                       HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-
     Opens key
444553540000}\shellfolder
                                                                       HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
     Opens key:
 444553540000}\treatas
     Opens key:
                                                                       HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\progid
     Opens key:
                                                                       HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
     Opens key:
                                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
                                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
     Opens key:
                                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
      Opens key:
 444553540000}\progid
     Opens key:
                                                                       HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
                                                                       HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
     Opens kev:
 444553540000}\inprochandler32
                                                                       Opens key:
444553540000}\inprochandler32
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\inprochandler
     Opens key
                                                                       HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler
     Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ ff393560-microsoft \ windows \ current \ version \ shell \ compatibility \ objects \ objects
 c2a7-11cf-bff4-444553540000}
                                                                       HKCU\software\microsoft\windows\currentversion\internet
     Opens key
settings\5.0\cache\extensible cache\mshist012016040820160409
                                                                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ app
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afhb.exe
                                                                       HKLM\software\wow6432node\microsoft\windows\currentversion\app
     Opens key:
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
Opens key: HKLM\software\microsoft\windows\currentversion\appaths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                                                       HKLM\software\microsoft\windows\currentversion\app
                                                                       HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
     Opens key:
3aea-1069-a2d8-08002b30309d}
     Opens key:
HKCU \ software \ microsoft \ windows \ current version \ vexplorer \ session in follows \ top \ name \ pace \ name \ current \ vexplorer \ session \ in follows \ name \ pace \ name 
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}
     Opens key:
                                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
     Opens key:
                                                                       HKCU\software\microsoft\internet explorer\main\windowssearch
                                                                       HKLM\software\policies\microsoft\internet explorer\feeds
     Opens key:
                                                                       HKCU\software\microsoft\internet explorer\feeds
      Opens key:
     Opens key:
                                                                       HKLM\software\wow6432node\microsoft\internet explorer\feeds
     Opens key:
68ad-4d8a-87bd-30b759fa33dd}
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
 68ad-4d8a-87bd-30b759fa33dd}\propertybag
     Opens key:
                                                                       HKLM\software\wow6432node\microsoft\windows search
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
 0000f81fe221}
                                                                       HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
     Opens key:
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\treatas
                                                                       \label{localization} HKCR\wow6432 node \clsid \{f5078f35-c551-11d3-89b9-0000f81fe221\} \treat as the second of the
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
      Opens key:
0000f81fe221}\progid
     Opens key:
                                                                       HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32
     Opens key:
                                                                       HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32
     Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{f5078f35 - c551 - 11d3 - 89b9 - c1841 + c1841
0000f81fe221}\inprochandler32
     Opens key:
                                                                       HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler32
      Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler
                                                                       HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
     Opens key:
 0000f81fe221}
                                      \inprochandler
     Opens key:
                                                                       \label{local-continuity} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \sime \database \content type \content ty
     Opens key:
                                                                       {\tt HKCR\mbox{\tt mime}\database\content\ type\limage/x-icon}
                                                                       HKCU\software\classes\protocols\filter\image/x-icon
     Opens key:
      Opens key:
                                                                       HKCR\protocols\filter\image/x-icon
                                                                       HKCU\software\microsoft\internet
     Opens key:
 \verb|explorer| main\featurecontrol\feature\_mime\_treat\_image\_as\_authoritative| \\
                                                                       HKLM\software\wow6432node\microsoft\internet
     Opens kev:
 explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
                                                                       HKCU\software\classes\shockwaveflash.shockwaveflash.7
     Opens key:
     Opens key:
                                                                       HKCR\shockwaveflash.shockwaveflash.7
                                                                       HKCU\software\classes\shockwaveflash.shockwaveflash.7\clsid
     Opens key:
      Opens key:
                                                                       HKCR\shockwaveflash.shockwaveflash.7\clsid
     Opens key:
                                                                       {\tt HKCU \backslash software \backslash microsoft \backslash internet}
explorer\main\featurecontrol\feature isolate named windows
     Opens key:
                                                                       HKLM\software\wow6432node\microsoft\internet
 explorer\mai
                                                                      trol\feature_isolate_named_windows
     Opens key:
                                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_navigation_sounds
     Opens key:
                                                                       HKLM\software\wow6432node\microsoft\internet
 \verb|explorer'| main feature control feature_disable_navigation\_sounds| \\
     Opens key:
                                                                       \label{lem:hkcu-appevents-schemes-apps-explorer-law-igating-current} \\
     Opens key:
                                                                       HKCU\appevents\schemes\
     Opens key:
                                                                       HKCU\appevents\schemes\apps\explorer\navigating\.current\active
     Opens key
                                                                       HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
 fd2b31b3eefd3
                                                                       HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\}
     Opens key:
      Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
```

fd2b31b3eefd}\treatas

```
Opens key:
                                                       HKCR\wow6432node\clsid\{e569hde7-a8dc-47f3-893f-fd2h31h3eefd}\treatas
                                                       HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
   Opens key:
fd2b31b3eefd}\progid
                                                       HKCR \verb|\wow6432| node \verb|\clsid| \{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\} \verb|\progid| node |\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\width=\wi
   Opens key:
                                                       HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
    Opens kev:
   Opens key:
    Opens key:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893fabber - a8dc - 47f3 - 893fabber - a8dc - 47f3 - 893fabbr - a8dc - 47f3 - 895fabbr - a8dc - 47f3 - 895fa
fd2b31b3eefd}\progid
                                                       HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid
   Opens key:
                                                       HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
   Opens key:
fd2b31b3eefd}\inprocserv
   Opens key:
                                                       HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32
                                                       HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893f - a8dc - 47f3 - 800f - a8dc - 47f3 - 893f - a8dc - 47f3 - 893f - a8dc - 47f3 - 800f - a8dc - 47f3 - 800f - a8dc - 47f3 - 800f - a8dc - 47f3 - a8dc 
   Opens key:
fd2b31b3eefd}\inprochandler32
   Opens key:
                                                       HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler32
   Opens key:
                                                       HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler
   Opens key:
                                                       HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler
                                                       HKCU\software\classes\mime\database\content type\text/html;charset=utf-8
    Opens key:
   Opens key:
                                                       HKCR\mime\database\content type\text/html;charset=utf-8
   Opens key:
                                                       HKCU\software\microsoft\internet explorer\searchproviders\
   Opens key:
                                                       HKCU\software\microsoft\internet
HKLM \ software \ wow 6432 node \ microsoft \ internet
   Opens key:
explorer\main\featurecontrol\feature_additional ie8 memory cleanum
   Opens key:
                                                       HKCU\appevents\schemes\apps\explorer\activatingdocument\.current
    Opens key:
                                                       HKCU\software\classes\mime\database\content type\image/jpeg
   Opens key:
                                                       HKCR\mime\database\content type\image/jpeg
                                                       HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\languagepack\surrogatefallback\arial
                                                       HKCU\software\classes\mime\database\content type\baiduapp/json;
v6.27.2.14; charset=utf-8
                                                       HKCR\mime\database\content type\baiduapp/json; v6.27.2.14; charset=utf-8
   Opens key:
    Opens key:
                                                       HKCU\software\classes\mime\database\content type\baiduapp/json
   Opens key:
                                                       HKCR\mime\database\content type\baiduapp/json
   Opens key:
                                                       HKCU\software\classes\protocols\filter\baiduapp/json; v6.27.2.14;
charset=utf-8
    Opens key:
                                                       HKCR\protocols\filter\baiduapp/json;\ v6.27.2.14;\ charset=utf-8
                                                       HKCU\software\classes\protocols\filter\application/javascript
   Opens key:
   Opens key:
                                                       HKCR\protocols\filter\application/javascript
   Opens key:
                                                       HKCU\software\classes\msxml2.xmlhttp
    Opens key:
                                                       {\tt HKCR\backslash msxml2.xmlhttp}
   Opens key:
                                                       HKCU\software\classes\msxml2.xmlhttp\clsid
   Opens key:
                                                       HKCR\msxml2.xmlhttp\clsid
    Opens key:
                                                       HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}
                                                       HKCR \setminus wow6432 node \\ \\ clsid \setminus \{f6d90f16-9c73-11d3-b32e-00c04f990bb4\}
   Opens key:
                                                       HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
   Opens kev:
00c04f990bb4}\treatas
                                                       HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\treatas
   Opens key:
   Opens key:
                                                       HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\progid
                                                       Opens key:
   Opens key:
                                                       00c04f990bb4}\inprocserver32
                                                       HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
   Opens key:
00c04f990bb4}\inprocserver32
   Opens key
                                                       HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprochandler32
   Opens key:
                                                       HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprochandler32
   Opens key:
                                                       HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprochandler
   Opens key:
                                                       HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprochandler
   Opens key:
                                                       HKCU\software\classes\shockwaveflash.shockwaveflash.12
   Opens key:
                                                       HKCR\shockwaveflash.shockwaveflash.12
                                                       HKCU \setminus software \setminus classes \setminus shockwave flash. 11
   Opens key:
   Opens key:
                                                       HKCR\shockwaveflash.shockwaveflash.11
   Opens key:
                                                       HKCU\software\classes\shockwaveflash.shockwaveflash.10
   Opens key:
                                                       HKCR\shockwaveflash.shockwaveflash.10
                                                       HKCU\software\classes\shockwaveflash.shockwaveflash.10\clsid
    Opens key:
   Opens key:
                                                       HKCR \verb|\shockwaveflash.shockwaveflash.10| clsid
                                                       HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_block_lmz_object
                                                       HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_block_lmz_object
                                                       HKLM\software\wow6432node\microsoft\internet
   Opens kev:
explorer\plugins\disableactivexcontrols
                                                       HKCU\software\classes\.swf
   Opens key:
   Opens key:
                                                       HKCR\.swf
   Opens key:
                                                       HKCU\software\classes\baidubar.tool.1
                                                       HKCR\baidubar.tool.1
    Opens key:
   Opens key:
                                                       HKCU\software\classes\baidubar.tool.2
   Opens key:
                                                       HKCR\baidubar.tool.2
                                                       HKCU\software\classes\baidubar.tool.3
   Opens key:
    Opens key:
                                                       HKCR\baidubar.tool.3
   Opens key:
                                                       HKCU\software\classes\baidubar.tool.4
                                                       HKCR\baidubar.tool.4
   Opens key:
   Opens key:
                                                       HKCU\software\classes\baidubar.tool.5
                                                       HKCR\baidubar.tool.5
    Opens key:
   Opens key:
                                                       HKCU\software\classes\baidubar.tool.6
                                                       HKCR\baidubar.tool.6
   Opens key:
   Opens key:
                                                       HKCU\software\classes\baidubar.tool.7
                                                       {\tt HKCR \ haidubar.tool.7}
    Opens key:
   Opens key:
                                                       HKCU\software\classes\baidubar.tool.8
                                                       HKCR\baidubar.tool.8
   Opens key:
    Opens key:
                                                       HKCU\software\classes\baidubar.tool.9
```

Opens key:

HKCR\baidubar.tool.9

```
Opens key:
                           HKCU \setminus software \setminus classes \setminus google.oneclick ctrl.1
 Opens key:
                           HKCR\google.oneclickctrl.1
  Opens key:
                           HKCU\software\classes\google.oneclickctrl.2
                           HKCR\google.oneclickctrl.2
  Opens key:
 Opens key:
                           {\tt HKCU \setminus software \setminus classes \setminus google.oneclickctrl.3}
                           HKCR\google.oneclickctrl.3
 Opens key:
  Opens key:
                           HKCU\software\classes\google.oneclickctrl.4
 Opens key:
                           HKCR\google.oneclickctrl.4
 Opens key:
                           {\tt HKCU \setminus software \setminus classes \setminus google.oneclickctrl.5}
                           HKCR\google.oneclickctrl.5
 Opens key:
  Opens key:
                           HKCU\software\classes\google.oneclickctrl.6
 Opens key:
                           HKCR\google.oneclickctrl.6
                           HKCU\software\classes\google.oneclickctrl.7
HKCR\google.oneclickctrl.7
 Opens key:
 Opens key:
                           HKCU\software\classes\google.oneclickctrl.8
  Opens key:
 Opens key:
                           HKCR\google.oneclickctrl.8
                           HKCU\software\classes\google.oneclickctrl.9
HKCR\google.oneclickctrl.9
 Opens kev:
  Opens key:
                           HKCU\software\classes\qvodinsert.qvodctrl.1
 Opens key:
 Opens key:
                           HKCR\qvodinsert.qvodctrl.1
                           HKCU\software\classes\qvodinsert.qvodctrl.2
 Opens kev:
  Opens key:
                           HKCR\qvodinsert.qvodctrl.2
 Opens key:
                           HKCU\software\classes\qvodinsert.qvodctr1.3
 Opens key:
                           HKCR\qvodinsert.qvodctrl.3
 Opens key:
                           HKCU\software\classes\qvodinsert.qvodctrl.4
  Opens key:
                           HKCR\qvodinsert.qvodctrl.4
 Opens key:
                           {\tt HKCU \setminus software \setminus classes \setminus qvodinsert.qvodctr1.5}
 Opens key:
                           HKCR\ayodinsert.ayodctrl.5
                           HKCU\software\classes\qvodinsert.qvodctrl.6
 Opens key:
  Opens key:
                           HKCR\qvodinsert.qvodctrl.6
 Opens key:
                           HKCU\software\classes\qvodinsert.qvodctrl.7
                           HKCR\qvodinsert.qvodctrl.7
 Opens key:
 Opens key:
                           HKCU\software\classes\qvodinsert.qvodctr1.8
                           HKCR\qvodinsert.qvodctrl.8
  Opens key:
 Opens key:
                           HKCU\software\classes\qvodinsert.qvodctrl.9
 Opens key:
                           HKCR\qvodinsert.qvodctrl.9
 Opens key:
                           HKCU\software\classes\pdf.pdfctrl.2
 Opens key:
                           HKCR\pdf.pdfctrl.2
                           HKCU\software\classes\pdf.pdfctrl.3
 Opens key:
 Opens key:
                           HKCR\pdf.pdfctrl.3
                           HKCU\software\classes\pdf.pdfctrl.4
  Opens key:
 Opens key:
                           HKCR\pdf.pdfctrl.4
 Opens key:
                           HKCU\software\classes\pdf.pdfctrl.5
 Opens key:
                           HKCR\pdf.pdfctrl.5
  Opens key:
                           HKCU\software\classes\pdf.pdfctrl.6
 Opens key:
                           HKCR\pdf.pdfctrl.6
 Opens key:
                           HKCU\software\classes\pdf.pdfctrl.7
  Opens key:
                           HKCR\pdf.pdfctrl.7
                           HKCU\software\classes\pdf.pdfctrl.8
  Opens key:
 Opens key:
                           HKCR\pdf.pdfctrl.8
                           HKCU\software\classes\pdf.pdfctrl.9
 Opens kev:
  Opens kev
                           HKCR\pdf.pdfctrl.9
                           HKCU\software\classes\pdf.pdfctrl.1
 Opens key:
 Opens key:
                           HKCR\pdf.pdfctrl.1
                           HKCU\software\classes\acropdf.pdf.1
 Opens key:
  Opens key:
                           HKCR\acropdf.pdf.1
 Opens key:
                           HKCU \setminus software \setminus classes \setminus acropdf.pdf.1 \setminus clsid
 Opens key:
                           HKCR\acropdf.pdf.1\clsid
                           HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
 Opens key:
444553540000}
 Opens key:
                           HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}
 Opens key:
                           HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\treatas
 Opens key:
                           \label{localized} HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\\\ \treat as \\
 Onens key
                           HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\progid
 Opens key:
                           HKCR \setminus wow 6432 \\ node \\ clsid \\ \{ca8a9780-280d-11cf-a24d-444553540000\} \\ \setminus progid
                           HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32
 Opens key:
                           HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32
 Opens key:
                           HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprochandler32
                           HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
 Opens key:
444553540000}\inprochandler32
 Opens key:
                           HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprochandler
 Opens key:
                           HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprochandler
 Opens key:
                           HKCU\software\adobe\acrobat reader\9.0\originals
 Opens kev:
                           HKCU\software\adobe\adobe acrobat\9.0\originals
                           HKCU\software\adobe\acrobat reader\8.0\originals
  Opens key:
                           HKCU\software\adobe\adobe acrobat\8.0\originals
 Opens key:
 Opens key:
                           HKCU\software\adobe\acrobat reader\7.0\originals
                           HKCU\software\adobe\adobe acrobat\7.0\originals
 Opens key:
 Opens key:
                           HKLM\software\wow6432node\microsoft\active setup\installed
components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}
 Opens key:
                           HKLM\software\wow6432node\microsoft\active setup\installed
components\{08b0e5c0-4fcb-11cf-aaa5-00401c608555}
 Opens key:
                           HKLM\software\wow6432node\microsoft\active setup\installed
components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}
                           HKLM\software\wow6432node\microsoft\active setup\installed
 Opens key:
components\{283807b5-2c60-11d0-a31d-00aa00b92c03}
 Opens key:
                           HKLM\software\wow6432node\microsoft\active setup\installed
components\{3af36230-a269-11d1-b5bf-0000f8051515}
                           HKLM\software\wow6432node\microsoft\active setup\installed
 Opens key:
components\{44bba840-cc51-11cf-aafa-00aa00b6015c}
                           HKLM\software\wow6432node\microsoft\active setup\installed
 Opens key:
components\{44bba842-cc51-11cf-aafa-00aa00b6015b}
                           HKLM\software\wow6432node\microsoft\active setup\installed
 Opens key:
components\{44bba848-cc51-11cf-aafa-00aa00b6015c}
 Opens key:
                           HKLM\software\wow6432node\microsoft\active setup\installed
```

```
components\{45ea75a0-a269-11d1-b5bf-0000f8051515}
                                            HKLM\software\wow6432node\microsoft\active setup\installed
  Opens key:
components\{4f216970-c90c-11d1-b5c7-0000f8051515}
                                            HKLM\software\wow6432node\microsoft\active setup\installed
  Opens key:
components\{5a8d6ee0-3e18-11d0-821e-444553540000}
                                            HKLM\software\wow6432node\microsoft\active setup\installed
  Opens key:
components\{7790769c-0471-11d2-af11-00c04fa35d02}
                                            Opens key:
components\{89820200-ecbd-11cf-8b85-00aa005b4340}
  Opens key:
                                            HKLM\software\wow6432node\microsoft\active setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4383}
  Opens key:
                                            HKLM\software\wow6432node\microsoft\active setup\installed
components\{9381d8f2-0288-11d0-9501-00aa00b911a5}
   Opens key:
                                            HKLM\software\wow6432node\microsoft\active setup\installed
components\{cc2a9ba0-3bdd-11d0-821e-444553540000}
  Opens key:
                                            HKLM\software\wow6432node\microsoft\active setup\installed
components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  Queries value:
                                            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
HKLM \verb|\system| current controlset| control \verb|\nls| language[install language fallback]|
   Queries value:
                                            \label{lem:hklm} \verb+kklm\+ system\+ current controlset\+ control\+ mui\+ uilanguages\+ en-us[type]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
   Queries value:
                                            {\tt HKCU \backslash control\ panel \backslash desktop[preferreduil anguages]}
   Oueries value
                                            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \software \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| side by side [preferex ternal manifest] \end{tabular}
                                            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:
   Oueries value:
                                            {\tt HKLM \ } system \verb| current control \verb| session manager[safedll search mode] \\
                                            HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:
                                            \verb|nt\currentversion| compatibility 32[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb]| and the surrentversion and the
   Queries value:
                                            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Queries value:
                                            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
                                            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Oueries value:
   Queries value:
   Queries value:
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
\verb|settings[disableimprovedzonecheck]| \\
                                            HKLM\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[security_hklm_only]
                                            HKLM\software\wow6432node\microsoft\windows\windows error
   Queries value:
reporting\wmr[disable]
   Oueries value:
                                            HKLM\svstem\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:
                                            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:
                                            HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                            \label{thm:language groups of the control language groups groups of the control language groups of the control language gr
   Oueries value:
   Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
   Queries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore v1.0[datafilepath]
                                            HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
  Oueries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
                                            HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|
   Oueries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Oueries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                                            HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
                                            HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                                            HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
                                            HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
                                            HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane11]|
                                            HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                                            HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
   Queries value:
                                            HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane15]|
  Queries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\cmf\config[system]
   Oueries value:
                                            HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
  Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
                                            HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:
   Queries value:
                                            HKLM\software\microsoft\com3[com+enabled]
                                            \label{locality} HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
   Queries value:
                                            HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
   Oueries value:
                                            HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
   Queries value:
00c04fd705a2}\inprocserver32[inprocserver32]
   Queries value:
                                            HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
```

```
00c04fd705a2}\inprocserver32[]
                                          HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
   Queries value:
00c04fd705a2}\inprocserver32[threadingmodel]
                                           HKLM\software\microsoft\ole[maxsxshashcount]
   Queries value:
   Oueries value:
                                          HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
HKLM \verb|\system| current control \verb|\computername| active computername| [computername]|
   Queries value:
                                          HKLM\system\setup[oobeinprogress]
   Oueries value:
                                           HKLM\system\setup[systemsetupinprogress]
                                           HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:
                                           Queries value
HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
   Oueries value:
   Queries value:
                                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:
                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Oueries value
                                          HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:
                                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:
                                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                           HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                          HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\\ \verb|main| featurecontrol| feature_http\_username\_password\_disable[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
   Queries value:
\label{local_ham} \begin{tabular}{ll} HKLM \end{tabular} which is a constraint of the control 
                                           HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:
   Oueries value
                                           HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
                                           HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
   Queries value:
                                           HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
   Queries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
                                           HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
   Oueries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
                                           HKCU\software\microsoft\internet explorer\main[frametabwindow]
   Queries value:
   Queries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main[frametabwindow]
   .
Queries value:
                                           HKCU\software\microsoft\internet explorer\main[framemerging]
                                           Queries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[sessionmerging]
   Oueries value:
                                          HKLM\software\wow6432node\microsoft\internet
explorer\main[sessionmerging]
                                           HKCU\software\microsoft\internet explorer\main[admintabprocs]
   Queries value:
   Queries value:
                                          HKLM\software\wow6432node\microsoft\internet
explorer\main[admintabprocs]
                                           HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
   Oueries value:
   Queries value:
                                          HKLM\software\wow6432node\microsoft\internet
explorer\main[tabprocgrowth]
                                          HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main[navigationdelay]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [no properties recyclebin] \ described a propertie of the properties \ described a propertie of the properties \ described a properties \ described \ described a properties \ described \ de
   Oueries value
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
   Oueries value
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Oueries value:
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea
08002b30309d}\shellfolder[attributes]
                                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsfordisplay]
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d \} \verb|\shellfolder[usedrophandler]|
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
                                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforoverlay]
   Queries value:
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[mapnetdriveverbs]
  Queries value:
                                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforinfotip]
   Oueries value
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideinwebview]
                                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value:
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d \verb|\shellfolder[wantsuniversaldelegate]|
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
```

08002b30309d}\shellfolder[pintonamespacetree]

```
Oueries value:
                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hasnavigationenum]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}1
   Queries value:
                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[]
                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Queries value:
08002b30309d}\inprocser
                                            ver32[loadwithoutcom]
  Queries value:
                                              HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xffff1
                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
   Queries value:
   Queries value:
                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
   Oueries value:
                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
                                              HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
   Queries value:
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:
                                              HKLM\software\wow6432node\microsoft\internet
Queries value:
                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature unc savedfilecheck[*1
   Queries value:
                                              HKLM\software\policies\microsoft\internet
explorer\security[disabl
                                             esecuritysettingscheck]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
  Queries value:
                                              \label{thm:local_equation} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
settings\zones\1[flags]
                                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\2[flags]
   Queries value:
                                              \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings\zones\3[flags]
  Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
   Queries value:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Oueries value:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Queries value:
                                              HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main\feature| a control \verb|\feature| a control \verb|\fea
  Oueries value:
                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Queries value:
                                              HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b7231
  Oueries value:
                                              HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
  Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                                               -
HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
  Queries value:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
  Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
  Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
  Queries value:
                                              \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[idnenabled]
  Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
   Queries value:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[enablehttp1_1]
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablehttp1_1]
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyhttp1.1]
   Queries value:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                              \label{thm:local_equation} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
  Queries value
settings[enablenegotiate]
Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
   Queries value:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
   .
Queries value:
                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecon
                                             ntrol[feature_clientauthcertfilter]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
  Queries value:
                                              settings[syncmode5]
  Oueries value:
                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache[signature]
  Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
                                              HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| internet | microsoft\\| windows \verb|\currentversion\\| internet | microsoft\\| windows\\| currentversion\\| internet\\| currentversion\\| curren
settings\5.0\cache\content[peruseritem]
```

Oueries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Oueries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \folds$

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \called \folder \f$

Oueries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{Constraint} \ abe-4251-ba85-6007 caed cf9d \footnote{Constraint} \ description \ description \footnote{Constraint} \ description \ description$

Oueries value:

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

Queries value:

 $HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Oueries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Queries value:

 $HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \lab$

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \called{HKLM} abe-4251-ba85-6007 caed \cf9d\cite{Grander} [icon]$

Queries value:

Queries value:

 $\label{thm:local-base-6007} HKLM \software \wow 6432 node \mbox{\scurrent} windows \current \version \explorer \folder descriptions \footnote{1} abe-4251-ba85-6007 caed \cf9d \footnote{1} stream resource]$

Queries value

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Oueries value

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Queries value:

Oueries value:

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \called{thm: descriptions} \label{thm: descriptions} \footnote{All the descriptions of the descriptions of the descriptions of the descriptions of the descriptions \called{thm: descriptions} \footnote{All the descriptions of the descriptions of the descriptions of the descriptions of the description of the desc$

Queries value

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \called{thm:linear} \label{fig:helm} \footnote{thm:linear} \label{fig:helm} Although \called{thm:linear} \label{fig:helm:linear} \footnote{thm:linear} \footnote{thm$

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \called{4352481e8-33be-4251-ba85-6007} (attributes)$

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \called{4352481e8-33be-4251-ba85-6007} \called{4352481e8-33be-4251-ba85-60$

Queries value:

 $\label{thm:mass} HKL^{M} software \now 6432 node \normalised in the label state of the$

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

Queries value: folders[cache]

6fba-4fcf-9d55-7b8e7f157091}[category]
Oueries value:

Queries value. $\label{lem:condition} $$HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[name]}$

Queries value:

 $\label{thm:hammon} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \final fields a final field of the second support \cite{thm:hammon}. The second support \cite{thm:hammon} \ci$

Queries value:

 $\label{lem:condition} $$\operatorname{KLM}\operatorname{Northware}\operatorname{Now6432}\operatorname{node}\operatorname{microsoft}\operatorname{Northware}\operatorname{Now6432}\operatorname{node}\operatorname{microsoft}\operatorname{Northware}$

Queries value:

 $\label{thm:local-ham} HK \dot{L} M software \noinder descriptions \fib 32785-65 ba-4fcf-9d55-7b \noinder \noinde$

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \final final field \current \$

Queries value:

 $\label{thm:hammon} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fifth 32785-67ba-4fcf-9d55-7b8e7f157091 \[infotip]$

Queries value:

 $\label{thm:loss} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fif1b32785-6fba-4fcf-9d55-7b8e7f157091\[] localized name]$

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \ff1b32785-6fba-4fcf-9d55-7b8e7f157091 \cite{Control of the control of$

Queries value

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fib 32785-6fba-4fcf-9d55-7b8e7f157091 \] [security]$

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fifth 32785-67ba-4fcf-9d55-7b8e7f157091 \footnote{The control of the c$

Queries value:

Queries value:

 $\label{thm:local_explorer_holder} HKL \begin{tabular}{l} MKL \begi$

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[roamable]
         Queries value:
HKLM\software\w
                                                                                                    -w6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785
6fba-4fcf-9d55-7b8e7f157091}[precreate]
         Queries value:
 6fba-4fcf-9d55-7b8e7f157091}[stream]
         Oueries value:
HKLM \label{lem:hkk} In the latest and the latest
6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
          Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[attributes]
          Queries value:
6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
          Oueries value:
HKLM \label{lem:hklm} In the latest and the lates
6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
          Oueries value:
                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[local appdata]
         Queries value:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \\ folder \\ folder \\ descriptions \\ folder \\ folder \\ descriptions \\ folder \\ folde
0e22-4760-9afe-ea3317b67173}[category]
          Queries value:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lkklm} White \label{l
0e22-4760-9afe-ea3317b67173}[name]
          Queries value:
0e22-4760-9afe-ea3317b67173}[parentfolder]
         Queries value:
 0e22-4760-9afe-ea3317b67173}[description]
          Oueries value:
HKLM \label{lem:hkk} Which was a substituted by the substitute of the substitute o
0e22-4760-9afe-ea3317b67173}[relativepath]
          Queries value:
0e22-4760-9afe-ea3317b67173}[parsingname]
          Queries value:
0e22-4760-9afe-ea3317b67173}[infotip]
          Queries value:
0e22-4760-9afe-ea3317b67173}[localizedname]
         Oueries value:
HKLM \label{lem:hkk} In the latest and the latest
0e22-4760-9afe-ea3317b67173}[icon]
         Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[security]
         Queries value:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \setminus \{5e6c858f-microsoft\} \\ if the first index \\ folder \\ descriptions \\ folder \\ folder \\ descriptions \\ folder \\ folder \\ descriptions \\ folder \\ folde
0e22-4760-9afe-ea3317b67173}[streamresource]
\label{thm:hklm:software} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 
          Queries value:
 HKLM \label{lem:hklm} While the latest and the la
0e22-4760-9afe-ea3317b67173}[localredirectonly]
         Oueries value:
 0e22-4760-9afe-ea3317b67173}[roamable]
          Oueries value:
HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} H
0e22-4760-9afe-ea3317b67173}[precreate]
          Queries value:
0e22-4760-9afe-ea3317b67173}[stream]
          Queries value:
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
          Oueries value:
0e22-4760-9afe-ea3317b67173}[attributes]
         Oueries value:
HKLM \label{lem:hkk} In the latest and the latest
0e22-4760-9afe-ea3317b67173}[foldertypeid]
         Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
          Queries value:
980053277-1733835069-2361817685-1001[profileimagepath]
                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\internet
         Queries value:
 settings\5.0\cache\content[cacheprefix]
         Queries value:
                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
         Queries value:
                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\cookies[peruseritem]
         Oueries value:
                                                                                                                                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
         Queries value:
HKLM \label{lem:hklm} White the latest and the la
c0e9-4171-908e-08a611b84ff6}[category]
         Queries value:
HKLM \label{lem:hkkk} In the large that the large
c0e9-4171-908e-08a611b84ff6}[name]
          Oueries value:
```

 $HK\`L M\ software \ wow 6432 node \ microsoft\ windows \ current version \ version \$

c0e9-4171-908e-08a611b84ff6}[parentfolder]
Queries value:

c0e9-4171-908e-08a611b84ff6}[description]

Queries value:

c0e9-4171-908e-08a611b84ff6}[relativepath]

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ c0e9-4171-908e-08a611b84ff6}[parsingname]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[infotip]

Queries value:

c0e9-4171-908e-08a611b84ff6}[localizedname]

c0e9-4171-908e-08a611b84ff6}[icon]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[security]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[streamresource]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[streamresourcetype]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[localredirectonly]

c0e9-4171-908e-08a611b84ff6}[roamable]

Queries value:

c0e9-4171-908e-08a611b84ff6}[precreate]

Queries value:

c0e9-4171-908e-08a611b84ff6}[stream]

Oueries value:

 $HKLM \label{limits} Which was considered as the constant of the constant of$ c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]

Queries value:

c0e9-4171-908e-08a611b84ff6}[attributes]

c0e9-4171-908e-08a611b84ff6}[foldertypeid]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[initfolderhandler]

Oueries value: folders[cookies] Queries value:

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

65f9-4cf6-a03a-e3ef65729f3d}[category]

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lkklm} White$ 65f9-4cf6-a03a-e3ef65729f3d}[name]

Queries value:

 $HKLM \label{lem:hklm} While the latest and the la$ 65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]

Oueries value:

 $\label{thm:hklm} HKL^{M} software \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| {3eb685db-plane} and the statement of the statemen$ 65f9-4cf6-a03a-e3ef65729f3d}[description]

Oueries value:

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

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[parsingname]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[infotip]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-10ex, 10ex, 10ex,$ 65f9-4cf6-a03a-e3ef65729f3d}[localizedname]

Oueries value:

 $HKLM \label{lem:hkkkk} Which was current version \explorer \folder descriptions \folder \fo$ 65f9-4cf6-a03a-e3ef65729f3d}[icon]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[streamresource]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

Queries value:

 $HKLM \label{lem:hklm} While the latest and the la$ 65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]

Oueries value:

 $\label{thm:hklm} HKL^{M} software \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| {3eb685db-properties of the context of the co$ 65f9-4cf6-a03a-e3ef65729f3d}[roamable]

Oueries value:

 $HKLM \label{lem:hklm} In the latest and the lates$ 65f9-4cf6-a03a-e3ef65729f3d}[precreate]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[stream]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-10ex, 10ex, 10ex,$

```
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
     Queries value:
 \label{thm:hklm} HKL^{M} software \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| {3eb685db-plane} and the statement of the statemen
 65f9-4cf6-a03a-e3ef65729f3d}[attributes]
      Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
      Queries value:
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
      Queries value:
 folders[appdata]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
 settings\5.0\cache\cookies[cacheprefix]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
     Oueries value:
                                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                                                                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
     Queries value:
 settings\5.0\cache\history[peruseritem]
     Oueries value:
 HK LM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d6der \ descriptions\} \ descriptions \ descriptions
b784-432e-a781-5a1130a75963}[category]
     Oueries value:
 HK \dot{L} M \land software \land wow 6432 node \land microsoft \land windows \land current version \land explorer \land folder descriptions \land \{d9 dc8 a 3b-d1 a 2b-d1 a 2b
b784-432e-a781-5a1130a75963}[name]
      Oueries value:
b784-432e-a781-5a1130a75963}[parentfolder]
b784-432e-a781-5a1130a75963}[description]
     Queries value:
b784-432e-a781-5a1130a75963}[relativepath]
     Queries value:
 b784-432e-a781-5a1130a75963}[parsingname]
     Oueries value:
HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HKL
b784-432e-a781-5a1130a75963}[infotip]
     Queries value:
b784-432e-a781-5a1130a75963}[localizedname]
b784-432e-a781-5a1130a75963}[icon]
      Oueries value:
HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} H
b784-432e-a781-5a1130a75963}[security]
     Oueries value:
 HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d8dc8a3b-d
b784-432e-a781-5a1130a75963}[streamresource]
     Oueries value:
 b784-432e-a781-5a1130a75963}[streamresourcetype]
      Oueries value:
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[localredirectonly]
      Queries value:
b784-432e-a781-5a1130a75963}[roamable]
     Queries value:
b784-432e-a781-5a1130a75963}[precreate]
     Queries value:
 b784-432e-a781-5a1130a75963}[stream]
      Oueries value:
b784-432e-a781-5a1130a75963}[publishexpandedpath]
      Oueries value:
b784-432e-a781-5a1130a75963}[attributes]
b784-432e-a781-5a1130a75963}[foldertypeid]
      Oueries value:
b784-432e-a781-5a1130a75963}[initfolderhandler]
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
      Oueries value:
 folders[history]
                                                                           \label{thm:local_hammon_hammon} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \ .
     Queries value:
Settings\5.0\cache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\history[cachelimit]
     Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
     Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\domstore[cachepath]
     Oueries value:
                                                                           \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
     Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\domstore[cachelimit]
     Oueries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
     Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings \verb|\5.0| cache \verb|\extensible| cache \verb|\feedplat[cacherepair]|
     Oueries value:
                                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
```

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

```
Oueries value
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
                                   sible cache\feedplat[cacheoptions]
settings\5.0\ca
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                                    {\tt HKCU \ } \dot{software \ } \dot{microsoft \ } vindows \ \\ current version \ \\ internet
  Queries value
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                                    HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\5.0| cache \verb|\extensible| cache \verb|\ietld[cacherepair]|
  Oueries value
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value
{\tt settings\5.0\cache\extensible\ cache\ietld[cacheprefix]}
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries 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]
  Queries value
                                   \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache
                                   sible cache\privacie:[cacheprefix]
  Oueries value
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Oueries value
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
                                    \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \part that the lemma is a simple of the lemma is
  Queries value
settings[displayscriptdownloadfailureui]
  Oueries value:
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
  Queries value:
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
                                   -
HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[utf8servernameres]
                                   HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[disableworkerthreadhibernation]}
  Oueries value:
                                   HKLM\software\wo
                                                             6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value
                                   HKCU\software\microsoft\windows\currentversion\internet
Queries value: Settings[disablereadrange]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
                                   \label{thm:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings[socketreceivebufferlength]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[keepalivetimeout]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxcon
                      nectionsperserver]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[maxco
  Oueries value
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
                                   erproxy]
settings[maxcor
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[connecttimeout]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
  Queries value
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelo
                                   werbound]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[certcachenovalidate]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[scavengecachefilelifetime]
  Oueries value:
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
                                   ngecachefilelimit]
settings\5.0\cache[scave
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[httpdefaultexpirytimesecs]
```

```
Oueries value
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:
                                        HKLM\software\wow6432node\microsoft\internet
                                        trol\feature_disable_unicode_handle_closing_callback[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
explorer\main\t
  Oueries value:
                                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:
                                        \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[leashlegacycookies]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value
settings[dialupuselansettings]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[wpadsearchall domains]}
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[bypasshttpnocad
                                        necheck]
  Queries value:
                                        HKLM\soft
                                                         ware\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypass
                         sslnocachecheck]
  Queries value:
                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                                        Queries value:
settings[dontusednsloadbalancing]
  Oueries value:
                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:
                                        \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[mimeexclusionlistforcache]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[dnscacheenabled]}
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscacheentries]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpost]
                                        \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version} \end{tabular} \label{thm:local_hammon_hammon}
  Queries value:
settings[warnalwaysonpost]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonzonecrossing]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonbadcertrecving]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredin
                                       ect]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[a]waysdrainonredirect]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonhttpstoht
                                        tpredirect]
  Oueries value:
                                        HKLM\software\wow6432node\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 \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [serial\_access\_num] \ pr
  Oueries value:
Oueries value:
Queries value:
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \code 000000000002 \[packed catalogitem] \end{subarray} \label{lem:lem:hklm}
  Oueries value:
HKL\label{lem:hklm} HKL\label{lem:hklm} HKL\label{lem:hklm} With the same ters \protocol\_catalog9 \catalog\_entries \000000000003 \packed \catalogitem] and the same term \protocol\_catalog9 \catalog\_entries \protocol\_catalog \pr
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000008[packedcatalogitem]
  Queries value:
Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
```

Oueries value

 $HKLM \ system \ current controls et \ services \ \ winsock \ 2 \ parameters \ namespace_catalog \ \ catalog_entries \ \ 000000000001 \ [displaystring]$ Queries value:

HKLM\system\cur entcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid] Oueries value:

 $HKLM \ system \ current controls et \ services \ \ winsock \ 2 \ parameters \ namespace_catalog5 \ \ catalog_entries \ \ 000000000001 \ [address family]$ Queries value:

Oueries value:

Queries value:

Oueries value:

 $HKLM \label{lem:hklm} White \label{lem:hklm} Hklm \label{lem:hklm} White \label{lem:hklm} Hklm \label{lem:hklm} White \label{lklm} White \label$

Oueries value:

Queries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ (catalog_entries \ 000000000002 \ [providerid]]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily] Oueries value:

 $HKLM \system \current control set \services \winsock 2 \parameters \name space_catalog \scatalog_entries \name space]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Queries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ \ namespace_catalog5 \ \ catalog_entries \ \ \ 0000000000002[storesserviceclassinfo]$ Queries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 000000000003 [library path]) \ details a simple of the system \ details and the system \ details a simple of the$ Queries value:

Oueries value:

 $HKL\\ M\system\current controls et\services\winsock2\parameters\namespace_catalog5\catalog_entries\space_id] For instance, and the sum of the$ Queries value:

Oueries value:

Queries value:

Oueries value:

 $HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ name space \\ catalog \\ services \\ winsock \\ 2 \\ parameters \\ name space \\ catalog \\ services \\ winsock \\ 2 \\ parameters \\ name space \\ catalog \\ services \\ winsock \\ 2 \\ parameters \\ name space \\ catalog \\ services \\ winsock \\ 2 \\ parameters \\ name space \\ catalog \\ services \\ winsock \\ 2 \\ parameters \\ name space \\ catalog \\ services \\ winsock \\ 2 \\ parameters \\ name space \\ catalog \\ services \\ name space \\ catalog \\ services \\ name space \\ catalog \\ services \\ name space \\ name$ Queries value:

Oueries value:

Queries value:

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

Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ set alog_entries \ (0000000000004 [providerid]) \ details \$

Queries value:

Oueries value

Queries value:

HKLM\system\cur rentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled] Oueries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ (catalog_entries \ 000000000005 \ [displaystring]$

Oueries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ (catalog_entries \ 000000000005 \ [address family]$

Queries value:

Oueries value:

 $HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ name space_catalog_entries \\ 00000000000005[enabled]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version] Queries value:

Queries value:

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

Oueries value:

 $HKLM \ system \ current controls et \ services \ \ win sock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ \ 000000000006 \ [displaystring]$ Queries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ \ winsock \ 2 \ parameters \ namespace_catalog5 \ \ catalog_entries \ \ 0000000000006 \ [address family]$ Queries value:

 $HKLM \system \current controls et \services \winsock 2 \parameters \name space_catalog \scatalog_entries \name space]$

Oueries value: $HKL\\ M\system\current control set\services\winsock2\parameters\namespace_catalog5\catalog_entries\space_catalog5\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog$

Oueries value $HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ names pace_catalog5 \ \ catalog_entries \ \ 0000000000006 \ [storesserviceclassinfo]$ Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadoverride] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial] Queries 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] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[disablebranchcache] HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing] Queries value: Queries value: $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus rasapi32 [enable file tracing]$ $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus rasapi32[filetracing mask]$ Oueries value: Queries value: $\label{local-equation} HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| tracing\\| rasapi 32[enable consoletracing]|$ Oueries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[consoletracingmask] HKLM\software\wow6432node\microsoft\tracing\rasapi32[maxfilesize] Queries value: Queries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[filedirectory] Queries value: $\label{lem:hklmsoftware} \verb| HKLM \| software \| wow 6432 node \| microsoft \| tracing \| rasmancs \| [enable file tracing] | lem to the lem t$ Oueries value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[filetracingmask] Queries value: $HKLM \verb|\software| wow 6432 node \verb|\microsoft| tracing \verb|\rasmancs| [enable consoletracing]|$ Oueries value: $\label{lem:hklm} \verb+Kklm\+ software\+ wow 6432 node\+ microsoft\+ tracing\+ rasmancs\+ [consoletracing mask]$ HKLM\software\wow6432node\microsoft\tracing\rasmancs[maxfilesize] Queries value: Queries value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[filedirectory] HKLM\software\microsoft\windows Queries value: nt\currentversion\profilelist[programdata] Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[2ac077a7] Queries value: $HKLM \verb|\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]|$ Oueries value: Queries value: $HKLM \setminus system \setminus current control \setminus sqmservice list[sqmservice list]$ Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxysettingsperuser] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxvoverride] Oueries value HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings] Queries value: HKCU\software\microsoft\windows\currentversion\internet ${\tt settings} \verb|\connections[defaultconnectionsettings]|\\$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zonemap[autodetect] Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} System \current control set \end{tabular} set \color= \color=$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall1] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value:

 $\label{thm:local_control} \begin{tabular}{ll} HKLM \end{tabular} A which is a parameter of the control of the$

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

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

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

Queries value:

Queries value:

```
Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
HKLM \verb|\system| current control set \verb|\services| dns cache \verb|\parameters[register primary name]|
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration refreshinterval]
   Queries value:
Queries value:
Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update to plevel domain zones]
  Oueries value:
Queries value:
HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[registration overwrite]|
   Oueries value:
                                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Queries value:
                                          HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Oueries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
Oueries value:
                                         HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set \current control set \cur
   Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Queries value:
HKLM \verb|\system| current control set \verb|\services| dns cache \verb|\parameters[use new registration]|
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Queries value
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [resolver registration only]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
   Queries value:
{\tt HKLM \ } system \ \verb| current control set \ \verb| services \ \verb| tcpip \ \verb| parameters [dnsquery time outs]|
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
                                         HKCU\software\microsoft\internet explorer[no3dborder]
                                         HKLM\software\wow6432node\microsoft\internet explorer[no3dborder]
   Oueries value:
   Oueries value:
                                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:
                                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
   Queries value:
                                         HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_mime_handling[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| the first of the
                                         HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_mime_handling[*]
   Queries value:
                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[]
                                         HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[compatible]
                                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[compatible]
  Queries value:
                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
                                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[version]
```

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet\+ settings [user the continuous] and the continuous con$

```
agent 1
   Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
                                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\user agent[platform]
                                                    HKLM\software\wow6432node\microsoft\internet
   Queries value:
Queries value:
                                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
    .
Queries value:
                                                    HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|main| featurecontrol| feature\_maxconnectionsperserver[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
    Queries value:
                                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature maxconnectionsperserver[*]
                                                    HKLM\software\wow6432node\microsoft\internet
    .
Queries value:
explorer\\ \verb|main| featurecontrol| feature\_maxconnectionsper1\_0server\\ [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Queries value:
                                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature maxconnectionsper1 Oserver[*1
                                                    HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    Oueries value:
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                                                    HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\winsock\setup
    Queries value:
migration\providers\tcpip[winsock 2.0 provider id]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
   Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} a meters \end{tabular} is a substitution of the local parameters \end{tabular} and the local parameters \end{tabular} is a substitution of the local parameters \end{tabular} and the local parameters \end{tabular} is a substitution of the local parameters \end{tabular} and the local parameters \end{tabular} and the local parameters \end{tabular} is a substitution of the local parameters \end{tabular} and the local parameters \end{tabular
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
   Queries value:
                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
                                                    \label{thm:cu} \parbox{$\tt HKCU\software\microsoft\internet explorer\international[acceptlanguage]} \parbox{$\tt HKCU\software\microsoft\internet explorer\simes and $\tt Internet\simes and $\tt Internet\
    Queries value:
    Oueries value:
                                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                                    HKLM\software\wow6432node\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
   Oueries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
                                                    {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  winsock \verb|\  setup | \\
    Queries value:
migration\providers\tcpip6[winsock 2.0 provider id]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Oueries value:
\label{local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} winsock [used elayed acceptance] \\ \end{tabular}
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ autocomplete [autosuggest]
    Oueries value
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[a]ways use tabl
   Queries value:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lkm} Whi
    Oueries value:
                                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
                                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
    Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
    Queries value:
                                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
   Queries value:
e1e01c1f69b5}[searchlist]
                                                    HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
   Oueries value:
                                                    HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
    Oueries value:
9fe3c77a297a}\inprocserver32[inprocserver32]
                                                   HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
   Queries value:
9fe3c77a297a}\inprocserver32[]
                                                    HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
    Oueries value:
9fe3c77a297a}\inprocserver32[threadingmodel]
    Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\explorer\runmru[mru]istl
    Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
                                                    HKCU\software\microsoft\windows\currentversion\explorer\runmru[d]
    Queries value:
    Queries value:
                                                    \label{thm:constant} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \runmru[c] \end{tabular}
                                                    HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
    Oueries value:
                                                    HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
    Queries value:
    Queries value:
                                                    HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                                    HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
   Oueries value:
00c04fd7d062}\inprocserver32[]
                                                    HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
    Queries value:
Occ04fd7d062}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
    Queries value:
                                                    HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                                   HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
   Oueries value:
00c04fd7d062}\inprocserver32[]
                                                    HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
```

00c04fd7d062}\inprocserver32[threadingmodel]

```
Oueries value:
                                                             HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[]
    Queries value:
                                        w6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
HKLM\software\w
                                                             HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
    Oueries value:
                                                             HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
    Queries value:
                                                             HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
    Queries value:
b61bb7cdd997}\inprocserver32[inprocserver32]
                                                             HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
    Oueries value:
b61bb7cdd997}\inprocserver32[]
                                                             HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
    Oueries value:
                                                             HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                                                             HKCU\control panel\desktop[smoothscroll]
    Queries value:
    Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [enable balloon tips]
    Oueries value:
\label{thm:culsoftware} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [list viewal phase lect] \end{tabular}
HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus explorer \setminus advanced [list views hadow]
    Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [acclist viewv6]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
   Queries value:
e1e01c1f69b5}[enabledhcp]
   Oueries value:
e1e01c1f69b5}[registrationenabled]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registeradaptername]
    Queries value:
Queries value:
e1e01c1f69b5}[dhcpdomain]
    Queries value:
e1e01c1f69b5}[dhcpv6domain]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[nameserver]
    Queries value:
e1e01c1f69b5}[nameserver]
    Queries value:
e1e01c1f69b5}[dhcpnameserver]
    Oueries value:
\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ HKLM \end{tabular} $$ 11de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9d20-1de-9
806e6f6e6963}[enabledhcp]
   Queries value:
806e6f6e6963}[registrationenabled]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registeradaptername]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[dhcpdomain]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus trip \setminus parameters \setminus interfaces \setminus \{846ee342-7039-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d
806e6f6e6963}[nameserver]
   Queries value:
806e6f6e6963}[dhcpnameserver]
    Oueries value:
                                                             HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
    Queries value:
e1e01c1f69b5}[queryadaptername]
   Oueries value:
e1e01c1f69b5}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[maxnumberofaddressestoregister]
    Queries value:
e1e01c1f69b5}[enablemulticast]
   Queries value:
\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} \textbf{NSystem} \correct control set \end{tabular} $$ 1 de-9d20-1 de-9d20
806e6f6e6963}[queryadaptername]
   Oueries value:
\label{thm:local_hklm} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$
806e6f6e6963}[disableadapterdomainname]
    Oueries value:
806e6f6e6963}[disabledynamicupdate]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enableadapterdomainnameregistration]
```

```
806e6f6e6963}[registrationmaxaddresscount]
      Queries value:
 \label{thm:local_hklm} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$
 806e6f6e6963}[maxnumberofaddressestoregister]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
 806e6f6e6963}[enablemulticast]
      Queries value:
                                                                              HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[searchlist]|
                                                                              HKCU\software\microsoft\windows\currentversion\internet
      Oueries value:
 settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
      Queries value:
                                                                              HKCU\software\microsoft\windows\currentversion\internet
 settings[privacyadvanced]
      Oueries value:
                                                                              HKCR\mime\database\content type\text/html[extension]
       Queries value
                                                                               HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_mime_sniffing[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| to the feature of the fea
Queries value: HKLM\software\wow6432node\mi explorer\main\featurecontrol\feature_mime_sniffing[*]
                                                                              HKLM\software\wow6432node\microsoft\internet
                                                                              HKCU\software\microsoft\windows\currentversion\internet
       Oueries value:
 settings[istextplainhonored]
     Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_feeds[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                                                               HKLM\software\wow6432node\microsoft\internet
       Queries value:
 explorer\main\featurecontrol\feature_feeds[*]
                                                                              HKLM\software\wow6432node\microsoft\internet
      Oueries value:
 explorer\main\featurecontrol\feature_safe_bindtoobject[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
      Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]

Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
       Queries value:
                                                                               HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
       Queries value:
                                                                               HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
00aa00686f13}\inprocserver32[inprocserver32]
                                                                              HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
     Queries value:
 00aa00686f13}\inprocserver32[]
                                                                              HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
      Queries value
OOaaOO686f13}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\microsoft\internet
 explorer\\ \verb|main| featurecontrol| feature_legacy_dispparams [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
      Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
 explorer \verb|\main| featurecontrol| feature\_object\_caching [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| feature\_object\_caching [62ddfbf757be511f30b6d330963c1345e8bef0774bb.exe]| feature\_object\_caching [62ddfbf757be511f30b6d330963c134bef0774bb.exe]| feature\_object\_caching [62ddfbf757bef07b]| feature\_object\_caching [62ddfbf757bef07bef07bef07bb]| feature\_object\_caching [62ddfbf757bef07bef07bb]| feature\_object\_caching [62ddfbf757bef07bef07bef07bef07bef07bef07bef07be
      Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_object_caching[*]
                                                                               HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
       .
Queries value:
       Queries value:
                                                                               HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-
91a2-7b624e0e7244]
                                                                              HKLM\software\wow6432node\microsoft\internet explorer\application
     Oueries value:
 compatibility[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
      Queries value:
                                                                              HKCU\software\microsoft\internet explorer\domstorage[totallimit]
      Queries value:
                                                                               HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
                                                                              HKCU\software\microsoft\windows
      Oueries value:
 nt\currentversion\windows[dragscrollinset]
      Queries value:
                                                                              HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
      Queries value:
                                                                              HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| internet|
 explorer\main\featurecontrol\feature_restrict_filedownload[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                                                              HKLM\software\wow6432node\microsoft\internet
      .
Queries value:
 explorer\main\featurecontrol\feature_restrict_filedownload[*]
      Oueries value:
                                                                              HKCR\protocols\handler\about[clsid]
                                                                              HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
      Queries value:
                                                                               HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
      Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                                                                              HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
      Oueries value:
00aa00bdce0b}\inprocserver32[]
     Queries value:
                                                                              HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
                                                                              HKLM\software\wow6432node\microsoft\internet
     Oueries value:
\verb|exp|| or the first of the f
                                                                              HKLM\software\wow6432node\microsoft\internet
      Queries value:
 explorer\main\featurecontrol\feature_protocol_lockdown[*]
     Oueries value:
                                                                              HKCU\software\microsoft\windows\currentversion\internet
 settings\zones\3[2106]
       Queries value:
                                                                               HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
      Queries value:
                                                                              HKLM\software\wow6432node\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]
      Queries value:
                                                                               HKCU\software\microsoft\internet explorer[rtfconverterflags]
                                                                               HKCU\software\microsoft\internet explorer\main[usecleartype]
      Oueries value:
                                                                               HKCU\software\microsoft\internet explorer\main[page_transitions]
       Queries value:
      Queries value:
                                                                               \label{localization} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main[use\_dlgbox\_colors]}} \label{localization}
                                                                              HKCU\software\microsoft\internet explorer\main[anchor underline]
HKCU\software\microsoft\internet explorer\main[css_compat]
      Queries value:
      Queries value:
                                                                               HKCU\software\microsoft\internet explorer\main[expand alt text]
       Queries value:
       Queries value:
                                                                               HKCU\software\microsoft\internet explorer\main[display inline images]
                                                                              \label{thm:local-hkcu} HKCU \ software \ microsoft \ internet\ explorer \ main[display\ inline\ videos] \ HKLM \ software \ wow 6432 node \ microsoft \ internet\ explorer \ main[display\ inline\ videos] \ display\ microsoft \ micros
      Oueries value:
      Queries value:
  inline videos]
       Queries value:
                                                                               \label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main[play\_background\_sounds]}} \label{local-operator}
                                                                              HKCU\software\microsoft\internet explorer\main[play_animations]
HKCU\software\microsoft\internet explorer\main[print_background]
      Queries value:
       Queries value:
       Queries value:
                                                                               HKCU\software\microsoft\internet explorer\main[use stylesheets]
                                                                              HKCU\software\microsoft\internet explorer\main[smoothscroll]
HKCU\software\microsoft\internet explorer\main[xmlhttp]
       Oueries value:
      Queries value:
       Queries value:
                                                                               HKCU\software\microsoft\internet explorer\main[show image placeholders]
       Queries value:
                                                                               HKCU\software\microsoft\internet explorer\main[disable script debugger]
                                                                              HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie] HKCU\software\microsoft\internet explorer\main[move system caret]
       Oueries value:
       Queries value:
                                                                               HKCU\software\microsoft\internet explorer\main[force offscreen
      Queries value:
```

composition]

```
Oueries value:
                                                                  HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
                                                                  HKCU\software\microsoft\internet explorer\main[usethemes]
    Queries value:
     Queries value:
                                                                  HKCU\software\microsoft\internet explorer\main[usehr]
                                                                  HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[q300829]
     Queries value:
                                                                 HKCU\software\microsoft\internet explorer\main[cleanup htcs]
HKCU\software\microsoft\internet explorer\main[xdomainrequest]
     Oueries value:
    Queries value:
                                                                  HKLM\software\wow6432node\microsoft\internet
     Queries value:
explorer\main[xdomainrequest]
                                                                 HKCU\software\microsoft\internet explorer\main[domstorage]
    Oueries value:
                                                                  HKCU\software\microsoft\internet
    Queries value:
explorer\international[default_codepage]
    Queries value:
                                                                 HKCU\software\microsoft\internet explorer\international[autodetect]
                                                                 HKCU\software\microsoft\internet
    Oueries value:
explorer\international\scripts[default_iefontsizeprivate]
                                                                  HKCU\software\microsoft\internet explorer\settings[anchor color]
     Queries value:
                                                                 HKCU\software\microsoft\internet explorer\settings[anchor color visited] HKCU\software\microsoft\internet explorer\settings[anchor color hover]
    Queries value:
    Oueries value:
     Oueries value:
                                                                  HKCU\software\microsoft\internet explorer\settings[always use my colors]
    Queries value:
                                                                  HKCU\software\microsoft\internet explorer\settings[always use my font
size]
    Oueries value:
                                                                 HKCU\software\microsoft\internet explorer\settings[always use my font
face]
    Queries value:
                                                                  \label{thm:condition} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\sc disable visited}} \\
hyperlinks]
    Queries value:
                                                                  HKCU\software\microsoft\internet explorer\settings[use anchor hover
color]
    Queries value:
                                                                 \label{local-operator} \mbox{HKCU\software\mbox{\sc miscflags}]} \mbox{\sc miscflags} \mbox
    Oueries value:
                                                                 HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
    Queries value
                                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
    Queries value:
settings[disablecachingofsslpages]
                                                                  HKCU\software\microsoft\internet explorer\pagesetup[print_background]
     Queries value:
     Oueries value:
                                                                  HKLM \verb|\system| current controlset \verb|\control| nls \verb|\codepage[950]|
                                                                 HKCU\software\microsoft\internet
    Queries value:
explorer\international\scripts\3[iefontsize]
    Queries value:
                                                                 HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
                                                                 HKCU\software\microsoft\internet
    Queries value:
explorer\international\scripts\3[iepropfontname]
    Queries value:
                                                                 HKCU\software\microsoft\internet
explorer\international\scripts\3[iefixedfontname]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\internet explorer\version
 vector[vml]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\internet explorer\version vector[ie]
    Oueries value:
                                                                 HKLM\software\wow6432node\microsoft\internet explorer\version
vector[windowsedition]
    Queries value:
                                                                  HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| feature| control \verb|\feature| cone_elevation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| the first of 
                                                                 HKLM\software\wow6432node\microsoft\internet
    Oueries value:
explorer\main\featurecom
                                                                 trol\feature_zone_elevation[*]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\internet
 \begin{array}{lll} \text{explorer} & \text{main} & \text{featurecontrol} & \text{feature} & \text{xssfilter} & \text{feature} & \text{ssfilter} & \text{feature} & \text{ssfilter} & \text{feature} &
explorer\main\featurecontrol\feature_xssfilter[*]
    Queries value:
                                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
                                                                  HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
    Queries value:
                                                                  HKLM\software\wow6432node\microsoft\internet explorer\low
     Queries value
\verb|rights[protected mode off for all zones]|\\
    Oueries value:
                                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[icon]
    Queries value:
                                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0[minlevel]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0[recommendedlevel]
    Queries value:
                                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[currentlevel]
    Queries value:
                                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[icon]
    Queries value:
                                                                 HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| internet | microsoft\\| windows \verb|\currentversion\\| internet | microsoft\\| windows\\| currentversion\\| internet\\| currentversion\\| curren
settings\zones\1[minlevel]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1[recom
                                                                 ndedlevel]
    Queries value:
                                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[currentlevel]
    Queries value:
                                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[2500]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1[2500]
    Queries value:
                                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[icon]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[minlevel]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[recom
                                                                 ndedlevel]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\zones\2[currentlevel]
    Queries value:
                                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[2500]
    Oueries value:
                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[2500]
    Queries value:
                                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[icon]
    Queries value:
                                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[minlevel]
                                                                  Queries value:
settings\zones\3[recom
                                                                 ndedlevel1
    Queries value:
                                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[currentlevel]
                                                                  HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
```

```
settings\zones\3[2500]
                                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
    Queries value:
settings\zones\3[2500]
    Queries value:
                                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[icon]
                                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
    Queries value:
settings\zones\4[minlevel]
    Queries value:
                                                                              HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| internet
settings\zones\4[recommendedlevel]
    Queries value:
                                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[currentlevel]
    Queries value:
                                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[2500]
    Queries value:
                                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4[2500]
    Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature mshtml autoload ieframe[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exel
                                                                              HKLM\software\wow6432node\microsoft\internet
      Oueries value:
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
    Queries value:
                                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
    Queries value:
settings[cointernetcombineiuricachesize]
                                                                              HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[cointernetcombineiuricachesize]
                                                                              HKLM\software\wo
                                                                                                                                      6432node\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                                                                              HKLM\software\wow6432node\microsoft\internet
    Queries value:
explorer \verb|\main| featurecontrol \verb|\feature_subdownload_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                                                              HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
\verb|explorer\main\featurecontrol\feature_subdownload_lockdown[*]|
                                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
    Queries value:
settings[securityidiuricachesize]
                                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
     Queries value:
settings[securityidiuricachesize]
                                                                              HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[securityidiuricachesize]
    Queries value:
                                                                              HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| internet | microsoft\\| windows \verb|\currentversion\\| internet | microsoft\\| windows\\| currentversion\\| internet\\| currentversion\\| curren
settings[securityidiuricachesize]
    Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| feature control| feature \verb|\solux| [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| for the first of the 
    Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature sslux[*]
     .
Queries value:
                                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
    Queries value:
                                                                              \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Software \begin{tabular}{ll} PKCU \label{thm:local_hammon} Software \begin
settings[warnonintranet]
     Queries value:
                                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
                                                                              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
     Queries value:
                                                                              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
     Oueries value:
 f4ceaaf59cfc}\inprocserver32[inprocserver32]
     Queries value:
                                                                              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[]
    Queries value:
                                                                              HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
 f4ceaaf59cfc}\inprocserver32[threadingmodel]
     Queries value:
                                                                              \label{lem:hkcrwow6432} HKCR\wow6432 node \clsid \f414c260-6ac0-11cf-b6d1-00aa00bbbb58 \progid[]
                                                                              HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
     Oueries value:
                                                                              HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1
     Queries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
     Oueries value:
                                                                              HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[]
    Queries value:
                                                                              HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
     Oueries value:
                                                                              HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
     Queries value:
                                                                              HKLM\software\microsoft\ole[defaultaccesspermission]
      Queries value:
                                                                              HKLM \setminus system \setminus current control \setminus lsa[everyone includes an onymous]
      Queries value:
HKLM \label{lem:hklm} In the large that the large
provider[type]
     Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{l
provider[image path]
    Queries value:
                                                                              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                                                              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
     Queries value:
                                                                              HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
     Oueries value:
      Oueries value:
                                                                              HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
      Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privkey cachepurge interval seconds]
                                                                              \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ in $\mathbb{Z}_{\mathbb{R}} $$ is the seconds $$] $$
     Oueries value:
                                                                              HKLM\software\microsoft\cryptography[machineguid]
      Oueries value:
                                                                              HKCR\wow6432node\interface\{00000134-0000-0000-c000-
      Queries value:
000000000046}\proxystubclsid32[]
     Queries value:
                                                                              HKLM\software\microsoft\rpc\extensions[remoterpcdll]
                                                                              HKCU\software\microsoft\internet explorer\recovery[autorecover]
      Queries value:
     Queries value:
                                                                              explorer \verb|\main| feature control \verb|\feature| scripturl\_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                                                              HKLM\software\wow6432node\microsoft\internet
     .
Queries value:
explorer\main\featurecor
                                                                            trol\feature_block_lmz_img[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
     Oueries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
     Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| feature method feature method feature fea
Queries value: HKLM\software\wow6432nodexplorer\main\featurecontrol\feature_behaviors[*]
                                                                              HKLM\software\wow6432node\microsoft\internet
     Queries value:
                                                                              HKLM\software\wow6432node\microsoft\internet explorer\default
behaviors[homepage]
                                                                              HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]
     Oueries value:
                                                                              HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[]
      Queries value:
                                                                              HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
```

00aa00bdce0b}\inprocserver32[inprocserver32]

```
Oueries value:
                                                                                          HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[]
      Queries value:
                                                                                          HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
                                                                                          HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]
      Oueries value:
                                                                                          HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]
      Queries value:
                                                                                           HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
       Queries value:
dc030521aabd}\inprocserver32[inprocserver32]
                                                                                          HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
     Oueries value:
dc030521aabd}\inprocserver32[]
      Queries value
                                                                                          HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[threadingmodel]
                                                                                          HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[]
      Oueries value:
                                                                                           HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
       Queries value:
3c8b00c10000}\inprocserver32[inprocserver32]
     Queries value:
                                                                                          HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[1
      Oueries value:
                                                                                          HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[threadingmodel]
     Queries value:
                                                                                          HKLM\software\wow6432node\microsoft\internet explorer\default
behaviors[dxtfilterbehavior]
       Queries value
                                                                                           HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]
      Oueries value:
                                                                                          HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[inprocserver32]
     Queries value:
                                                                                          HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[]
      Oueries value:
                                                                                          HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
                                                                                          HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
      Queries value:
       Queries value:
                                                                                           HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current version [device path]
      Oueries value:
                                                                                          HKLM\hardware\devicemap\video[maxobjectnumber]
                                                                                          HKLM\hardware\devicemap\video[\device\video3]
      Queries value:
      Queries value:
                                                                                           HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-
1e1a187c13e9}\0000[pruningmode]
      Oueries value:
                                                                                           HKLM\hardware\devicemap\video[\device\video0]
                                                                                          Queries value:
9dd4432fa2e9}\0000[pruningmode]
      Queries value:
                                                                                           HKLM\hardware\devicemap\video[\device\video1]
                                                                                          Oueries value:
Od8e74595f78}\0000[pruningmode]
      Queries value:
                                                                                           HKLM\hardware\devicemap\video[\device\video2]
      Queries value:
                                                                                          8ed0c8eb59a8}\0000[pruningmode]
      Queries value:
                                                                                           HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![name]
                                                                                           Queries value:
      Queries value:
                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![id]
      Oueries value:
HKLM \label{limits} \label{limits} HKLM \label{limits} HKLM \label{limits} Wow 6432 node \mbox{$\operatorname{microsoft}$ directdraw \compatibility \demolition derby 2 [name] } \label{limits} The limits \mbox{$\operatorname{M}$ is a simple of the limits of the l
      Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2[flags]
     Oueries value:
HKLM \label{limits} \label{limits} HKLM \label{limits} HKLM \label{limits} A software \label{limits} Wow 6432 node \label{limits} in the limit \label{limits} If the limit \label{limits} is a software \label{limits} \label{limits} HKLM \label{limits} \label{limits} Software \label{limits} Wow 6432 node \label{limits} \label{limits} Wow 6432 node \label{limits} A software \label{limits} Wow 6432 node \label{limits} \label{limits} Wow 6432 node \label{limits} Wow 6432 node \label{limits} Wow 6432 node \label{limits} Wow 6432 node \label{limits} \label{limits} Wow 6432 node \label{limits} Wo
      Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[name]
     Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[flags]
      Queries value:
                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[id]
      Oueries value:
\label{thm:local_hamma} \begin{tabular}{ll} HKLM \end{tabular} Software \wow 6432 node \end{tabular} note that the local compatibility \end{tabular} which is the local compatibility \end{tabular} and the local compatibility \end{tabular} which is the local compatibility \end{tabular} and the local compatibility \end{tabular} which is the local compatibility \end{tabular} and the local compatibility \end{tabular} which is the local compatibili
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[flags]
     Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} software \wow 6432 node \microsoft \direct draw \compatibility \mortal kombat 3 [id] \end{tabular}
      Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\msgolf98[name]
     Queries value:
HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| directdraw\\| compatibility\\| msgolf98[flags]|
      Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[id]
     Queries value:
HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| direct draw \verb|\compatibility\\| nhl power play [name] | line | li
     Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[flags]
      Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[id]
      Queries value:
Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
     Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\nortonsvsteminfo[id]
                                                                                           HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
      Oueries value:
squadron[name]
     Queries value:
                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron[flags]
      Queries value:
                                                                                           HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron[id]
     Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[name]
      Queries value:
HKLM \verb|\software| wow 6432 node \verb|\microsoft| direct draw| compatibility \verb|\savage| [flags]|
                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[id]
      Oueries value:
       Queries value
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[name]
      Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[flags]
      Queries value:
HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} White \label{limit} White \label{limit} HKLM \label{limit} White \la
     Oueries value:
HKLM \label{limit} \verb+KLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} A software \label{limit} wow 6432 node \label{limit} and \label{limit} if \label{limit} if \label{limit} A software \label{limit} Wow 6432 node \label{limit} wow 6432 node \label{limit} A software \label{limit} A software \label{limit} A software \label{limit} wow 6432 node \label{limit} A software \label{limit} A softwar
HKLM \verb|\software| wow 6432 node \verb|\microsoft| direct draw \verb|\compatibility| silent thunder [flags] | the following the following properties of the following properties
```

```
Oueries value
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[id]
    Queries value:
                                              w6432node\microsoft\directdraw\compatibility\starcraft100[name]
HKLM\software\v
    Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[flags]
     Queries value:
HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} If the limit \labellimit 
    Oueries value:
HKLM \label{limit} \begin{tabular}{ll} HKLM \label{limit} White 
    Queries value
Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[id]
HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| direct draw \verb|\compatibility| \verb|\starcraft demo[name]| \\
    Oueries value:
HKLM \label{limits} LKLM \label{limits} HKLM \label{limits} LKLM \label{limits} HKLM \label{limits} LKLM \label{limits} LKLM
    Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[id]
    Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[name]
    Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[flags]
    Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[id]
    Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[name]
    Queries value:
HKLM \ software \ \ wow 6432 node \ \ \ icrosoft \ \ \ directdraw \ \ compatibility \ \ third dimension [flags]
    Oueries value
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[id]
    Queries value:
HKLM\software\v
                                                6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
    Oueries value
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus direct \\ draw \setminus compatibility \setminus ziff \\ davis \\ quality \\ benchmark \lceil flags \rceil
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ direct draw \ compatibility \ ziff davis quality benchmark \ [id]
    Oueries value:
HKLM \label{limits} KLM \label{limits} HKLM \label{limits} Wow 6432 node \mbox{$\operatorname{microsoft} = \operatorname{microsoft} $\operatorname{microsoft} $\operatorname{m
    Queries value
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
    Oueries value:
Queries value:
                                                                    HKLM\software\wow6432node\microsoft\directdraw[modexonly]
    Queries value:
                                                                     HKLM\software\wow6432node\microsoft\directdraw[emulationonly]
                                                                    HKLM\software\wow6432node\microsoft\directdraw[showframerate]
    Oueries value:
     Oueries value:
                                                                     HKLM\software\wow6432node\microsoft\directdraw[enableprintscreen]
                                                                     HKLM\software\wow6432node\microsoft\directdraw[forceagpsupport]
     Queries value:
    Queries value:
                                                                     HKLM\software\wow6432node\microsoft\directdraw[disableagpsupport]
                                                                     HKLM\software\wow6432node\microsoft\directdraw[disablemmx]
    Oueries value:
                                                                     HKLM\software\wow6432node\microsoft\directdraw[disableddscapsinddsd]
     Oueries value:
    Queries value:
                                                                     HKLM \verb|\software| wow 6432 node \verb|\microsoft| direct draw[disable wider surfaces]|
    Oueries value:
                                                                     HKLM\software\wow6432node\microsoft\directdraw[usenonlocalvidmem]
                                                                     HKLM\software\wow6432node\microsoft\directdraw[forcerefreshrate]
    Queries value:
                                                                     HKLM\software\wow6432node\microsoft\direct3d[flipnovsync]
     Queries value:
    Queries value:
                                                                     HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus directdraw[owndc]
                                                                     HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
    Oueries value:
                                                                     HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
     Queries value:
                                                                     Queries value
f941e9b7e1fe}\inprocserver32[inprocserver32]
    Queries value:
                                                                    HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
 f941e9b7e1fe}\inprocserver32[]
    Queries value
                                                                    HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[threadingmodel]
                                                                    HKCR\dximagetransform.microsoft.shadow\clsid[]
    Queries value:
     Queries value:
                                                                     \label{localized} HKCR\wow64\bar{3}2node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
                                                                     HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
     Queries value:
    Oueries value:
                                                                    HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[inprocserver32]
     Queries value:
                                                                    HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[]
                                                                    HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
    Oueries value:
00c04fa34f05}\inprocserver32[threadingmodel]
    Queries value:
                                                                     HKCR\mime\database\content type\image/png[extension]
    Queries value:
                                                                     HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
                                                                    HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
    Oueries value:
     Oueries value:
                                                                     HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724
00aa006c1a01}\inprocserver32[inprocserver32]
    Queries value:
                                                                    HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[]
    Oueries value
                                                                    HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
    Queries value:
                                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
                                                                     HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
    Queries value:
                                                                     HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
     Queries value
00aa006c1a01}\inprocserver32[inprocserver32]
    Queries value:
                                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[]
     Queries value:
                                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
                                                                    HKCR\mime\database\content type\image/bmp\bits[0]
    Oueries value:
     Queries value:
                                                                     HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[]
                                                                     HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
     Queries value
0000f87557db}\inprocserver32[inprocserver32]
                                                                    HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
    Queries value:
0000f87557db}\inprocserver32[]
                                                                    HKCR\mime\database\content type\image/gif\bits[0]
    Queries value:
     Oueries value:
                                                                    {\tt HKCR\mime\database\content\ type\image/jpeg\bits[0]}
                                                                    HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
    Queries value:
0000f87557db}\inprocserver32[threadingmodel]
```

HKCR\mime\database\content type\image/pjpeg\bits[0]

```
Oueries value:
                           HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt bits} \mbox{\tt [0]}
                           HKCR\mime\database\content type\image/x-png\bits[0]
 Queries value:
  Queries value:
                           HKCR\mime\database\content type\image/x-wmf\bits[0]
                           HKCR\mime\database\content type\image/x-png[image filter clsid]
HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid[]
  Queries value:
  Oueries value:
 Queries value:
                           HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
                           HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
 Queries value:
00a0c913f750}\inprocserver32[inprocserver32]
                           HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
 Oueries value:
00a0c913f750}\inprocserver32[]
                           HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
 Queries value:
00a0c913f750}\inprocserver32[threadingmodel]
                           HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]
 Oueries value:
                           HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]
  Queries value:
                           HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Queries value
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
                           HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Oueries value:
f4fc1e6ca1bd}\inprocserver32[]
                           HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Queries value:
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
Queries value: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
                           HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
  Queries value
 Queries value:
                           HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
                           HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
 Oueries value:
00aa003f8646}\inprocserver32[inprocserver32]
  Queries value:
                           HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[]
                           HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
 Queries value:
00aa003f8646}\inprocserver32[threadingmodel]
                           HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:
 Oueries value
                           HKLM\system\currentcontrolset\control\nls\codepage[1251]
                           HKLM\system\currentcontrolset\control\nls\codepage[1253]
 Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1254]
 Queries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Oueries value
                           HKLM\system\currentcontrolset\control\nls\codepage[1256]
                           HKLM\system\currentcontrolset\control\nls\codepage[1257]
 Queries value:
                           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]
 Oueries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[936]
                           HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:
 Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[1361]
 Oueries value:
                           HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsize]
  Queries value:
                           HKCU\software\microsoft\internet
\verb|explorer\international\scripts\26[iefontsize private]|\\
                           HKCU\software\microsoft\internet
 Oueries value:
explorer\international\scripts\26[iepropfontname]
 .
Queries value:
                           HKCU\software\microsoft\internet
explorer\international\scripts\26[iefixedfontname]
 Oueries value:
                           HKCR\mime\database\content type\image/gif[extension]
                           HKLM\software\wow6432node\microsoft\internet
  Oueries value
explorer\\ \verb|main| featurecontrol| feature_block_lmz_script[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
 Queries value:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[*]
                           HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_use\_windowedselect control[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                           HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
                           HKCU\software\microsoft\windows script\settings[jitdebug]
  Queries value:
 Oueries value:
                           HKCU\software\microsoft\internet explorer\ne
windows[accuserinitonclick]
 Queries value:
                           HKLM\software\wow6432node\microsoft\direct3d[disablemmx]
  Queries value:
                           HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus direct3d[disablex3d]
  Oueries value
                           HKI M\software\wow6432node\microsoft\direct3d[fewvertices]
                           HKLM\software\wow6432node\microsoft\direct3d[disablevidmemvbs]
 Queries value:
  Queries value:
                           HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane1]|
 Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane2]
                           HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane3]|
                           HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane4]
                           HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane5]|
                           HKLM\software\microsoft\window
 Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane6]
                           HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane7]|
                           HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane8]
                           HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane9]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane10]
 Queries value:
                           HKLM\software\microsoft\windows
\label{lem:nt-current-version-language-pack-surrogatefall-back-simsun[plane11]} Queries value: \\ HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane12]
 Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane13]
 Queries value:
                           HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane14]|
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsun[plane15]
 Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane16]
                           HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
 Oueries value:
00aa00389b71}\proxystubclsid32[]
                           HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32[]
```

```
Oueries value:
                                                      HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}[]
                                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
   Queries value:
00000000046}\inprocserver32[inprocserver32]
                                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
   Oueries value:
00000000046}\inprocserver32[]
                                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
   Queries value:
00000000046}\inprocserver32[threadingmodel]
   Queries value:
                                                     HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
                                                     HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
   Oueries value:
                                                      HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
    Queries value:
                                                      HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
    Queries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
                                                     HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
   Oueries value:
00c04fb6bfc4}\inprocserver32[]
                                                     HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
{\tt 00c04fb6bfc4} \verb|\inprocserver32[threading model]
                                                     HKCR\shockwaveflash.shockwaveflash\clsid[]
   Oueries value:
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid[]
    Oueries value:
                                                      HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
    Queries value:
   Queries value:
                                                     HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32[inprocserver32]
                                                     HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Queries value
444553540000}\inprocserver32[]
                                                     HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Oueries value:
444553540000}\inprocserver32[threadingmodel]
   Queries value:
                                                      HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
bc58-54c27d745f8f]
   Queries value:
                                                     HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
958a-dad20c90073c]
    Queries value:
                                                      HKLM \verb|\hardware\description\system\centralprocessor\0[\abelleft]
   Oueries value:
                                                     HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ micro
types\type 001[name]
   Queries value:
                                                      HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
                                                      HKLM\software\wow6432node\microsoft\internet explorer\default
   Queries value:
behaviors[userdata]
                                                     HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\\ \verb|main| featurecontrol| feature_activex\_repurpose detection[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
   Queries value:
                                                      HKLM\software\wow6432node\microsoft\internet
\label{lem:control} explorer\mbox{\sc https://general.ps} explorer\m
explorer\\ \verb|main| featurecontrol| feature\_addon\_management[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature addon management[*]
   .
Queries value:
                                                     HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus\1[]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]
   Oueries value:
                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\internet explorer\feed
discovery[sound]
                                                     HKCU\software\microsoft\ftp[use web based ftp]
   Oueries value:
    Queries value:
                                                      HKCR\mime\database\content type\application/x-shockwave-flash[extension]
                                                      HKLM\software\wow6432node\microsoft\windows
   Queries value:
nt\currentversion\drivers32[wave]
                                                     HKLM\software\wow6432node\microsoft\windows
   Queries value:
nt\currentversion\drivers32[wave1]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave21
                                                     HKLM\software\wow6432node\microsoft\windows
   Queries value:
nt\currentversion\drivers32[wave3]
   Oueries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave4]
                                                     HKLM\software\wow6432node\microsoft\windows
   Queries value:
nt\currentversion\drivers32[wave5]
   Oueries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave6]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave7]
   Oueries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave8]
                                                     HKCR \\ wow 6432 \\ node \\ clsid \\ \{2933bf90-7b36-11d2-b20e-00c04f983e60\} \\ \\ progid[]
   Queries value:
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave91
                                                     HKLM\software\wow6432node\microsoft\windows
   Queries value:
nt\currentversion\drivers32[midi]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi1]
   Oueries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi2]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi3]
   Oueries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi4]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi5]
                                                     HKLM\software\wow6432node\microsoft\windows
   Queries value:
nt\currentversion\drivers32[midi6]
   Oueries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi7]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi8]
                                                     HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[]
   Oueries value:
    Queries value:
                                                      HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[inprocserver32]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi9]
   Queries value:
\label{thm:local_mediaproperties} I know the label{thm:local_mediaproperties} I know the label{thm:local_med
   Oueries value:
                                                     HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e
00c04f983e60}\inprocserver32[]
                                                     HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[threadingmodel]
```

```
Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1606]
  Queries value:
                                            \label{thm:local_equation} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
                                           sible cache\userdata[cacherepair]
settings\5.0\cache\exter
  Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheprefix]
  Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachelimit]
                                           \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version} \end{tabular} \label{thm:local_hammon_hammon}
   Queries value:
settings\5.0\cache\extensible cache\userdata[cacheoptions]
  Oueries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
   Queries value:
   Queries value:
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
   Queries value:
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
   Oueries value:
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
   Queries value:
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
Oueries value:
\label{thm:local_transform} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} is supposed to the local control \end{tabular} $$ exclaim \end{tabular} $$ is supposed to the local control \end{tabular} $$ is supposed to the local contr
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount]
   Queries value:
                                           HKCU\software\microsoft\internet explorer\domstorage\total[]
   Queries value:
\label{thm:local_hammon_hammon} HKLM \software \mbox{$\mbox{$m$icrosoft$} \windows \current version \policies \system [enablelua] } \\
                                           HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
   Oueries value:
                                           HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
   Queries value:
   Queries value:
                                            HKCU\software\macromedia\flashplayer[flashplayerversion]
   Queries value:
                                           HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32[]
   Queries value:
                                           HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib[]
   Queries value:
                                           HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib[version]
                                           HKCU\software\microsoft\internet
   Oueries value:
explorer\services[selectionactivitybuttondisable]
   Queries value:
                                           HKCU\software\microsoft\internet explorer\suggested sites[enabled]
                                           HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
   Oueries value:
   Oueries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8
08002b30309d}\shellfolder[attributes]
  Oueries value:
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[usedrophandler]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsforparsing]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                            HKLM\software\microsoft\rpc[udtalignmentpolicy]
   Queries value:
   Oueries value
                                           HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32[]
   Queries value:
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d \} \verb|\shellfolder[queryforoverlay]|
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d \} \verb|\shellfolder[pintonamespacetree]|
                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
   Queries value:
                                           HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}[]
                                           HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{00020420-0000-0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c000-c000-c0000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c000-c000-c000-c000-c000-c00-c000-c000-c000-c00-c00-c00-c00-c00-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00
   Oueries value:
00000000046}\inprocserver32[inprocserver32]
   Queries value:
                                           HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[data]
   Queries value:
                                           HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Oueries value:
```

11e3-a68e-806e6f6e6963}[generation]

```
Oueries value
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-
11e3-a68e-806e6f6e6963}[data]
     Oueries value:
11e3-a68e-806e6f6e6963}[generation]
                                                                                     HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034
00aa006009fa}\proxystubclsid32[]
                                                                                     HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
     Oueries value:
409d6c4515e9}[drivemask]
                                                                                     HKCR \\ wow 6432 \\ node \\ clsid \\ \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}[]
      Queries value:
      Queries value:
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
                                                                                     HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
      Oueries value:
e4fddd701cba}\inprocserver32[inprocserver32]
                                                                                     HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
      Queries value:
e4fddd701cba}\inprocserver32[]
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
     Oueries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
      Queries value:
b8dc300d9f9d}\inprocserver32[]
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
      Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
     Oueries value:
                                                                                     HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[threadingmodel]
     Queries value:
\label{thm:local_hammon_holicies} \\ \textbf{HKLM} \setminus \textbf{Software} \setminus \textbf{microsoft} \setminus \textbf{windows} \setminus \textbf{currentversion} \setminus \textbf{policies} \setminus \textbf{explorer} [\textbf{dontshowsuperhidden}] \\ \textbf{HKLM} \setminus \textbf{Software} \setminus \textbf{microsoft} \setminus \textbf{windows} \setminus \textbf{currentversion} \setminus \textbf{policies} \setminus \textbf{explorer} [\textbf{dontshowsuperhidden}] \\ \textbf{HKLM} \setminus \textbf{Software} \setminus \textbf{microsoft} \setminus \textbf{windows} \setminus \textbf{microsoft} \setminus \textbf{microsoft
      Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
      Oueries value:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in various \end{tabular} explorer [nowebview]
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
     Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} software \verb|\microsoft| windows \end{tabular} current version \end{tabular} policies \end{tabular} explorer [separate process]
      Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
     Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]|
      Queries value:
                                                                                     \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+ advanced[hidden]+ of the lemma o
      Oueries value:
\label{thm:conversion} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [showcompcolor] \end{tabular}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
      Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
      Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
     Oueries value:
\label{thm:constraint} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [hideicons] \end{tabular}
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [mapnet drvbtn] \setminus drvbtn \setminus drvb
     Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
      Queries value:
                                                                                     \label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [filter] \end{tabular}
      Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
     Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
     Queries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is consistent \cite{tabular} and \cite{tabular} is consistent \cite{tabular} and \cite{tabular} is consistent \cite{tabular} is consistent \cite{tabular} and \
      Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlav]
     Queries value:
                                                                                     HKCR\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32[]
      Queries value:
                                                                                     HKCR\directory[docobject]
                                                                                     HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}[]
      Oueries value:
      Queries value:
                                                                                      HKCR\folder[docobject]
                                                                                      HKCR\allfilesystemobjects[docobject]
      Queries value:
      Queries value:
                                                                                     HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
      Queries value:
                                                                                     HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[]
      Queries value:
                                                                                     HKCR\directory[browseinplace]
                                                                                     HKCR\folder[browseinplace]
      Oueries value:
                                                                                      HKCR\allfilesystemobjects[browseinplace]
      Oueries value:
                                                                                     HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
      Queries value:
00000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\directory[isshortcut]
                                                                                      HKCR\folder[isshortcut]
      Oueries value:
      Queries value:
                                                                                      HKCR\allfilesystemobjects[isshortcut]
      Oueries value:
                                                                                     HKCR\directory[alwaysshowext]
HKCR\directory[nevershowext]
      Queries value:
      Queries value:
                                                                                      HKCR\folder[nevershowext]
      Queries value:
                                                                                      HKCR\allfilesystemobjects[nevershowext]
                                                                                     HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
      Oueries value:
444553540000}\inprocserver32[]
                                                                                     HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[loadwithoutcom]
     Oueries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-00000000046}
0xffff]
                                                                                     HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000\f1
      Oueries value:
                                                                                     HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
      Queries value:
444553540000}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\cl: 444553540000}\inprocserver32[threadingmodel]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
      Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
      Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache\extensible cache\mshist012016040820160409[cachenath]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheprefix]
                                                                           \label{thm:linear} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt linear} \mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt linear} \mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt linear\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentversion\currentve
    Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cachelimit]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
    Queries value:
                                                                           3aea-1069-a2d8-08002b30309d}[1
    Queries value:
                                                                           HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}[localizedstring]
                                                                           HKCU\software\microsoft\internet
    Queries value:
explorer\main\windowssearch[enabledscopes]
     .
Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[category]
    Oueries value:
HK LM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777 f761-1976 from 1976 
68ad-4d8a-87bd-30b759fa33dd}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[parentfolder]
     Queries value:
68ad-4d8a-87bd-30b759fa33dd}[description]
68ad-4d8a-87bd-30b759fa33dd}[relativepath]
     Queries value:
68ad-4d8a-87bd-30b759fa33dd}[parsingname]
    Queries value:
\label{thm:hklm} HKL^{M} software \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{1777f761-1646, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 1987, 19
68ad-4d8a-87bd-30b759fa33dd}[infotip]
     Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[localizedname]
     Queries value:
68ad-4d8a-87bd-30b759fa33dd}[icon]
68ad-4d8a-87bd-30b759fa33dd}[security]
     Oueries value:
68ad-4d8a-87bd-30b759fa33dd \} \verb|[streamresource]| \\
    Oueries value:
HK LM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-161644, 1777f761-161644, 1777f761-16164, 1777f76164, 1777f76164, 1777f76164, 1777f76164, 1777f76164, 1777f76164, 1777f76164, 1777f7616
68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype]
     Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[localredirectonly]
     Queries value:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{1777f761-161\} \\ note that the first interest is the first of the first interest in 
68ad-4d8a-87bd-30b759fa33dd}[roamable]
HKLM \label{lem:hklm} Which is a constant with the statement of the stat
68ad-4d8a-87bd-30b759fa33dd}[precreate]
     Queries value:
68ad-4d8a-87bd-30b759fa33dd}[stream]
    Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]
     Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[attributes]
     Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]
68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler]
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
     Queries value:
folders[favorites]
     Queries value:
                                                                            HKLM\software\wow6432node\microsoft\windows search[currentversion]
                                                                           HKLM\software\wow6432node\microsoft\downloadmanager[cacheok]
     Oueries value:
                                                                            HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid[]
      Queries value:
                                                                            HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}[]
      Queries value:
     Queries value:
                                                                           HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[inprocserver32]
                                                                           HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
      Oueries value
0000f81fe221}\inprocserver32[]
                                                                           HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
     Oueries value:
0000f81fe221}\inprocserver32[threadingmodel]
                                                                           HKLM\software\wow6432node\microsoft\internet
     Queries value:
explorer\main[maxrenderline]
                                                                           HKCR\mime\database\content type\image/x-icon[extension]
HKCR\shockwaveflash.shockwaveflash.7\clsid[]
     Oueries value:
     Queries value:
      Queries value:
                                                                            HKCU\appevents\schemes\apps\explorer\navigating\.current[]
     Oueries value:
                                                                           HKCU\appevents\schemes[]
                                                                           \label{local-hkcu-appevents-schemes-apps-explorer-navigating-current[default flags]} \\ \text{HKCR-wow6432node-clsid-} \{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}[]
     Oueries value:
     Queries value:
                                                                           HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
      Queries value:
fd2b31b3eefd}\inprocserver32[inprocserver32]
                                                                           HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
     Queries value:
fd2b31b3eefd}\inprocserver32[]
     Queries value:
                                                                           HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
                                                                           HKCU\appevents\schemes\apps\explorer\activatingdocument\.current[]
     Queries value:
      Queries value:
                                                                            HKCR\mime\database\content type\image/jpeg[extension]
     Queries value:
                                                                           HKLM\software\wow6432node\microsoft\internet explorer\default
```

```
behaviors[clientcaps]
                                       HKCR\msxml2.xmlhttp\clsid[]
  Queries value:
   Queries value:
                                       HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\progid[]
                                       HKCR \setminus wow 6432 \\ node \\ clsid \\ \{f6d90f16-9c73-11d3-b32e-00c04f990bb4\}[]
   Queries value:
                                      HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
  Oueries value:
00c04f990bb4}\inprocserver32[inprocserver32]
  Queries value:
                                      HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32[]
                                      HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-
  Oueries value:
00c04f990bb4}\inprocserver32[threadingmodel]
                                       HKCR\shockwaveflash.shockwaveflash.10\clsid[]
   Queries value:
  Queries value:
                                      HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_block_lmz_object[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]| \\
                                      HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_block_lmz_object[*]
  Queries value:
                                      HKCR\.swf[content type]
                                      Oueries value:
   Oueries value:
settings\zones\3[1c00]
  Queries value:
                                       HKCR\acropdf.pdf.1\clsid[]
                                      HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\progid[]
   Oueries value:
                                       HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}[]
   Queries value
  Queries value:
                                      HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32[inprocserver32]
  Queries value:
                                      HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32[]
  Queries value:
                                      HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-
444553540000}\inprocserver32[threadingmodel]
  Queries value:
                                       HKCU\software\adobe\acrobat reader\9.0\originals[bbrowserintegration]
   Queries value
                                       HKLM \backslash software \backslash wow 6432 node \backslash microsoft \backslash active \ setup \backslash installed
components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}[isinstalled]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Queries value:
components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}[version]
                                      HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| active setup\\| installed
components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}{keyfilename}

Queries value: HKLM\software\wow6432node\microsoft\active setup\installed
components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[isinstalled]
  Queries value:
                                      components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[version]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Queries value:
components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[keyfilename]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{3af36230-a269-11d1-b5bf-0000f8051515}[isinstalled]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Queries value:
components\{3af36230-a269-11d1-b5bf-0000f8051515}[version]
Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{3af36230-a269-11d1-b5bf-0000f8051515}[keyfilename]
  Oueries value
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{44bba840-cc51-11cf-aafa-00aa00b6015c}[isinstalled]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{44bba840-cc51-11cf-aafa-00aa00b6015c}[version]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{44bba840-cc51-11cf-aafa-00aa00b6015c}[keyfilename]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{45ea75a0-a269-11d1-b5bf-0000f8051515}[isinstalled]
                                       \label{local-observative} HKLM\software\wow6432 node\microsoft\active\ setup\installed
components \verb|\{45ea75a0-a269-11d1-b5bf-0000f8051515\}[version]|\\
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Queries value:
components\{45ea75a0-a269-11d1-b5bf-0000f8051515}[keyfilename]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Queries value:
components\{7790769c-0471-11d2-af11-00c04fa35d02}[isinstalled]
  Oueries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{7790769c-0471-11d2-af11-00c04fa35d02}[version]
                                      HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| active setup\\| installed
components\{7790769c-0471-11d2-af11-00c04fa35d02}[keyfilename]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Queries value:
components\{89820200-ecbd-11cf-8b85-00aa005b4340}[isinstalled]
  Queries value
                                      HKLM \verb|\software| wow 6432 node \verb|\microsoft| active setup \verb|\installed|
components\{89820200-ecbd-11cf-8b85-00aa005b4340}[version]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4340}[keyfilename]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4383}[isinstalled]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Queries value:
components\{89820200-ecbd-11cf-8b85-00aa005b4383}[version]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4383}[keyfilename]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
  Oueries value:
components\{9381d8f2-0288-11d0-9501-00aa00b911a5}[isinstalled]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components\{9381d8f2-0288-11d0-9501-00aa00b911a5}[version]
                                       HKLM\software\wow6432node\microsoft\active setup\installed
  Oueries value:
components\{9381d8f2-0288-11d0-9501-00aa00b911a5}[keyfilename]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\active setup\installed
components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}[isinstalled]
                                      HKLM\software\wow6432node\microsoft\active setup\installed
components \verb|\{de5aed00-a4bf-11d1-9948-00c04f98bbc9\}[version]|\\
                                      HKLM \label{lem:hklm} \begin{tabular}{ll} HKLM \label{lem:hklm} & setup \label{lem:hklm} \end{tabular} \\
  Queries value:
components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}[keyfilename]
  Sets/Creates value:
                                       HKLM\software\wow6432node\microsoft\internet
explorer\\ \texttt{main}\\ \texttt{feature}\\ \texttt{control}\\ \texttt{feature}\\ \texttt{scripturl\_mitigation}\\ \texttt{[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]}\\ \texttt{explorer}\\ \texttt{main}\\ \texttt{feature}\\ \texttt{featu
                                       HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| tracing\\| rasapi 32[enable file tracing]|
  Sets/Creates value:
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\rasapi32[enableconsoletracing]
                                      \label{thm:hklm} HKLM \ software \ wow 6432 node \ microsoft \ tracing \ rasapi 32 [file tracing mask] \\ HKLM \ software \ wow 6432 node \ microsoft \ tracing \ rasapi 32 [consoletracing mask] \\
  Sets/Creates value:
  Sets/Creates value:
   Sets/Creates value:
                                       HKLM\software\wow6432node\microsoft\tracing\rasapi32[maxfilesize]
   Sets/Creates value:
                                       Sets/Creates value:
                                       HKLM\software\wow6432node\microsoft\tracing\rasmancs[enablefiletracing]
  Sets/Creates value:
```

 $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus rasmancs[filetracing mask]$

Sets/Creates value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \begin{tabular}{ll} wow 6432 node \end{tabular} microsoft \end{tabular} tracing \end{tabular} ras mancs \end{tabular} [consolet racing \end{tabular} mask]$ Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[maxfilesize] Sets/Creates value: Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[filedirectory] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet $settings \verb|\|5.0\> cache \verb|\| extensible | cache \verb|\| userdata[cachepath]|$ HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\userdata[cacheprefix] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata[cachelimit] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\exter sible cache\userdata[cacheoptions] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata[cacherepair] HKCU\software\microsoft\internet explorer\domstorage\baidu.com[] Sets/Creates value: Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016040820160409[cachepath] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\mshist012016040820160409[cacheprefix] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016040820160409[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair] HKCU\software\microsoft\internet explorer\main[disable script debugger] Value changes: Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zonemap[autodetect] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\connections[savedlegacysettings] Value changes: HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[name]

HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[id] Value changes: HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication[name] Value changes:

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

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

Value changes: HKCU\software\microsoft\internet explorer\domstorage\total[] HKCU\software\microsoft\internet explorer\domstorage\baidu.com[] Value changes:

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]